

Διακήρυξη για τη Σύναψη Συμφωνίας-Πλαίσιο σε Τμήματα για το Έργο «Δράσεις για την Ενίσχυση της Ασφάλειας των Πληροφοριών και των Συστημάτων του Δημοσίου Τομέα»

Κωδ. ΟΠΣ:	ΤΑ 5201793
Επιχειρησιακό Πρόγραμμα:	Ταμείο Ανάκαμψης και Ανθεκτικότητας
Προϋπολογισμός- Εκτιμώμενη αξία σύμβασης:	<p>Προϋπολογισμός Έργου - εκτιμώμενη αξία συμφωνίας-πλαίσιο</p> <p>Η εκτιμώμενη αξία της συμφωνίας-πλαίσιο ανέρχεται στο ποσό των εκατόν δύο εκατομμυρίων εκατόν εξήντα επτά χιλιάδων εννιακοσίων ενενήντα εννιά ευρώ και ενενήντα εννέα λεπτών (102.167.999,99 €) συμπεριλαμβανομένου ΦΠΑ 24 % (προϋπολογισμός χωρίς ΦΠΑ: 82.393.548,38 €, ΦΠΑ: 19.774.451,61 €)</p> <p>- Η εκτιμώμενη αξία της αρχικής συμφωνίας-πλαίσιο ανέρχεται στο ποσό των τριάντα οχτώ εκατομμυρίων εκατόν σαράντα πέντε χιλιάδων εκατόν εξήντα ενός ευρώ και είκοσι εννέα λεπτών (38.145.161,29 €) μη περιλαμβανομένου ΦΠΑ (προϋπολογισμός με ΦΠΑ: 47.300.000,00 €, ΦΠΑ 24% 9.154.838,71 €). Η πηγή χρηματοδότησης είναι το ΕΣΑΑ Ελλάδα 2.0, ΣΑΤΑ ΤΑΧΧΧΧΧ (Κωδ. Έργου: 2022ΤΑΧΧΧΧΧΧΧ).</p> <p>- Το δικαίωμα προαίρεσης ως προς το φυσικό αντικείμενο ανέρχεται σε πενήντα τοις εκατό (50%) της αξίας της αρχικής συμφωνίας - πλαίσιο στο ποσό των δεκαεννέα εκατομμυρίων εβδομήντα δύο χιλιάδων πεντακοσίων ογδόντα ευρώ και εξήντα τεσσάρων λεπτών (19.072.580,64 €) μη περιλαμβανομένου ΦΠΑ (προϋπολογισμός με ΦΠΑ: 23.650.000,00 €, ΦΠΑ 24% 4.577.419,35 €). Η προαίρεση δύναται να χρηματοδοτηθεί από οποιαδήποτε άλλη πηγή.</p> <p>- Το δικαίωμα προαίρεσης ως προς τη συντήρηση ανέρχεται στο ποσό των είκοσι πέντε εκατομμυρίων εκατόν εβδομήντα πέντε χιλιάδων οχτακοσίων έξι ευρώ και σαράντα πέντε λεπτών (25.175.806,45 €) μη περιλαμβανομένου ΦΠΑ (προϋπολογισμός με ΦΠΑ: 31.218.000,00 €, ΦΠΑ 24% 6.042.193,55 €). Η προαίρεση δύναται να χρηματοδοτηθεί από οποιαδήποτε άλλη πηγή.</p>

	30200000-1 - Εξοπλισμός ηλεκτρονικών υπολογιστών και προμήθειες 48730000-4 - Πακέτα λογισμικού ασφαλείας 48731000-1 - Πακέτα λογισμικού ασφάλειας αρχείων 48732000-8 - Πακέτα λογισμικού ασφάλειας δεδομένων 79417000-0 - Υπηρεσίες παροχής συμβουλών σε θέματα ασφαλείας 72246000-1 - Υπηρεσίες παροχής συμβουλών σε θέματα συστημάτων πληροφορικής CPV: 72263000-6 - Υπηρεσίες υλοποίησης λογισμικού	
Κριτήριο Ανάθεσης:	Η πλέον συμφέρουσα από οικονομική άποψη προσφορά βάσει βέλτιστης σχέσης ποιότητας – τιμής	
Ημερομηνία Διενέργειας:		
	Ημερομηνία Ανάρτησης στο ΚΗΜΔΗΣ	
	Ημερομηνία Ανάρτησης στο ΕΣΗΔΗΣ	
	Ημερομηνία Αποστολής Διακήρυξης σε Ε.Ε. (Υπ. Επίσημων Εκδόσεων)	
	Ημερομηνία Δημοσίευσης Διακήρυξης σε Ε.Ε.	
	Ημερομηνία Ανάρτησης στον Διαδικτυακό τόπο της Αναθέτουσας Αρχής www.ktpae.gr	

1.1 ΓΕΝΙΚΕΣ ΠΛΗΡΟΦΟΡΙΕΣ

1.1.1 Συνοπτικά στοιχεία Έργου	
ΤΙΤΛΟΣ ΕΡΓΟΥ	Δράσεις για την Ενίσχυση της Ασφάλειας των Πληροφοριών και των Συστημάτων του Δημοσίου Τομέα
ΑΝΑΘΕΤΟΥΣΑ ΑΡΧΗ	«Κοινωνία της Πληροφορίας Μ.Α.Ε.» (ΚτΠ Μ.Α.Ε.)
ΦΟΡΕΑΣ ΛΕΙΤΟΥΡΓΙΑΣ	Υπουργείο Ψηφιακής Διακυβέρνησης
ΚΥΡΙΟΣ ΤΟΥ ΕΡΓΟΥ	Υπουργείο Ψηφιακής Διακυβέρνησης
ΦΟΡΕΑΣ ΧΡΗΜΑΤΟΔΟΤΗΣΗΣ	Υπουργείο Ψηφιακής Διακυβέρνησης
ΤΟΠΟΣ ΠΑΡΑΔΟΣΗΣ – ΤΟΠΟΣ ΠΑΡΟΧΗΣ ΥΠΗΡΕΣΙΩΝ	Τόπος παράδοσης: η Αναθέτουσα Αρχή. Τόπος παροχής υπηρεσιών: Κατά κύριο λόγο η ΓΓΠΣΔΔ, η ΗΔΙΚΑ, το ΚΤΗΜΑΤΟΛΟΓΙΟ, το ΕΔΥΤΕ αλλά και όποια άλλα σημεία απαιτηθούν με βάση τις ανάγκες του έργου.
ΕΙΔΟΣ ΣΥΜΒΑΣΗΣ	30200000-1 - Εξοπλισμός ηλεκτρονικών υπολογιστών και προμήθειες 48730000-4 - Πακέτα λογισμικού ασφαλείας 48731000-1 - Πακέτα λογισμικού ασφαλείας αρχείων 48732000-8 - Πακέτα λογισμικού ασφαλείας δεδομένων 79417000-0 - Υπηρεσίες παροχής συμβουλών σε θέματα ασφαλείας 72246000-1 - Υπηρεσίες παροχής συμβουλών σε θέματα συστημάτων πληροφορικής 72263000-6 - Υπηρεσίες υλοποίησης λογισμικού
ΕΙΔΟΣ ΔΙΑΔΙΚΑΣΙΑΣ	Ηλεκτρονικός Ανοικτός Διεθνής άνω των ορίων Διαγωνισμός με κριτήριο ανάθεσης την πλέον συμφέρουσα από οικονομική άποψη προσφορά: βάσει βέλτιστης σχέσης ποιότητας – τιμής
ΠΡΟΥΠΟΛΟΓΙΣΜΟΣ – ΕΚΤΙΜΩΜΕΝΗ ΑΞΙΑ ΣΥΜΒΑΣΗΣ	Η εκτιμώμενη αξία της συμφωνίας-πλαίσιο ανέρχεται στο ποσό των εκατόν δύο εκατομμυρίων εκατόν εξήντα επτά χιλιάδων εννιακοσίων ενενήντα εννιά ευρώ και ενενήντα εννέα λεπτών (102.167.999,99 €) συμπεριλαμβανομένου ΦΠΑ 24 % (προϋπολογισμός χωρίς ΦΠΑ: 82.393.548,38 € ΦΠΑ: 19.774.451,61 €)

1.1.1 Συνοπτικά στοιχεία Έργου

	<p>- Η εκτιμώμενη αξία της αρχικής συμφωνίας-πλαίσιο ανέρχεται στο ποσό των τριάντα οχτώ εκατομμυρίων εκατόν σαράντα πέντε χιλιάδων εκατόν εξήντα ενός ευρώ και είκοσι εννέα λεπτών (38.145.161,29 €) μη περιλαμβανομένου ΦΠΑ (προϋπολογισμός με ΦΠΑ: 47.300.000,00 €, ΦΠΑ 24% 9.154.838,71 €). Η πηγή χρηματοδότησης είναι το ΕΣΑΑ Ελλάδα 2.0, ΣΑΤΑ ΤΑΧΧΧΧΧ (Κωδ. Έργου: 2022ΤΑΧΧΧΧΧΧΧ).</p> <p>- Το δικαίωμα προαίρεσης ως προς το φυσικό αντικείμενο ανέρχεται σε πενήντα τοις εκατό (50%) της αξίας της αρχικής συμφωνίας - πλαίσιο στο ποσό των δεκαεννέα εκατομμυρίων εβδομήντα δύο χιλιάδων πεντακοσίων ογδόντα ευρώ και εξήντα τεσσάρων λεπτών (19.072.580,64 €) μη περιλαμβανομένου ΦΠΑ (προϋπολογισμός με ΦΠΑ: 23.650.000,00 €, ΦΠΑ 24% 4.577.419,35 €). Η προαίρεση δύναται να χρηματοδοτηθεί από οποιαδήποτε άλλη πηγή.</p> <p>- Το δικαίωμα προαίρεσης ως προς τη συντήρηση ανέρχεται στο ποσό των είκοσι πέντε εκατομμυρίων εκατόν εβδομήντα πέντε χιλιάδων οχτακοσίων έξι ευρώ και σαράντα πέντε λεπτών (25.175.806,45 €) μη περιλαμβανομένου ΦΠΑ (προϋπολογισμός με ΦΠΑ: 31.218.000,00 €, ΦΠΑ 24% 6.042.193,55 €). Η προαίρεση δύναται να χρηματοδοτηθεί από οποιαδήποτε άλλη πηγή.</p>
ΧΡΗΜΑΤΟΔΟΤΗΣΗ ΕΡΓΟΥ	Το Έργο χρηματοδοτείται από το Ταμείο Ανάκαμψης και Ανθεκτικότητας
ΔΙΑΡΚΕΙΑ ΣΥΜΒΑΣΗΣ	Τριάντα (30) μήνες
ΗΜΕΡΟΜΗΝΙΑ ΔΙΑΚΗΡΥΞΗΣ	
ΠΡΟΘΕΣΜΙΑ ΓΙΑ ΥΠΟΒΟΛΗ ΔΙΕΥΚΡΙΝΙΣΕΩΝ ΕΠΙ ΤΩΝ ΟΡΩΝ ΤΗΣ ΔΙΑΚΗΡΥΞΗΣ	
ΗΜΕΡΟΜΗΝΙΑ ΈΝΑΡΞΗΣ ΗΛΕΚΤΡΟΝΙΚΗΣ ΥΠΟΒΟΛΗΣ ΠΡΟΣΦΟΡΩΝ	
ΚΑΤΑΛΗΚΤΙΚΗ ΗΜΕΡΟΜΗΝΙΑ ΚΑΙ ΩΡΑ ΥΠΟΒΟΛΗΣ ΠΡΟΣΦΟΡΩΝ	ΧΧ-ΧΧ-2023, ημέρα ΧΧΧΧΧΧΧΧΧ και ώρα 14:00
ΤΟΠΟΣ & ΤΡΟΠΟΣ ΚΑΤΑΘΕΣΗΣ	Ηλεκτρονική Υποβολή:

1.1.1 Συνοπτικά στοιχεία Έργου	
ΠΡΟΣΦΟΡΩΝ	Στη διαδικτυακή πύλη www.promitheus.gov.gr του Εθνικού Συστήματος Ηλεκτρονικών Δημοσίων Συμβάσεων (ΕΣΗΔΗΣ) (ηλεκτρονική μορφή) Έντυπη Υποβολή: Η έδρα της ΚτΠ Μ.Α.Ε.
ΗΜΕΡΟΜΗΝΙΑ ΑΝΑΡΤΗΣΗΣ ΣΤΗ ΔΙΑΔΙΚΤΥΑΚΗ ΠΥΛΗ ΤΟΥ ΕΣΗΔΗΣ	ΧΧ-ΧΧ-2023
ΗΜΕΡΟΜΗΝΙΑ ΚΑΙ ΩΡΑ ΑΠΟΣΦΡΑΓΙΣΗΣ ΠΡΟΣΦΟΡΩΝ	ΧΧ-ΧΧ-2023, ημέρα ΧΧΧΧΧΧΧΧ και ώρα 14:00

Περιεχόμενα

1.1	ΓΕΝΙΚΕΣ ΠΛΗΡΟΦΟΡΙΕΣ	3
1.1.1	Συνοπτικά στοιχεία Έργου	3
1.	ΑΝΑΘΕΤΟΥΣΑ ΑΡΧΗ ΚΑΙ ΑΝΤΙΚΕΙΜΕΝΟ ΣΥΜΒΑΣΗΣ	11
1.1	ΣΤΟΙΧΕΙΑ ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ.....	11
1.2	ΣΤΟΙΧΕΙΑ ΔΙΑΔΙΚΑΣΙΑΣ - ΧΡΗΜΑΤΟΔΟΤΗΣΗ	12
1.3	ΣΥΝΟΠΤΙΚΗ ΠΕΡΙΓΡΑΦΗ ΦΥΣΙΚΟΥ ΚΑΙ ΟΙΚΟΝΟΜΙΚΟΥ ΑΝΤΙΚΕΙΜΕΝΟΥ ΤΗΣ ΣΥΜΦΩΝΙΑΣ-ΠΛΑΙΣΙΟ.....	12
1.3.1	Αντικείμενο της συμφωνίας-πλαίσιο	12
1.3.2	Αριθμός συμβαλλομένων οικονομικών φορέων και Υποδιαίρεση σε Τμήματα	17
1.3.3	Διάρκεια συμφωνίας-πλαίσιο	18
1.3.4	Κριτήριο Ανάθεσης	18
1.4	ΘΕΣΜΙΚΟ ΠΛΑΙΣΙΟ	19
1.5	ΠΡΟΘΕΣΜΙΑ ΠΑΡΑΛΑΒΗΣ ΠΡΟΣΦΟΡΩΝ ΚΑΙ ΔΙΕΝΕΡΓΕΙΑ ΔΙΑΓΩΝΙΣΜΟΥ	23
1.6	ΔΗΜΟΣΙΟΤΗΤΑ	23
1.7	ΑΡΧΕΣ ΕΦΑΡΜΟΖΟΜΕΝΕΣ ΣΤΗ ΔΙΑΔΙΚΑΣΙΑ ΣΥΝΑΨΗΣ.....	24
2	ΓΕΝΙΚΟΙ ΚΑΙ ΕΙΔΙΚΟΙ ΟΡΟΙ ΣΥΜΜΕΤΟΧΗΣ.....	25
2.1	ΓΕΝΙΚΕΣ ΠΛΗΡΟΦΟΡΙΕΣ	25
2.1.1	Έγγραφο της σύμβασης.....	25
2.1.2	Επικοινωνία – Πρόσβαση στα έγγραφα της Σύμβασης.....	25
2.1.3	Παροχή Διευκρινίσεων.....	25
2.1.4	Γλώσσα	26
2.1.5	Εγγυήσεις.....	26
2.1.6	Προστασία Προσωπικών Δεδομένων.....	27
2.2	ΔΙΚΑΙΩΜΑ ΣΥΜΜΕΤΟΧΗΣ - ΚΡΙΤΗΡΙΑ ΠΟΙΟΤΙΚΗΣ ΕΠΙΛΟΓΗΣ.....	28
2.2.1	Δικαιούμενοι συμμετοχής.....	28
2.2.2	Εγγύηση συμμετοχής	29
2.2.3	Λόγοι αποκλεισμού	31
2.2.3.1	31
2.2.3.2	32
2.2.3.3	33
2.2.3.4	34
2.2.3.5	34
2.2.3.6	35
2.2.3.7	35
2.2.3.8	35
2.2.4	Καταλληλότητα άσκησης επαγγελματικής δραστηριότητας.....	35
2.2.5	Οικονομική και χρηματοοικονομική επάρκεια	36
2.2.6	Τεχνική και επαγγελματική ικανότητα	36
2.2.7	Πρότυπα διασφάλισης ποιότητας.....	42
2.2.8	Στήριξη στην ικανότητα τρίτων– Υπεργολαβία.....	43
2.2.8.1	Στήριξη στην ικανότητα τρίτων	43
2.2.8.2	Υπεργολαβία	44
2.2.9	Κανόνες απόδειξης ποιοτικής επιλογής	44
2.2.9.1	Προκαταρκτική απόδειξη κατά την υποβολή προσφορών	44
2.2.9.2	Αποδεικτικά μέσα- Δικαιολογητικά προσωρινού αναδόχου.....	46
2.3	ΚΡΙΤΗΡΙΑ ΑΝΑΘΕΣΗΣ.....	57
2.3.1	Κριτήριο ανάθεσης	57
2.3.2	Βαθμολόγηση και κατάταξη προσφορών.....	68
2.3.2.1	Βαθμολόγηση Τεχνικών Προσφορών	68
2.3.2.2	Α. Κατάταξη προσφορών	69
2.3.2.3	Διαμόρφωση συγκριτικού κόστους Προσφοράς	69

2.4	ΚΑΤΑΡΤΙΣΗ - ΠΕΡΙΕΧΟΜΕΝΟ ΠΡΟΣΦΟΡΩΝ	70
2.4.1	Γενικοί όροι υποβολής προσφορών	70
2.4.2	Χρόνος και Τρόπος υποβολής προσφορών	70
2.4.2.1		70
2.4.2.2		70
2.4.2.3		71
2.4.2.4		71
2.4.2.5		72
2.4.3	Περιεχόμενα Φακέλου «Δικαιολογητικά Συμμετοχής - Τεχνική Προσφορά»	74
2.4.3.1	Δικαιολογητικά Συμμετοχής	74
2.4.3.2	Τεχνική Προσφορά	75
2.4.4	Περιεχόμενα Φακέλου «Οικονομική Προσφορά» / Τρόπος σύνταξης και υποβολής οικονομικών προσφορών	76
2.4.5	Χρόνος ισχύος των προσφορών	76
2.4.6	Λόγοι απόρριψης προσφορών	77
3	ΔΙΕΝΕΡΓΕΙΑ ΔΙΑΔΙΚΑΣΙΑΣ - ΑΞΙΟΛΟΓΗΣΗ ΠΡΟΣΦΟΡΩΝ	79
3.1	ΑΠΟΣΦΡΑΓΙΣΗ ΚΑΙ ΑΞΙΟΛΟΓΗΣΗ ΠΡΟΣΦΟΡΩΝ	79
3.1.1	Ηλεκτρονική αποσφράγιση προσφορών	79
3.1.2	Αξιολόγηση προσφορών	79
3.2	ΠΡΟΣΚΛΗΣΗ ΥΠΟΒΟΛΗΣ ΔΙΚΑΙΟΛΟΓΗΤΙΚΩΝ ΠΡΟΣΩΡΙΝΟΥ ΑΝΑΔΟΧΟΥ- ΔΙΚΑΙΟΛΟΓΗΤΙΚΑ ΠΡΟΣΩΡΙΝΟΥ ΑΝΑΔΟΧΟΥ	82
3.3	ΚΑΤΑΚΥΡΩΣΗ - ΣΥΝΑΨΗ ΣΥΜΒΑΣΗΣ	84
3.4	ΠΡΟΔΙΚΑΣΤΙΚΕΣ ΠΡΟΣΦΥΓΕΣ - ΠΡΟΣΩΡΙΝΗ ΚΑΙ ΟΡΙΣΤΙΚΗ ΔΙΚΑΣΤΙΚΗ ΠΡΟΣΤΑΣΙΑ	85
3.5	ΜΑΤΑΙΩΣΗ ΔΙΑΔΙΚΑΣΙΑΣ	89
4	ΟΡΟΙ ΕΚΤΕΛΕΣΗΣ ΤΗΣ ΣΥΜΒΑΣΗΣ	90
4.1	ΕΓΓΥΗΣΕΙΣ(ΚΑΛΗΣ ΕΚΤΕΛΕΣΗΣ, ΠΡΟΚΑΤΑΒΟΛΗΣ, ΚΑΛΗΣ ΛΕΙΤΟΥΡΓΙΑΣ)	90
4.1.1	Εγγύηση καλής εκτέλεσης συμφωνίας-πλαίσιο	90
4.1.2	Εγγύηση καλής εκτέλεσης εκτελεστικών συμβάσεων	90
4.2	ΣΥΜΒΑΤΙΚΟ ΠΛΑΙΣΙΟ – ΕΦΑΡΜΟΣΤΕΑ ΝΟΜΟΘΕΣΙΑ	91
4.3	ΌΡΟΙ ΕΚΤΕΛΕΣΗΣ ΤΗΣ ΣΥΜΦΩΝΙΑΣ - ΠΛΑΙΣΙΟ	92
4.4	ΥΠΕΡΓΟΛΑΒΙΑ	95
4.5	ΤΡΟΠΟΠΟΙΗΣΗ ΣΥΜΦΩΝΙΑΣ-ΠΛΑΙΣΙΟ Η ΤΗΣ ΕΚΤΕΛΕΣΤΙΚΗΣ ΣΥΜΒΑΣΗΣ ΚΑΤΑ ΤΗΔΙΑΡΚΕΙΑ ΤΗΣ	96
4.6	ΔΙΚΑΙΩΜΑ ΜΟΝΟΜΕΡΟΥΣ ΛΥΣΗΣ ΤΗΣ ΣΥΜΒΑΣΗΣ	96
5	ΕΙΔΙΚΟΙ ΟΡΟΙ ΕΚΤΕΛΕΣΗΣ ΕΚΤΕΛΕΣΤΙΚΩΝ ΣΥΜΒΑΣΕΩΝ	98
5.1	ΤΡΟΠΟΣ ΠΛΗΡΩΜΗΣ	98
5.2	ΑΝΑΠΡΟΣΑΡΜΟΓΗ ΤΙΜΗΣ	99
5.3	ΠΑΡΑΚΟΛΟΥΘΗΣΗ ΤΩΝ ΕΚΤΕΛΕΣΤΙΚΩΝ ΣΥΜΒΑΣΕΩΝ	99
5.4	ΠΑΡΑΛΑΒΗ ΤΩΝ ΕΚΤΕΛΕΣΤΙΚΩΝ ΣΥΜΒΑΣΕΩΝ	100
5.5	ΑΠΟΡΡΙΨΗ ΠΑΡΑΔΟΤΕΩΝ – ΑΝΤΙΚΑΤΑΣΤΑΣΗ	101
5.6	ΚΗΡΥΞΗ ΟΙΚΟΝΟΜΙΚΟΥ ΦΟΡΕΑ ΕΚΠΤΩΤΟΥ - ΚΥΡΩΣΕΙΣ	101
5.7	ΔΙΟΙΚΗΤΙΚΕΣ ΠΡΟΣΦΥΓΕΣ ΚΑΤΑ ΤΗ ΔΙΑΔΙΚΑΣΙΑ ΕΚΤΕΛΕΣΗΣ	102
5.8	ΔΙΚΑΣΤΙΚΗ ΕΠΙΛΥΣΗ ΔΙΑΦΟΡΩΝ	103
6	ΕΚΤΕΛΕΣΤΙΚΕΣ ΣΥΜΒΑΣΕΙΣ	104
6.1	ΛΕΙΤΟΥΡΓΙΑ ΤΗΣ ΣΥΜΦΩΝΙΑΣ ΠΛΑΙΣΙΟ - ΑΝΑΘΕΣΗ ΤΩΝ ΕΚΤΕΛΕΣΤΙΚΩΝ ΣΥΜΒΑΣΕΩΝ	104
6.2	ΥΠΟΓΡΑΦΗ ΕΚΤΕΛΕΣΤΙΚΩΝ ΣΥΜΒΑΣΕΩΝ	104
6.3	ΚΑΤΑΡΤΙΣΗ ΚΑΙ ΥΠΟΒΟΛΗ ΠΡΟΣΦΟΡΩΝ	104
6.4	ΠΑΡΑΛΑΒΗ – ΑΠΟΣΦΡΑΓΙΣΗ ΠΡΟΣΦΟΡΩΝ	105
6.5	ΔΙΚΑΙΟΛΟΓΗΤΙΚΑ ΤΟΥ ΑΝΤΙΣΥΜΒΑΛΛΟΜΕΝΟΥ ΣΤΟΝ ΟΠΟΙΟ ΠΡΟΚΕΙΤΑΙ ΝΑ ΓΙΝΕΙ ΗΚΑΤΑΚΥΡΩΣΗ ΤΗΣ ΕΚΤΕΛΕΣΤΙΚΗΣ ΣΥΜΒΑΣΗΣ	105
6.6	ΑΞΙΟΛΟΓΗΣΗ ΔΙΚΑΙΟΛΟΓΗΤΙΚΩΝ ΠΡΟΣΩΡΙΝΟΥ ΑΝΑΔΟΧΟΥ	105
6.7	ΚΑΤΑΚΥΡΩΣΗ – ΣΥΝΑΨΗ ΕΚΤΕΛΕΣΤΙΚΗΣ ΣΥΜΒΑΣΗΣ	105
6.8	ΕΚΤΕΛΕΣΗ ΕΚΤΕΛΕΣΤΙΚΗΣ ΣΥΜΒΑΣΗΣ	106

7 ΠΑΡΑΡΤΗΜΑΤΑ.....107

7.1	ΠΑΡΑΡΤΗΜΑ Ι – ΑΝΑΛΥΤΙΚΗ ΠΕΡΙΓΡΑΦΗ ΦΥΣΙΚΟΥ ΚΑΙ ΟΙΚΟΝΟΜΙΚΟΥ ΑΝΤΙΚΕΙΜΕΝΟΥ ΤΗΣ ΣΥΜΦΩΝΙΑΣ - ΠΛΑΙΣΙΟ	107
7.1.1	<i>Περιβάλλον της συμφωνίας - πλαίσιο</i>	107
7.1.1.1	Εμπλεκόμενοι στην υλοποίηση του Έργου	107
7.1.1.2	Φορέας Υλοποίησης – Αναθέτουσα Αρχή	107
7.1.1.3	Φορέας Χρηματοδότησης	109
7.1.1.4	Κύριος του Έργου – Φορέας Λειτουργίας	109
7.1.2	<i>Σκοπός και στόχοι του Έργου</i>	109
7.1.3	<i>Φυσικό αντικείμενο Τμήματος 1 «Υπηρεσίες εξασφάλισης επιχειρησιακής συνέχειας, ασφάλειας διακίνησης δεδομένων και μέτρα και πολιτικές πρόληψης και αντιμετώπισης κινδύνων για τη Γ.Γ.Π.Σ.Δ.Δ.»</i>	110
7.1.3.1	Διαστασιολόγηση λογισμικού, εξοπλισμού και υπηρεσιών	110
7.1.3.2	Πολιτικές – Διαδικασίες και Μέτρα Αντιμετώπισης και Πρόληψης	111
7.1.3.3	Εξειδικευμένες Λύσεις Ασφάλειας Πληροφοριών, Εγγράφων και εφαρμογών	125
7.1.3.4	Υπηρεσίες νεφοϋπολογιστικών υποδομών και υπηρεσιών	126
7.1.3.5	Εξειδικευμένες λύσεις ασφάλειας	126
7.1.4	<i>Φυσικό αντικείμενο Τμήματος 2 «Εξειδικευμένες λύσεις και υπηρεσίες ασφάλειας για την Η.ΔΙ.Κ.Α. Α.Ε.»</i>	128
7.1.4.1	Διαστασιολόγηση λογισμικού, εξοπλισμού και υπηρεσιών	128
7.1.4.2	Πολιτικές – Διαδικασίες και Μέτρα Αντιμετώπισης και Πρόληψης	131
7.1.4.3	Εξειδικευμένες Λύσεις Ασφάλειας Πληροφοριών, Εγγράφων και εφαρμογών	148
7.1.4.4	Υπηρεσίες νεφοϋπολογιστικών υποδομών και υπηρεσιών	152
7.1.4.5	Λύση Ddos	153
7.1.4.6	Εξειδικευμένες λύσεις ασφάλειας	153
7.1.5	<i>Φυσικό αντικείμενο Τμήματος 3 «Εξειδικευμένες λύσεις και υπηρεσίες ασφάλειας για το Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο»</i>	162
7.1.5.1	Διαστασιολόγηση λογισμικού, εξοπλισμού και υπηρεσιών	162
7.1.5.2	Πολιτικές – Διαδικασίες και Μέτρα Αντιμετώπισης και Πρόληψης	163
7.1.5.3	Εξειδικευμένες Λύσεις Ασφάλειας Πληροφοριών, Εγγράφων και εφαρμογών	180
7.1.5.4	Υπηρεσίες νεφοϋπολογιστικών υποδομών και υπηρεσιών	184
7.1.5.5	Υπηρεσίες SOC & Ddos	184
7.1.5.6	Εξειδικευμένες λύσεις ασφάλειας	188
7.1.6	<i>Φυσικό αντικείμενο Τμήματος 4 «Εξειδικευμένες λύσεις και υπηρεσίες ασφάλειας για την Ε.Δ.Υ.Τ.Ε. Α.Ε.»</i>	195
7.1.6.1	Διαστασιολόγηση λογισμικού, εξοπλισμού και υπηρεσιών	195
7.1.6.2	Πολιτικές – Διαδικασίες και Μέτρα Αντιμετώπισης και Πρόληψης	196
7.1.6.3	Εξειδικευμένες Λύσεις Ασφάλειας Πληροφοριών, Εγγράφων και εφαρμογών	213
7.1.6.4	Υπηρεσίες νεφοϋπολογιστικών υποδομών και υπηρεσιών	217
7.1.6.5	Υπηρεσίες SOC & Ddos	217
7.1.6.6	Εξειδικευμένες λύσεις ασφάλειας	221
7.1.7	<i>Φάσεις - παραδοτέα</i>	227
7.1.7.1	Χρονοδιάγραμμα υλοποίησης εκτελεστικών συμβάσεων	227
7.1.7.2	Παραδοτέα ανά λύση	227
7.1.7.3	Όροι και προϋποθέσεις παραλαβών	248
7.1.8	<i>Περίοδος Εγγύησης Συντήρησης (ΠΕΣ)</i>	249
7.1.8.1	Υπηρεσίες Περιόδου Εγγύησης-Συντήρησης	250
7.1.8.2	Τήρηση Εγγυημένου Επιπέδου Υπηρεσιών – Ρήτρες	252
7.1.8.3	Προγραμματισμένες Διακοπές Υπηρεσίας	254
7.1.9	<i>Σχήμα Διοίκησης Έργου</i>	255
7.1.9.1	Υπεύθυνος Έργου Αναδόχου	255
7.1.9.2	Μέλη Ομάδας Έργου	255
7.1.10	<i>Μεθοδολογία διοίκησης και διασφάλισης ποιότητας</i>	256
7.1.11	<i>Μεθοδολογία διαχείρισης κινδύνων</i>	256
7.1.12	<i>ΟΙΚΟΝΟΜΙΚΟ ΑΝΤΙΚΕΙΜΕΝΟ ΤΗΣ ΣΥΜΒΑΣΗΣ</i>	256
7.2	ΠΑΡΑΡΤΗΜΑ ΙΙ – ΠΙΝΑΚΕΣ ΣΥΜΜΟΡΦΩΣΗΣ	257

7.2.1	Πίνακες Συμμόρφωσης Τμήματος 1 «Υπηρεσίες εξασφάλισης επιχειρησιακής συνέχειας, ασφάλειας διακίνησης δεδομένων και μέτρα και πολιτικές πρόληψης και αντιμετώπισης κινδύνων για τη Γ.Γ.Π.Σ.Δ.Δ.»	257
7.2.1.1	Υπηρεσίες Ransomware readiness assessment	257
7.2.1.2	Μηχανισμός Ελέγχου Πρόσβασης Χρηστών Πολλαπλών Παραγόντων (MFA)	258
7.2.1.3	Παροχή υπηρεσιών ανάκαμψης από καταστροφή & λήψης αντιγράφων ασφαλείας (disaster recovery as a service & data backup as as service)	261
7.2.1.4	Λύση δημιουργίας αντιγράφων ασφαλείας σε ταινίες με PhysicalAirGap – TrueAirGap 1.960PB χωρητικότητα	268
7.2.1.5	Λύση δημιουργίας αντιγράφων ασφαλείας σε δίσκο Backup με Logical Air Gap για το 50% της χωρητικότητας	269
7.2.1.6	Λύση προστασίας ηλεκτρονικού ταχυδρομείου Mail Security - 20.000 σταθμούς εργασίας	273
7.2.1.7	Λύση Endpoint Detection and Response - 20.000 σταθμούς εργασίας	275
7.2.1.8	Λύση που αφορά τον έλεγχο της πρόσβασης των εσωτερικών χρηστών στο Διαδίκτυο	277
7.2.1.9	Λύση Ασφαλείας και προστασίας των χρηστών από απειλές του διαδικτύου (Web Security Gateway)	281
7.2.2	Πίνακες Συμμόρφωσης Τμήματος 2 «Εξειδικευμένες λύσεις και υπηρεσίες ασφάλειας για την Η.Δ.Ι.Κ.Α. Α.Ε.»	286
7.2.2.1	Λύση Διαβάθμισης και Σήμανσης Εγγράφων	286
7.2.2.2	Λύση Προστασίας Δεδομένων από Διαρροή	295
7.2.2.3	Λύση Διαχείρισης Δικαιωμάτων Εγγράφων	308
7.2.2.4	Λύση Διαχείρισης Λογαριασμών και Δικαιωμάτων Πρόσβασης Χρηστών	311
7.2.2.5	Λύση Διαχείρισης Προνομιούχων Λογαριασμών Πρόσβασης	319
7.2.2.6	Λύση μηχανισμών ισχυρής ταυτοποίησης	329
7.2.2.7	Υπηρεσίες ανάκαμψης από καταστροφή και λήψης αντιγράφων ασφαλείας	331
7.2.2.8	Ddos	336
7.2.2.9	NGFW για το Data Center, για την πρόσβαση των εσωτερικών χρηστών στο Διαδίκτυο και την ανάλυση των επικοινωνιών τους και για την απομακρυσμένη πρόσβαση. Άδειες για προστασία IPS, antimalware, Application Control. Διαχειριστικό εργαλείο για τα firewall	346
7.2.2.10	Switches για τη διασύνδεση των firewalls	352
7.2.2.11	Virtual firewall Για 10 tenants με High availability Καιάδειες IPS και antimalware	355
7.2.2.12	Λύση Microsegmentation	362
7.2.2.13	Λύση Ασφαλείας και προστασίας των χρηστών από απειλές του διαδικτύου (Web Security Gateway) - 250 χρήστες και Συσκευές υλικού (HW appliances)	368
7.2.2.14	Λύση Αυστηρής πιστοποίησης για την απομακρυσμένη πρόσβαση (MFA, Zero Trust)	374
7.2.2.15	Λύση Cloud Proxy προστασίας απομακρυσμένων χρηστών	380
7.2.2.16	Λύση Antimalware απομακρυσμένων χρηστών (AV, EDR, XDR)	389
7.2.2.17	Λύση εκπαίδευσης για 250 χρήστες σε phishing campaigns και cyber attacks	404
7.2.2.18	Λύση Ασφαλούς Πρόσβασης χρηστών στο εταιρικό δίκτυο	412
7.2.2.19	Λύση Πλατφόρμας Ενορχήστρωσης Ασφαλείας, Αυτοματοποίησης	419
7.2.2.20	Πλατφόρμα Κυβερνοασφάλειας – Εκτεταμένης Ανίχνευσης & Απόκρισης (Cyber Security)	421
7.2.2.21	Λύση Προστασίας Βάσεων Δεδομένων	429
7.2.2.22	Λογισμικό κυβερνοασφάλειας ΑΙ, συμπεριλαμβανομένης εγκατάστασης, εκπαίδευσης και υποστήριξης	433
24/7.	1000 Άδειες	
7.2.3	Πίνακες Συμμόρφωσης Τμήματος 3 «Εξειδικευμένες λύσεις και υπηρεσίες ασφάλειας για το Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο»	438
7.2.3.1	Παροχή υπηρεσίας SOC	438
7.2.3.2	Λύση DDOS	454
7.2.3.3	Υπηρεσίες ανάκαμψης από καταστροφή και λήψης αντιγράφων ασφαλείας	461
7.2.3.4	Λύση Προστασίας Βάσεων Δεδομένων	466
7.2.3.5	Πλατφόρμα Κυβερνοασφάλειας – Εκτεταμένης Ανίχνευσης & Απόκρισης (Cyber Security)	470
7.2.3.6	Λογισμικό κυβερνοασφάλειας ΑΙ, συμπεριλαμβανομένης εγκατάστασης, εκπαίδευσης και υποστήριξης	478
24/7.	1000 Άδειες	
7.2.3.7	Λύση προστασίας ηλεκτρονικού ταχυδρομείου Mail Security - 3.000 σταθμούς εργασίας	483
7.2.3.8	Λύση Endpoint Detection and Response - 3.000 σταθμούς εργασίας	485
7.2.3.9	Λύση Διαβάθμισης και Σήμανσης Εγγράφων	487
7.2.3.10	Λύση Προστασίας Δεδομένων από Διαρροή	495
7.2.3.11	Λύση Διαχείρισης Δικαιωμάτων Εγγράφων	509
7.2.3.12	Λύση Διαχείρισης Λογαριασμών και Δικαιωμάτων Πρόσβασης Χρηστών	512
7.2.3.13	Λύση Διαχείρισης Προνομιούχων Λογαριασμών Πρόσβασης	519

7.2.4	Πίνακες Συμμόρφωσης Τμήματος 4 «Εξειδικευμένες λύσεις και υπηρεσίες ασφάλειας για την Ε.Δ.Υ.Τ.Ε. Α.Ε.».....	529
7.2.4.1	Παροχή υπηρεσίας SOC	530
7.2.4.2	Λύση DDOS.....	545
7.2.4.3	Υπηρεσίες ανάκαμψης από καταστροφή και λήψης αντιγράφων ασφάλειας	556
7.2.4.4	Λύση Προστασίας Βάσεων Δεδομένων.....	561
7.2.4.5	Πλατφόρμα Κυβερνοασφάλειας – Εκτεταμένης Ανίχνευσης & Απόκρισης (Cyber Security)	566
7.2.4.6	Λογισμικό κυβερνοασφάλειας ΑΙ, συμπεριλαμβανομένης εγκατάστασης, εκπαίδευσης και υποστήριξης 24/7. 1000 Άδειες	573
7.2.4.7	Λύση Διαβάθμισης και Σήμανσης Εγγράφων.....	578
7.2.4.8	Λύση Προστασίας Δεδομένων από Διαρροή	586
7.2.4.9	Λύση Διαχείρισης Δικαιωμάτων Εγγράφων	600
7.2.4.10	Λύση Διαχείρισης Λογαριασμών και Δικαιωμάτων Πρόσβασης Χρηστών	603
7.2.4.11	Λύση Διαχείρισης Προνομιούχων Λογαριασμών Πρόσβασης.....	610
7.3	ΠΑΡΑΡΤΗΜΑ ΙΙΙ – ΕΥΡΩΠΑΙΚΟ ΕΝΙΑΙΟ ΕΓΓΡΑΦΟ ΣΥΜΒΑΣΗΣ (ΕΕΕΣ)	621
7.4	ΠΑΡΑΡΤΗΜΑ ΙV – ΥΠΟΔΕΙΓΜΑ ΒΙΟΓΡΑΦΙΚΟΥ ΣΗΜΕΙΩΜΑΤΟΣ	622
7.5	ΠΑΡΑΡΤΗΜΑ V – ΥΠΟΔΕΙΓΜΑ ΤΕΧΝΙΚΗΣ ΠΡΟΣΦΟΡΑΣ.....	625
7.6	ΠΑΡΑΡΤΗΜΑ VI – ΥΠΟΔΕΙΓΜΑ ΟΙΚΟΝΟΜΙΚΗΣ ΠΡΟΣΦΟΡΑΣ	626
1.	Εξοπλισμός	626
2.	Εφαρμογές – Λογισμικά.....	626
3.	Υπηρεσίες	627
4.	Άλλες δαπάνες.....	627
5.	Συγκεντρωτικός Πίνακας Οικονομικής Προσφοράς Έργου.....	627
6.	Συγκεντρωτικός Πίνακας Οικονομικής Προσφοράς Συντήρησης.....	628
7.7	ΠΑΡΑΡΤΗΜΑ VII – ΆΛΛΕΣ ΔΗΛΩΣΕΙΣ.....	629
7.8	ΠΑΡΑΡΤΗΜΑ VIII – ΥΠΟΔΕΙΓΜΑΤΑ ΕΓΓΥΗΤΙΚΩΝ ΕΠΙΣΤΟΛΩΝ	629
I.	Εγγυητική Επιστολή Συμμετοχής	629
II.	Εγγυητική Επιστολή Καλής Εκτέλεσης	630
III.	Εγγυητική Επιστολή Προκαταβολής.....	632
IV.	Εγγυητική Επιστολή Καλής Λειτουργίας	634
7.9	ΠΑΡΑΡΤΗΜΑ ΙΧ – ΕΝΗΜΕΡΩΣΗ ΓΙΑ ΤΗΝ ΕΠΕΞΕΡΓΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ.....	635

1. ΑΝΑΘΕΤΟΥΣΑ ΑΡΧΗ ΚΑΙ ΑΝΤΙΚΕΙΜΕΝΟ ΣΥΜΒΑΣΗΣ

1.1 Στοιχεία Αναθέτουσας Αρχής

Επωνυμία	ΚΟΙΝΩΝΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ Μ.Α.Ε.
ΑΦΜ	999983307
Κωδικός Ηλεκτρονικής Τιμολόγησης	1053.E00553.00005
Ταχυδρομική διεύθυνση	Λεωφ. Συγγρού 194
Πόλη	Καλλιθέα
Ταχυδρομικός Κωδικός	176 71
Χώρα	ΕΛΛΑΔΑ
Κωδικός NUTS	GR 300
Τηλέφωνο	213 1300700
Φαξ	213 1300801
Ηλεκτρονικό Ταχυδρομείο	info@ktpae.gr
Αρμόδιος για πληροφορίες	Δήμητρα Παγώνη
Γενική Διεύθυνση στο διαδίκτυο(URL)	http://www.ktpae.gr
Διεύθυνση του προφίλ αγοραστή στο διαδίκτυο (URL)	https://www.ktpae.gr/

Είδος Αναθέτουσας Αρχής

Η Αναθέτουσα Αρχή είναι η Κοινωνία της Πληροφορίας Μονοπρόσωπη Ανώνυμη Εταιρία του Δημόσιου Τομέα (μη Κεντρική Αναθέτουσα Αρχή) και ανήκει στην Κεντρική Κυβέρνηση – Υποτομέας Νομικά Πρόσωπα Κεντρικής Κυβέρνησης και Δημόσιες Επιχειρήσεις

Κύρια δραστηριότητα Α.Α.

Η κύρια δραστηριότητα της Αναθέτουσας Αρχής είναι «Γενικές Δημόσιες Υπηρεσίες».

Εφαρμοστέο εθνικό δίκαιο είναι το Ελληνικό:

Στοιχεία Επικοινωνίας

- Τα έγγραφα της σύμβασης είναι διαθέσιμα για ελεύθερη, πλήρη, άμεση & δωρεάν ηλεκτρονική πρόσβαση στην διεύθυνση (URL) : μέσω της διαδικτυακής πύλης www.promitheus.gov.gr του Ε.Σ.Η.ΔΗ.Σ. και μέσω της διαδικτυακής πύλης της Αναθέτουσας Αρχής <http://www.ktpae.gr>. Κάθε είδους επικοινωνία και ανταλλαγή πληροφοριών πραγματοποιείται μέσω της διαδικτυακής πύλης www.promitheus.gov.gr του Ε.Σ.Η.ΔΗ.Σ.
- Οι προσφορές πρέπει να υποβάλλονται ηλεκτρονικά στην διεύθυνση : www.promitheus.gov.gr

1.2 Στοιχεία Διαδικασίας - Χρηματοδότηση

Είδος διαδικασίας

Ο διαγωνισμός για την ανάδειξη οικονομικών φορέων που θα συμμετέχουν στη συμφωνία-πλαίσιο θα διεξαχθεί με την ανοικτή διαδικασία του άρθρου 27 του ν. 4412/16.

Χρηματοδότηση της συμφωνίας-πλαίσιο

Η δαπάνη για την εν λόγω συμφωνία-πλαίσιο και τις εκτελεστικές αυτής συμβάσεις, έχει καταρχήν ενταχθεί στο Πρόγραμμα Δημοσίων Επενδύσεων (Συλλογική Απόφαση Ένταξης με ΑΔΑ: ΧΧΧΧΧΧΧΧΧΧΧΧ, αριθ. ενάρθ. έργου ΧΧΧΧΧΧΧΧΧΧΧΧ), αλλά συμπεριλαμβάνεται στο Εθνικό Σχέδιο Ανάκαμψης και Ανθεκτικότητας Ελλάδα 2.0 όπως αυτό εγκρίθηκε από τις υπηρεσίες της Ε.Ε. για να χρηματοδοτηθεί από το Ταμείο Ανάκαμψης και Ανθεκτικότητας. Το δικαίωμα προαίρεσης μπορεί να χρηματοδοτηθεί από οποιαδήποτε άλλη πηγή.

1.3 Συνοπτική Περιγραφή φυσικού και οικονομικού αντικείμενου της συμφωνίας-πλαίσιο

1.3.1 Αντικείμενο της συμφωνίας-πλαίσιο

Α. Σκοπιμότητα

Η διαχείριση κινδύνων στον Κυβερνοχώρο είναι μια δυναμικά μεταβαλλόμενη διαδικασία, βρίσκεται σε συνεχή εξέλιξη και μεταβάλλεται σύμφωνα με το εκάστοτε περιβάλλον απειλών. Η απεικόνιση της εξέλιξης του περιβάλλοντος Κυβερνοασφάλειας τα τελευταία δέκα χρόνια εμφανίζει ξεκάθαρα την ανάγκη για ολιστική προσέγγιση, που εστιάζει στην πρόληψη ώστε να βελτιστοποιηθεί η κυβερνοανθεκτικότητα των οργανισμών.

Όλα τα μέτρα για την Κυβερνοασφάλεια πρέπει να εστιάζουν σε τρεις (3) βασικούς και κρίσιμους παράγοντες :

- **Στους χρήστες.** Οι χρήστες πρέπει να κατανοήσουν και να ακολουθήσουν βασικές αρχές ασφαλείας όπως η σωστή διαχείριση των passwords, να προσέχουν τα συνημμένα αρχεία, να μπορούν να κρίνουν ποια Sites μοιάζουν επικίνδυνα, να κάνουν συχνά backup και γενικότερα να ενημερωθούν κατάλληλα για να μπορούν να αναγνωρίσουν τις απειλές. Ότι εργαλεία και να χρησιμοποιηθούν, εάν ο τελικός χρήστης δεν έχει γνώση για να εποπτεύει τις διαδικασίες και τα εργαλεία ή δεν μπορεί να αναγνωρίσει τις κυβερνοαπειλές, είναι ο αδύνατος κρίκος στην αλυσίδα της κυβερνοασφάλειας.
- **Στις διαδικασίες** που θέτει ένας οργανισμός. Οι οργανισμοί πρέπει να έχουν μελετήσει και εφαρμόσει ένα πλαίσιο στο πώς θα αντιμετωπίζουν οι χρήστες τις επιτυχημένες ή αποτυχημένες απόπειρες κυβερνοεπιθέσεων. Διαδικασίες φυσικά υπάρχουν ακόμα και σε ατομικό επίπεδο, για παράδειγμα η σωστή διαχείριση των Passwords, ασφαλής καταστροφή ευαίσθητων δεδομένων, οι ενέργειες που πρέπει να κάνει κάποιος για να διασφαλίσει τα προσωπικά του δεδομένα και αρκετά άλλα θέματα που πρέπει να μελετηθούν. Ακόμα και η εκπαίδευση των ίδιων των χρηστών ή των μελών ενός οργανισμού, ανήκει στις διαδικασίες της CyberSecurity.
- **Στις τεχνολογικές υποδομές.** Η τεχνολογία είναι απαραίτητη ούτως ώστε να δώσει στους οργανισμούς και στους ιδιώτες τα εργαλεία τα οποία απαιτούνται για να προστατευτούν από

τις κυβερνοεπιθέσεις. Οι βασικές οντότητες που πρέπει να προστατευτούν μέσω των τεχνολογικών εργαλείων είναι: Endpoints (τερματικά), Έξυπνες συσκευές και Routers , το δίκτυο στο σύνολο του αλλά και το Cloud.

Στο παραπάνω πλαίσιο η Δράση για την ενίσχυση της Κυβερνοανθεκτικότητας των κρίσιμων οντοτήτων του ΥΨΗΔ και των εποπτευόμενων φορέων του πρέπει να εστιάσει σε ένα πλέγμα δράσεων που αφορά το σύνολο των παραπάνω παραγόντων και συγκεκριμένα :

B1. Πολιτικές – Διαδικασίες και Μέτρα Αντιμετώπισης και Πρόληψης

Στο πλαίσιο αυτής της ενότητας θα παρασχεθούν μια σειρά από υπηρεσίες (συμβουλευτικές και τεχνολογικές) που στοχεύουν :

- Στην αξιολόγηση της ετοιμότητας για ανταπόκριση σε επιθέσεις τύπου ransomware
- Στη διαμόρφωση πολιτικών ασφάλειας κρίσιμων οντοτήτων με στόχο την ανάδειξη τεχνικών και οργανωτικών μέτρων για την προστασία τους από Κυβερνοαπειλές
- Στη διαμόρφωση πολιτικών ορθής χρήσης Πληροφοριακών συστημάτων και εφαρμογών
- Στη διενέργεια δράσεων ενημέρωσης για τη μεταφορά τεχνογνωσίας και την διαμόρφωση κουλτούρας ενεργούς ευαισθητοποίησης για τους κινδύνους κυβερνοασφάλειας
- Τη διαμόρφωση πλάνου επιχειρησιακής συνέχειας για κρίσιμες οντότητες
- Την Εκπόνηση Μελέτης Ανάλυσης και Αξιολόγησης Κινδύνων
- Την Εκπόνηση Μελέτης εξωτερικού και εσωτερικού περιβάλλοντος και την ανάδειξη βέλτιστων πρακτικών
- Τη διαμόρφωση πολιτικής αντιγράφων ασφαλείας, που θα περιγράφει σκοπό, πεδίο εφαρμογής, ρόλους και ευθύνες
- Τη διαμόρφωση Συστήματος Διαχείρισης της Ασφάλειας των Πληροφοριών (ΣΔΑΠ) με βάση το πρότυπο ISO 27001
- Τη διενέργεια ελέγχων διείσδυσης εξωτερικών δικτύων για τον εντοπισμό των ευπαθειών σε υποδομές, συσκευές και διακομιστές που είναι προσβάσιμοι από το διαδίκτυο.
- Στη διενέργεια ελέγχων διείσδυσης διαδικτυακών εφαρμογών, οι οποίοι στοχεύουν στον εντοπισμό τρωτών σημείων ασφαλείας που προκύπτουν από ανασφαλείς πρακτικές ανάπτυξης στη δημιουργία τη σχεδίαση και τη διαχείριση του λογισμικού ή ιστότοπου.
- Στη διενέργεια ελέγχων του εσωτερικού δικτύου που συνήθως αποτελεί το πιο κρίσιμο σημείο της ευρύτερης υποδομής καθώς περιλαμβάνει όλα εκείνα τα δεδομένα και τα συστήματα που συντελούν στην ομαλή λειτουργία του οργανισμού.
- Στη διενέργεια ελέγχων φυσικής ασφάλειας ώστε να αξιολογούνται τα μέτρα ασφαλείας που προστατεύουν τα περιουσιακά στοιχεία των οργανισμών από απειλές και συμβάλλουν στον εντοπισμό τυχόν βελτιώσεων
- Στη διενέργεια ελέγχων για τη διαρροή δεδομένων και ιδίως στο σκοτεινό δίκτυο, που αποτελεί μια βασική αφετηρία απειλών και κινδύνων
- Στην αξιοποίηση της τεχνολογικής καινοτομίας και ερευνητικής πρωτοπορίας στον τομέα της κυβερνοασφάλειας

B2. Εξειδικευμένες Λύσεις Ασφάλειας Πληροφοριών, Εγγράφων και εφαρμογών

Στο Πλαίσιο αυτής της ενότητας θα εφαρμοστούν λύσεις λογισμικού και λογισμικού με στόχο :

- Την επαύξηση του επιπέδου ασφάλειας των φορέων
- Την προστασία των εγγράφων τους
- Την οργάνωση των δικαιωμάτων πρόσβασης των χρηστών

- Τη συμμόρφωση με το Κανονιστικό/Νομοθετικό πλαίσιο (Ελληνικό και Ευρωπαϊκό)
- Την Εναρμόνιση με τις απαιτήσεις του ISO 27001
- Την αύξηση του επιπέδου πρόληψης κακόβουλων ενεργειών (εσωτερικές και εξωτερικές)
- Την συμμόρφωση με τον Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων (ΓΚΠΔ)
- Την εφαρμογή της αρχής της λογοδοσίας (ΓΚΠΔ)

Συγκεκριμένα, θα εφαρμοστούν λύσεις που αφορούν :

- Την Αποτροπή Διαρροής Πληροφοριών (Data Loss Prevention - DLP).
- Τη Διαβάθμιση εγγράφων.
- Τη Διαχείριση Δικαιωμάτων Εγγράφων (Information Rights Management)..
- Τη Διαχείριση Λογαριασμών και Δικαιωμάτων πρόσβασης χρηστών (Identity & Access Rights Management - IAM).
- Την υλοποίηση μηχανισμών ελέγχου πρόσβασης χρηστών πολλαπλών παραγόντων (Multi Factor Authentication MFA)
- Την υλοποίηση μηχανισμών ισχυρής ταυτοποίησης (strong authentication)
- Τη Διαχείριση Προσβάσεων με Αυξημένα Δικαιώματα (Privileged Access Management - PAM).

B3. Υπηρεσίες νεφοϋπολογιστικών υποδομών και υπηρεσιών

Τα τελευταία χρόνια οι κυβερνοεπιθέσεις σε συστήματα Δημοσίων Φορέων και Οργανισμών έχουν γίνει συχνότερες και εξυνότερες. Η επιτυχής ανταπόκριση προϋποθέτει, μεταξύ άλλων, την ενδυνάμωση των μηχανισμών ανάκαμψης από καταστροφή. Στα πλαίσια αυτά, προβλέπεται η παροχή υπηρεσιών κέντρου ανάκαμψης από καταστροφή, με βάση υποδομές δημόσιου υπολογιστικού νέφους. Στο πλαίσιο του έργου θα γίνει προμήθεια κατ' ελάχιστον, των υποδομών, υπηρεσιών και στοιχείων που αναφέρονται παρακάτω. Με βάση το είδος κάθε προσφερόμενου υπολογιστικού πόρου, αυτοί έχουν ταξινομηθεί στις παρακάτω κεντρικές ενότητες νεφοϋπολογιστικών μοντέλων (υπάρχουν υπολογιστικοί πόροι που είναι εφικτό να δίνονται με διαφορετικά μοντέλα υλοποίησης Νέφους):

A) Υποδομές και Υπηρεσίες Νέφους - Infrastructure as a Service (IaaS): Στο μοντέλο υλοποίησης IaaS ο ανάδοχος που θα επιλεγεί θα πρέπει να προσφέρει τα ακόλουθα στοιχεία:

- Υποδομές Εικονικών μηχανών (VMs) διαφόρων υπολογιστικών προφίλ, μεγεθών και επεξεργαστικών δυνατοτήτων.
- Υποδομές Αποθηκευτικών Μέσων (Storage disks) διαφόρων χωρητικότητων.
- Υποδομές εικονικών δικτυακών πόρων (Virtual Network resources).
- Υποδομές δεσμευμένων, απομονωμένων φυσικών διακομιστών εικονικοποίησης (Physical Virtualization Hosts).

B) Υποδομές και Υπηρεσίες Νέφους – Platform as a Service (PaaS): Στο μοντέλο υλοποίησης PaaS ο ανάδοχος που θα επιλεγεί θα πρέπει να προσφέρει τα ακόλουθα στοιχεία:

- Υπηρεσίες πλατφόρμας Ονοματολογίας Περιοχής DNS
- Υπηρεσίες πλατφόρμας Database as a Service (DBaaS) για διάφορα είδη Βάσεων Δεδομένων Σχεσιακών (RDBMS) και Μη Σχεσιακών (noSQL DBs).
- Υπηρεσίες πλατφόρμας παροχής αποθηκευτικού χώρου (Storage as a Service).

- Υπηρεσίες πλατφόρμας Αντιγράφων ασφαλείας (Backup) / Επαναφοράς (Recovery) ώστε να λαμβάνονται αντίγραφα ασφαλείας σε υπολογιστικούς πόρους που βρίσκονται εγκατεστημένοι είτε τοπικά (On-premises) είτε στον πάροχο του Νέφος (Cloud).
- Υπηρεσίες πλατφόρμας Προστασίας/Ασφάλειας έναντι επιθέσεων Άρνησης Υπηρεσίας (DDoS) για την προστασία συστημάτων και υπηρεσιών έναντι DDoS επιθέσεων.
- Υπηρεσίες πλατφόρμας φιλοξενίας διαχείρισης και υποστήριξης εφαρμογών Internet of Things (IoT)
- Υπηρεσίες πλατφόρμας παρακολούθησης του κόστους χρήσης όλων των ανωτέρω προσφερόμενων νεφοϋπολογιστικών υπηρεσιών

B4. Υπηρεσίες SOC & Ddos

Αφορά υπηρεσία αδιάλειπτης και σε πραγματικό χρόνο (24x7) επιτήρησης των συστημάτων του Φορέα από εξειδικευμένο και σε διεθνώς αναγνωρισμένο πάροχο για την πρόληψη και αντιμετώπιση κυβερνοαπειλών.

Η προτεινόμενη πρωτοβουλία στοχεύει στην ενδυνάμωση του επιπέδου ασφάλειας για τις υποδομές του Φορέα και η πλήρης συμμόρφωση της με τις κανονιστικές απαιτήσεις (όπως ο νόμος ν. 4577/2018 «Ενσωμάτωση στην ελληνική νομοθεσία της Οδηγίας 2016/1148/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση και άλλες διατάξεις», ο Γενικός Κανονισμός Προσωπικών Δεδομένων, κλπ.).

Επίσης περιλαμβάνεται η παροχή υπηρεσιών συστήματος ανίχνευσης δικτυακών ανωμαλιών και αντιμετώπισης επιθέσεων άρνησης υπηρεσίας (DDoS - Distributed Denial-of-Service), βασισμένο σε δεδομένα ροών (flow-records) από τους υφιστάμενους δρομολογητές IP του δικτύου του Φορέα.

B5. Εξειδικευμένες λύσεις ασφάλειας

Στο πλαίσιο αυτό περιλαμβάνονται εξειδικευμένες λύσεις ασφάλειας που στόχο έχουν την ενίσχυση της περιμετρικής ασφάλειας των κρίσιμων πληροφοριακών υποδομών του Υπουργείου Ψηφιακής Διακυβέρνησης και των εποπτευόμενων φορέων του, όπως :

- Λύση Next Generation Firewall και Virtual firewall
- Λύση που αφορά τον έλεγχο της πρόσβασης των εσωτερικών χρηστών στο Διαδίκτυο και την ανάλυση των επικοινωνιών τους.
- Λύση Ασφάλειας και προστασίας των χρηστών από απειλές του διαδικτύου (Web Security Gateway)
- Λύση Cloud Proxy και προστασίας απομακρυσμένων χρηστών (DNS)
- Λύση Microsegmentation
- Κεντρική Πλατφόρμα Ενορχήστρωσης Ασφάλειας, Αυτοματοποίησης και Απόκρισης (SOAR)
- Λύση δημιουργίας αντιγράφων ασφαλείας σε ταινίες με Physical Air Gap – True Air Gap.
- Λύση δημιουργίας αντιγράφων ασφαλείας σε δίσκο Backup με Logical Air Gap.
- Λύση προστασίας ηλεκτρονικού ταχυδρομείου Mail Security.
- Λύση Security information and event management (SIEM)
- Λύση εκπαίδευσης σε Phishing campaigns και Cyber attacks
- Λύση Ασφαλούς Πρόσβασης χρηστών στο εταιρικό δίκτυο
- Λύση Endpoint Detection and Response.

- Λυση Visibility και Threat Response
- Managed services security endpoint & mail.
- Λύση Προστασίας Βάσεων Δεδομένων.
- Λύση ΑΙ για αυτοματοποίηση εντοπισμού και απόκρισης κυβερνοεπιθέσεων σε πραγματικό χρόνο.

Τα είδη προς προμήθεια και οι παρεχόμενες υπηρεσίες κατατάσσονται στους ακόλουθους κωδικούς του Κοινού Λεξιλογίου δημοσίων συμβάσεων (CPV) :

30200000-1	Εξοπλισμός ηλεκτρονικών υπολογιστών και προμήθειες
48730000-4	Πακέτα λογισμικού ασφαλείας
48731000-1	Πακέτα λογισμικού ασφάλειας αρχείων
48732000-8	Πακέτα λογισμικού ασφάλειας δεδομένων
79417000-0	Υπηρεσίες παροχής συμβουλών σε θέματα ασφαλείας
72246000-1	Υπηρεσίες παροχής συμβουλών σε θέματα συστημάτων πληροφορικής
72263000-6	Υπηρεσίες υλοποίησης λογισμικού
30200000-1	Εξοπλισμός ηλεκτρονικών υπολογιστών και προμήθειες

Η εκτιμώμενη αξία της συμφωνίας-πλαίσιο ανέρχεται στο ποσό των εκατόν δύο εκατομμυρίων εκατόν εξήντα επτά χιλιάδων εννιακοσίων ενενήντα εννιά ευρώ και ενενήντα εννέα λεπτών (102.167.999,99 €) συμπεριλαμβανομένου ΦΠΑ 24 % (προϋπολογισμός χωρίς ΦΠΑ: 82.393.548,38 € ΦΠΑ: 19.774.451,61 €)

- Η εκτιμώμενη αξία της αρχικής συμφωνίας-πλαίσιο ανέρχεται στο ποσό των τριάντα οχτώ εκατομμυρίων εκατόνσάραντα πέντε χιλιάδων εκατόν εξήντα ενός ευρώ και είκοσι εννέα λεπτών (38.145.161,29 €) μη περιλαμβανομένου ΦΠΑ (προϋπολογισμός με ΦΠΑ: 47.300.000,00 €, ΦΠΑ 24% 9.154.838,71 €). Η πηγή χρηματοδότησης είναι το ΕΣΑΑ Ελλάδα 2.0, ΣΑΤΑ ΤΑΧΧΧΧΧ (Κωδ. Έργου: 2022ΤΑΧΧΧΧΧΧΧ).
- Το δικαίωμα προαίρεσης ως προς το φυσικό αντικείμενο ανέρχεται σε πενήντα τοις εκατό (50%) της αξίας της αρχικής συμφωνίας - πλαίσιο στο ποσό των δεκαεννέα εκατομμυρίων εβδομήντα δύο χιλιάδων πεντακοσίων ογδόντα ευρώ και εξήντα τεσσάρων λεπτών (19.072.580,64 €) μη περιλαμβανομένου ΦΠΑ (προϋπολογισμός με ΦΠΑ: 23.650.000,00 €, ΦΠΑ 24% 4.577.419,35 €). Η προαίρεση δύναται να χρηματοδοτηθεί από οποιαδήποτε άλλη πηγή.
- Το δικαίωμα προαίρεσης ως προς τη συντήρηση ανέρχεται στο ποσό των είκοσι πέντε εκατομμυρίων εκατόν εβδομήντα πέντε χιλιάδων οχτακοσίων έξι ευρώ και σάραντα πέντε λεπτών (25.175.806,45 €) μη περιλαμβανομένου ΦΠΑ (προϋπολογισμός με ΦΠΑ:

31.218.000,00 €, ΦΠΑ 24% 6.042.193,55 €). Η προαίρεση δύναται να χρηματοδοτηθεί από οποιαδήποτε άλλη πηγή.

Η διάρκεια της συμφωνίας-πλαίσιο ορίζεται σε **τριάντα (30) μήνες**, από την υπογραφή της σχετικής σύμβασης.

Οι εκτελεστικές συμβάσεις μπορούν να συνάπτονται έως και τη συμπλήρωση του χρόνου διάρκειας της συμφωνίας - πλαίσιο.

Αναλυτική περιγραφή του φυσικού και οικονομικού αντικείμενου της συμφωνίας-πλαίσιο δίδεται στο ΠΑΡΑΡΤΗΜΑ Ι της παρούσας διακήρυξης.

Η συμφωνία - πλαίσιο θα ανατεθεί με το κριτήριο της πλέον συμφέρουσας από οικονομική άποψη προσφοράς, βάσει της **βέλτιστης σχέσης ποιότητας – τιμής**.

1.3.2 Αριθμός συμβαλλομένων οικονομικών φορέων και Υποδιαίρεση σε Τμήματα

Η ολοκλήρωση αυτής της διαγωνιστικής διαδικασίας θα οδηγήσει στη σύναψη συμφωνίας-πλαίσιο με ένα οικονομικό φορέα ανά Τμήμα, δηλαδή συνολικά με τέσσερις (4) οικονομικούς φορείς. Σε περίπτωση υποβολής λιγότερων παραδεκτών προσφορών είναι δυνατή η σύναψη συμφωνιών πλαίσιο με τον ίδιο οικονομικό φορέα για περισσότερα του ενός (1) Τμήματα, ακόμη και για το σύνολο των Τμημάτων.

Το φυσικό αντικείμενο της συμφωνίας πλαίσιο διαιρείται σε τμήματα όπως αναλύεται στο ΠΑΡΑΡΤΗΜΑ Ι – Αναλυτική Περιγραφή Φυσικού και Οικονομικού Αντικείμενου της .

Το οικονομικό αντικείμενο της συμφωνίας – πλαίσιο χωρίς τα δικαιώματα προαίρεσης διαιρείται σε τμήματα ως εξής:

Α/Α	ΠΕΡΙΓΡΑΦΗ ΤΜΗΜΑΤΟΣ	ΚΟΣΤΟΣ (χωρίς ΦΠΑ)	ΦΠΑ	ΣΥΝΟΛΙΚΟ ΚΟΣΤΟΣ
1	Τμήμα 1 «Υπηρεσίες εξασφάλισης επιχειρησιακής συνέχειας, ασφάλειας διακίνησης δεδομένων και μέτρα και πολιτικές πρόληψης και αντιμετώπισης κινδύνων για τη Γ.Γ.Π.Σ.Δ.Δ.»	12.012.400,00 €	2.882.976,00 €	14.895.375,99 €
2	Τμήμα 2 «Εξειδικευμένες λύσεις και υπηρεσίες ασφάλειας για την Η.ΔΙ.Κ.Α. Α.Ε.»	10.135.911,30 €	2.432.618,71 €	12.568.530,01 €
3	Τμήμα 3 «Εξειδικευμένες λύσεις και υπηρεσίες ασφάλειας για το Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο»»	8.837.600,00 €	2.121.024,00 €	10.958.624,00 €
4	Τμήμα 4 «Εξειδικευμένες λύσεις και υπηρεσίες ασφάλειας για την Ε.Δ.Υ.Τ.Ε. Α.Ε.»	7.159.250,00 €	1.718.220,00 €	8.877.470,00 €
Σύνολο		38.145.161,29 €	9.154.838,71 €	47.300.000,00 €

Το οικονομικό αντικείμενο των δικαιωμάτων προαίρεσης διαιρείται σε τμήματα ως εξής:

Α/Α	ΠΕΡΙΓΡΑΦΗ ΤΜΗΜΑΤΟΣ	ΔΙΚΑΙΩΜΑ ΠΡΟΑΙΡΕΣΗΣ ΩΣ ΠΡΟΣ ΤΟ ΦΥΣΙΚΟ ΑΝΤΙΚΕΙΜΕΝΟ			ΔΙΚΑΙΩΜΑ ΠΡΟΑΙΡΕΣΗΣ ΣΥΝΤΗΡΗΣΗΣ		
		ΚΟΣΤΟΣ (χωρίς ΦΠΑ)	ΦΠΑ	ΣΥΝΟΛΙΚΟ ΚΟΣΤΟΣ	ΚΟΣΤΟΣ (χωρίς ΦΠΑ)	ΦΠΑ	ΣΥΝΟΛΙΚΟ ΚΟΣΤΟΣ
1	Τμήμα 1 «Υπηρεσίες εξασφάλισης επιχειρησιακής συνέχειας, ασφάλειας διακίνησης δεδομένων και μέτρα και πολιτικές πρόληψης και αντιμετώπισης κινδύνων για τη Γ.Γ.Π.Σ.Δ.Δ.»	6.006.200,00 €	1.441.488,00 €	7.447.688,00 €	7.928.184,00 €	1.902.764,16 €	9.830.948,16 €
2	Τμήμα 2 «Εξειδικευμένες λύσεις και υπηρεσίες ασφάλειας για την Η.ΔΙ.Κ.Α. Α.Ε.»	5.067.955,65 €	1.216.309,36 €	6.284.265,00 €	6.689.701,46 €	1.605.528,35 €	8.295.229,80 €
3	Τμήμα 3 «Εξειδικευμένες λύσεις και υπηρεσίες ασφάλειας για το Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο»»	4.418.800,00 €	1.060.512,00 €	5.479.312,00 €	5.832.816,00 €	1.399.875,84 €	7.232.691,84 €
4	Τμήμα 4 «Εξειδικευμένες λύσεις και υπηρεσίες ασφάλειας για την Ε.Δ.Υ.Τ.Ε. Α.Ε.»	3.579.625,00 €	859.110,00 €	4.438.735,00 €	4.725.105,00 €	1.134.025,20 €	5.859.130,20 €
Σύνολο		19.072.580,64 €	4.577.419,35 €	23.650.000,00 €	25.175.806,45 €	6.042.193,55 €	31.218.000,00 €

Προσφορές υποβάλλονται για ένα ή περισσότερα ή και όλα τα Τμήματα.
Η σύμβαση θα ανατεθεί με το κριτήριο της πλέον συμφέρουσας από οικονομική άποψη προσφοράς, βάσει της βέλτιστης σχέση ποιότητας – τιμής ανά τμήμα.

1.3.3 Διάρκεια συμφωνίας-πλαίσιο

Η διάρκεια της Συμφωνίας Πλαίσιο ορίζεται για **διάστημα τριάντα (30) μηνών** από την υπογραφή της σχετικής σύμβασης.

Οι εκτελεστικές συμβάσεις μπορούν να συνάπτονται έως και τη συμπλήρωση του χρόνου διάρκειας της συμφωνίας-πλαίσιο.

Αναλυτική περιγραφή του φυσικού και οικονομικού αντικειμένου της συμφωνίας-πλαίσιο δίδεται στο ΠΑΡΑΡΤΗΜΑ Ι της παρούσας διακήρυξης.

1.3.4 Κριτήριο Ανάθεσης

Η σύμβαση θα ανατεθεί με το κριτήριο της πλέον συμφέρουσας από οικονομική άποψη προσφοράς, βάσει της βέλτιστης σχέση ποιότητας – τιμής ανά τμήμα, όπως αναφέρεται στο άρθρο 2.3.1 της παρούσας.

1.4 Θεσμικό πλαίσιο

Η ανάθεση και εκτέλεση της συμφωνίας-πλαίσιο διέπεται από την κείμενη νομοθεσία και τις κατ' εξουσιοδότηση αυτής εκδοθείσες κανονιστικές πράξεις, όπως ισχύουν και ιδίως:

1. Τον Κανονισμό (ΕΕ) αριθ. 2021/241 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12ης Φεβρουαρίου 2021 για τη θέσπιση του μηχανισμού ανάκαμψης και ανθεκτικότητας (L 57/17).
2. Τον Κανονισμό (ΕΕ) αριθ. 2021/240 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 10ης Φεβρουαρίου 2021 για τη θέσπιση Μέσου Τεχνικής Υποστήριξης (L 57/1).
3. Τον Κανονισμό (ΕΕ, Ευρατόμ) αριθ. 2018/1046 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 18ης Ιουλίου 2018 σχετικά με τους δημοσιονομικούς κανόνες που εφαρμόζονται στον γενικό προϋπολογισμό της Ένωσης, την τροποποίηση των κανονισμών (ΕΕ) αριθ. 1296/2013, (ΕΕ) αριθ. 1301/2013, (ΕΕ) αριθ. 1303/2013, (ΕΕ) αριθ. 1304/2013, (ΕΕ) αριθ. 1309/2013, (ΕΕ) αριθ. 1316/2013, (ΕΕ) αριθ. 223/2014, (ΕΕ) αριθ. 283/2014 και της απόφασης αριθ. 541/2014/ΕΕ και για την κατάργηση του κανονισμού (ΕΕ, Ευρατόμ) αριθ. 966/2012 (L 193/1).
4. Την υπ' αριθμ. 2021/0159/17.06.2021 Πρόταση της Ευρωπαϊκής Επιτροπής για την Εκτελεστική Απόφαση του Συμβουλίου για την έγκριση της αξιολόγησης του Σχεδίου Ανάκαμψης και Ανθεκτικότητας της Ελλάδας (στο εξής το «Σ.Α.Α.»).
5. Την από 13 Ιουλίου 2021 εκτελεστική απόφαση του Συμβουλίου της Ευρωπαϊκής Ένωσης, για την έγκριση της αξιολόγησης του σχεδίου ανάκαμψης και ανθεκτικότητας για την Ελλάδα (ST 10152/21, ST 10152/21 ADD 1).
6. Τον Ν. 4772/2021 «Διενέργεια Γενικών Απογραφών έτους 2021 από την Ελληνική Στατιστική Αρχή, επείγουσες ρυθμίσεις για την αντιμετώπιση των επιπτώσεων της πανδημίας του κορωνοϊού COVID- 19, επείγουσες δημοσιονομικές και φορολογικές ρυθμίσεις και άλλες διατάξεις» (ΦΕΚ 17/Α/05-02-2021)
7. Τον Ν. 4820/2021 «Οργανικός Νόμος του Ελεγκτικού Συνεδρίου και άλλες ρυθμίσεις» (ΦΕΚ 130/Α/23-07-2021) και ιδίως το άρθρο 189 περί ορισμού της Επιτροπής Δημοσιονομικού Ελέγχου ως αρμόδιας για τον έλεγχο του Μηχανισμού Ανάκαμψης και Ανθεκτικότητας.
8. Τον Ν. 4822/2021 «Κύρωση της Σύμβασης Χρηματοδότησης μεταξύ της Ευρωπαϊκής Επιτροπής και της Ελληνικής Δημοκρατίας, της Δανειακής Σύμβασης μεταξύ της Ευρωπαϊκής Επιτροπής και της Ελληνικής Δημοκρατίας και των Παραρτημάτων τους και άλλες διατάξεις για το Ταμείο Ανάκαμψης και Ανθεκτικότητας» (ΦΕΚ 135/Α/02-08-2021).
9. Τα Α. 270 έως και Α.281 του Ν. 4738/2020 «Ρύθμιση οφειλών και παροχή δεύτερης ευκαιρίας και άλλες διατάξεις» (ΦΕΚ 207/Α/27-10-2020) και ιδίως το Α.272 για την σύσταση στο Υπουργείο Οικονομικών της αυτοτελούς Ειδικής Υπηρεσίας Συντονισμού Ταμείου Ανάκαμψης.
10. Τον Ν. 4413/2016 «Ανάθεση και εκτέλεση συμβάσεων παραχώρησης Εναρμόνιση με την Οδηγία 2014/23/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 26ης Φεβρουαρίου 2014 σχετικά με την ανάθεση συμβάσεων παραχώρησης (ΕΕ L 94/1/28.3.2014) και άλλες διατάξεις» (ΦΕΚ 148/Α/08-08-2016).

11. Τον Ν. 3389/2005 «Συμπράξεις Δημόσιου και Ιδιωτικού Τομέα» (ΦΕΚ 232/Α/ 22-09-2005).
12. Την υπ' αρ. 134453/23-12-2015 κοινή απόφαση των Υπουργών Οικονομίας, Ανάπτυξης και Τουρισμού και Οικονομικών «Ρυθμίσεις για τις πληρωμές των δαπανών του Προγράμματος Δημοσίων Επενδύσεων - ΠΔΕ» (ΦΕΚ 2857/Β/28-12-2015), όπως εκάστοτε ισχύει.
13. Την υπ' αρ. 35259/24-03-2021 κοινή απόφαση των Υπουργών Οικονομικών και Ανάπτυξης και Επενδύσεων «Σύσταση και Λειτουργία Λογαριασμού για την εθνική χρηματοδότηση των έργων του Ταμείου Ανάκαμψης και Ανθεκτικότητας της Ευρωπαϊκής Ένωσης» (ΦΕΚ 1197/Β/29-03-2021).
14. Την υπ' αριθμ. 119126 ΕΞ 2021/28-09-2021 (ΦΕΚ 4498/Β/29-09-2021) απόφαση του Αναπληρωτή Υπουργού Οικονομικών περί καθορισμού του Συστήματος Διαχείρισης και Ελέγχου των Δράσεων και των Έργων του Ταμείου Ανάκαμψης και Ανθεκτικότητας.
15. Την υπ' αριθμ. 119138 ΕΞ 2021/29-09-2021 (ΦΕΚ 4499/Β/30-09-2021), με θέμα «Συμπλήρωση και εξειδίκευση των Αρμοδιοτήτων της Ειδικής Υπηρεσίας Συντονισμού Ταμείου Ανάκαμψης του Υπουργείου Οικονομικών».
16. Το εγκεκριμένο Εγχειρίδιο Διαδικασιών του Ταμείου Ανάκαμψης και Ανθεκτικότητας.
17. Τον Ν. 4412/2016 «Δημόσιες Συμβάσεις Έργων, Προμηθειών και Υπηρεσιών (προσαρμογή στις Οδηγίες 2014/24/ΕΕ και 2014/25/ΕΕ)» (ΦΕΚ 147/Α/08-08-2016), όπως τροποποιήθηκε και ισχύει δυνάμει των διατάξεων του Ν. 4782/2021 (ΦΕΚ 36/Β/09-03-2021).
18. Τον Ν. 4727/2020 «Ψηφιακή Διακυβέρνηση (Ενσωμάτωση στην Ελληνική Νομοθεσία της Οδηγίας (ΕΕ) 2016/2102 και της Οδηγίας (ΕΕ) 2019/1024) - Ηλεκτρονικές Επικοινωνίες (Ενσωμάτωση στο Ελληνικό Δίκαιο της Οδηγίας (ΕΕ) 2018/1972) και άλλες διατάξεις» (ΦΕΚ 184/Α/23-09-2020).
19. Τον Ν. 4700/2020 «Ενιαίο κείμενο Δικονομίας για το Ελεγκτικό Συνέδριο, ολοκληρωμένο νομοθετικό πλαίσιο για τον προσυμβατικό έλεγχο, τροποποιήσεις στον Κώδικα Νόμων για το Ελεγκτικό Συνέδριο, διατάξεις για την αποτελεσματική απονομή της δικαιοσύνης και άλλες διατάξεις» (ΦΕΚ 127/Α/29-06-2020).
20. Τον Ν. 4635/2019 «Επενδύω στην Ελλάδα και άλλες διατάξεις» (ΦΕΚ 167/Α/30-10-2019).
21. Τον Ν. 4270/2014 «Αρχές δημοσιονομικής διαχείρισης και εποπτείας (ενσωμάτωση της Οδηγίας 2011/85/ΕΕ) - δημόσιο λογιστικό και άλλες διατάξεις» και ειδικότερα το υποκεφάλαιο 3 - Προϋπολογισμός Δημοσίων Επενδύσεων - Ανακατανομές πιστώσεων έργων, Ανάλυση υποχρεώσεων, Εκτέλεση προϋπολογισμού (ΦΕΚ 143/Α/28-06-2014).
22. Τον Ν. 4152/2013 «Επείγοντα μέτρα εφαρμογής των νόμων 4046/2012, 4093/2012 και 4127/2013» (ΦΕΚ 107/Α/09-05-2013).
23. Το Π.Δ. 80/2016 «Ανάληψη υποχρεώσεων από τους Διατάκτες» (ΦΕΚ 145/Α/05-08-2016).
24. Τον Ν. 4013/2011 «Σύσταση ενιαίας Ανεξάρτητης Αρχής Δημοσίων Συμβάσεων και Κεντρικού Ηλεκτρονικού Μητρώου Δημοσίων Συμβάσεων - Αντικατάσταση του έκτου κεφαλαίου του Ν. 3588/2007 (πτωχευτικός κώδικας) - Προπτωχευτική διαδικασία εξυγίανσης και άλλες διατάξεις» (ΦΕΚ 204/Α/15-09-2011).

25. Τον Ν. 3213/2003 "Δήλωση και έλεγχος περιουσιακής κατάστασης βουλευτών, δημόσιων λειτουργών και υπαλλήλων, ιδιοκτητών μέσων μαζικής ενημέρωσης και άλλων κατηγοριών προσώπων." (ΦΕΚ 309/Α/31-12-2003), όπως τούτος τροποποιήθηκε και ισχύει.
26. Τον Ν. 2121/1993 "Πνευματική Ιδιοκτησία, Συγγενικά Δικαιώματα και Πολιτιστικά Θέματα", (ΦΕΚ 25/Α/04-03-1993), όπως τούτος τροποποιήθηκε και ισχύει δυνάμει των διατάξεων του Ν. 4481/2017 (ΦΕΚ 100/Α/2017).
27. Τον Ν. 3310/2005 «Μέτρα για τη διασφάλιση της διαφάνειας και την αποτροπή καταστρατηγήσεων κατά τη διαδικασία σύναψης δημοσίων συμβάσεων» (ΦΕΚ 30/Α/14-02-2005) σε συνδυασμό με την υπ' αρ. 1108437/2565/ΔΟΣ/15.11.2005 απόφαση του Υφυπουργού Οικονομίας και Οικονομικών «Καθορισμός χωρών στις οποίες λειτουργούν εξωχώριες εταιρίες» (1590/Β/16-11-2005).
28. Το Α.88 του Ν. 1892/1990 «Για τον εκσυγχρονισμό και την ανάπτυξη και άλλες διατάξεις» (ΦΕΚ 101/Α/31-07-1990).
29. Την υπ' αρ. 20977 Κοινή Απόφαση των Υπουργών Ανάπτυξης και Επικρατείας «Δικαιολογητικά για την τήρηση των μητρώων του Ν.3310/2005, όπως τροποποιήθηκε με το Ν. 3414/2005» (ΦΕΚ 1673/Β/23-08-2007).
30. Τον Κανονισμό (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (L 119).
31. Τον Ν. 4624/2019 «Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις» (ΦΕΚ 137/Α/29-08-2019).
32. Τη με αριθμό 3/2018 Γνωμοδότηση του Νομικού Συμβουλίου του Κράτους.
33. Το από 13-07-2018 έντυπο της ΕΑΔΔΗΣΥ με θέμα: «ΥΠΟΧΡΕΩΣΕΙΣ ΔΗΜΟΣΙΕΥΣΕΩΝ ΣΤΟΝ ΕΘΝΙΚΟ ΤΥΠΟ ΚΑΤΑ ΤΟΝ Ν.4412/2016».
34. Τη με αριθμό 76928/13-07-2021 (ΦΕΚ 3075/Β/13-07-2021) με θέμα: «Ρύθμιση ειδικότερων θεμάτων λειτουργίας και διαχείρισης του Κεντρικού Ηλεκτρονικού Μητρώου Δημοσίων Συμβάσεων (ΚΗΜΔΗΣ).»
35. Την με αρ. 64233/08.06.2021 (Β' 2453/ 09.06.2021) Κοινή Υπουργική Απόφαση «Ρυθμίσεις τεχνικών ζητημάτων που αφορούν την ανάθεση και εκτέλεση των Δημοσίων Συμβάσεων Προμηθειών και Υπηρεσιών με χρήση των επιμέρους εργαλείων και διαδικασιών του Εθνικού Συστήματος Ηλεκτρονικών Δημοσίων Συμβάσεων (ΕΣΗΔΗΣ)».
36. Τον Ν. 3429/2005 «Δημόσιες Επιχειρήσεις και Οργανισμοί (Δ.Ε.Κ.Ο.).» ΦΕΚ (314/Α/27-12-2005), όπως τροποποιήθηκε από Α.31, Κεφ. Β, Ν. 4465/2017 (ΦΕΚ 47/Α/04-04-2017) και «Αριθ.

30422/ΕΓΔΕΚΟ 342 «Εξαίρεση από το πεδίο εφαρμογής του άρθρου 3 του ν. 3429/2005 της Ανώνυμης Εταιρείας «Κοινωνία της Πληροφορίας Α.Ε.» ΦΕΚ (967/Β/21-07-2006).

37. Το Α.24 του Ν. 2860/2000 «Διαχείριση, παρακολούθηση και έλεγχος του κοινοτικού πλαισίου στήριξης και άλλες διατάξεις» (ΦΕΚ 251/Α/14-11-2000), όπως τροποποιήθηκε με το Α.32 του Ν. 3614/2007 «Διαχείριση, έλεγχος και εφαρμογή αναπτυξιακών παρεμβάσεων για την προγραμματική περίοδο 2007 - 2013» (ΦΕΚ 267/Α/03-12-2007), συμπληρώθηκε με το Α.59, παρ. 17 του Ν. 4314/2014 «Α) Για τη διαχείριση, τον έλεγχο και την εφαρμογή αναπτυξιακών παρεμβάσεων για την προγραμματική περίοδο 2014 - 2020, Β) Ενσωμάτωση της Οδηγίας 2012/17 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 13ης Ιουνίου 2012 (ΕΕ L 156/16.6.2012) στο ελληνικό δίκαιο, τροποποίηση του ν. 3419/2005 (Α 297) και άλλες διατάξεις» (ΦΕΚ 265/Α/23-12-2014) και ισχύει.
38. Το Α.1, παρ. 2.1 του ΠΔ 81 "Σύσταση, συγχώνευση, μετονομασία και κατάργηση Υπουργείων και καθορισμός των αρμοδιοτήτων τους - Μεταφορά υπηρεσιών και αρμοδιοτήτων μεταξύ Υπουργείων." (ΦΕΚ 119/Α/08-07-2019).
39. Το Α.39 του Ν. 4578/2018 «Μείωση ασφαλιστικών εισφορών και άλλες διατάξεις» (ΦΕΚ 200/Α/03-12-2018).
40. Το Καταστατικό της μονοπρόσωπης ανώνυμης εταιρείας με την επωνυμία "Κοινωνία της Πληροφορίας Μονοπρόσωπη Α.Ε.", όπως δημοσιεύτηκε στο Γ.Ε.ΜΗ. στις 14-10-2021 και εγκρίθηκε με την υπ' αρ. 38427 ΕΞ 2021 Απόφαση του Υπουργού Επικρατείας «Τροποποίηση του καταστατικού της ανώνυμης εταιρείας "Κοινωνία της Πληροφορίας Μ.Α.Ε." και κωδικοποίηση αυτού» (ΦΕΚ 5111/Β/04-11-2021).
41. Τον Κανονισμό της μονοπρόσωπης ανώνυμης εταιρείας "Κοινωνία της Πληροφορίας Μονοπρόσωπη Α.Ε.", ο οποίος εγκρίθηκε με την υπ' αρ. 43345 ΕΞ 2021 Απόφαση του Υπουργού Επικρατείας «Έγκριση του Κανονισμού της Ανώνυμης Εταιρείας «Κοινωνία της Πληροφορίας Μονοπρόσωπη Α.Ε.», με κατάργηση της υπό στοιχεία 13845 ΕΞ 2021/12.05.2021 υπουργικής απόφασης με θέμα: «Έγκριση του Κανονισμού της Ανώνυμης Εταιρείας «Κοινωνία της Πληροφορίας Μονοπρόσωπη Α.Ε.», με κατάργηση της υπό στοιχεία 252/ΓΔΟΔΥ/ΔΔΥ/2020/22-1-2020 υπουργικής απόφασης «Έγκριση του Κανονισμού της Ανώνυμης Εταιρείας «Κοινωνία της Πληροφορίας Α.Ε.», με κατάργηση της υπό στοιχεία ΔΙΑΚ/ΚτΠ/οικ. 21588/04-11-2011 (Β' 2541) υπουργικής απόφασης «Κανονισμός της Ανώνυμης Εταιρείας "Κοινωνία της Πληροφορίας Α.Ε."», όπως τροποποιήθηκε με την υπό στοιχεία ΔΙΑΚ/οικ 35181/11-11-2015 (Β' 2532) κοινή υπουργική απόφαση «Τροποποίηση άρθρων του Κανονισμού της Ανώνυμης Εταιρείας "Κοινωνία της Πληροφορίας Α.Ε."» (Β' 164)» ΦΕΚ 2060/Β'/2021))» (ΦΕΚ 5807/Β/10-12-2021).
42. Την υπ' αρ. 13216 ΕΞ 2021 Απόφαση του Υπουργού Επικρατείας «Τροποποίηση της υπ' αρ. 146/25.07.2019 απόφασης του Υπουργού Επικρατείας «Ορισμός του Προέδρου και των Μελών του Διοικητικού Συμβουλίου της Ανώνυμης Εταιρείας «Κοινωνία της Πληροφορίας Α.Ε.» (Υ.Ο.Δ.Δ. 474), όπως τροποποιήθηκε με τις υπό στοιχεία 90/13.01.2020 (Υ.Ο.Δ.Δ. 60) και 32273/16.11.2020 (Υ.Ο.Δ.Δ. 977) όμοιες.» (ΦΕΚ 376/ΥΟΔΔ/14-05-2021).
43. Την Απόφαση του ΔΣ της ΚτΠ Μ.Α.Ε. κατά την υπ' αρ. 688/30-07-2019 Συνεδρίασή του, με θέμα Εκλογή Διευθύνοντος Συμβούλου (Θέμα 1).

44. Την Απόφαση του Διευθύνοντος Συμβούλου της ΚτΠ Μ.Α.Ε. με Αρ. Πρωτ. 22683/20-12-2022 και θέμα «Εξουσιοδοτήσεις προς τους Γενικούς Διευθυντές και Διευθυντές».
45. Τη ΣΑΤΑ ΤΑΧΧΧΧΧ με ενάριθμο κωδικό 2022ΤΑΧΧΧΧΧΧ του Υπουργείου Ψηφιακής Διακυβέρνησης, με την οποία εγκρίθηκε η ένταξη του έργου στο Πρόγραμμα Δημοσίων Επενδύσεων (ΠΔΕ).
46. Την από ΧΧ-ΧΧ-2022 έως ΧΧ-ΧΧ-2022 διαβούλευση και τα αποτελέσματα αυτής.
47. Την από 07-09-2022 (Α.Π. ΚτΠ Μ.Α.Ε.: 17345/04-10-2022) Προγραμματική Συμφωνία μεταξύ του Υπουργείου Ψηφιακής Διακυβέρνησης και της Κοινωνίας της Πληροφορίας Μ.Α.Ε. (ΚτΠ Μ.Α.Ε.), για το Έργο «Ενίσχυση της Επιχειρησιακής Συνέχειας του Δημοσίου Τομέα στο Πλαίσιο του Εθνικού Σχεδίου Ανάκαμψης και Ανθεκτικότητας».
48. Το υπ' αρ. πρωτ. ΧΧΧΧΧΧ 2022/ΧΧ-ΧΧ-2022 (αρ. πρωτ. ΚτΠ Μ.Α.Ε. ΧΧΧΧΧ/ΧΧ-ΧΧ-2022) έγγραφο της Ειδικής Υπηρεσίας Συντονισμού Ταμείου Ανάκαμψης (ΕΥΣΤΑ) με θέμα: "Έγκριση διακήρυξης για την ανάθεση της σύμβασης «» του έργου «» της Δράσης « - ID » (Κωδικός ΟΠΣ ΤΑ ΧΧΧΧΧΧΧΧΧΧΧΧΧΧ)".
49. Την Απόφαση του Διοικητικού Συμβουλίου της ΚτΠ Μ.Α.Ε. κατά την υπ' αρ. ΧΧΧΧ/ΧΧ-ΧΧ-2022 Συνεδρίασή του (Θέμα ΧΧΧΧΧΧ).
- 50.

1.5 Προθεσμία παραλαβής προσφορών και διενέργεια διαγωνισμού

Η καταληκτική ημερομηνία παραλαβής των προσφορών είναι η **ΧΧ-ΧΧ-2022** και ώρα **14:00** και η Ημερομηνία έναρξης υποβολής προσφορών είναι η **ΧΧ-ΧΧ-2022**.

Η διαδικασία θα διενεργηθεί με χρήση της πλατφόρμας του Εθνικού Συστήματος Ηλεκτρονικών Δημοσίων Συμβάσεων (Ε.Σ.Η.Δ.Η.Σ.), μέσω της Διαδικτυακής πύλης www.promitheus.gov.gr του ως άνω συστήματος, **την ΧΧ-ΧΧ-2022** και ώρα **14:00**.

1.6 Δημοσιότητα

A. Δημοσίευση στην Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης

Προκήρυξη της παρούσας σύμβασης απεστάλη με ηλεκτρονικά μέσα για δημοσίευση στις **ΧΧ-ΧΧ-2022** στην Υπηρεσία Εκδόσεων της Ευρωπαϊκής Ένωσης και δημοσιεύτηκε στις **ΧΧ-ΧΧ-2022**.

B. Δημοσίευση σε εθνικό επίπεδο

Η προκήρυξη και το πλήρες κείμενο της παρούσας Διακήρυξης καταχωρήθηκε στο Κεντρικό Ηλεκτρονικό Μητρώο Δημοσίων Συμβάσεων (ΚΗΜΔΗΣ) στις **ΧΧ-ΧΧ-2022**.

Το πλήρες κείμενο της παρούσας Διακήρυξης καταχωρήθηκε ακόμη και στη διαδικτυακή πύλη του Ε.Σ.Η.Δ.Η.Σ <http://www.promitheus.gov.gr>, όπου έλαβε τους εξής Συστημικούς Αριθμούς:

Τμήμα 1	α/α ΕΣΗΔΗΣ:
Τμήμα 2	α/α ΕΣΗΔΗΣ:
Τμήμα 3	α/α ΕΣΗΔΗΣ:
Τμήμα 4	α/α ΕΣΗΔΗΣ:

Περίληψη της παρούσας Διακήρυξης όπως προβλέπεται στην περίπτωση (ιστ) της παραγράφου 3 του άρθρου 76 του Ν.4727/23-09-2020 (ΦΕΚ/Α/184/23.09.2020), αναρτήθηκε στο διαδίκτυο, στον ιστότοπο <http://et.dianveia.gov.gr/> (ΠΡΟΓΡΑΜΜΑ ΔΙΑΥΓΕΙΑ) στις **XX-XX-2022**.

Η Διακήρυξη θα αναρτηθεί στο διαδίκτυο, στην ιστοσελίδα της αναθέτουσας αρχής, στη διεύθυνση (URL) :<http://www.ktpae.gr> στη θέση Διαγωνισμοί στις **XX-XX-2022**.

1.7 Αρχές εφαρμοζόμενες στη διαδικασία σύναψης

Οι οικονομικοί φορείς δεσμεύονται ότι:

α) τηρούν και θα εξακολουθήσουν να τηρούν κατά την εκτέλεση της συμφωνίας-πλαίσιο και των εκτελεστικών συμβάσεων, εφόσον επιλεγούν, τις υποχρεώσεις τους που απορρέουν από τις διατάξεις της περιβαλλοντικής, κοινωνικοασφαλιστικής και εργατικής νομοθεσίας, που έχουν θεσπιστεί με το δίκαιο της Ένωσης, το εθνικό δίκαιο, συλλογικές συμβάσεις ή διεθνείς διατάξεις περιβαλλοντικού, κοινωνικού και εργατικού δικαίου, οι οποίες απαριθμούνται στο Παράρτημα Χ του Προσαρτήματος Α του ν. 4412/2016. Η τήρηση των εν λόγω υποχρεώσεων ελέγχεται και βεβαιώνεται από τα όργανα που επιβλέπουν την εκτέλεση των δημοσίων συμβάσεων και τις αρμόδιες δημόσιες αρχές και υπηρεσίες που ενεργούν εντός των ορίων της ευθύνης και της αρμοδιότητάς τους

β) δεν θα ενεργήσουν αθέμιτα, παράνομα ή καταχρηστικά καθ' όλη τη διάρκεια της διαδικασίας ανάθεσης, αλλά και κατά το στάδιο εκτέλεσης της συμφωνίας-πλαίσιο και των εκτελεστικών συμβάσεων, εφόσον επιλεγούν

γ) λαμβάνουν τα κατάλληλα μέτρα για να διαφυλάξουν την εμπιστευτικότητα των πληροφοριών που έχουν χαρακτηριστεί ως τέτοιες.

2 ΓΕΝΙΚΟΙ ΚΑΙ ΕΙΔΙΚΟΙ ΟΡΟΙ ΣΥΜΜΕΤΟΧΗΣ

2.1 Γενικές Πληροφορίες

2.1.1 Έγγραφα της σύμβασης

Τα έγγραφα της παρούσας διαδικασίας σύναψης είναι τα ακόλουθα:

- η από **XX-XX-2022** Προκήρυξη της Σύμβασης, όπως αυτή έχει σταλεί για δημοσίευση στην Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης
- η παρούσα Διακήρυξη με τα Παραρτήματα που αποτελούν αναπόσπαστο μέρος αυτής
- το Ευρωπαϊκό Ενιαίο Έγγραφο Σύμβασης [ΕΕΕΣ]
- οι συμπληρωματικές πληροφορίες που τυχόν παρέχονται στο πλαίσιο της διαδικασίας, ιδίως σχετικά με τις προδιαγραφές και τα σχετικά δικαιολογητικά

2.1.2 Επικοινωνία – Πρόσβαση στα έγγραφα της Σύμβασης

Όλες οι επικοινωνίες σε σχέση με τα βασικά στοιχεία της διαδικασίας σύναψης της συμφωνίας-πλαίσιο, και των εκτελεστικών συμβάσεων αυτής, καθώς και όλες οι ανταλλαγές πληροφοριών, ιδίως η ηλεκτρονική υποβολή, εκτελούνται με τη χρήση της πλατφόρμας του Εθνικού Συστήματος Ηλεκτρονικών Δημοσίων Συμβάσεων (ΕΣΗΔΗΣ), η οποία είναι προσβάσιμη μέσω της Διαδικτυακής πύλης (www.promitheus.gov.gr).

2.1.3 Παροχή Διευκρινίσεων

Τα σχετικά αιτήματα παροχής διευκρινίσεων υποβάλλονται ηλεκτρονικά, το αργότερο το αργότερο δέκα τρεις (13) ημέρες πριν την καταληκτική ημερομηνία υποβολής των προσφορών και απαντώνται αντίστοιχα στο πλαίσιο της παρούσας, στη σχετική ηλεκτρονική διαδικασία σύναψης δημόσιας σύμβασης στην πλατφόρμα του ΕΣΗΔΗΣ, η οποία είναι προσβάσιμη μέσω της Διαδικτυακής πύλης www.promitheus.gov.gr. Αιτήματα παροχής συμπληρωματικών πληροφοριών – διευκρινίσεων υποβάλλονται από εγγεγραμμένους στο σύστημα οικονομικούς φορείς, δηλαδή από εκείνους που διαθέτουν σχετικά διαπιστευτήρια που τους έχουν χορηγηθεί (όνομα χρήστη και κωδικός πρόσβασης) και απαραίτητα το ηλεκτρονικό αρχείο με το κείμενο των ερωτημάτων είναι ηλεκτρονικά υπογεγραμμένο. Αιτήματα παροχής διευκρινίσεων που υποβάλλονται είτε με άλλο τρόπο είτε το ηλεκτρονικό αρχείο που τα συνοδεύει δεν είναι ηλεκτρονικά υπογεγραμμένο, δεν εξετάζονται.

Η αναθέτουσα αρχή μπορεί να παρατείνει την προθεσμία παραλαβής των προσφορών, ούτως ώστε όλοι οι ενδιαφερόμενοι οικονομικοί φορείς να μπορούν να λάβουν γνώση όλων των αναγκαίων πληροφοριών για την κατάρτιση των προσφορών στις ακόλουθες περιπτώσεις:

α) όταν, για οποιονδήποτε λόγο, πρόσθετες πληροφορίες, αν και ζητήθηκαν από τον οικονομικό φορέα έγκαιρα, δεν έχουν παρασχεθεί το αργότερο **έξι (6) ημέρες** πριν από την προθεσμία που ορίζεται για την παραλαβή των προσφορών,

β) όταν τα έγγραφα της σύμβασης υφίστανται σημαντικές αλλαγές.

Η διάρκεια της παράτασης θα είναι ανάλογη με τη σπουδαιότητα των πληροφοριών που ζητήθηκαν ή των αλλαγών.

Όταν οι πρόσθετες πληροφορίες δεν έχουν ζητηθεί έγκαιρα ή δεν έχουν σημασία για την προετοιμασία κατάλληλων προσφορών, η παράταση της προθεσμίας εναπόκειται στη διακριτική ευχέρεια της αναθέτουσας αρχής.

Τροποποίηση των όρων της διαγωνιστικής διαδικασίας (πχ αλλαγή/μετάθεση της καταληκτικής ημερομηνίας υποβολής προσφορών καθώς και σημαντικές αλλαγές των εγγράφων της σύμβασης, σύμφωνα με την προηγούμενη παράγραφο) δημοσιεύεται στην ΕΕΕΕ (με το τυποποιημένο έντυπο «Διορθωτικό») και στο ΚΗΜΔΗΣ.

2.1.4 Γλώσσα

Τα έγγραφα της σύμβασης έχουν συνταχθεί στην ελληνική γλώσσα.

Τυχόν προδικαστικές προσφυγές υποβάλλονται στην ελληνική γλώσσα.

Οι προσφορές, τα στοιχεία που περιλαμβάνονται σε αυτές, καθώς και τα αποδεικτικά έγγραφα σχετικά με τη μη ύπαρξη λόγου αποκλεισμού και την πλήρωση των κριτηρίων ποιοτικής επιλογής¹ συντάσσονται στην ελληνική γλώσσα ή συνοδεύονται από επίσημη μετάφρασή τους στην ελληνική γλώσσα.

Τα αλλοδαπά δημόσια και ιδιωτικά έγγραφα συνοδεύονται από μετάφρασή τους στην ελληνική γλώσσα, επικυρωμένη είτε από πρόσωπο αρμόδιο κατά τις κείμενες διατάξεις της εθνικής νομοθεσίας είτε από πρόσωπο κατά νόμο αρμόδιο της χώρας στην οποία έχει συνταχθεί το έγγραφο.

Ενημερωτικά και τεχνικά φυλλάδια και άλλα έντυπα -εταιρικά ή μη- με ειδικό τεχνικό περιεχόμενο μπορούν να υποβάλλονται στην Αγγλική γλώσσα, χωρίς να συνοδεύονται από μετάφραση στην ελληνική.

Κάθε μορφής επικοινωνία με την αναθέτουσα αρχή, καθώς και μεταξύ αυτής και του αναδόχου, θα γίνονται υποχρεωτικά στην ελληνική γλώσσα.

2.1.5 Εγγυήσεις

Οι εγγυητικές επιστολές των παραγράφων 2.2.2 και 4.1 της παρούσας εκδίδονται από πιστωτικά ή χρηματοδοτικά ιδρύματα ή ασφαλιστικές επιχειρήσεις κατά την έννοια των περιπτώσεων β' και γ' της παρ. 1 του άρθρου 14 του ν. 4364/ 2016 (Α' 13)» που λειτουργούν νόμιμα στα κράτη - μέλη της Ένωσης ή του Ευρωπαϊκού Οικονομικού Χώρου ή στα κράτη-μέλη της ΣΔΣ και έχουν, σύμφωνα με τις ισχύουσες διατάξεις, το δικαίωμα αυτό. Μπορούν, επίσης, να εκδίδονται από το Τ.Μ.Ε.Δ.Ε. ή να παρέχονται με γραμμάτιο του Ταμείου Παρακαταθηκών και Δανείων με παρακατάθεση σε αυτό του αντίστοιχου χρηματικού ποσού. Αν συσταθεί παρακαταθήκη με γραμμάτιο παρακατάθεσης χρεογράφων στο Ταμείο Παρακαταθηκών και Δανείων, τα τοκομερίδια ή μερίσματα που λήγουν κατά τη διάρκεια της εγγύησης επιστρέφονται μετά τη λήξη τους στον υπέρ ου η εγγύηση οικονομικό φορέα.

¹Πρβλ. άρθρο 80 παρ. 10 ν. 4412/2016

Οι εγγυητικές επιστολές εκδίδονται κατ' επιλογή των οικονομικών φορέων από έναν ή περισσότερους εκδότες της παραπάνω παραγράφου.

Οι εγγυήσεις αυτές περιλαμβάνουν κατ' ελάχιστον τα ακόλουθα στοιχεία: α) την ημερομηνία έκδοσης, β) τον εκδότη, γ) την αναθέτουσα αρχή προς την οποία απευθύνονται, δ) τον αριθμό της εγγύησης, ε) το ποσό που καλύπτει η εγγύηση, στ) την πλήρη επωνυμία, τον Α.Φ.Μ. και τη διεύθυνση του οικονομικού φορέα υπέρ του οποίου εκδίδεται η εγγύηση (στην περίπτωση ένωσης αναγράφονται όλα τα παραπάνω για κάθε μέλος της ένωσης), ζ) τους όρους ότι: αα) η εγγύηση παρέχεται ανέκκλητα και ανεπιφύλακτα, ο δε εκδότης παραιτείται του δικαιώματος της διαιρέσεως και της διζήσεως, και ββ) ότι σε περίπτωση κατάρπτωσης αυτής, το ποσό της κατάρπτωσης υπόκειται στο εκάστοτε ισχύον τέλος χαρτοσήμου, η) τα στοιχεία της σχετικής διακήρυξης και την καταληκτική ημερομηνία διενέργειας του διαγωνισμού, θ) την ημερομηνία λήξης ή τον χρόνο ισχύος της εγγύησης, ι) την ανάληψη υποχρέωσης από τον εκδότη της εγγύησης να καταβάλει το ποσό της εγγύησης ολικά ή μερικά εντός πέντε (5) ημερών μετά από απλή έγγραφη ειδοποίηση εκείνου προς τον οποίο απευθύνεται και ια) στην περίπτωση των εγγυήσεων καλής εκτέλεσης και προκαταβολής, τον αριθμό και τον τίτλο της σχετικής σύμβασης.

Η περ. αα' του προηγούμενου εδαφίου ζ' δεν εφαρμόζεται για τις εγγυήσεις που παρέχονται με γραμμάτιο του Ταμείου Παρακαταθηκών και Δανείων.

Οι εγγυητικές επιστολές συντάσσονται σύμφωνα με τα υποδείγματα του Παραρτήματος VIII της παρούσας.

Επισημαίνεται ότι εγγυήσεις που εκδίδονται από το Τ.Μ.Ε.Δ.Ε και το Ταμείο Παρακαταθηκών και Δανείων δεν συμμορφώνονται με τα υποδείγματα των εγγυητικών επιστολών της παρούσας αλλά εκδίδονται σύμφωνα με τις οικείες διατάξεις που διέπουν τους εν λόγω φορείς.

Η αναθέτουσα αρχή επικοινωνεί με τους εκδότες των εγγυητικών επιστολών προκειμένου να διαπιστώσει την εγκυρότητά τους.

2.1.6 Προστασία Προσωπικών Δεδομένων

Η αναθέτουσα αρχή ενημερώνει το φυσικό πρόσωπο που υπογράφει την προσφορά ως Προσφέρων ή ως Νόμιμος Εκπρόσωπος Προσφέροντος, ότι η ίδια ή και τρίτοι, κατ' εντολή και για λογαριασμό της, θα επεξεργάζονται προσωπικά δεδομένα που περιέχονται στους φακέλους της προσφοράς και τα αποδεικτικά μέσα τα οποία υποβάλλονται σε αυτήν, στο πλαίσιο του παρόντος Διαγωνισμού, για το σκοπό της αξιολόγησης των προσφορών και της ενημέρωσης έτερων συμμετεχόντων σε αυτόν, λαμβάνοντας κάθε εύλογο μέτρο για τη διασφάλιση του απόρρητου και της ασφάλειας της επεξεργασίας των δεδομένων και της προστασίας τους από κάθε μορφής αθέμιτη επεξεργασία, σύμφωνα με τις διατάξεις της κείμενης νομοθεσίας περί προστασίας προσωπικών δεδομένων, κατά τα αναλυτικώς αναφερόμενα στην αναλυτική ενημέρωση που επισυνάπτεται στο **π α ρ ᾶ ρ τ η μ α Ι Χ** στην παρούσα.

2.2 Δικαίωμα Συμμετοχής - Κριτήρια Ποιοτικής Επιλογής

2.2.1 Δικαιούμενοι συμμετοχής

1. Δικαίωμα συμμετοχής στη διαδικασία σύναψης της παρούσας σύμβασης έχουν φυσικά ή νομικά πρόσωπα και, σε περίπτωση ενώσεων οικονομικών φορέων, τα μέλη αυτών, που είναι εγκατεστημένα σε:

α) κράτος-μέλος της Ένωσης,

β) κράτος-μέλος του Ευρωπαϊκού Οικονομικού Χώρου (Ε.Ο.Χ.),

γ) τρίτες χώρες που έχουν υπογράψει και κυρώσει τη ΣΔΣ, στο βαθμό που η υπό ανάθεση δημόσια σύμβαση καλύπτεται από τα Παραρτήματα 1, 2, 4, 5, 6 και 7 και τις γενικές σημειώσεις του σχετικού με την Ένωση Προσαρτήματος Ι της ως άνω Συμφωνίας, καθώς και

δ) σε τρίτες χώρες που δεν εμπίπτουν στην περίπτωση γ' της παρούσας παραγράφου και έχουν συνάψει διμερείς ή πολυμερείς συμφωνίες με την Ένωση σε θέματα διαδικασιών ανάθεσης δημοσίων συμβάσεων.

Στο βαθμό που καλύπτονται από τα Παραρτήματα 1, 2, 4, 5, 6 και 7 και τις γενικές σημειώσεις του σχετικού με την Ένωση Προσαρτήματος Ι της ΣΔΣ, καθώς και τις λοιπές διεθνείς συμφωνίες από τις οποίες δεσμεύεται η Ένωση, οι αναθέτουσες αρχές επιφυλάσσουν για τα έργα, τα αγαθά, τις υπηρεσίες και τους οικονομικούς φορείς των χωρών που έχουν υπογράψει τις εν λόγω συμφωνίες μεταχείριση εξίσου ευνοϊκή με αυτήν που επιφυλάσσουν για τα έργα, τα αγαθά, τις υπηρεσίες και τους οικονομικούς φορείς της Ένωσης

2. Απαγορεύεται η συμμετοχή στην διαδικασία σύναψης της παρούσας συμφωνίας-πλαίσιο οικονομικών φορέων, με οποιονδήποτε τρόπο, εφόσον εμπίπτουν στις απαγορεύσεις του Κανονισμού (ΕΕ) 2022/576 για την τροποποίηση του Κανονισμού (ΕΕ) αριθ. 833/2014 σχετικά με περιοριστικά μέτρα λόγω ενεργειών της Ρωσίας που αποσταθεροποιούν την κατάσταση στην Ουκρανία (L 111/1) και συγκεκριμένα αν ο οικονομικός φορέας είναι : α) Ρώσος υπήκοος ή φυσικό ή νομικό πρόσωπο, οντότητα ή φορέας που έχει την έδρα του στη Ρωσία, ή β) νομικό πρόσωπο, οντότητα ή φορέας του οποίου τα δικαιώματα ιδιοκτησίας κατέχει άμεσα ή έμμεσα σε ποσοστό άνω του 50 % οντότητα αναφερόμενη στο στοιχείο α) της παρούσας παραγράφου ή γ) φυσικό ή νομικό πρόσωπο, οντότητα ή φορέας που ενεργεί εξ ονόματος ή κατ' εντολή οντότητας αναφερόμενης στο στοιχείο α) ή β) της παρούσας παραγράφου, συμπεριλαμβανομένων, όταν αντιστοιχούν σε περισσότερο από το 10 % της αξίας της σύμβασης, των υπεργολάβων, προμηθευτών ή οντοτήτων στις ικανότητες των οποίων στηρίζεται κατά την έννοια της οδηγίας 2014/24 και του ν. 4412/2016.

3. Οικονομικός φορέας συμμετέχει είτε μεμονωμένα είτε ως μέλος ένωσης. Οι ενώσεις οικονομικών φορέων, συμπεριλαμβανομένων και των προσωρινών συμπράξεων, δεν απαιτείται να περιβληθούν συγκεκριμένη νομική μορφή για την υποβολή προσφοράς. Η αναθέτουσα αρχή μπορεί να απαιτήσει από τις ενώσεις οικονομικών φορέων να περιβληθούν συγκεκριμένη νομική μορφή, εφόσον τους ανατεθεί η σύμβαση.

4. Στις περιπτώσεις υποβολής προσφοράς από ένωση οικονομικών φορέων, όλα τα μέλη της ευθύνονται έναντι της αναθέτουσας αρχής αλληλέγγυα και εις ολόκληρον.

2.2.2 Εγγύηση συμμετοχής

2.2.2.1. Για την έγκυρη συμμετοχή στη διαδικασία σύναψης της παρούσας σύμβασης, κατατίθεται από τους συμμετέχοντες οικονομικούς φορείς (προσφέροντες), εγγυητική επιστολή συμμετοχής, σύμφωνα με το αντίστοιχο υπόδειγμα στο «ΠΑΡΑΡΤΗΜΑ VIII – Υποδείγματα Εγγυητικών Επιστολών» της παρούσας.

Το ποσό της εγγυητικής επιστολής θα πρέπει να καλύπτει σε ευρώ (€) ποσοστό **2%** του προϋπολογισμού του Έργου (μη συμπεριλαμβανομένου ΦΠΑ και δικαιωμάτων προαίρεσης), και συμπληρώνεται σύμφωνα με τα οριζόμενα στην Παράγραφο 2.1.5 για το σύνολο της ποσότητας εκάστου Τμήματος ή για το σύνολο των ποσοτήτων όλων των Τμημάτων, που επιθυμεί να συμμετάσχει κάθε οικονομικός φορέας.

Αναλυτικά το ποσό της εγγυητικής που θα αντιστοιχεί στο δυο (2) τοις εκατό (%) επί της συνολικής προϋπολογισθείσας δαπάνης, μη συμπεριλαμβανομένου του Φ.Π.Α., για κάθε Τμήμα, αναγράφεται στον παρακάτω πίνακα:

A/A	ΚΑΘΑΡΗ ΑΞΙΑ ΑΡΧΙΚΗΣ ΣΥΜΦΩΝΙΑΣ- ΠΛΑΙΣΙΟ (ΣΕ ΕΥΡΩ)	ΠΟΣΟ ΕΓΓΥΗΤΙΚΗΣ ΕΠΙΣΤΟΛΗΣ ΣΥΜΜΕΤΟΧΗΣ (ΣΕ ΕΥΡΩ)
Τμήμα 1 «Υπηρεσίες εξασφάλισης επιχειρησιακής συνέχειας, ασφάλειας διακίνησης δεδομένων και μέτρα και πολιτικές πρόληψης και αντιμετώπισης κινδύνων για τη Γ.Γ.Π.Σ.Δ.Δ.»	12.012.400,00 €	240.248,00 €
Τμήμα 2 «Εξειδικευμένες λύσεις και υπηρεσίες ασφάλειας για την Η.ΔΙ.Κ.Α. Α.Ε.»	10.135.911,30 €	202.718,23 €
Τμήμα 3 «Εξειδικευμένες λύσεις και υπηρεσίες ασφάλειας για το Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο»»	8.837.600,00 €	176.752,00 €
Τμήμα 4 «Εξειδικευμένες λύσεις και υπηρεσίες ασφάλειας για την Ε.Δ.Υ.Τ.Ε. Α.Ε.»	7.159.250,00 €	143.185,00 €

Στην περίπτωση ένωσης οικονομικών φορέων, η εγγύηση συμμετοχής περιλαμβάνει και τον όρο ότι η εγγύηση καλύπτει τις υποχρεώσεις όλων των οικονομικών φορέων που συμμετέχουν στην ένωση.

Η εγγύηση συμμετοχής πρέπει να ισχύει τουλάχιστον για τριάντα (30) ημέρες μετά τη λήξη του χρόνου ισχύος της προσφοράς της παρ. 2.4.5 «Χρόνος Ισχύος των Προσφορών» της παρούσας, άλλως η προσφορά απορρίπτεται. Η αναθέτουσα αρχή μπορεί, πριν τη λήξη της προσφοράς, να ζητά από τους προσφέροντες να παρατείνουν, πριν τη λήξη τους, τη διάρκεια ισχύος της προσφοράς και της εγγύησης συμμετοχής.

Οι πρωτότυπες εγγυήσεις συμμετοχής, πλην των εγγυήσεων που εκδίδονται ηλεκτρονικά, προσκομίζονται, σε κλειστό φάκελο με ευθύνη του οικονομικού φορέα, το αργότερο πριν την ημερομηνία και ώρα αποσφράγισης των προσφορών που ορίζεται στην παρ. 3.1 της παρούσας, άλλως η προσφορά απορρίπτεται ως απαράδεκτη, μετά από γνώμη της Επιτροπής Διαγωνισμού.

2.2.2.2. Η εγγύηση συμμετοχής επιστρέφεται στον ανάδοχο με την προσκόμιση της εγγύησης καλής εκτέλεσης.

Η εγγύηση συμμετοχής επιστρέφεται στους λοιπούς προσφέροντες σύμφωνα με τα ειδικότερα οριζόμενα στην παρ. 3 του άρθρου 72 του ν. 4412/2016.² μετά από :

αα) την άπρακτη πάροδο της προθεσμίας άσκησης ενδικοφανούς προσφυγής ή την έκδοση απόφασης επί ασκηθείσας προσφυγής κατά της απόφασης κατακύρωσης,

ββ) την άπρακτη πάροδο της προθεσμίας άσκησης ενδίκων βοηθημάτων προσωρινής δικαστικής προστασίας ή την έκδοση απόφασης επ' αυτών,

γγ) την ολοκλήρωση του προσυμβατικού ελέγχου από το Ελεγκτικό Συνέδριο, σύμφωνα με τα άρθρα 324 έως 327 του ν. 4700/2020 (Α' 127), εφόσον απαιτείται.

Για τα προηγούμενα στάδια της κατακύρωσης η εγγύηση συμμετοχής επιστρέφεται στους συμμετέχοντες σε περίπτωση:

α) λήξης του χρόνου ισχύος της προσφοράς και μη ανανέωσης αυτής και

β) απόρριψης της προσφοράς τους και εφόσον δεν έχει ασκηθεί ενδικοφανής προσφυγή ή ένδικο βοήθημα ή έχει εκπνεύσει άπρακτη η προθεσμία άσκησης ενδικοφανούς προσφυγής ή ενδίκων βοηθημάτων ή έχει λάβει χώρα παραίτηση από το δικαίωμα άσκησης αυτών ή αυτά έχουν απορριφθεί αμετακλήτως.

2.2.2.3. Η εγγύηση συμμετοχής καταπίπτει, εάν ο προσφέρων α) αποσύρει την προσφορά του κατά τη διάρκεια ισχύος αυτής, β) παρέχει, εν γνώσει του, ψευδή στοιχεία ή πληροφορίες που αναφέρονται στις παραγράφους 2.2.3 έως 2.2.8 της παρούσας γ) δεν προσκομίζει εγκαίρως τα προβλεπόμενα από την παρούσα δικαιολογητικά (παρ. 2.2.9.2 & 3.2) ή δ) δεν προσέλθει εγκαίρως για υπογραφή της σύμβασης, ε) υποβάλει μη κατάλληλη προσφορά, με την έννοια της περ. 46 της παρ. 1 του άρθρου 2 του ν. 4412/2016, στ) δεν ανταποκριθεί στη σχετική πρόσκληση της αναθέτουσας αρχής να εξηγήσει την τιμή ή το κόστος της προσφοράς του εντός της τεθείσας προθεσμίας και η προσφορά του απορριφθεί, ζ) στις περιπτώσεις των παρ. 3, 4 και 5 του άρθρου 103 του ν. 4412/2016, περί πρόσκλησης για υποβολή δικαιολογητικών από τον προσωρινό ανάδοχο, αν, κατά τον έλεγχο των παραπάνω δικαιολογητικών, σύμφωνα με τις παραγράφους 3.2 και 3.4 της παρούσας, διαπιστωθεί ότι τα στοιχεία που δηλώθηκαν στο ΕΕΕΣ είναι εκ προθέσεως απατηλά, ή ότι έχουν υποβληθεί πλαστά αποδεικτικά στοιχεία, ή αν, από τα παραπάνω δικαιολογητικά που προσκομίσθηκαν νομίμως και εμπροθέσμως, δεν αποδεικνύεται η μη συνδρομή των λόγων αποκλεισμού της παραγράφου 2.2.3 ή η πλήρωση μιας ή περισσότερων από τις απαιτήσεις των κριτηρίων ποιοτικής επιλογής.

² Πρβ. άρθρο 72 παρ. 1 του ν. 4412/2016, όπως τροποποιήθηκε με την περ. 4 του άρθρου 107 του ν. 4497/2017 (Α' 171).

2.2.3 Λόγοι αποκλεισμού

Αποκλείεται από τη συμμετοχή στην παρούσα διαδικασία σύναψης συμφωνίας-πλαίσιο (διαγωνισμό) προσφέρων οικονομικός φορέας, εφόσον συντρέχει στο πρόσωπό του (εάν πρόκειται για μεμονωμένο φυσικό ή νομικό πρόσωπο) ή σε ένα από τα μέλη του (εάν πρόκειται για ένωση οικονομικών φορέων) ένας ή περισσότεροι από τους ακόλουθους λόγους:

2.2.3.1

Όταν υπάρχει σε βάρος του αμετάκλητη καταδικαστική απόφαση για ένα από τα ακόλουθα εγκλήματα:

α) συμμετοχή σε εγκληματική οργάνωση, όπως αυτή ορίζεται στο άρθρο 2 της απόφασης-πλαίσιο 2008/841/ΔΕΥ του Συμβουλίου της 24ης Οκτωβρίου 2008, για την καταπολέμηση του οργανωμένου εγκλήματος (ΕΕ L 300 της 11.11.2008 σ.42 και τα εγκλήματα του άρθρου 187 του Ποινικού Κώδικα (εγκληματική οργάνωση),

β) ενεργητική δωροδοκία, όπως ορίζεται στο άρθρο 3 της σύμβασης περί της καταπολέμησης της διαφθοράς στην οποία ενέχονται υπάλληλοι των Ευρωπαϊκών Κοινοτήτων ή των κρατών-μελών της Ένωσης (ΕΕ C 195 της 25.6.1997, σ. 1) και στην παράγραφο 1 του άρθρου 2 της απόφασης-πλαίσιο 2003/568/ΔΕΥ του Συμβουλίου της 22ας Ιουλίου 2003, για την καταπολέμηση της δωροδοκίας στον ιδιωτικό τομέα (ΕΕ L 192 της 31.7.2003, σ. 54), καθώς και όπως ορίζεται στο εθνικό δίκαιο του οικονομικού φορέα, και τα εγκλήματα των άρθρων 159^Α (δωροδοκία πολιτικών προσώπων), 236 (δωροδοκία υπαλλήλου), 237 παρ.2-4 (δωροδοκία δικαστικών λειτουργών), 237^Α παρ.2 (εμπορία επιρροής – μεσάζοντες) 396 παρ.2 (δωροδοκία στον ιδιωτικό τομέα) του Ποινικού Κώδικα.

γ) απάτη εις βάρος των οικονομικών συμφερόντων της Ένωσης, κατά την έννοια των άρθρων 3 και 4 της Οδηγίας (ΕΕ) 2017/1371 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 5ης Ιουλίου 2017 σχετικά με την καταπολέμηση, μέσω του ποινικού δικαίου, της απάτης εις βάρος των οικονομικών συμφερόντων της Ένωσης (L 198/28.07.2017) και τα εγκλήματα των άρθρων 159Α (δωροδοκία πολιτικών προσώπων), 216 (πλαστογραφία), 236 (δωροδοκία υπαλλήλου), 237 παρ. 2-4 (δωροδοκία δικαστικών λειτουργών), 242 (ψευδής βεβαίωση, νόθευση κ.λπ.), 374 (διακεκριμένη κλοπή), 375 (υπεξαίρεση), 386 (απάτη), 386Α (απάτη με υπολογιστή), 386Β (απάτη σχετική με τις επιχορηγήσεις), 390 (απιστία) του Ποινικού Κώδικα και των άρθρων 155 επ. του Εθνικού Τελωνειακού Κώδικα (ν. 2960/2001, Α' 265), όταν αυτά στρέφονται κατά των οικονομικών συμφερόντων της Ευρωπαϊκής Ένωσης ή συνδέονται με την προσβολή αυτών των συμφερόντων, καθώς και τα εγκλήματα των άρθρων 23 (διασυνοριακή απάτη σχετικά με τον ΦΠΑ) και 24 (επικουρικές διατάξεις για την ποινική προστασία των οικονομικών συμφερόντων της Ευρωπαϊκής Ένωσης) του ν. 4689/2020 (Α' 103),

δ) τρομοκρατικά εγκλήματα ή εγκλήματα συνδεόμενα με τρομοκρατικές δραστηριότητες, όπως ορίζονται, αντιστοίχως στα άρθρα 3-4 και 5-12 της Οδηγίας (ΕΕ) 2017/541 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 15ης Μαρτίου 2017 για την καταπολέμηση της τρομοκρατίας και την αντικατάσταση της απόφασης - πλαισίου 2002/475/ΔΕΥ του Συμβουλίου και για την τροποποίηση της απόφασης 2005/671/ΔΕΥ του Συμβουλίου (ΕΕ L 88/31.03.2017) ή ηθική αυτουργία ή συνέργεια ή απόπειρα διάπραξης εγκλήματος, όπως ορίζονται στο άρθρο 14 αυτής, και τα

εγκλήματα των άρθρων 187Α και 187Β του Ποινικού Κώδικα, καθώς και τα εγκλήματα των άρθρων 32-35 του ν. 4689/2020 (Α' 103),

ε) νομιμοποίηση εσόδων από παράνομες δραστηριότητες ή χρηματοδότηση της τρομοκρατίας, όπως αυτές ορίζονται στο άρθρο 1 της Οδηγίας (ΕΕ) 2015/849 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 20ης Μαΐου 2015, σχετικά με την πρόληψη της χρησιμοποίησης του χρηματοπιστωτικού συστήματος για τη νομιμοποίηση εσόδων από παράνομες δραστηριότητες ή για τη χρηματοδότηση της τρομοκρατίας, την τροποποίηση του κανονισμού (ΕΕ) αριθμ. 648/2012 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, και την κατάργηση της οδηγίας 2005/60/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου και της οδηγίας 2006/70/ΕΚ της Επιτροπής (ΕΕL 141/05.06.2015) και τα εγκλήματα των άρθρων 2 και 39 του ν. 4557/2018 (Α' 139),

στ) παιδική εργασία και άλλες μορφές εμπορίας ανθρώπων, όπως ορίζονται στο άρθρο 2 της Οδηγίας 2011/36/ ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 5ης Απριλίου 2011, για την πρόληψη και την καταπολέμηση της εμπορίας ανθρώπων και για την προστασία των θυμάτων της, καθώς και για την αντικατάσταση της απόφασης - πλαίσιο 2002/629/ΔΕΥ του Συμβουλίου (ΕΕ L 101 της 15.4.2011, σ. 1) και τα εγκλήματα του άρθρου 323Α του Ποινικού κώδικα (εμπορία ανθρώπων).

Ο οικονομικός φορέας αποκλείεται, επίσης, όταν το πρόσωπο εις βάρος του οποίου εκδόθηκε τελεσίδικη αμετάκλητη καταδικαστική απόφαση είναι μέλος του διοικητικού, διευθυντικού ή εποπτικού οργάνου του ή έχει εξουσία εκπροσώπησης, λήψης αποφάσεων ή ελέγχου σε αυτό.

Η υποχρέωση του προηγούμενου εδαφίου αφορά:

- στις περιπτώσεις εταιρειών περιορισμένης ευθύνης (Ε.Π.Ε.) ιδιωτικών κεφαλαιουχικών εταιρειών (Ι.Κ.Ε.) και προσωπικών εταιρειών (Ο.Ε. και Ε.Ε.) τους διαχειριστές.
- στις περιπτώσεις ανωνύμων εταιρειών (Α.Ε.), τον διευθύνοντα Σύμβουλο, τα μέλη του Διοικητικού Συμβουλίου, καθώς και τα πρόσωπα στα οποία με απόφαση του Διοικητικού Συμβουλίου έχει ανατεθεί το σύνολο της διαχείρισης και εκπροσώπησης της εταιρείας.
- στις περιπτώσεις Συνεταιρισμών, τα μέλη του Διοικητικού Συμβουλίου.
- σε όλες τις υπόλοιπες περιπτώσεις νομικών προσώπων, τον κατά περίπτωση νόμιμο εκπρόσωπο.

Εάν στις ως άνω περιπτώσεις (α) έως (στ) η κατά τα ανωτέρω περίοδος αποκλεισμού δεν έχει καθοριστεί με αμετάκλητη απόφαση, αυτή ανέρχεται σε πέντε (5) έτη από την ημερομηνία της καταδίκης με αμετάκλητη απόφαση.

2.2.3.2

Στις ακόλουθες περιπτώσεις

α) όταν ο οικονομικός φορέας έχει αθετήσει τις υποχρεώσεις του όσον αφορά στην καταβολή φόρων ή εισφορών κοινωνικής ασφάλισης και αυτό έχει διαπιστωθεί από δικαστική ή διοικητική απόφαση με τελεσίδικη και δεσμευτική ισχύ, σύμφωνα με διατάξεις της χώρας όπου είναι εγκατεστημένος ή την εθνική νομοθεσία ή

β) όταν η αναθέτουσα αρχή μπορεί να αποδείξει με τα κατάλληλα μέσα ότι ο οικονομικός φορέας έχει αθετήσει τις υποχρεώσεις του όσον αφορά την καταβολή φόρων ή εισφορών κοινωνικής ασφάλισης.

Αν ο οικονομικός φορέας είναι Έλληνας πολίτης ή έχει την εγκατάστασή του στην Ελλάδα, οι υποχρεώσεις του που αφορούν τις εισφορές κοινωνικής ασφάλισης καλύπτουν τόσο την κύρια όσο και την επικουρική ασφάλιση.

Οι υποχρεώσεις των περ. α' και β' της παρ. [2.2.3.2](#) θεωρείται ότι δεν έχουν αθετηθεί εφόσον δεν έχουν καταστεί ληξιπρόθεσμες ή εφόσον αυτές έχουν υπαχθεί σε δεσμευτικό διακανονισμό που τηρείται.

Δεν αποκλείεται ο οικονομικός φορέας, όταν έχει εκπληρώσει τις υποχρεώσεις του είτε καταβάλλοντας τους φόρους ή τις εισφορές κοινωνικής ασφάλισης που οφείλει, συμπεριλαμβανομένων, κατά περίπτωση, των δεδουλευμένων τόκων ή των προστίμων είτε υπαγόμενος σε δεσμευτικό διακανονισμό για την καταβολή τους στο μέτρο που τηρεί τους όρους του δεσμευτικού κανονισμού.

2.2.3.3

Αποκλείεται απότη συμμετοχήστη διαδικασία σύναψης της παρούσας σύμβασης,οικονομικός φορέας σε οποιαδήποτε απο τις ακόλουθες καταστάσεις:

(α) εάν έχει αθετήσει τις υποχρεώσεις που προβλέπονται στην παρ. 2 του άρθρου 18 του ν. 4412/2016, περί αρχών που εφαρμόζονται στις διαδικασίες σύναψης δημοσίων συμβάσεων

(β) εάν τελεί υπό πτώχευση ή έχει υπαχθεί σε διαδικασία ειδικής εκκαθάρισής τελεί υπό αναγκαστική διαχείριση από εκκαθαριστή ή από το δικαστήριο ή έχει υπαχθεί σε διαδικασία πτωχευτικού συμβιβασμού ή έχει αναστείλει τις επιχειρηματικές του δραστηριότητες ή έχει υπαχθεί σε διαδικασία εξυγίανσης και δεν τηρεί τους όρους αυτής ή εάν βρίσκεται σε οποιαδήποτε ανάλογη κατάσταση προκύπτουσα από παρόμοια διαδικασία, προβλεπόμενη σε εθνικές διατάξεις νόμου.

(γ) εάν, με την επιφύλαξη της παραγράφου 3β του άρθρου 44 του ν. 3959/2011 περί ποινικών κυρώσεων και άλλων διοικητικών συνεπειών, υπάρχουν επαρκώς εύλογες ενδείξεις που οδηγούν στο συμπέρασμα ότι ο οικονομικός φορέας συνήψε συμφωνίες με άλλους οικονομικούς φορείς με στόχο τη στρέβλωση του ανταγωνισμού,

δ) εάν μία κατάσταση σύγκρουσης συμφερόντων κατά την έννοια του άρθρου 24 του ν. 4412/2016 δεν μπορεί να θεραπευθεί αποτελεσματικά με άλλα, λιγότερο παρεμβατικά, μέσα,

(ε) εάν μία κατάσταση στρέβλωσης του ανταγωνισμού από την πρότερη συμμετοχή του οικονομικού φορέα κατά την προετοιμασία της διαδικασίας σύναψης σύμβασης, κατά τα οριζόμενα στο άρθρο 48 του ν. 4412/2016 όπως ισχύει, δεν μπορεί να θεραπευθεί με άλλα, λιγότερο παρεμβατικά, μέσα,

(στ) εάν έχει επιδείξει σοβαρή ή επαναλαμβανόμενη πλημμέλεια κατά την εκτέλεση ουσιώδους απαίτησης στο πλαίσιο προηγούμενης δημόσιας σύμβασης, προηγούμενης σύμβασης με αναθέτοντα φορέα ή προηγούμενης σύμβασης παραχώρησης που είχε ως αποτέλεσμα την πρόωρη καταγγελία της προηγούμενης σύμβασης, αποζημιώσεις ή άλλες παρόμοιες κυρώσεις,

(ζ) εάν έχει κριθεί ένοχος εκ προθέσεως σοβαρών απατηλών δηλώσεων κατά την παροχή των πληροφοριών που απαιτούνται για την εξακρίβωση της απουσίας των λόγων αποκλεισμού ή την πλήρωση των κριτηρίων επιλογής, έχει αποκρύψει τις πληροφορίες αυτές ή δεν είναι σε θέση να

προσκομίσει τα δικαιολογητικά που απαιτούνται κατ' εφαρμογή της παραγράφου 2.2.9.2 Αποδεικτικά μέσα- Δικαιολογητικά προσωρινού αναδόχου της παρούσας.

(η) εάν επιχειρήσει να επηρεάσει με αθέμιτο τρόπο τη διαδικασία λήψης αποφάσεων της αναθέτουσας αρχής, να αποκτήσει εμπιστευτικές πληροφορίες που ενδέχεται να του αποφέρουν αθέμιτο πλεονέκτημα στη διαδικασία σύναψης σύμβασης ή να παράσχει με απατηλό τρόπο παραπλανητικές πληροφορίες που ενδέχεται να επηρεάσουν ουσιωδώς τις αποφάσεις που αφορούν τον αποκλεισμό, την επιλογή ή την ανάθεση,

(θ) εάν η αναθέτουσα αρχή μπορεί να αποδείξει, με κατάλληλα μέσα ότι έχει διαπράξει σοβαρό επαγγελματικό παράπτωμα, το οποίο θέτει εν αμφιβόλω την ακεραιότητά του.

Εάν στις ως άνω περιπτώσεις (α) έως (θ) η περίοδος αποκλεισμού δεν έχει καθοριστεί με αμετάκλητη απόφαση, αυτή ανέρχεται σε τρία (3) έτη από την ημερομηνία έκδοσης πράξης που βεβαιώνει το σχετικό γεγονός.

2.2.3.4

Αποκλείεται, επίσης, οικονομικός φορέας από τη συμμετοχή στη διαδικασία σύναψης της παρούσας σύμβασης εάν συντρέχουν οι προϋποθέσεις εφαρμογής της παρ. 4 του άρθρου 8 του ν. 3310/2005, όπως ισχύει (αμιγώς εθνικός λόγος αποκλεισμού). Οι υποχρεώσεις της παρούσας αφορούν τις ανώνυμες εταιρείες που υποβάλλουν προσφορά αυτοτελώς ή ως μέλη ένωσης ή που συμμετέχουν στο μετοχικό κεφάλαιο άλλου νομικού προσώπου που υποβάλλει προσφορά ή νομικά πρόσωπα της αλλοδαπής που αντιστοιχούν σε ανώνυμη εταιρεία.

Εξαιρούνται της υποχρέωσης αυτής: α) οι εισηγμένες στα χρηματιστήρια κρατών-μελών της Ευρωπαϊκής Ένωσης ή του Οργανισμού Οικονομικής Συνεργασίας και Ανάπτυξης (Ο.Ο.Σ.Α.) εταιρείες, β) οι εταιρείες, τα δικαιώματα ψήφου των οποίων ελέγχονται από μία ή περισσότερες επιχειρήσεις επενδύσεων (investment firms), εταιρείες διαχείρισης κεφαλαίων/ενεργητικού (asset/fund managers) ή εταιρείες διαχείρισης κεφαλαίων επιχειρηματικών συμμετοχών (private equity firms), υπό την προϋπόθεση ότι οι τελευταίες αυτές εταιρείες ελέγχουν, συνολικά ποσοστό που υπερβαίνει το εβδομήντα πέντε τοις εκατό (75%) των δικαιωμάτων ψήφων και είναι εποπτευόμενες από Επιτροπές Κεφαλαιαγοράς ή άλλες αρμόδιες χρηματοοικονομικές αρχές κρατών μελών της Ευρωπαϊκής Ένωσης ή του Ο.Ο.Σ.Α.

2.2.3.5

Ο οικονομικός φορέας αποκλείεται σε οποιοδήποτε χρονικό σημείο κατά τη διάρκεια της διαδικασίας σύναψης της παρούσας συμφωνίας - πλαίσιο, όταν αποδεικνύεται ότι βρίσκεται, λόγω πράξεων ή παραλείψεων του, είτε πριν είτε κατά τη διαδικασία, σε μία από τις ως άνω περιπτώσεις.

2.2.3.6

Ο οικονομικός φορέας που εμπίπτει σε μια από τις καταστάσεις που αναφέρονται στις παραγράφους 2.2.3.1 και 2.2.3.3 εκτός από την περ. β αυτής, μπορεί να προσκομίζει στοιχεία προκειμένου να αποδείξει ότι τα μέτρα που έλαβε επαρκούν για να αποδείξουν την αξιοπιστία του, παρότι συντρέχει ο σχετικός λόγος αποκλεισμού (αυτοκάθαρση). Για τον σκοπό αυτόν, ο οικονομικός φορέας αποδεικνύει ότι έχει καταβάλει ή έχει δεσμευθεί να καταβάλει αποζημίωση για ζημιές που προκλήθηκαν από το ποινικό αδίκημα ή το παράπτωμα, ότι έχει διευκρινίσει τα γεγονότα και τις περιστάσεις με ολοκληρωμένο τρόπο, μέσω ενεργού συνεργασίας με τις ερευνητικές αρχές, και έχει λάβει συγκεκριμένα τεχνικά και οργανωτικά μέτρα, καθώς και μέτρα σε επίπεδο προσωπικού κατάλληλα για την αποφυγή περαιτέρω ποινικών αδικημάτων ή παραπτωμάτων. Τα μέτρα που λαμβάνονται από τους οικονομικούς φορείς αξιολογούνται σε συνάρτηση με τη σοβαρότητα και τις ιδιαίτερες περιστάσεις του ποινικού αδικήματος ή του παραπτώματος. Εάν τα στοιχεία κριθούν επαρκή, ο εν λόγω οικονομικός φορέας δεν αποκλείεται από τη διαδικασία σύναψης σύμβασης. Αν τα μέτρα κριθούν ανεπαρκή, γνωστοποιείται στον οικονομικό φορέα το σκεπτικό της απόφασης αυτής. Οικονομικός φορέας που έχει αποκλειστεί, σύμφωνα με τις κείμενες διατάξεις, με τελεσίδικη απόφαση, σε εθνικό επίπεδο, από τη συμμετοχή σε διαδικασίες σύναψης σύμβασης ή ανάθεσης παραχώρησης δεν μπορεί να κάνει χρήση της ανωτέρω δυνατότητας κατά την περίοδο του αποκλεισμού που ορίζεται στην εν λόγω απόφαση.

2.2.3.7

Η απόφαση για την διαπίστωση της επάρκειας ή μη των επανορθωτικών μέτρων κατά την προηγούμενη παράγραφο εκδίδεται σύμφωνα με τα οριζόμενα στις παρ. 8 και 9 του άρθρου 73 του ν. 4412/2016.

2.2.3.8

Οικονομικός φορέας, σε βάρος του οποίου έχει επιβληθεί η κύρωση του οριζόντιου αποκλεισμού σύμφωνα με τις κείμενες διατάξεις και για το χρονικό διάστημα που αυτή ορίζει, αποκλείεται από την παρούσα διαδικασία σύναψης της σύμβασης.

Κριτήρια Ποιοτικής Επιλογής

2.2.4 Καταλληλότητα άσκησης επαγγελματικής δραστηριότητας

Οι οικονομικοί φορείς που συμμετέχουν στη διαδικασία σύναψης της παρούσας απαιτείται να ασκούν επαγγελματική δραστηριότητα συναφή με το αντικείμενο των προς παροχή υπηρεσιών, **ήτοι παροχή υπηρεσιών σχετικά με την κυβερνοασφάλεια, προμήθεια έτοιμου λογισμικού και ανάπτυξη και υποστήριξη εφαρμογών λογισμικού.**

Οι οικονομικοί φορείς που είναι εγκατεστημένοι σε κράτος μέλος της Ευρωπαϊκής Ένωσης απαιτείται να είναι εγγεγραμμένοι σε ένα από τα επαγγελματικά ή εμπορικά μητρώα που τηρούνται στο κράτος εγκατάστασής τους ή να ικανοποιούν οποιαδήποτε άλλη απαίτηση ορίζεται στο Παράρτημα XI του Προσαρτήματος Α' του ν. 4412/2016. Εφόσον οι οικονομικοί φορείς απαιτείται να διαθέτουν ειδική έγκριση ή να είναι μέλη συγκεκριμένου οργανισμού για να μπορούν να παράσχουν τη σχετική υπηρεσία στη χώρα καταγωγής τους, η αναθέτουσα αρχή μπορεί να τους ζητεί να αποδείξουν ότι

διαθέτουν την έγκριση αυτή ή ότι είναι μέλη του εν λόγω οργανισμού ή να τους καλέσει να προβούν σε ένορκη δήλωση ενώπιον συμβολαιογράφου σχετικά με την άσκηση του συγκεκριμένου επαγγέλματος.

Στην περίπτωση οικονομικών φορέων εγκατεστημένων σε κράτος μέλους του Ευρωπαϊκού Οικονομικού Χώρου (Ε.Ο.Χ) ή σε τρίτες χώρες που προσχωρήσει στη ΣΔΣ, ή σε τρίτες χώρες που δεν εμπίπτουν στην προηγούμενη περίπτωση και έχουν συνάψει διμερείς ή πολυμερείς συμφωνίες με την Ένωση σε θέματα διαδικασιών ανάθεσης δημοσίων συμβάσεων, απαιτείται να είναι εγγεγραμμένοι σε αντίστοιχα επαγγελματικά μητρώα.

Οι εγκατεστημένοι στην Ελλάδα οικονομικοί φορείς θα πρέπει να είναι εγγεγραμμένοι στο οικείο επαγγελματικό μητρώο, εφόσον, κατά την κείμενη νομοθεσία, απαιτείται η εγγραφή τους για την υπό ανάθεση υπηρεσία.

Στην περίπτωση ένωσης οικονομικών φορέων η καταλληλότητα άσκησης επαγγελματικής δραστηριότητας απαιτείται να καλύπτεται σωρευτικά από τα μέλη της ένωσης.

2.2.5 Οικονομική και χρηματοοικονομική επάρκεια

Οι οικονομικοί φορείς που συμμετέχουν στη διαδικασία σύναψης της παρούσας απαιτείται να έχουν μέσο γενικό ετήσιο κύκλο εργασιών για τις τρεις (3) τελευταίες οικονομικές χρήσεις ή, τις οικονομικές χρήσεις κατά τις οποίες ο οικονομικός φορέας δραστηριοποιείται, αν είναι λιγότερες από τρεις (2020-2021-2022) συνολικά κατ' ελάχιστον ίσο με το διακόσια τοις εκατό (200%) του προϋπολογισμού του τμήματος ή των τμημάτων για το/ταποιο/οποία υποβάλλει προσφορά.

Σε περίπτωση ένωσης οικονομικών φορέων, η παραπάνω απαίτηση καλύπτεται αθροιστικά από τα μέλη της ένωσης.

2.2.6 Τεχνική και επαγγελματική ικανότητα

Οι οικονομικοί φορείς που συμμετέχουν στη διαδικασία σύναψης της παρούσας απαιτείται:

1. να έχουν ολοκληρώσει, τα τελευταία τρία (3) έτη (2022-2021-2020) την υλοποίηση (σε ιδιωτικό ή δημόσιο τομέα) δύο (2) αντίστοιχων έργων που περιλαμβάνουν αντικείμενα που περιγράφονται στο υπό προκήρυξη Τμήμα που συμμετέχουν. Τα αντίστοιχα έργα ορίζονται παρακάτω ανά τμήμα του παρόντος έργου.
2. να διαθέτουν ανθρώπινο δυναμικό και πόρους ικανούς και αξιόπιστους για να φέρουν σε πέρας επιτυχώς τις απαιτήσεις του έργου, σε επίπεδο απαιτούμενης εξειδίκευσης, επαγγελματικών προσόντων και εμπειρίας. Οι ελάχιστες απαιτήσεις ορίζονται παρακάτω ανά τμήμα του παρόντος έργου.

Τμήμα 1

Όσον αφορά στην τεχνική και επαγγελματική ικανότητα για το παρόν τμήμα, οι οικονομικοί φορείς θα πρέπει να πληρούν και να τεκμηριώνουν επαρκώς, με ποινή αποκλεισμού, τις παρακάτω ελάχιστες προϋποθέσεις συμμετοχής, στο Διαγωνισμό.

α) Κατά τα τελευταία **τρία (3) έτη** να έχουν ολοκληρώσει επιτυχώς τουλάχιστον δύο (2) αντίστοιχα έργα προϋπολογισμού μεγαλύτερου ή ίσου με 1.000.000 Ευρώ που να περιλαμβάνουν αθροιστικά:

Τουλάχιστον πέντε (5) από τα παρακάτω αντικείμενα:

- Υπηρεσίες Ransomware readiness assessment
- Εκπόνηση Μελέτης Ανάλυσης και Αξιολόγησης Κινδύνων
- Διενέργεια δράσεων ενημέρωσης τη μεταφορά τεχνογνωσίας και την διαμόρφωση κουλτούρας ενεργούς ευαισθητοποίησης για τους κινδύνους κυβερνοασφάλειας
- Διαμόρφωση πλάνου ανάκαμψης από καταστροφές
- Εκπόνηση Μελέτης εξωτερικού και εσωτερικού περιβάλλοντος και την ανάδειξη βέλτιστων πρακτικών στον τομέα της κυβερνοασφάλειας
- Διενέργεια ελέγχων διεύθυνσης εξωτερικών δικτύων ή/και ελέγχων εφαρμογών Ιστού ή/και ελέγχων φυσικής ασφάλειας ή/και ελέγχων διαρροής δεδομένων
- Την υλοποίηση ή προμήθεια ή συντήρηση λύσης Μηχανισμού Ελέγχου Πρόσβασης Χρηστών Πολλαπλών Παραγόντων (MFA).
- Την παροχή υπηρεσιών ανάκαμψης από καταστροφή και λήψης αντιγράφων ασφαλείας

Την υλοποίηση ή προμήθεια ή συντήρηση τουλάχιστον τεσσάρων (4) από τις παρακάτω λύσεις:

- Λύση δημιουργίας αντιγράφων ασφαλείας σε ταινίες με Physical Air Gap – True Air Gap
- Λύση δημιουργίας αντιγράφων ασφαλείας σε δίσκο Backup με Logical Air Gap
- Λύση προστασίας ηλεκτρονικού ταχυδρομείου Mail Security
- Λύση Endpoint Detection and Response
- Λύση που αφορά τον έλεγχο της πρόσβασης των εσωτερικών χρηστών στο Διαδίκτυο
- Λύση Ασφαλείας και προστασίας των χρηστών από απειλές του διαδικτύου (Web Security Gateway)

Ένα έργο δύναται να καλύπτει περισσότερες από μία από τις παραπάνω κατηγορίες.

Σε περίπτωση συμμετοχής σε ένωση ή κοινοπραξία, λαμβάνεται υπόψη μόνο το ποσοστό που αντιστοιχεί στη συμμετοχή του.

Επιτρέπεται η τεκμηρίωση εμπειρίας που υπερβαίνει τα τρία έτη αλλά δεν ξεπερνά την τελευταία πενταετία για λόγους ανάπτυξης του ανταγωνισμού.

β) να διαθέτουν ομάδα έργου με στελέχη επαρκή σε πλήθος και δεξιότητες για την ανάληψη του Έργου η οποία να αποτελείται τουλάχιστον από τα ακόλουθα βασικά στελέχη (key experts):

- έναν (1) Υπεύθυνο Έργου, ο οποίος να διαθέτει Πανεπιστημιακό Τίτλο Σπουδών και τουλάχιστον 10ετή επαγγελματική εμπειρία σε Διαχείριση Έργων Πληροφορικής,
- έναν (1) αναπληρωτή Υπεύθυνο Έργου, ο οποίος να διαθέτει Πανεπιστημιακό Τίτλο Σπουδών και τουλάχιστον 7ετή επαγγελματική εμπειρία σε Διαχείριση Έργων Πληροφορικής,
- τρεις (3) Μηχανικούς Πληροφορικής, οι οποίοι να διαθέτουν τουλάχιστον 5ετή επαγγελματική εμπειρία στην Ασφάλεια των Πληροφοριών,
- **δύο (2) Ειδικούς Ασφάλειας Πληροφοριακών Συστημάτων**, οι οποίοι να διαθέτουν τουλάχιστον 5ετή επαγγελματική εμπειρία σε ασφάλεια πληροφοριακών συστημάτων.
- Έναν υπεύθυνο σχεδιασμού και υλοποίησης, ο οποίος να διαθέτει πτυχίο τριτοβάθμιας εκπαίδευσης στο γνωστικό αντικείμενο που έχει άμεση συνάφεια με τον τύπο των παρεχόμενων υπηρεσιών, στο πλαίσιο του Έργου. Τουλάχιστον 7ετή επαγγελματική εμπειρία

στην Ασφάλεια των Πληροφοριών και πιο συγκεκριμένα γύρω από τον Αρχιτεκτονικό Σχεδιασμό Συστημάτων Ασφάλειας Πληροφοριών.

Επισημαίνεται ότι σε περίπτωση που ο υποψήφιος Ανάδοχος αποτελεί Ένωση / Κοινοπραξία, επιτρέπεται η μερική κάλυψη των προϋποθέσεων από τα Μέλη της, αρκεί όμως συνολικά αθροιστικά να καλύπτονται όλες.

Τμήμα 2

Όσον αφορά στην τεχνική και επαγγελματική ικανότητα για το παρόν τμήμα, οι οικονομικοί φορείς θα πρέπει να πληρούν και να τεκμηριώνουν επαρκώς, με ποινή αποκλεισμού, τις παρακάτω ελάχιστες προϋποθέσεις συμμετοχής, στο Διαγωνισμό.

α) Κατά τα τελευταία **τρία (3) έτη** να έχουν ολοκληρώσει επιτυχώς τουλάχιστον δύο (2) αντίστοιχα έργα προϋπολογισμού μεγαλύτερου ή ίσου με 1.000.000 Ευρώ που να περιλαμβάνουν αθροιστικά:

Τουλάχιστον πέντε (5) από τα παρακάτω αντικείμενα:

- ο Διαμόρφωση πολιτικών ορθής χρήσης Πληροφοριακών συστημάτων και εφαρμογών
- ο Διαμόρφωση πλάνου ανάκαμψης από καταστροφές
- ο Διαμόρφωση πολιτικής αντιγράφων ασφαλείας
- ο Διαμόρφωση Συστήματος Διαχείρισης της Ασφάλειας των Πληροφοριών (ΣΔΑΠ) με βάση το πρότυπο ISO 27001 & Εκπόνηση Μελέτης Ανάλυσης και Αξιολόγησης Κινδύνων
- ο Διενέργεια δράσεων ενημέρωσης τη μεταφορά τεχνογνωσίας και την διαμόρφωση κουλτούρας ενεργούς ευαισθητοποίησης για τους κινδύνους κυβερνοασφάλειας
- ο Εκπόνηση Μελέτης εξωτερικού και εσωτερικού περιβάλλοντος και την ανάδειξη βέλτιστων πρακτικών στον τομέα της κυβερνοασφάλειας
- ο Διενέργεια ελέγχων διεξόδου εξωτερικών δικτύων ή/και ελέγχων εφαρμογών Ιστού ή/και ελέγχων φυσικής ασφάλειας ή/και ελέγχων διαρροής δεδομένων

Την υλοποίηση ή προμήθεια ή συντήρηση τουλάχιστον πέντε (5) από τις παρακάτω λύσεις.

- ο Λύση Διαβάθμισης και Σήμανσης Εγγράφων
- ο Λύση Προστασίας Δεδομένων από Διαρροή
- ο Λύση Διαχείρισης Δικαιωμάτων Εγγράφων
- ο Λύση Διαχείρισης Λογαριασμών και Δικαιωμάτων Πρόσβασης Χρηστών
- ο Λύση Διαχείρισης Προνομιούχων Λογαριασμών Πρόσβασης
- ο Λύση μηχανισμών ισχυρής ταυτοποίησης
- ο Την παροχή υπηρεσιών ανάκαμψης από καταστροφή και λήψης αντιγράφων ασφαλείας
- ο Την παροχή λύσης Ddos

Την υλοποίηση ή προμήθεια ή συντήρηση τουλάχιστον δέκα (10) από τις παρακάτω λύσεις:

- ο Next Generation Firewall για Data Center
- ο Virtual firewall για πολλαπλούς tenants σε High availability
- ο IPS και antimalware

- ο Λύση Microsegmentation
- ο Λύση Ασφαλείας και προστασίας των χρηστών από απειλές του διαδικτύου (Web Security Gateway)
- ο Λύση Αυστηρής πιστοποίησης για την απομακρυσμένη πρόσβαση (MFA, Zero Trust)
- ο Λύση Cloud Proxy προστασίας απομακρυσμένων χρηστών
- ο Λύση Antimalware απομακρυσμένων χρηστών (AV, EDR, XDR)
- ο Λύση εκπαίδευσης σε phishing campaigns και cyber attacks
- ο Λύση Ασφαλούς Πρόσβασης χρηστών στο εταιρικό δίκτυο
- ο Λύση Πλατφόρμας Ενορχήστρωσης Ασφαλείας, Αυτοματοποίησης
- ο Πλατφόρμα Κυβερνοασφάλειας – Εκτεταμένης Ανίχνευσης & Απόκρισης (Cyber Security)
- ο Λύση Προστασίας Βάσεων Δεδομένων
- ο Λογισμικό κυβερνοασφάλειας AI

Ένα έργο δύναται να καλύπτει περισσότερες από μία από τις παραπάνω κατηγορίες.

Σε περίπτωση συμμετοχής σε ένωση ή κοινοπραξία, λαμβάνεται υπόψη μόνο το ποσοστό που αντιστοιχεί στη συμμετοχή του.

Επιτρέπεται η τεκμηρίωση εμπειρίας που υπερβαίνει τα τρία έτη αλλά δεν ξεπερνά την τελευταία πενταετία για λόγους ανάπτυξης του ανταγωνισμού.

β) να διαθέτουν ομάδα έργου με στελέχη επαρκή σε πλήθος και δεξιότητες για την ανάληψη του Έργου η οποία να αποτελείται τουλάχιστον από τα ακόλουθα βασικά στελέχη (keyexperts):

- έναν (1) Υπεύθυνο Έργου, ο οποίος να διαθέτει Πανεπιστημιακό Τίτλο Σπουδών και τουλάχιστον 10ετή επαγγελματική εμπειρία σε Διαχείριση Έργων Πληροφορικής,
- έναν (1) αναπληρωτή Υπεύθυνο Έργου, ο οποίος να διαθέτει Πανεπιστημιακό Τίτλο Σπουδών και τουλάχιστον 7ετή επαγγελματική εμπειρία σε Διαχείριση Έργων Πληροφορικής,
- τρεις (3) Μηχανικούς Πληροφορικής, οι οποίοι να διαθέτουν τουλάχιστον 5ετή επαγγελματική εμπειρία στην Ασφάλεια των Πληροφοριών,
- **δύο (2) Ειδικούς Ασφάλειας Πληροφοριακών Συστημάτων**, οι οποίοι να διαθέτουν τουλάχιστον 5ετή επαγγελματική εμπειρία σε ασφάλεια πληροφοριακών συστημάτων.
- Έναν υπεύθυνο σχεδιασμού και υλοποίησης, ο οποίος να διαθέτει πτυχίο τριτοβάθμιας εκπαίδευσης στο γνωστικό αντικείμενο που έχει άμεση συνάφεια με τον τύπο των παρεχόμενων υπηρεσιών, στο πλαίσιο του Έργου. Τουλάχιστον 7ετή επαγγελματική εμπειρία στην Ασφάλεια των Πληροφοριών και πιο συγκεκριμένα γύρω από τον Αρχιτεκτονικό Σχεδιασμό Συστημάτων Ασφάλειας Πληροφοριών.

Επισημαίνεται ότι σε περίπτωση που ο υποψήφιος Ανάδοχος αποτελεί Ένωση / Κοινοπραξία, επιτρέπεται η μερική κάλυψη των προϋποθέσεων από τα Μέλη της, αρκεί όμως συνολικά αθροιστικά να καλύπτονται όλες.

Τμήμα 3

Όσον αφορά στην τεχνική και επαγγελματική ικανότητα για το παρόν τμήμα, οι οικονομικοί φορείς θα πρέπει να πληρούν και να τεκμηριώνουν επαρκώς, με ποινή αποκλεισμού, τις παρακάτω ελάχιστες προϋποθέσεις συμμετοχής, στο Διαγωνισμό.

α) Κατά τα τελευταία **τρία (3) έτη** να έχουν ολοκληρώσει επιτυχώς τουλάχιστον δύο (2) αντίστοιχα έργα προϋπολογισμού μεγαλύτερου ή ίσου με 1.000.000 Ευρώ που να περιλαμβάνουν αθροιστικά:

Τουλάχιστον πέντε (5) από τα παρακάτω αντικείμενα:

- ο Διαμόρφωση πολιτικών ορθής χρήσης Πληροφοριακών συστημάτων και εφαρμογών
- ο Διαμόρφωση πλάνου ανάκαμψης από καταστροφές
- ο Διαμόρφωση πολιτικής αντιγράφων ασφαλείας
- ο Διαμόρφωση Συστήματος Διαχείρισης της Ασφάλειας των Πληροφοριών (ΣΔΑΠ) με βάση το πρότυπο ISO 27001 & Εκπόνηση Μελέτης Ανάλυσης και Αξιολόγησης Κινδύνων
- ο Διενέργεια δράσεων ενημέρωσης τη μεταφορά τεχνογνωσίας και την διαμόρφωση κουλτούρας ενεργούς ευαισθητοποίησης για τους κινδύνους κυβερνοασφάλειας
- ο Εκπόνηση Μελέτης εξωτερικού και εσωτερικού περιβάλλοντος και την ανάδειξη βέλτιστων πρακτικών στον τομέα της κυβερνοασφάλειας
- ο Διενέργεια ελέγχων διεύθυνσης εξωτερικών δικτύων ή/και ελέγχων εφαρμογών Ιστού ή/και ελέγχων φυσικής ασφάλειας ή/και ελέγχων διαρροής δεδομένων

Την υλοποίηση ή προμήθεια ή συντήρηση τουλάχιστον τεσσάρων (4) από τις παρακάτω λύσεις.

- ο Λύση Διαβάθμισης και Σήμανσης Εγγράφων
- ο Λύση Προστασίας Δεδομένων από Διαρροή
- ο Λύση Διαχείρισης Δικαιωμάτων Εγγράφων
- ο Λύση Διαχείρισης Λογαριασμών και Δικαιωμάτων Πρόσβασης Χρηστών
- ο Λύση Διαχείρισης Προνομιούχων Λογαριασμών Πρόσβασης
- ο Την παροχή υπηρεσιών ανάκαμψης από καταστροφή και λήψης αντιγράφων ασφαλείας
- ο Την παροχή υπηρεσιών Soc
- ο Την παροχή υπηρεσιών Ddos

Την υλοποίηση ή προμήθεια ή συντήρηση τουλάχιστον δύο (2) από τις παρακάτω λύσεις:

- ο Πλατφόρμα Κυβερνοασφάλειας – Εκτεταμένης Ανίχνευσης & Απόκρισης (Cyber Security)
- ο Λύση Προστασίας Βάσεων Δεδομένων
- ο Λύση προστασίας ηλεκτρονικού ταχυδρομείου Mail Security
- ο Λύση Endpoint Detection and Response

Ένα έργο δύναται να καλύπτει περισσότερες από μία από τις παραπάνω κατηγορίες.

Σε περίπτωση συμμετοχής σε ένωση ή κοινοπραξία, λαμβάνεται υπόψη μόνο το ποσοστό που αντιστοιχεί στη συμμετοχή του.

Επιτρέπεται η τεκμηρίωση εμπειρίας που υπερβαίνει τα τρία έτη αλλά δεν ξεπερνά την τελευταία πενταετία για λόγους ανάπτυξης του ανταγωνισμού.

β) να διαθέτουν ομάδα έργου με στελέχη επαρκή σε πλήθος και δεξιότητες για την ανάληψη του Έργου η οποία να αποτελείται τουλάχιστον από τα ακόλουθα βασικά στελέχη (keyexperts):

- έναν (1) Υπεύθυνο Έργου, ο οποίος να διαθέτει Πανεπιστημιακό Τίτλο Σπουδών και τουλάχιστον 10ετή επαγγελματική εμπειρία σε Διαχείριση Έργων Πληροφορικής,
- έναν (1) αναπληρωτή Υπεύθυνο Έργου, ο οποίος να διαθέτει Πανεπιστημιακό Τίτλο Σπουδών και τουλάχιστον 7ετή επαγγελματική εμπειρία σε Διαχείριση Έργων Πληροφορικής,
- τρεις (3) Μηχανικούς Πληροφορικής, οι οποίοι να διαθέτουν τουλάχιστον 5ετή επαγγελματική εμπειρία στην Ασφάλεια των Πληροφοριών,
- **δύο (2) Ειδικούς Ασφάλειας Πληροφοριακών Συστημάτων**, οι οποίοι να διαθέτουν τουλάχιστον 5ετή επαγγελματική εμπειρία σε ασφάλεια πληροφοριακών συστημάτων.
- Έναν υπεύθυνο σχεδιασμού και υλοποίησης, ο οποίος να διαθέτει πτυχίο τριτοβάθμιας εκπαίδευσης στο γνωστικό αντικείμενο που έχει άμεση συνάφεια με τον τύπο των παρεχόμενων υπηρεσιών, στο πλαίσιο του Έργου. Τουλάχιστον 7ετή επαγγελματική εμπειρία στην Ασφάλεια των Πληροφοριών και πιο συγκεκριμένα γύρω από τον Αρχιτεκτονικό Σχεδιασμό Συστημάτων Ασφάλειας Πληροφοριών.

Επισημαίνεται ότι σε περίπτωση που ο υποψήφιος Ανάδοχος αποτελεί Ένωση / Κοινοπραξία, επιτρέπεται η μερική κάλυψη των προϋποθέσεων από τα Μέλη της, αρκεί όμως συνολικά αθροιστικά να καλύπτονται όλες.

Τμήμα 4

Όσον αφορά στην τεχνική και επαγγελματική ικανότητα για το παρόν τμήμα, οι οικονομικοί φορείς θα πρέπει να πληρούν και να τεκμηριώνουν επαρκώς, με ποινή αποκλεισμού, τις παρακάτω ελάχιστες προϋποθέσεις συμμετοχής, στο Διαγωνισμό.

α) Κατά τα τελευταία **τρία (3) έτη** να έχουν ολοκληρώσει επιτυχώς τουλάχιστον δύο (2) αντίστοιχα έργα προϋπολογισμού μεγαλύτερου ή ίσου με 1.000.000 Ευρώ που να περιλαμβάνουν αθροιστικά:

Τουλάχιστον πέντε (5) από τα παρακάτω αντικείμενα:

- ο Διαμόρφωση πολιτικών ορθής χρήσης Πληροφοριακών συστημάτων και εφαρμογών
- ο Διαμόρφωση πλάνου ανάκαμψης από καταστροφές
- ο Διαμόρφωση πολιτικής αντιγράφων ασφαλείας
- ο Διαμόρφωση Συστήματος Διαχείρισης της Ασφάλειας των Πληροφοριών (ΣΔΑΠ) με βάση το πρότυπο ISO 27001 & Εκπόνηση Μελέτης Ανάλυσης και Αξιολόγησης Κινδύνων
- ο Διενέργεια δράσεων ενημέρωσης τη μεταφορά τεχνογνωσίας και την διαμόρφωση κουλτούρας ενεργούς ευαισθητοποίησης για τους κινδύνους κυβερνοασφάλειας
- ο Εκπόνηση Μελέτης εξωτερικού και εσωτερικού περιβάλλοντος και την ανάδειξη βέλτιστων πρακτικών στον τομέα της κυβερνοασφάλειας
- ο Διενέργεια ελέγχων διείσδυσης εξωτερικών δικτύων ή/και ελέγχων εφαρμογών Ιστού ή/και ελέγχων φυσικής ασφάλειας ή/και ελέγχων διαρροής δεδομένων

Την υλοποίηση ή προμήθεια ή συντήρηση τουλάχιστον τεσσάρων (4) από τις παρακάτω λύσεις.

- ο Λύση Διαβάθμισης και Σήμανσης Εγγράφων

- ο Λύση Προστασίας Δεδομένων από Διαρροή
- ο Λύση Διαχείρισης Δικαιωμάτων Εγγράφων
- ο Λύση Διαχείρισης Λογαριασμών και Δικαιωμάτων Πρόσβασης Χρηστών
- ο Λύση Διαχείρισης Προνομιούχων Λογαριασμών Πρόσβασης
- ο Την παροχή υπηρεσιών ανάκαμψης από καταστροφή και λήψης αντιγράφων ασφαλείας
- ο Την παροχή υπηρεσιών Soc
- ο Την παροχή υπηρεσιών Ddos

Την υλοποίηση ή προμήθεια ή συντήρηση τουλάχιστον μίας (1) από τις παρακάτω λύσεις:

- ο Πλατφόρμα Κυβερνοασφάλειας – Εκτεταμένης Ανίχνευσης & Απόκρισης (Cyber Security)
- ο Λύση Προστασίας Βάσεων Δεδομένων

Ένα έργο δύναται να καλύπτει περισσότερες από μία από τις παραπάνω κατηγορίες.

Σε περίπτωση συμμετοχής σε ένωση ή κοινοπραξία, λαμβάνεται υπόψη μόνο το ποσοστό που αντιστοιχεί στη συμμετοχή του.

Επιτρέπεται η τεκμηρίωση εμπειρίας που υπερβαίνει τα τρία έτη αλλά δεν ξεπερνά την τελευταία πενταετία για λόγους ανάπτυξης του ανταγωνισμού.

β) να διαθέτουν ομάδα έργου με στελέχη επαρκή σε πλήθος και δεξιότητες για την ανάληψη του Έργου η οποία να αποτελείται τουλάχιστον από τα ακόλουθα βασικά στελέχη (keyexperts):

- έναν (1) Υπεύθυνο Έργου, ο οποίος να διαθέτει Πανεπιστημιακό Τίτλο Σπουδών και τουλάχιστον 10ετή επαγγελματική εμπειρία σε Διαχείριση Έργων Πληροφορικής,
- έναν (1) αναπληρωτή Υπεύθυνο Έργου, ο οποίος να διαθέτει Πανεπιστημιακό Τίτλο Σπουδών και τουλάχιστον 7ετή επαγγελματική εμπειρία σε Διαχείριση Έργων Πληροφορικής,
- τρεις (3) Μηχανικούς Πληροφορικής, οι οποίοι να διαθέτουν τουλάχιστον 5ετή επαγγελματική εμπειρία στην Ασφάλεια των Πληροφοριών,
- **δύο (2) Ειδικούς Ασφάλειας Πληροφοριακών Συστημάτων**, οι οποίοι να διαθέτουν τουλάχιστον 5ετή επαγγελματική εμπειρία σε ασφάλεια πληροφοριακών συστημάτων.
- Έναν υπεύθυνο σχεδιασμού και υλοποίησης, ο οποίος να διαθέτει πτυχίο τριτοβάθμιας εκπαίδευσης στο γνωστικό αντικείμενο που έχει άμεση συνάφεια με τον τύπο των παρεχόμενων υπηρεσιών, στο πλαίσιο του Έργου. Τουλάχιστον 7ετή επαγγελματική εμπειρία στην Ασφάλεια των Πληροφοριών και πιο συγκεκριμένα γύρω από τον Αρχιτεκτονικό Σχεδιασμό Συστημάτων Ασφάλειας Πληροφοριών.

Επισημαίνεται ότι σε περίπτωση που ο υποψήφιος Ανάδοχος αποτελεί Ένωση / Κοινοπραξία, επιτρέπεται η μερική κάλυψη των προϋποθέσεων από τα Μέλη της, αρκεί όμως συνολικά αθροιστικά να καλύπτονται όλες.

2.2.7 Πρότυπα διασφάλισης ποιότητας

Οι οικονομικοί φορείς που συμμετέχουν στη διαδικασία σύναψης της παρούσας απαιτείται να εξασφαλίζουν την ποιότητα των παρεχόμενων υπηρεσιών και να διαθέτουν:

α) Πρότυπο διαχείρισης ποιότητας ISO 9001:2015 ή ισοδύναμο.

β) Πρότυπο διαχείρισης ασφάλειας πληροφοριών ISO 27001:2013 ή ισοδύναμο.

Η αναθέτουσα αρχή αναγνωρίζει ισοδύναμα πιστοποιητικά που έχουν εκδοθεί από φορείς διαπιστευμένους από ισοδύναμους Οργανισμούς διαπίστευσης, εδρεύοντες και σε άλλα κράτη - μέλη. Επίσης, κάνει δεκτά άλλα αποδεικτικά στοιχεία για ισοδύναμα μέτρα διασφάλισης ποιότητας, εφόσον ο ενδιαφερόμενος οικονομικός φορέας δεν είχε τη δυνατότητα να αποκτήσει τα εν λόγω πιστοποιητικά εντός των σχετικών προθεσμιών για λόγους για τους οποίους δεν ευθύνεται ο ίδιος, υπό την προϋπόθεση ότι ο οικονομικός φορέας αποδεικνύει ότι τα προτεινόμενα μέτρα διασφάλισης ποιότητας πληρούν τα απαιτούμενα πρότυπα διασφάλισης ποιότητας.

Σε περίπτωση ένωσης οικονομικών φορέων, οι παραπάνω ελάχιστες απαιτήσεις καλύπτονται από κάθε μέλος της ένωσης.

2.2.8 Στήριξη στην ικανότητα τρίτων– Υπεργολαβία

2.2.8.1 Στήριξη στην ικανότητα τρίτων

Οι οικονομικοί φορείς μπορούν, όσον αφορά τα κριτήρια της οικονομικής και χρηματοοικονομικής επάρκειας (της παραγράφου 2.2.5) και τα σχετικά με την τεχνική και επαγγελματική ικανότητα (της παραγράφου 2.2.6), να στηρίζονται στις ικανότητες άλλων φορέων, ασχέτως της νομικής φύσης των δεσμών τους με αυτούς. Στην περίπτωση αυτή, αποδεικνύουν ότι θα έχουν στη διάθεσή τους τους αναγκαίους πόρους, με την προσκόμιση της σχετικής δέσμευσης των φορέων στην ικανότητα των οποίων στηρίζονται.

Ειδικά, όσον αφορά στα κριτήρια επαγγελματικής ικανότητας που σχετίζονται με τους τίτλους σπουδών και τα επαγγελματικά προσόντα που ορίζονται στην περίπτωση στ' του Μέρους ΙΙ του Παραρτήματος ΧΙΙ του Προσαρτήματος Α' του ν. 4412/2016 ή με την σχετική επαγγελματική εμπειρία, οι οικονομικοί φορείς, μπορούν να στηρίζονται στις ικανότητες άλλων φορέων, μόνο, εάν οι τελευταίοι θα εκτελέσουν τις εργασίες ή τις υπηρεσίες για τις οποίες απαιτούνται οι συγκεκριμένες ικανότητες

Όταν οι οικονομικοί φορείς στηρίζονται στις ικανότητες άλλων φορέων όσον αφορά τα κριτήρια που σχετίζονται με την απαιτούμενη με τη διακήρυξη οικονομική και χρηματοοικονομική επάρκεια, οι εν λόγω οικονομικοί φορείς και αυτοί στους οποίους στηρίζονται είναι από κοινού υπεύθυνοι για την εκτέλεση της σύμβασης.

Υπό τους ίδιους όρους οι ενώσεις οικονομικών φορέων μπορούν να στηρίζονται στις ικανότητες των συμμετεχόντων στην ένωση ή άλλων φορέων.

Επισημαίνεται ότι σε περίπτωση που ο υποψήφιος Ανάδοχος αποτελεί Ένωση / Κοινοπραξία:

- τα απαιτούμενα στην παρούσα παράγραφο στοιχεία τεκμηρίωσης πρέπει να υποβάλλονται ανάλογα με τη φύση τους χωριστά για κάθε Μέλος της Ένωσης / Κοινοπραξίας

επιτρέπεται η μερική κάλυψη των προϋποθέσεων από τα Μέλη της, αρκεί όμως συνολικά-αθροιστικά να καλύπτονται όλες.

Η αναθέτουσα αρχή ελέγχει αν οι φορείς, στις ικανότητες των οποίων προτίθεται να στηριχθεί ο οικονομικός φορέας, πληρούν κατά περίπτωση τα σχετικά κριτήρια επιλογής και εάν συντρέχουν λόγοι αποκλεισμού της παραγράφου 2.2.3. Ο οικονομικός φορέας υποχρεούται να αντικαταστήσει

έναν φορέα στην ικανότητα του οποίου στηρίζεται, εφόσον ο τελευταίος δεν πληροί το σχετικό κριτήριο επιλογής ή για τον οποίο συντρέχουν λόγοι αποκλεισμού, εντός προθεσμίας τριάντα (30) ημερών από τηνσχετική ηλεκτρονική πρόσκληση της αναθέτουσας αρχής, η οποία απευθύνεται στον οικονομικό φορέα μέσω της λειτουργικότητας «Επικοινωνία» του ΕΣΗΔΗΣ. Ο φορέας που αντικαθιστά φορέα του προηγούμενου εδαφίου δεν επιτρέπεται να αντικατασταθεί εκ νέου.

2.2.8.2 Υπεργολαβία

Ο οικονομικός φορέας αναφέρει στην προσφορά του το τμήμα της σύμβασης που προτίθεται να αναθέσει υπό μορφή υπεργολαβίας σε τρίτους, καθώς και τους υπεργολάβους που προτείνει. Στην περίπτωση που ο προσφέρων αναφέρει στην προσφορά του, ότι προτίθεται να αναθέσει τμήμα(τα) της σύμβασης υπό μορφή υπεργολαβίας σε τρίτους σε ποσοστό που υπερβαίνει το τριάντα τοις εκατό (30%) της συνολικής αξίας τουτμήματος ή τμημάτων της συμφωνίας - πλαίσιο για τα οποία υποβάλουν προσφορά, η αναθέτουσα αρχή ελέγχει ότι δεν συντρέχουν οι λόγοι αποκλεισμού της παραγράφου 2.2.3 της παρούσας. Ο οικονομικός φορέας υποχρεούται να αντικαταστήσει έναν υπεργολάβο, εφόσον συντρέχουν στο πρόσωπό του λόγοι αποκλεισμού της ως άνω παραγράφου 2.2.3.

2.2.9 Κανόνες απόδειξης ποιοτικής επιλογής

Το δικαίωμα συμμετοχής των οικονομικών φορέων και οι όροι και προϋποθέσεις συμμετοχής τους, όπως ορίζονται στις παραγράφους 2.2.1 έως 2.2.8, κρίνονται κατά την υποβολή της προσφοράς δια του ΕΕΕΣ κατά τα οριζόμενα στην παράγραφο 2.2.9.1, κατά την υποβολή των δικαιολογητικών της παραγράφου 2.2.9.2 και κατά τη σύναψη της σύμβασης δια της υπεύθυνης δήλωσης, της περ. δ' της παρ. 3 του άρθρου 105 του ν. 4412/2016.

Στην περίπτωση που ο οικονομικός φορέας στηρίζεται στις ικανότητες άλλων φορέων, σύμφωνα με την παράγραφο 2.2.8 της παρούσας, οι φορείς στην ικανότητα των οποίων στηρίζεται υποχρεούνται να αποδεικνύουν, κατά τα οριζόμενα στις παραγράφους 2.2.9.1 και 2.2.9.2 και κατά τη σύναψη της σύμβασης δια της υπεύθυνης δήλωσης, της περ. δ' της παρ. 3 του άρθρου, ότι δεν συντρέχουν οι λόγοι αποκλεισμού της παραγράφου 2.2.3 της παρούσας και ότι πληρούν τα σχετικά κριτήρια επιλογής κατά περίπτωση (παράγραφοι 2.2.5 και 2.2.6).

Στην περίπτωση που ο οικονομικός φορέας αναφέρει στην προσφορά του ότι προτίθεται να αναθέσει τμήμα(τα) της σύμβασης υπό μορφή υπεργολαβίας σε τρίτους σε ποσοστό που υπερβαίνει το τριάντα τοις εκατό (30%) της συνολικής αξίας της σύμβασης, οι υπεργολάβοι υποχρεούνται να αποδεικνύουν, κατά τα οριζόμενα στις παραγράφους 2.2.9.1 και 2.2.9.2, ότι δεν συντρέχουν οι λόγοι αποκλεισμού της παραγράφου 2.2.3 της παρούσας.

Αν επέλθουν μεταβολές στις προϋποθέσεις τις οποίες οι προσφέροντες δηλώσουν ότι πληρούν, σύμφωνα με το παρόν άρθρο, οι οποίες επέλθουν ή για τις οποίες λάβουν γνώση μετά την συμπλήρωση του ΕΕΕΣ και μέχρι την ημέρα της έγγραφης πρόσκλησης για την σύναψη του συμφωνητικού οι προσφέροντες οφείλουν να ενημερώσουν αμελλητί την αναθέτουσα αρχή.

2.2.9.1 Προκαταρκτική απόδειξη κατά την υποβολή προσφορών

Προς προκαταρκτική απόδειξη ότι οι προσφέροντες οικονομικοί φορείς: α) έχουν δικαίωμα συμμετοχής στη παρούσα διαδικασία σύμφωνα με το άρθρο 2.2.1.2 β) δεν βρίσκονται σε μία από

τις καταστάσεις της παραγράφου 2.2.3 «Λόγοι Αποκλεισμού» και γ) πληρούν τα «Κριτήρια Ποιοτικής Επιλογής» των παραγράφων 2.2.4, 2.2.5, 2.2.6 και 2.2.7 της παρούσης, προσκομίζουν κατά την υποβολή της προσφοράς τους, ως δικαιολογητικό συμμετοχής,

α) υπεύθυνη δήλωση του ν. 1599/1986 με το ακόλουθο περιεχόμενο: ««Δηλώνω υπεύθυνα ότι δεν υπάρχει ρωσική συμμετοχή στην εταιρεία που εκπροσωπώ και εκτελεί τη σύμβαση, σύμφωνα με τους περιορισμούς που περιλαμβάνονται στο άρθρο 5ια του κανονισμού του Συμβουλίου (ΕΕ) αριθ. 833/2014 της 31ης Ιουλίου 2014 σχετικά με περιοριστικά μέτρα λόγω των ενεργειών της Ρωσίας που αποσταθεροποιούν την κατάσταση στην Ουκρανία, όπως τροποποιήθηκε από τον με αριθ. 2022/578 Κανονισμό του Συμβουλίου (ΕΕ) της 8ης Απριλίου 2022. Συγκεκριμένα δηλώνω ότι : (α) ο ανάδοχος που εκπροσωπώ (και καμία από τις εταιρείες που εκπροσωπούν μέλη της κοινοπραξίας μας) δεν είναι Ρώσος υπήκοος, ούτε φυσικό ή νομικό πρόσωπο, οντότητα ή φορέας εγκατεστημένος στη Ρωσία· (β) ο ανάδοχος που εκπροσωπώ (και καμία από τις εταιρείες που εκπροσωπούν μέλη της κοινοπραξίας μας) δεν είναι νομικό πρόσωπο, οντότητα ή φορέας του οποίου τα δικαιώματα ιδιοκτησίας κατέχει άμεσα ή έμμεσα σε ποσοστό άνω του πενήντα τοις εκατό (50%) οντότητα αναφερόμενη στο στοιχείο α) της παρούσας παραγράφου· (γ) ούτε ο υπεύθυνος δηλώνων ούτε η εταιρεία που εκπροσωπώ δεν είμαστε φυσικό ή νομικό πρόσωπο, οντότητα ή όργανο που ενεργεί εξ ονόματος ή κατ' εντολή οντότητας που αναφέρεται στο σημείο(α) ή (β) παραπάνω, (δ) δεν υπάρχει συμμετοχή φορέων και οντοτήτων που απαριθμούνται στα ανωτέρω στοιχεία α) έως γ), άνω του 10 % της αξίας της σύμβασης των υπερβολάβων, προμηθευτών ή φορέων στις ικανότητες των οποίων να στηρίζεται ο ανάδοχος τον οποίον εκπροσωπώ.»

β) το προβλεπόμενο από το άρθρο 79 παρ. 1 και 3 του ν. 4412/2016 Ευρωπαϊκό Ενιαίο Έγγραφο Σύμβασης (ΕΕΕΣ), σύμφωνα με το επισυναπτόμενο στην παρούσα ΕΥΡΩΠΑΙΚΟ ΕΝΙΑΙΟ ΕΓΓΡΑΦΟ ΣΥΜΒΑΣΗΣ (ΕΕΕΣ) **ΠΑΡΑΡΤΗΜΑ ΙΙΙ – ΕΥΡΩΠΑΙΚΟ ΕΝΙΑΙΟ ΕΓΓΡΑΦΟ ΣΥΜΒΑΣΗΣ (ΕΕΕΣ)**, το οποίο ισοδυναμεί με ενημερωμένη υπεύθυνη δήλωση, με τις συνέπειες του ν. 1599/1986. Το ΕΕΕΣ καταρτίζεται βάσει του τυποποιημένου εντύπου του Παραρτήματος 2 του Κανονισμού (ΕΕ) 2016/7 και συμπληρώνεται από τους προσφέροντες οικονομικούς φορείς σύμφωνα με τις οδηγίες του Παραρτήματος 1.

Επισημαίνεται ότι οι προσφέροντες για το μέρος IV Κριτήρια επιλογής του ΕΕΕΣ συμπληρώνουν μόνο την **ενότητα α «Γενική ένδειξη για όλα τα κριτήρια επιλογής».**

Το ΕΕΕΣ φέρει υπογραφή με ημερομηνία εντός του χρονικού διαστήματος κατά το οποίο μπορούν να υποβάλλονται προσφορές. Αν στο διάστημα που μεσολαβεί μεταξύ της ημερομηνίας υπογραφής του ΕΕΕΣ και της καταληκτικής ημερομηνίας υποβολής προσφορών έχουν επέλθει μεταβολές στα δηλωθέντα στοιχεία, εκ μέρους του, στο ΕΕΕΣ, ο οικονομικός φορέας αποσύρει την προσφορά του, χωρίς να απαιτείται απόφαση της αναθέτουσας αρχής. Στη συνέχεια μπορεί να την υποβάλει εκ νέου με επίκαιρο ΕΕΕΣ. Ο οικονομικός φορέας δύναται να διευκρινίζει τις δηλώσεις και πληροφορίες που παρέχει στο ΕΕΕΣ με συνοδευτική υπεύθυνη δήλωση, την οποία υποβάλλει μαζί με το ΕΕΕΣ.

Κατά την υποβολή του ΕΕΕΣ, καθώς και της συνοδευτικής υπεύθυνης δήλωσης, είναι δυνατή, με μόνη την υπογραφή του κατά περίπτωση εκπροσώπου του οικονομικού φορέα, η προκαταρκτική απόδειξη των λόγων αποκλεισμού που αναφέρονται στην παράγραφο 2.2.3 της παρούσας, για το

σύνολο των φυσικών προσώπων που είναι μέλη του διοικητικού, διευθυντικού ή εποπτικού οργάνου του ή έχουν εξουσία εκπροσώπησης, λήψης αποφάσεων ή ελέγχου σε αυτόν.

Ως εκπρόσωπος του οικονομικού φορέα νοείται ο νόμιμος εκπρόσωπος αυτού, όπως προκύπτει από το ισχύον καταστατικό ή το πρακτικό εκπροσώπησης του κατά το χρόνο υποβολής της προσφοράς ή το αρμοδίως εξουσιοδοτημένο φυσικό πρόσωπο να εκπροσωπεί τον οικονομικό φορέα για διαδικασίες σύναψης συμβάσεων ή για συγκεκριμένη διαδικασία σύναψης σύμβασης.

Στην περίπτωση υποβολής προσφοράς από ένωση οικονομικών φορέων, το Ευρωπαϊκό Ενιαίο Έγγραφο Σύμβασης (ΕΕΕΣ), υποβάλλεται χωριστά από κάθε μέλος της ένωσης. Στο ΕΕΕΣ απαραίτητως πρέπει να προσδιορίζεται η έκταση και το είδος της συμμετοχής του (συμπεριλαμβανομένης της κατανομής αμοιβής μεταξύ τους) κάθε μέλους της ένωσης, καθώς και ο εκπρόσωπος/συντονιστής αυτής.

Ο οικονομικός φορέας φέρει την ειδική υποχρέωση, να δηλώσει, μέσω του ΕΕΕΣ, την κατάστασή του σε σχέση με τους λόγους που προβλέπονται στο άρθρο 73 του ν. 4412/2016 και παραγράφου 2.2.3 της παρούσης και ταυτόχρονα να επικαλεσθεί και τυχόν ληφθέντα μέτρα προς αποκατάσταση της αξιοπιστίας του.

Ιδίως επισημαίνεται ότι, κατά την απάντηση οικονομικού φορέα στο σχετικό πεδίο του ΕΕΕΣ για τυχόν σύναψη συμφωνιών με άλλους οικονομικούς φορείς με στόχο τη στρέβλωση του ανταγωνισμού, η συνδρομή περιστάσεων, όπως η πάροδος της τριετούς περιόδου της ισχύος του λόγου αποκλεισμού (παραγράφου 10 του άρθρου 73) ή η εφαρμογή της διάταξης της παραγράφου 3β του άρθρου 44 του ν. 3959/2011, σύμφωνα με την περ. γ της παραγράφου 2.2.3.3 της παρούσης, αναλύεται στο σχετικό πεδίο που προβάλλει κατόπιν θετικής απάντησης.

Όσον αφορά στις υποχρεώσεις του όσον αφορά στην καταβολή φόρων ή εισφορών κοινωνικής ασφάλισης (περ. α' και β' της παρ. 2 του άρθρου 73 του ν. 4412/2016) αυτές θεωρείται ότι δεν έχουν αθετηθεί εφόσον δεν έχουν καταστεί ληξιπρόθεσμες ή εφόσον έχουν υπαχθεί σε δεσμευτικό διακανονισμό που τηρείται. Στην περίπτωση αυτή, ο οικονομικός φορέας δεν υποχρεούται να απαντήσει καταφατικά στο σχετικό πεδίο του ΕΕΕΣ με το οποίο ερωτάται εάν ο οικονομικός φορέας έχει ανεκπλήρωτες υποχρεώσεις όσον αφορά στην καταβολή φόρων ή εισφορών κοινωνικής ασφάλισης ή, κατά περίπτωση, εάν έχει αθετήσει τις παραπάνω υποχρεώσεις του.

2.2.9.2 Αποδεικτικά μέσα- Δικαιολογητικά προσωρινού αναδόχου

Α. Για την απόδειξη του δικαιώματος συμμετοχής κατά την παράγραφο 2.2.1.2, της μη συνδρομής λόγων αποκλεισμού κατ' άρθρο [2.2.3](#) και της πλήρωσης των κριτηρίων ποιοτικής επιλογής κατά τις παραγράφους [2.2.4](#), [2.2.5](#), [2.2.6](#) και [2.2.7](#), οι οικονομικοί φορείς προσκομίζουν τα δικαιολογητικά του παρόντος. Η προσκόμιση των εν λόγω δικαιολογητικών γίνεται κατά τα οριζόμενα στην παράγραφο 3.2 από τον προσωρινό ανάδοχο. Η αναθέτουσα αρχή μπορεί να ζητεί από προσφέροντες, σε οποιοδήποτε χρονικό σημείο κατά τη διάρκεια της διαδικασίας, να υποβάλλουν όλα ή ορισμένα δικαιολογητικά, όταν αυτό απαιτείται για την ορθή διεξαγωγή της διαδικασίας.

Οι οικονομικοί φορείς δεν υποχρεούνται να υποβάλλουν δικαιολογητικά ή άλλα αποδεικτικά στοιχεία, αν και στο μέτρο που η αναθέτουσα αρχή έχει τη δυνατότητα να λαμβάνει τα πιστοποιητικά ή τις

συναφείς πληροφορίες απευθείας μέσω πρόσβασης σε εθνική βάση δεδομένων σε οποιοδήποτε κράτος - μέλος της Ένωσης, η οποία διατίθεται δωρεάν, όπως εθνικό μητρώο συμβάσεων, εικονικό φάκελο επιχείρησης, ηλεκτρονικό σύστημα αποθήκευσης εγγράφων ή σύστημα προεπιλογής. Η δήλωση για την πρόσβαση σε εθνική βάση δεδομένων εμπεριέχεται στο Ευρωπαϊκό Ενιαίο Έγγραφο Σύμβασης (ΕΕΕΣ), στο οποίο περιέχονται επίσης οι πληροφορίες που απαιτούνται για τον συγκεκριμένο σκοπό, όπως η ηλεκτρονική διεύθυνση της βάσης δεδομένων, τυχόν δεδομένα αναγνώρισης και, κατά περίπτωση, η απαραίτητη δήλωση συναίνεσης.

Οι οικονομικοί φορείς δεν υποχρεούνται να υποβάλουν δικαιολογητικά, όταν η αναθέτουσα αρχή που έχει αναθέσει τη σύμβαση διαθέτει ήδη τα ως άνω δικαιολογητικά και αυτά εξακολουθούν να ισχύουν.

Τα δικαιολογητικά του παρόντος υποβάλλονται και γίνονται αποδεκτά σύμφωνα με την παράγραφο 2.4.2.5 και 3.2 της παρούσας.

Τα αποδεικτικά έγγραφα συντάσσονται στην ελληνική γλώσσα ή συνοδεύονται από επίσημη μετάφρασή τους στην ελληνική γλώσσα σύμφωνα με την παράγραφο [2.1.4](#).

B.1.

Για την απόδειξη του δικαιώματος συμμετοχής κατά την παράγραφο 2.2.1.2. οι προσφέροντες οικονομικοί φορείς προσκομίζουν επικαιροποιημένη υπεύθυνη δήλωση του ν. 1599/1986, της παρούσας, με περιεχόμενο το αναφερόμενο στην παράγραφο 2.2.9.1 (α) της παρούσας.

Για την απόδειξη της μη συνδρομής των λόγων αποκλεισμού της παραγράφου [2.2.3](#) οι προσφέροντες οικονομικοί φορείς προσκομίζουν αντίστοιχα τα δικαιολογητικά που αναφέρονται παρακάτω:

Αν το αρμόδιο για την έκδοση των ανωτέρω κράτος-μέλος ή χώρα δεν εκδίδει τέτοιου είδους έγγραφα ή πιστοποιητικά ή όπου το έγγραφο ή τα πιστοποιητικά αυτά δεν καλύπτουν όλες τις περιπτώσεις που αναφέρονται στις παραγράφους **2.2.3.1** και 2.2.3.2 περ. α' και β', καθώς και στην περ. β' της παραγράφου 2.2.3.3, τα έγγραφα ή τα πιστοποιητικά μπορεί να αντικαθίστανται από ένορκη βεβαίωση ή, στα κράτη - μέλη ή στις χώρες όπου δεν προβλέπεται ένορκη βεβαίωση, από υπεύθυνη δήλωση του ενδιαφερομένου ενώπιον αρμόδιας δικαστικής ή διοικητικής αρχής, συμβολαιογράφου ή αρμόδιου επαγγελματικού ή εμπορικού οργανισμού του κράτους - μέλους ή της χώρας καταγωγής ή της χώρας όπου είναι εγκατεστημένος ο οικονομικός φορέας. Οι αρμόδιες δημόσιες αρχές παρέχουν, όπου κρίνεται αναγκαίο, επίσημη δήλωση στην οποία αναφέρεται ότι δεν εκδίδονται τα έγγραφα ή τα πιστοποιητικά της παρούσας παραγράφου ή ότι τα έγγραφα αυτά δεν καλύπτουν όλες τις περιπτώσεις που αναφέρονται στις παραγράφους 2.2.3.1 και **2.2.3.2** περ. α' και β', καθώς και στην περ. β' της παραγράφου 2.2.3.3. Οι επίσημες δηλώσεις καθίστανται διαθέσιμες μέσω του επιγραμμικού αποθετηρίου πιστοποιητικών (e-Certis) του άρθρου 81 του ν. 4412/2016.

Ειδικότερα οι οικονομικοί φορείς προσκομίζουν:

α) για την παράγραφο **2.2.3.1** απόσπασμα του σχετικού μητρώου, όπως του ποινικού μητρώου ή, ελλείψει αυτού, ισοδύναμο έγγραφο που εκδίδεται από αρμόδια δικαστική ή διοικητική αρχή του κράτους-μέλους ή της χώρας καταγωγής ή της χώρας όπου είναι εγκατεστημένος ο οικονομικός φορέας, από το οποίο προκύπτει ότι πληρούνται αυτές οι προϋποθέσεις, που να έχει εκδοθεί έως τρεις (3) μήνες πριν από την υποβολή του.

Η υποχρέωση προσκόμισης του ως άνω αποσπάσματος αφορά και στα μέλη του διοικητικού, διευθυντικού ή εποπτικού οργάνου του εν λόγω οικονομικού φορέα ή στα πρόσωπα που έχουν εξουσία εκπροσώπησης, λήψης αποφάσεων ή ελέγχου σε αυτό κατά τα ειδικότερα αναφερόμενα στην ως άνω παράγραφο 2.2.3.1,

β) για την παράγραφο **2.2.3.2** πιστοποιητικό που εκδίδεται από την αρμόδια αρχή του οικείου κράτους - μέλους ή χώρας, που να είναι εν ισχύ κατά το χρόνο υποβολής του, άλλως, στην περίπτωση που δεν αναφέρεται σε αυτό χρόνος ισχύος, που να έχει εκδοθεί έως τρεις (3) μήνες πριν από την υποβολή του

Ιδίως οι οικονομικοί φορείς που είναι εγκατεστημένοι στην Ελλάδα προσκομίζουν:

i) Για την απόδειξη της εκπλήρωσης των φορολογικών υποχρεώσεων της παραγράφου 2.2.3.2 περίπτωση α' αποδεικτικό ενημερότητας εκδιδόμενο από την Α.Α.Δ.Ε.

ii) Για την απόδειξη της εκπλήρωσης των υποχρεώσεων προς τους οργανισμούς κοινωνικής ασφάλισης της παραγράφου **2.2.3.2** περίπτωση α' πιστοποιητικό εκδιδόμενο από τον e-ΕΦΚΑ. Επιπλέον προσκομίζεται υπεύθυνη δήλωση του οικονομικού φορέα αναφορικά με τους οργανισμούς κοινωνικής ασφάλισης (στην περίπτωση που ο οικονομικός φορέας έχει την εγκατάστασή του στην Ελλάδα αφορά Οργανισμούς κύριας και επικουρικής ασφάλισης) στους οποίους οφείλει να καταβάλει εισφορές.

iii) Για την παράγραφο 2.2.3.2 περίπτωση α', πλέον των ως άνω πιστοποιητικών, υπεύθυνη δήλωση ότι δεν έχει εκδοθεί δικαστική ή διοικητική απόφαση με τελεσίδικη και δεσμευτική ισχύ για την αθέτηση των υποχρεώσεων τους όσον αφορά στην καταβολή φόρων ή εισφορών κοινωνικής ασφάλισης.

γ) για την παράγραφο 2.2.3.3 περίπτωση β' πιστοποιητικό που εκδίδεται από την αρμόδια αρχή του οικείου κράτους - μέλους ή χώρας, που να έχει εκδοθεί έως τρεις (3) μήνες πριν από την υποβολή του.

Ιδίως οι οικονομικοί φορείς που είναι εγκατεστημένοι στην Ελλάδα προσκομίζουν:

i) Ενιαίο Πιστοποιητικό Δικαστικής Φερεγγυότητας από το αρμόδιο Πρωτοδικείο, από το οποίο προκύπτει ότι δεν τελούν υπό πτώχευση, πτωχευτικό συμβιβασμό ή υπό αναγκαστική διαχείριση ή δικαστική εκκαθάριση ή ότι δεν έχουν υπαχθεί σε διαδικασία εξυγίανσης. Για τις ΙΚΕ προσκομίζεται επιπλέον και πιστοποιητικό του Γ.Ε.Μ.Η. περί μη έκδοσης απόφασης λύσης ή κατάθεσης αίτησης λύσης του νομικού προσώπου, ενώ για τις ΕΠΕ προσκομίζεται επιπλέον πιστοποιητικό μεταβολών.

ii) Πιστοποιητικό του Γ.Ε.Μ.Η. από το οποίο προκύπτει ότι το νομικό πρόσωπο δεν έχει λυθεί και τεθεί υπό εκκαθάριση με απόφαση των εταίρων.

iii) Εκτύπωση της καρτέλας "Στοιχεία Μητρώου/ Επιχείρησης" από την ηλεκτρονική πλατφόρμα της Ανεξάρτητης Αρχής Δημοσίων Εσόδων, όπως αυτά εμφανίζονται στο taxisnet, από την οποία να προκύπτει η μη αναστολή της επιχειρηματικής δραστηριότητάς τους.

Προκειμένου για τα σωματεία και τους συνεταιρισμούς, το Ενιαίο Πιστοποιητικό Δικαστικής Φερεγγυότητας εκδίδεται για τα σωματεία από το αρμόδιο Πρωτοδικείο, και για τους συνεταιρισμούς για το χρονικό διάστημα έως τις 31.12.2019 από το Ειρηνοδικείο και μετά την παραπάνω ημερομηνία από το Γ.Ε.Μ.Η.

δ) Για τις λοιπές περιπτώσεις της παραγράφου 2.2.3.3, υπεύθυνη δήλωση του προσφέροντος οικονομικού φορέα ότι δεν συντρέχουν στο πρόσωπό του οι οριζόμενοι στην παράγραφο λόγοι αποκλεισμού

ε) για την παράγραφο 2.2.3.8 υπεύθυνη δήλωση του προσφέροντος οικονομικού φορέα περί μη επιβολής σε βάρος του της κύρωσης του οριζόντιου αποκλεισμού, σύμφωνα τις διατάξεις της κείμενης νομοθεσίας.

στ) για την παράγραφο [2.2.3.4](#), δικαιολογητικά ονομαστικοποίησης των μετοχών, που καθορίζονται κατωτέρω, εφόσον ο προσωρινός ανάδοχος είναι ανώνυμη εταιρία ή νομικό πρόσωπο στη μετοχική σύνθεση του οποίου συμμετέχει ανώνυμη εταιρία ή νομικό πρόσωπο της αλλοδαπής που αντιστοιχεί σε ανώνυμη εταιρία (πλην των περιπτώσεων που αναφέρθηκαν στην παρ. [2.2.3.4](#) της παρούσας ανωτέρω).

Συγκεκριμένα, προσκομίζονται:

i) Για την απόδειξη της εξαίρεσης από την υποχρέωση ονομαστικοποίησης των μετοχών τους κατά την περ. α) της παραγράφου 2.2.3.4 βεβαίωση του αρμοδίου Χρηματιστηρίου.

ii) Όσον αφορά την εξαίρεση της περ. β) της παραγράφου [2.2.3.4](#), για την απόδειξη του ελέγχου δικαιωμάτων ψήφου υπεύθυνη δήλωση της ελεγχόμενης εταιρείας και, εάν αυτή είναι διαφορετική του προσωρινού αναδόχου, πρόσθετη υπεύθυνη δήλωση του τελευταίου, στις οποίες αναφέρονται οι επιχειρήσεις επενδύσεων, οι εταιρείες διαχείρισης κεφαλαίων/ενεργητικού ή κεφαλαίων επιχειρηματικών συμμετοχών, ανά περίπτωση και το συνολικό ποσοστό των δικαιωμάτων ψήφου που ελέγχουν στην ελεγχόμενη από αυτές εταιρεία. Οι υπεύθυνες αυτές δηλώσεις συνοδεύονται υποχρεωτικά από βεβαίωση ή άλλο έγγραφο από το οποίο προκύπτει ότι οι ελέγχουσες τα δικαιώματα ψήφου εταιρείες είναι εποπτευόμενες κατά τα οριζόμενα στην παράγραφο [2.2.3.4](#).

iii) Δικαιολογητικά ονομαστικοποίησης μετοχών του προσωρινού αναδόχου:

- Πιστοποιητικό αρμόδιας αρχής του κράτους της έδρας, από το οποίο να προκύπτει ότι οι μετοχές είναι ονομαστικές, που να έχει εκδοθεί έως τριάντα (30) εργάσιμες ημέρες πριν από την υποβολή του.

- Αναλυτική κατάσταση με τα στοιχεία των μετόχων της εταιρείας και τον αριθμό των μετοχών κάθε μετόχου (μετοχολόγιο), όπως τα στοιχεία αυτά είναι καταχωρημένα στο βιβλίο μετόχων της εταιρείας, το πολύ τριάντα (30) εργάσιμες ημέρες πριν από την ημέρα υποβολής της προσφοράς.

Ειδικότερα:

- Όσον αφορά στις **εγκατεστημένες στην Ελλάδα ανώνυμες εταιρείες** υποβάλλεται πιστοποιητικό του Γ.Ε.Μ.Η. από το οποίο να προκύπτει ότι οι μετοχές τους είναι ονομαστικές και αναλυτική κατάσταση με τα στοιχεία των μετόχων της εταιρείας και τον αριθμό των μετοχών κάθε μετόχου (μετοχολόγιο), όπως τα στοιχεία αυτά είναι καταχωρημένα στο βιβλίο μετόχων της εταιρείας, το πολύ τριάντα (30) εργάσιμες ημέρες πριν από την ημέρα υποβολής της προσφοράς.

- Όσον αφορά στις **αλλοδαπές ανώνυμες εταιρείες ή αλλοδαπά νομικά πρόσωπα που αντιστοιχούν σε ανώνυμες εταιρείες**:

Α) εφόσον έχουν κατά το δίκαιο της έδρας τους ονομαστικές μετοχές, προσκομίζουν :

- i) Πιστοποιητικό αρμόδιας αρχής του κράτους της έδρας, από το οποίο να προκύπτει ότι οι μετοχές τους είναι ονομαστικές
- ii) Αναλυτική κατάσταση μετόχων, με τον αριθμό των μετοχών του κάθε μετόχου, όπως τα στοιχεία αυτά είναι καταχωρημένα στο βιβλίο μετόχων της εταιρείας με ημερομηνία το πολύ 30 εργάσιμες ημέρες πριν την υποβολή της προσφοράς.
- iii) Κάθε άλλο στοιχείο από το οποίο να προκύπτει η ονομαστικοποίηση μέχρι φυσικού προσώπου των μετοχών, που έχει συντελεστεί τις τελευταίες 30 (τριάντα) εργάσιμες ημέρες πριν την υποβολή της προσφοράς.

Β) εφόσον δεν έχουν υποχρέωση ονομαστικοποίησης μετοχών ή δεν προβλέπεται η ονομαστικοποίηση των μετοχών, προσκομίζουν:

- i) βεβαίωση περί μη υποχρέωσης ονομαστικοποίησης των μετοχών από αρμόδια αρχή, εφόσον υπάρχει σχετική πρόβλεψη, διαφορετικά προσκομίζεται υπεύθυνη δήλωση του διαγωνιζόμενου. Για την περίπτωση μη πρόβλεψης ονομαστικοποίησης προσκομίζεται υπεύθυνη δήλωση του διαγωνιζόμενου
- ii) έγκυρη και ενημερωμένη κατάσταση προσώπων που κατέχουν τουλάχιστον 1% των μετοχών ή δικαιωμάτων ψήφου,
- iii) εάν δεν τηρείται τέτοια κατάσταση, προσκομίζεται σχετική κατάσταση προσώπων, που κατέχουν τουλάχιστον ένα τοις εκατό (1%) των μετοχών ή δικαιωμάτων ψήφου, σύμφωνα με την τελευταία Γενική Συνέλευση, αν τα πρόσωπα αυτά είναι γνωστά στην εταιρεία. Σε αντίθετη περίπτωση, η εταιρεία αιτιολογεί τους λόγους που δεν είναι γνωστά τα ως άνω πρόσωπα, η δε αναθέτουσα αρχή δεν διαθέτει διακριτική ευχέρεια κατά την κρίση της αιτιολογίας αυτής. Εναπόκειται στην αναθέτουσα αρχή να αποδείξει τη δυνατότητα της εταιρείας να υποβάλλει την προαναφερόμενη κατάσταση, διαφορετικά η μη υποβολή της σχετικής κατάστασης δεν επιφέρει έννομες συνέπειες σε βάρος της εταιρείας.

Όλα τα ανωτέρω έγγραφα πρέπει να είναι επικυρωμένα από την κατά νόμον αρμόδια αρχή του κράτους της έδρας του υποψηφίου και να συνοδεύονται από επίσημη μετάφραση στην ελληνική.

Ελλείψεις στα δικαιολογητικά ονομαστικοποίησης των μετοχών συμπληρώνονται κατά την παράγραφο [3.1.2](#) της παρούσας.

Η αναθέτουσα αρχή ελέγχει επίσης, επί ποινή απαραδέκτου της προσφοράς, εάν στη διαδικασία συμμετέχει εξωχώρια εταιρεία από «μη συνεργάσιμα κράτη στον φορολογικό τομέα» κατά την έννοια των παρ. 3 και 4 του άρθρου 65 του ν. 4172/2013, καθώς και από κράτη που έχουν προνομιακό φορολογικό καθεστώς, όπως αυτά ορίζονται στον κατάλογο της απόφασης της παρ. 7 του άρθρου 65 του ως άνω Κώδικα, κατά τα αναφερόμενα στην περίπτωση α της παραγράφου 4 του άρθρου 4 του ν. 3310/2005. Επιπλέον ο προσωρινός ανάδοχος, πέραν των ως άνω δικαιολογητικών ονομαστικοποίησης, προσκομίζει κατά το στάδιο κατακύρωσης υπεύθυνη δήλωση ότι δεν είναι εξωχώρια εταιρεία, κατά την ανωτέρω έννοια και δεν εμπίπτει στις διατάξεις της παρ. 4 εδαφ. α & β του άρθρου 4 του Ν. 3310/2005 όπως ισχύει.

Β. 2. Για την απόδειξη της απαίτησης της παραγράφου 2.2.4 (απόδειξη καταλληλότητας για την άσκηση επαγγελματικής δραστηριότητας) οι οικονομικοί φορείς προσκομίζουν τα αναφερόμενα στον κατωτέρω πίνακα :

1.	<p>Οι οικονομικοί φορείς που συμμετέχουν στη διαδικασία σύναψης της παρούσας απαιτείται να ασκούν επαγγελματική δραστηριότητα συναφή με το αντικείμενο των προς παροχή υπηρεσιών, ήτοι ανάπτυξη και υποστήριξη εφαρμογών λογισμικού</p> <p>Οι οικονομικοί φορείς οφείλουν να αποδείξουν το ανωτέρω κριτήριο ποιοτικής επιλογής υποβάλλοντας τα ακόλουθα στοιχεία τεκμηρίωσης:</p>
1.1	<p>Πιστοποιητικό/βεβαίωση του οικείου επαγγελματικού (ή εμπορικού) μητρώου του κράτους εγκατάστασης. Οι οικονομικοί φορείς που είναι εγκατεστημένοι σε κράτος μέλος της Ευρωπαϊκής Ένωσης προσκομίζουν πιστοποιητικό/βεβαίωση του αντίστοιχου επαγγελματικού (ή εμπορικού) μητρώου του Παραρτήματος XI του Προσαρτήματος Α' του ν. 4412/2016, με το οποίο πιστοποιείται αφενός η εγγραφή τους σε αυτό και αφετέρου το ειδικό επάγγελμά τους. Στην περίπτωση που χώρα δεν τηρεί τέτοιο μητρώο, το έγγραφο ή το πιστοποιητικό μπορεί να αντικαθίσταται από ένορκη βεβαίωση ή, στα κράτη - μέλη ή στις χώρες όπου δεν προβλέπεται ένορκη βεβαίωση, από υπεύθυνη δήλωση του ενδιαφερομένου ενώπιον αρμόδιας δικαστικής ή διοικητικής αρχής, συμβολαιογράφου ή αρμόδιου επαγγελματικού οργανισμού της χώρας καταγωγής ή της χώρας όπου είναι εγκατεστημένος ο οικονομικός φορέας ότι δεν τηρείται τέτοιο μητρώο και ότι ασκεί τη δραστηριότητα που απαιτείται για την εκτέλεση του αντικείμενου της υπό ανάθεση σύμβασης.</p> <p>Οι εγκατεστημένοι στην Ελλάδα οικονομικοί φορείς προσκομίζουν βεβαίωση εγγραφής στο οικείο επαγγελματικό μητρώο ή πιστοποιητικό που εκδίδεται από την οικεία υπηρεσία του Γ.Ε.ΜΗ.</p>

Επισημαίνεται ότι, τα δικαιολογητικά που αφορούν στην απόδειξη της απαίτησης της 2.2.4 (απόδειξη καταλληλότητας για την άσκηση επαγγελματικής δραστηριότητας) γίνονται αποδεκτά, εφόσον έχουν εκδοθεί έως τριάντα (30) εργάσιμες ημέρες πριν από την υποβολή τους, εκτός αν, σύμφωνα με τις ειδικότερες διατάξεις αυτών, φέρουν συγκεκριμένο χρόνο ισχύος.

Β.3. Για την απόδειξη της οικονομικής και χρηματοοικονομικής επάρκειας της παραγράφου 2.2.5 οι οικονομικοί φορείς προσκομίζουν τα αναφερόμενα στον κατωτέρω πίνακα:

2.	<p>Οι οικονομικοί φορείς που συμμετέχουν στη διαδικασία σύναψης της παρούσας απαιτείται να έχουν μέσο γενικό ετήσιο κύκλο εργασιών για τις τρεις (3) τελευταίες οικονομικές χρήσεις (2020-2021-2022) ή, τις οικονομικές χρήσεις κατά τις οποίες ο οικονομικός φορέας δραστηριοποιείται, αν είναι λιγότερες από τρεις συνολικά κατ' ελάχιστον ίσο με το 200% του</p>
----	---

	<p>προϋπολογισμού του/των υπό ανάθεση Τμήματος/Τμημάτων, για το/τα οποίο/οποία υποβάλλει προσφορά.</p> <p>Οι οικονομικοί φορείς οφείλουν να αποδείξουν το ανωτέρω κριτήριο ποιοτικής επιλογής υποβάλλοντας τα ακόλουθα στοιχεία τεκμηρίωσης:</p>
2.1	<p>Ισολογισμούς σύμφωνα με την περί εταιρειών νομοθεσία της χώρας όπου είναι εγκατεστημένοι, των τελευταίων τριών (3) κλεισμένων διαχειριστικών χρήσεων, σε περίπτωση που υποχρεούται στην έκδοση Ισολογισμών φορολογικά έγγραφα για την επιβεβαίωση του κύκλου εργασιών του ή Ένορκη Βεβαίωση του συνολικού ύψους του ετήσιου κύκλου εργασιών, σε περίπτωση που δεν υποχρεούται στην έκδοση Ισολογισμών τραπεζική βεβαίωση για την πιστοληπτική ικανότητα του οικονομικού φορέα (ημεδαπού ή αλλοδαπού) ή/ και αποσπάσματα οικονομικών καταστάσεων, τα οποία αντιστοιχούν, σε κάθε περίπτωση, στα κριτήρια οικονομικής και χρηματοοικονομικής επάρκειας που έχουν τεθεί στο άρθρο 2.2.5.</p> <p>Εάν ο οικονομικός φορέας, για βάσιμο λόγο, δεν είναι σε θέση να προσκομίσει τα ανωτέρω δικαιολογητικά, μπορεί να αποδεικνύει την οικονομική και χρηματοοικονομική του επάρκεια με οποιοδήποτε άλλο κατάλληλο έγγραφο.</p>

Β.4. Για την απόδειξη της τεχνικής ικανότητας της παραγράφου 2.2.6 οι οικονομικοί φορείς προσκομίζουν τα αναφερόμενα στον κατωτέρω πίνακα:

3	<p>Οι οικονομικοί φορείς που συμμετέχουν στη διαδικασία σύναψης της παρούσας απαιτείται να διαθέτουν την κατάλληλα τεκμηριωμένη και αποδεδειγμένη επαγγελματική ικανότητα στην υλοποίηση έργων αντίστοιχου μεγέθους και πολυπλοκότητας με το υπό ανάθεση Έργο σύμφωνα με την παρ.2.2.6.</p> <p>Οι οικονομικοί φορείς οφείλουν να αποδείξουν το ανωτέρω κριτήριο ποιοτικής επιλογής υποβάλλοντας τα ακόλουθα στοιχεία τεκμηρίωσης:</p>																						
3.1	<p>Κατάλογο των κυριότερων συναφών έργων που υλοποίησε επιτυχώς ο οικονομικός φορέας με βάση τα προβλεπόμενα στην παρ.2.2.6, σύμφωνα με το ακόλουθο Υπόδειγμα:</p> <table border="1"> <thead> <tr> <th>Α / Α</th><th>ΠΕΛΑΤΗΣ</th><th>ΣΥΝΤΟΜΗ ΠΕΡΙΓΡΑΦΗ ΤΟΥ ΕΡΓΟΥ</th><th>ΔΙΑΡΚΕΙΑ ΕΚΤΕΛΕΣΗΣ ΕΡΓΟΥ</th><th>ΠΡΟΫΠΟ - ΛΟΓΙΣΜΟΣ</th><th>ΣΥΝΟΠΤΙΚΗ ΠΕΡΙΓΡΑΦΗ ΣΥΝΕΙΣΦΟΡΑΣ ΣΤΟ ΕΡΓΟ (αντικείμενο)</th><th>ΠΟΣΟΣΤΟ ΣΥΜΜΕΤΟΧΗΣ ΣΤΟ ΕΡΓΟ (προϋπολογισμός)</th><th>ΣΤΟΙΧΕΙΟ ΤΕΚΜΗΡΙΩΣΗΣ (τύπος & ημ/νία)</th></tr> </thead> <tbody> <tr> <td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> </tbody> </table> <p>όπου «ΣΤΟΙΧΕΙΟ ΤΕΚΜΗΡΙΩΣΗΣ»:</p>							Α / Α	ΠΕΛΑΤΗΣ	ΣΥΝΤΟΜΗ ΠΕΡΙΓΡΑΦΗ ΤΟΥ ΕΡΓΟΥ	ΔΙΑΡΚΕΙΑ ΕΚΤΕΛΕΣΗΣ ΕΡΓΟΥ	ΠΡΟΫΠΟ - ΛΟΓΙΣΜΟΣ	ΣΥΝΟΠΤΙΚΗ ΠΕΡΙΓΡΑΦΗ ΣΥΝΕΙΣΦΟΡΑΣ ΣΤΟ ΕΡΓΟ (αντικείμενο)	ΠΟΣΟΣΤΟ ΣΥΜΜΕΤΟΧΗΣ ΣΤΟ ΕΡΓΟ (προϋπολογισμός)	ΣΤΟΙΧΕΙΟ ΤΕΚΜΗΡΙΩΣΗΣ (τύπος & ημ/νία)								
Α / Α	ΠΕΛΑΤΗΣ	ΣΥΝΤΟΜΗ ΠΕΡΙΓΡΑΦΗ ΤΟΥ ΕΡΓΟΥ	ΔΙΑΡΚΕΙΑ ΕΚΤΕΛΕΣΗΣ ΕΡΓΟΥ	ΠΡΟΫΠΟ - ΛΟΓΙΣΜΟΣ	ΣΥΝΟΠΤΙΚΗ ΠΕΡΙΓΡΑΦΗ ΣΥΝΕΙΣΦΟΡΑΣ ΣΤΟ ΕΡΓΟ (αντικείμενο)	ΠΟΣΟΣΤΟ ΣΥΜΜΕΤΟΧΗΣ ΣΤΟ ΕΡΓΟ (προϋπολογισμός)	ΣΤΟΙΧΕΙΟ ΤΕΚΜΗΡΙΩΣΗΣ (τύπος & ημ/νία)																



	<ul style="list-style-type: none">- Εάν ο Πελάτης είναι Δημόσιος Φορέας ως στοιχείο τεκμηρίωσης υποβάλλεται πιστοποιητικό ή πρωτόκολλο παραλαβής ή βεβαίωση καλής εκτέλεσης που συντάσσεται από την αρμόδια Δημόσια Αρχή.- Εάν ο Πελάτης είναι ιδιώτης, ως στοιχείο τεκμηρίωσης υποβάλλεται δήλωση είτε του ιδιώτη όπως εκπροσωπείται από το Νόμιμο Εκπρόσωπο, είτε του υποψηφίου οικονομικού φορέα.																																																												
4.	<p>Οι οικονομικοί φορείς που συμμετέχουν στη διαδικασία σύναψης της παρούσας απαιτείται να διαθέτουν ομάδα έργου με στελέχη επαρκή σε πλήθος και δεξιότητες για την ανάληψη του Έργου σύμφωνα με την παράγραφο 2.2.6</p> <p>Σε περίπτωση ένωσης οικονομικών φορέων, οι παραπάνω ελάχιστες απαιτήσεις καλύπτονται αθροιστικά από όλα τα μέλη της ένωσης.</p> <p>Οι οικονομικοί φορείς οφείλουν να αποδείξουν το ανωτέρω κριτήριο ποιοτικής επιλογής υποβάλλοντας τα ακόλουθα στοιχεία τεκμηρίωσης:</p>																																																												
4.1	<p>Πίνακα των υπαλλήλων του Οικονομικού Φορέα που συμμετέχουν στην Ομάδα Έργου, σύμφωνα με το ακόλουθο υπόδειγμα:</p> <table border="1"><thead><tr><th>A/A</th><th>Εταιρεία (σε περίπτωση Ένωσης / Κοινοπραξίας)</th><th>Ονοματεπώνυμο Μέλους Ομάδας Έργου</th><th>Θέση στην Ομάδα Έργου</th><th>Ανθρωπο μήνες</th><th>Ποσοστό συμμετοχής* (%)</th></tr></thead><tbody><tr><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td colspan="4">ΜΕΡΙΚΟ ΣΥΝΟΛΟ (1)</td><td></td><td></td></tr></tbody></table> <p>Πίνακα των στελεχών των Υπεργολάβων του Οικονομικού Φορέα που συμμετέχουν στην Ομάδα Έργου, σύμφωνα με το ακόλουθο υπόδειγμα:</p> <table border="1"><thead><tr><th>A/A</th><th>Επωνυμία Εταιρείας Υπεργολάβου</th><th>Ονοματεπώνυμο Μέλους Ομάδας Έργου</th><th>Θέση στην Ομάδα Έργου</th><th>Ανθρωπο μήνες</th><th>Ποσοστό συμμετοχής* (%)</th></tr></thead><tbody><tr><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td colspan="4">ΜΕΡΙΚΟ ΣΥΝΟΛΟ (2)</td><td></td><td></td></tr></tbody></table>	A/A	Εταιρεία (σε περίπτωση Ένωσης / Κοινοπραξίας)	Ονοματεπώνυμο Μέλους Ομάδας Έργου	Θέση στην Ομάδα Έργου	Ανθρωπο μήνες	Ποσοστό συμμετοχής* (%)																			ΜΕΡΙΚΟ ΣΥΝΟΛΟ (1)						A/A	Επωνυμία Εταιρείας Υπεργολάβου	Ονοματεπώνυμο Μέλους Ομάδας Έργου	Θέση στην Ομάδα Έργου	Ανθρωπο μήνες	Ποσοστό συμμετοχής* (%)																			ΜΕΡΙΚΟ ΣΥΝΟΛΟ (2)					
A/A	Εταιρεία (σε περίπτωση Ένωσης / Κοινοπραξίας)	Ονοματεπώνυμο Μέλους Ομάδας Έργου	Θέση στην Ομάδα Έργου	Ανθρωπο μήνες	Ποσοστό συμμετοχής* (%)																																																								
ΜΕΡΙΚΟ ΣΥΝΟΛΟ (1)																																																													
A/A	Επωνυμία Εταιρείας Υπεργολάβου	Ονοματεπώνυμο Μέλους Ομάδας Έργου	Θέση στην Ομάδα Έργου	Ανθρωπο μήνες	Ποσοστό συμμετοχής* (%)																																																								
ΜΕΡΙΚΟ ΣΥΝΟΛΟ (2)																																																													

Πίνακα των **εξωτερικών συνεργατών του Οικονομικού Φορέα** που συμμετέχουν στην Ομάδα Έργου, σύμφωνα με το ακόλουθο υπόδειγμα:

A/A	Ονοματεπώνυμο Μέλους Ομάδας Έργου	Θέση στην Ομάδα Έργου	Ανθρωπομην ες	Ποσοστό συμμετοχής * (%)
ΜΕΡΙΚΟ ΣΥΝΟΛΟ (3)				

*ως **Ποσοστό Συμμετοχής** του Μέλους ορίζεται το πηλίκο των ανθρωπομηνών του δια των συνολικών προσφερόμενων ανθρωπομηνών (άθροισμα των μερικών συνόλων 1,2,3)

Ο Οικονομικός Φορέας, συμπληρωματικά με τον παραπάνω Πίνακα, θα πρέπει να καταθέσει υπεύθυνες δηλώσεις συνεργασίας, των εξωτερικών συνεργατών και των υπεργολάβων. Οι εξωτερικοί Συνεργάτες και οι υπεργολάβοι, θα δηλώνουν ότι το έργο (αντικείμενο της παρούσας Διακήρυξης), καθώς και οι υποχρεώσεις που απορρέουν από αυτό, τελούν σε γνώση τους.

4.2 Βιογραφικά σημειώματα της Ομάδας Έργου (βάσει του υποδείγματος / βλ. «ΠΑΡΑΡΤΗΜΑ IV – Υπόδειγμα Βιογραφικού Σημειώματος»)

B.5. Για την απόδειξη της συμμόρφωσής τους με πρότυπα διασφάλισης ποιότητας της παραγράφου 2.2.7 οι οικονομικοί φορείς προσκομίζουν τα αναφερόμενα στον κατωτέρω πίνακα :

5.	<p>Οι οικονομικοί φορείς που συμμετέχουν στη διαδικασία σύναψης της παρούσας απαιτείται να εξασφαλίζουν την ποιότητα των παρεχόμενων υπηρεσιών και να διαθέτουν οργανωμένο σύστημα σύμφωνα με το:</p> <p>α) Πρότυπο διαχείρισης ποιότητας ISO 9001:2015.</p> <p>β) Πρότυπο διαχείρισης ασφάλειας πληροφοριών ISO 27001:2013 ή ισοδύναμο.</p> <p>Οι οικονομικοί φορείς οφείλουν να αποδείξουν το ανωτέρω κριτήριο ποιοτικής επιλογής υποβάλλοντας τα ακόλουθα στοιχεία τεκμηρίωσης:</p>
5.1	<p>Οι οικονομικοί φορείς προσκομίζουν πιστοποιητικά συστήματος διαχείρισης ποιότητας (ISO ή ισοδύναμο) εν ισχύ, από διαπιστευμένο φορέα, στο πεδίο που ζητείται ή άλλα αποδεικτικά στοιχεία για ισοδύναμα μέτρα διασφάλισης ποιότητας, εφόσον ο υποψήφιος οικονομικός φορέας δεν είχε τη δυνατότητα να αποκτήσει τα εν λόγω πιστοποιητικά εντός των σχετικών προθεσμιών για λόγους για τους οποίους δεν ευθύνεται ο ίδιος, υπό την προϋπόθεση ότι ο οικονομικός φορέας αποδεικνύει ότι τα προτεινόμενα μέτρα διασφάλισης ποιότητας πληρούν τα απαιτούμενα πρότυπα διασφάλισης ποιότητας.</p>

B.6.Για την απόδειξη της νόμιμης σύστασης και εκπροσώπησης:

Για την απόδειξη της νόμιμης εκπροσώπησης, στις περιπτώσεις που ο οικονομικός φορέας είναι νομικό πρόσωπο και εγγράφεται υποχρεωτικά ή προαιρετικά, κατά την κείμενη νομοθεσία, και δηλώνει την εκπροσώπηση και τις μεταβολές της σε αρμόδια αρχή (πχ ΓΕΜΗ), προσκομίζει σχετικό πιστοποιητικό ισχύουσας εκπροσώπησης, το οποίο πρέπει να έχει εκδοθεί έως τριάντα (30) εργάσιμες ημέρες πριν από την υποβολή του, εκτός αν αυτό φέρει συγκεκριμένο χρόνο ισχύος.

Ειδικότερα για τους ημεδαπούς οικονομικούς φορείς προσκομίζονται:

i) **για την απόδειξη της νόμιμης εκπροσώπησης**, στις περιπτώσεις που ο οικονομικός φορέας είναι νομικό πρόσωπο και υποχρεούται, κατά την κείμενη νομοθεσία, να δηλώνει την εκπροσώπηση και τις μεταβολές της στο ΓΕΜΗ, προσκομίζει σχετικό πιστοποιητικό ισχύουσας εκπροσώπησης, το οποίο πρέπει να έχει εκδοθεί έως τριάντα (30) εργάσιμες ημέρες πριν από την υποβολή του.

ii) Για την **απόδειξη της νόμιμης σύστασης και των μεταβολών** του νομικού προσώπου γενικό πιστοποιητικό μεταβολών του ΓΕΜΗ, εφόσον έχει εκδοθεί έως τρεις (3) μήνες πριν από την υποβολή του.

Στις λοιπές περιπτώσεις τα κατά περίπτωση νομιμοποιητικά έγγραφα σύστασης και νόμιμης εκπροσώπησης (όπως καταστατικά, πιστοποιητικά μεταβολών, αντίστοιχα ΦΕΚ, αποφάσεις συγκρότησης οργάνων διοίκησης σε σώμα, κλπ., ανάλογα με τη νομική μορφή του οικονομικού φορέα), συνοδευόμενα από υπεύθυνη δήλωση του νόμιμου εκπροσώπου ότι εξακολουθούν να ισχύουν κατά την υποβολή τους.

Σε περίπτωση που για τη διενέργεια της παρούσας διαδικασίας ανάθεσης έχουν χορηγηθεί εξουσίες σε πρόσωπο πλέον αυτών που αναφέρονται στα παραπάνω έγγραφα, προσκομίζεται επιπλέον απόφαση- πρακτικό του αρμοδίου καταστατικού οργάνου διοίκησης του νομικού προσώπου με την οποία χορηγήθηκαν οι σχετικές εξουσίες. Όσον αφορά τα φυσικά πρόσωπα, εφόσον έχουν χορηγηθεί εξουσίες σε τρίτα πρόσωπα, προσκομίζεται εξουσιοδότηση του οικονομικού φορέα.

Οι αλλοδαποί οικονομικοί φορείς προσκομίζουν τα προβλεπόμενα, κατά τη νομοθεσία της χώρας εγκατάστασης, αποδεικτικά έγγραφα, και εφόσον δεν προβλέπονται, υπεύθυνη δήλωση του νόμιμου εκπροσώπου, από την οποία αποδεικνύονται τα ανωτέρω ως προς τη νόμιμη σύσταση, μεταβολές και εκπροσώπηση του οικονομικού φορέα.

Οι ως άνω υπεύθυνες δηλώσεις γίνονται αποδεκτές, εφόσον έχουν συνταχθεί μετά την κοινοποίηση της πρόσκλησης για την υποβολή των δικαιολογητικών.

Από τα ανωτέρω έγγραφα πρέπει να προκύπτουν η νόμιμη σύσταση του οικονομικού φορέα, όλες οι σχετικές τροποποιήσεις των καταστατικών, το/τα πρόσωπο/α που δεσμεύει/ουν νόμιμα την εταιρία κατά την ημερομηνία διενέργειας του διαγωνισμού (νόμιμος εκπρόσωπος, δικαίωμα υπογραφής κλπ.), τυχόν τρίτοι, στους οποίους έχει χορηγηθεί εξουσία εκπροσώπησης, καθώς και η θητεία του/των ή/και των μελών του οργάνου διοίκησης/ νόμιμου εκπροσώπου.

B.7. Οι οικονομικοί φορείς που είναι εγγεγραμμένοι σε επίσημους καταλόγους που προβλέπονται από τις εκάστοτε ισχύουσες εθνικές διατάξεις ή διαθέτουν πιστοποίηση από οργανισμούς πιστοποίησης που συμμορφώνονται με τα ευρωπαϊκά πρότυπα πιστοποίησης, κατά την έννοια του Παραρτήματος

VII του Προσαρτήματος Α' του ν. 4412/2016, μπορούν να προσκομίζουν στις αναθέτουσες αρχές πιστοποιητικό εγγραφής εκδιδόμενο από την αρμόδια αρχή ή το πιστοποιητικό που εκδίδεται από τον αρμόδιο οργανισμό πιστοποίησης.

Στα πιστοποιητικά αυτά αναφέρονται τα δικαιολογητικά βάσει των οποίων έγινε η εγγραφή των εν λόγω οικονομικών φορέων στον επίσημο κατάλογο ή η πιστοποίηση και η κατάταξη στον εν λόγω κατάλογο.

Η πιστοποιούμενη εγγραφή στους επίσημους καταλόγους από τους αρμόδιους οργανισμούς ή το πιστοποιητικό, που εκδίδεται από τον οργανισμό πιστοποίησης, συνιστά τεκμήριο καταλληλότητας όσον αφορά τις απαιτήσεις ποιοτικής επιλογής, τις οποίες καλύπτει ο επίσημος κατάλογος ή το πιστοποιητικό.

Οι οικονομικοί φορείς που είναι εγγεγραμμένοι σε επίσημους καταλόγους απαλλάσσονται από την υποχρέωση υποβολής των δικαιολογητικών που αναφέρονται στο πιστοποιητικό εγγραφής τους. Ειδικώς όσον αφορά την καταβολή των εισφορών κοινωνικής ασφάλισης και των φόρων και τελών, προσκομίζονται επιπροσθέτως της βεβαίωσης εγγραφής στον επίσημο κατάλογο και πιστοποιητικά, κατά τα οριζόμενα ανωτέρω στην περίπτωση Β.1, υποπερ. i, ii και iii της περ. β.

Β.8. Οι ενώσεις οικονομικών φορέων που υποβάλλουν κοινή προσφορά, υποβάλλουν τα παραπάνω, κατά περίπτωση δικαιολογητικά, για κάθε οικονομικό φορέα που συμμετέχει στην ένωση, σύμφωνα με τα ειδικότερα προβλεπόμενα στο άρθρο 19 παρ. 2 του ν. 4412/2016.

Επιπλέον υποβάλλεται συμφωνητικό μεταξύ των μελών της Ένωσης με το οποίο α) συστήνεται η Ένωση β) αναγράφεται να οριοθετείται με σαφήνεια το μέρος του Έργου και το ποσοστό (όχι απόλυτη τιμή) του συμβατικού τιμήματος που θα αντιστοιχεί σε κάθε μέλος της ένωσης στο σύνολο της Προσφοράς, γ) δηλώνεται ένα Μέλος ως υπεύθυνο για το συντονισμό και τη διοίκηση όλων των Μελών της Ένωσης (leader) δ) και ορίζεται κοινός εκπρόσωπος της Ένωσης και των μελών της για τη συμμετοχή της στο Διαγωνισμό και την εκπροσώπηση της Ένωσης και των μελών της έναντι της Αναθέτουσας Αρχής.

Β.9. Στην περίπτωση που οικονομικός φορέας επιθυμεί να στηριχθεί στις ικανότητες άλλων φορέων, σύμφωνα με την παράγραφο 2.2.8 για την απόδειξη ότι θα έχει στη διάθεσή του τους αναγκαίους πόρους, προσκομίζει, ιδίως, σχετική έγγραφη δέσμευση των φορέων αυτών για τον σκοπό αυτό. Ειδικότερα, προσκομίζεται έγγραφο (συμφωνητικό ή σε περίπτωση νομικού προσώπου απόφαση του αρμοδίου οργάνου διοίκησης αυτού ή σε περίπτωση φυσικού προσώπου υπεύθυνη δήλωση), δυνάμει του οποίου αμφότεροι, διαγωνιζόμενος οικονομικός φορέας και τρίτος φορέας, εγκρίνουν τη μεταξύ τους συνεργασία για την κατά περίπτωση παροχή προς τον διαγωνιζόμενο της χρηματοοικονομικής ή/και τεχνικής ή/και επαγγελματικής ικανότητας του φορέα, ώστε αυτή να είναι στη διάθεση του διαγωνιζόμενου για την εκτέλεση της Σύμβασης.

Η σχετική αναφορά θα πρέπει να είναι λεπτομερής και να αναφέρει κατ' ελάχιστον τους συγκεκριμένους πόρους που θα είναι διαθέσιμοι για την εκτέλεση της σύμβασης και τον τρόπο δια του οποίου θα χρησιμοποιηθούν αυτοί για την εκτέλεση της σύμβασης. Ο τρίτος θα δεσμεύεται ρητά ότι θα διαθέσει στον διαγωνιζόμενο τους συγκεκριμένους πόρους κατά τη διάρκεια της σύμβασης και ο διαγωνιζόμενος ότι θα κάνει χρήση αυτών σε περίπτωση που του ανατεθεί η σύμβαση. Σε

περίπτωση που ο τρίτος διαθέτει χρηματοοικονομική επάρκεια, θα δηλώνει επίσης ότι καθίσταται από κοινού με τον διαγωνιζόμενο υπεύθυνος για την εκτέλεση της σύμβασης.

Σε περίπτωση που ο τρίτος διαθέτει στοιχεία τεχνικής ή επαγγελματικής καταλληλότητας που σχετίζονται με τους τίτλους σπουδών και τα επαγγελματικά προσόντα που ορίζονται στην περίπτωση στ' του Μέρους ΙΙ του Παραρτήματος ΧΙΙ του Προσαρτήματος Α του ν. 4412/2016 ή με την σχετική επαγγελματική εμπειρία, θα δεσμεύεται ότι θα εκτελέσει τις εργασίες ή υπηρεσίες για τις οποίες απαιτούνται οι συγκεκριμένες ικανότητες, δηλώνοντας το τμήμα της σύμβασης που θα εκτελέσει.

B.10. Στην περίπτωση που ο οικονομικός φορέας δηλώνει στην προσφορά του ότι θα κάνει χρήση υπεργολάβων, στις ικανότητες των οποίων δεν στηρίζεται, προσκομίζεται υπεύθυνη δήλωση του προσφέροντος με αναφορά του τμήματος της σύμβασης το οποίο προτίθεται να αναθέσει σε τρίτους υπό μορφή υπεργολαβίας και υπεύθυνη δήλωση των υπεργολάβων ότι αποδέχονται την εκτέλεση των εργασιών.

B.11. Επισημαίνεται ότι γίνονται αποδεκτές:

- οι ένορκες βεβαιώσεις που αναφέρονται στην παρούσα Διακήρυξη, εφόσον έχουν συνταχθεί έως τρεις (3) μήνες πριν από την υποβολή τους,
- οι υπεύθυνες δηλώσεις, εφόσον έχουν συνταχθεί μετά την κοινοποίηση της πρόσκλησης για την υποβολή των δικαιολογητικών. Σημειώνεται ότι δεν απαιτείται θεώρηση του γνησίου της υπογραφής τους

2.3 Κριτήρια Ανάθεσης

2.3.1 Κριτήριο ανάθεσης

Κριτήριο ανάθεσης της συμφωνίας - πλαίσιο είναι η πλέον συμφέρουσα από οικονομική άποψη προσφορά βάσει βέλτιστης σχέσης ποιότητας – τιμής, η οποία εκτιμάται ανά Τμήμα βάσει των κάτωθι κριτηρίων.

Τμήμα 1

Κριτήριο	Περιγραφή	Συντελεστής Βαρύτητας	Παραπομπή σε παρ. απαίτησης της διακήρυξης
A	ΠΡΟΔΙΑΓΡΑΦΕΣ ΤΕΧΝΙΚΗΣ ΛΥΣΗΣ	5%	
A1	Αντίληψη και κατανόηση του έργου από τον υποψήφιο Ανάδοχο	5%	ΠΑΡΑΡΤΗΜΑ Ι ΚΕΦΑΛΑΙΑ 7.1.1 και 7.1.2
B	ΠΡΟΔΙΑΓΡΑΦΕΣ ΛΥΣΕΩΝ ΚΑΙ ΥΠΗΡΕΣΙΩΝ ΑΣΦΑΛΕΙΑΣ	90%	
B1	Πολιτικές – Διαδικασίες και Μέτρα Αντιμετώπισης και Πρόληψης Κινδύνων	8%	ΠΑΡΑΡΤΗΜΑ Ι ΚΕΦΑΛΑΙΟ 7.1.3.2

Κριτήριο	Περιγραφή	Συντελεστής Βαρύτητας	Παραπομπή σε παρ. απαίτησης της διακήρυξης
B2	Υπηρεσίες νεφοϋπολογιστικών υποδομών και υπηρεσιών	15%	ΠΑΡΑΡΤΗΜΑ Ι ΚΕΦΑΛΑΙΟ 7.1.3.4
B3	Εξειδικευμένες Λύσεις Ασφάλειας	65%	ΠΑΡΑΡΤΗΜΑ Ι ΚΕΦΑΛΑΙΟ 7.1.3.5
B4	Εξειδικευμένες Λύσεις Ασφάλειας Πληροφοριών και Εγγράφων	2%	ΠΑΡΑΡΤΗΜΑ Ι ΚΕΦΑΛΑΙΟ 7.1.3.3
Γ	ΜΕΘΟΔΟΛΟΓΙΑ ΥΛΟΠΟΙΗΣΗΣ - ΔΙΟΙΚΗΣΗΣ	5%	
Γ1	Οργάνωση Υλοποίησης Έργου	3%	ΠΑΡΑΡΤΗΜΑ Ι ΚΕΦΑΛΑΙΟ 7.1.7
Γ2	Μεθοδολογία Διοίκησης και Υλοποίησης Έργου - Προτεινόμενο σχήμα Διοίκησης Έργου	2%	ΠΑΡΑΡΤΗΜΑ Ι ΚΕΦΑΛΑΙΑ 7.1.9, 7.1.10, 7.1.11
ΣΥΝΟΛΟ		100%	

Επεξήγηση Κριτηρίων:

Ανά κατηγορία και κριτήριο αξιολογούνται:

Ομάδα Α - ΠΡΟΔΙΑΓΡΑΦΕΣ ΤΕΧΝΙΚΗΣ ΛΥΣΗΣ

A1: Αντίληψη και κατανόηση του έργου από τον υποψήφιο Ανάδοχο

Αντίληψη και κατανόηση του φυσικού αντικείμενου του έργου από τον υποψήφιο Ανάδοχο

Το κριτήριο A1 «Αντίληψη και κατανόηση του φυσικού αντικείμενου του έργου από τον υποψήφιο Ανάδοχο» αξιολογεί το βαθμό της κατανόησης των ειδικών απαιτήσεων του πλαισίου (context), τη στοχευμένη προσέγγιση στις ιδιαιτερότητες και την αναγνώριση-ανάλυση των ειδικών θεμάτων (κίνδυνοι, κρίσιμοι παράγοντες) που σχετίζονται με το συγκεκριμένο έργο.

Ομάδα Β– ΠΡΟΔΙΑΓΡΑΦΕΣ ΛΥΣΕΩΝ ΚΑΙ ΥΠΗΡΕΣΙΩΝ ΑΣΦΑΛΕΙΑΣ

B1 Πολιτικές – Διαδικασίες και Μέτρα Αντιμετώπισης και Πρόληψης Κινδύνων

Το κριτήριο B1 αξιολογεί το βαθμό καταλληλότητας της προτεινόμενης μεθοδολογίας και το βαθμό συμβατότητας της μεθόδου παροχής των υπηρεσιών με τις συνθήκες λειτουργίας του φορέα και

τους στόχους του έργου. Αξιολογείται η κάλυψη των προδιαγραφών του κεφαλαίου 7.1.3.2 του Παραρτήματος Ι της διακήρυξης.

B2 Υπηρεσίες νεφοϋπολογιστικών υποδομών και υπηρεσιών

Το κριτήριο B2 αξιολογεί το βαθμό καταλληλότητας της προτεινόμενης μεθοδολογίας και το βαθμό συμβατότητας της μεθόδου παροχής των υπηρεσιών με τις συνθήκες λειτουργίας του φορέα και τους στόχους του έργου. Αξιολογείται η κάλυψη των προδιαγραφών του κεφαλαίου 7.1.3.4 του Παραρτήματος Ι της διακήρυξης.

B3 Εξειδικευμένες Λύσεις Ασφάλειας

Το κριτήριο B3 αξιολογεί το βαθμό καταλληλότητας της προτεινόμενης μεθοδολογίας και τα τεχνικά χαρακτηριστικά των προσφερόμενων λύσεων με τις συνθήκες λειτουργίας του φορέα και τους στόχους του έργου. Αξιολογείται η κάλυψη των προδιαγραφών του κεφαλαίου 7.1.3.5 του Παραρτήματος Ι της διακήρυξης.

B4 Εξειδικευμένες Λύσεις Ασφάλειας Πληροφοριών και Εγγράφων

Το κριτήριο B4 αξιολογεί το βαθμό καταλληλότητας της προτεινόμενης μεθοδολογίας και τα τεχνικά χαρακτηριστικά των προσφερόμενων λύσεων με τις συνθήκες λειτουργίας του φορέα και τους στόχους του έργου. Αξιολογείται η κάλυψη των προδιαγραφών του κεφαλαίου 7.1.3.3 του Παραρτήματος Ι της διακήρυξης.

Ομάδα Γ – ΜΕΘΟΔΟΛΟΓΙΑ ΥΛΟΠΟΙΗΣΗΣ - ΔΙΟΙΚΗΣΗΣ

Γ1: Οργάνωση Υλοποίησης Έργου

Στα πλαίσια του κριτηρίου Γ1 αξιολογούνται:

- η σαφήνεια και πληρότητα ανάλυσης των προσφερόμενων υπηρεσιών του Υποψήφιου Αναδόχου, σε συνάρτηση με τον προσφερόμενο ανθρωποχρόνο,
- η ορθολογική ανάλυση του αντικειμένου του έργου σε Ενότητες Εργασίας και επιμέρους δραστηριότητες / ενέργειες υλοποίησης του Έργου και των μεταξύ τους αλληλεξαρτήσεων, λαμβάνοντας υπόψη το φυσικό αντικείμενο και το χρονοδιάγραμμα υλοποίησής του,
- η ανάλυση, δομή και οργάνωση των παραδοτέων και η σύνδεσή τους με τις Ενότητες Εργασίας, σε σχέση με την προτεινόμενη Μεθοδολογία, τη ρεαλιστικότητα της προσέγγισης και την ολοκληρωμένη αντίληψη του υποψήφιου Αναδόχου για το Έργο,
- η λίστα με τα ορόσημα του Έργου, που αφορούν κρίσιμα σημεία/στιγμιότυπα του χρονοδιαγράμματος του Έργου, στα οποία το Έργο απομπλέκεται από κάποιο σημαντικό ρίσκο ή/και επιτυγχάνει κάποιο σημαντικό (ενδιάμεσο) στόχο.

Γ2: Μεθοδολογία Διοίκησης και Υλοποίησης Έργου - Προτεινόμενο σχήμα Διοίκησης Έργου

Στα πλαίσια του κριτηρίου Γ2 αξιολογούνται:

- ο βαθμός επάρκειας, σαφήνειας και αποτελεσματικότητας του τρόπου διακυβέρνησης του έργου. Ελέγχεται κατά πόσον από την προσφορά είναι ευδιάκριτα τα όρια λογοδοσίας όλων των ρόλων, καθ' όλον τον κύκλο ζωής του έργου και κατά πόσο ο τρόπος αξιοποίησης

εξωτερικών συνεργατών, ή υπερβολών συντελεί στην ομαλή διακυβέρνηση χωρίς να αυξάνεται η πολυπλοκότητα,

- η καταλληλότητα και η επάρκεια των διαδικασιών και των μηχανισμών επικοινωνίας της Ομάδας Έργου με τα αρμόδια εμπλεκόμενα τμήματα/μονάδες, με στόχο τόσο τη μεταφορά τεχνογνωσίας όσο και την αποτελεσματικότερη υλοποίηση του έργου,
- η αποτελεσματικότητα της προτεινόμενης μεθοδολογίας διοίκησης και διασφάλισης ποιότητας.

Τμήμα 2

Κριτήριο	Περιγραφή	Συντελεστής Βαρύτητας	Παραπομπή σε παρ. απαίτησης της διακήρυξης
A	ΠΡΟΔΙΑΓΡΑΦΕΣ ΤΕΧΝΙΚΗΣ ΛΥΣΗΣ	5%	
A1	Αντίληψη και κατανόηση του έργου από τον υποψήφιο Ανάδοχο	5%	ΠΑΡΑΡΤΗΜΑ Ι ΚΕΦΑΛΑΙΑ 7.1.1 και 7.1.2
B	ΠΡΟΔΙΑΓΡΑΦΕΣ ΛΥΣΕΩΝ ΚΑΙ ΥΠΗΡΕΣΙΩΝ ΑΣΦΑΛΕΙΑΣ	90%	
B1	Πολιτικές – Διαδικασίες και Μέτρα Αντιμετώπισης και Πρόληψης Κινδύνων	8%	ΠΑΡΑΡΤΗΜΑ Ι ΚΕΦΑΛΑΙΟ 7.1.4.2
B2	Λύση DDOS	5%	ΠΑΡΑΡΤΗΜΑ Ι ΚΕΦΑΛΑΙΟ 7.1.4.5
B3	Υπηρεσίες νεφοϋπολογιστικών υποδομών και υπηρεσιών	7%	ΠΑΡΑΡΤΗΜΑΙ ΚΕΦΑΛΑΙΟ 7.1.4.4
B4	Εξειδικευμένες Λύσεις Ασφάλειας	40%	ΠΑΡΑΡΤΗΜΑ Ι ΚΕΦΑΛΑΙΟ 7.1.4.6
B5	Εξειδικευμένες Λύσεις Ασφάλειας Πληροφοριών και Εγγράφων	30%	ΠΑΡΑΡΤΗΜΑ Ι ΚΕΦΑΛΑΙΟ 7.1.4.3
Γ	ΜΕΘΟΔΟΛΟΓΙΑ ΥΛΟΠΟΙΗΣΗΣ - ΔΙΟΙΚΗΣΗΣ	5%	
Γ1	Οργάνωση Υλοποίησης Έργου (Χρονοδιάγραμμα, Παραδοτέα)	3%	ΠΑΡΑΡΤΗΜΑ Ι ΚΕΦΑΛΑΙΟ 7.1.7
Γ2	Μεθοδολογία Διοίκησης και Υλοποίησης Έργου - Προτεινόμενο σχήμα Διοίκησης Έργου	2%	ΠΑΡΑΡΤΗΜΑ Ι ΚΕΦΑΛΑΙΑ 7.1.9, 7.1.10, 7.1.11

Κριτήριο	Περιγραφή	Συνεπελεστής Βαρύτητας	Παραπομπή σε παρ. απαίτησης της διακήρυξης
ΣΥΝΟΛΟ		100%	

Επεξήγηση Κριτηρίων:

Ανά κατηγορία και κριτήριο αξιολογούνται:

Ομάδα Α - ΠΡΟΔΙΑΓΡΑΦΕΣ ΤΕΧΝΙΚΗΣ ΛΥΣΗΣ

A1: Αντίληψη και κατανόηση του έργου από τον υποψήφιο Ανάδοχο

Αντίληψη και κατανόηση του φυσικού αντικειμένου του έργου από τον υποψήφιο Ανάδοχο

Το κριτήριο A1 «Αντίληψη και κατανόηση του φυσικού αντικειμένου του έργου από τον υποψήφιο Ανάδοχο» αξιολογεί το βαθμό της κατανόησης των ειδικών απαιτήσεων του πλαισίου (context), τη στοχευμένη προσέγγιση στις ιδιαιτερότητες και την αναγνώριση-ανάλυση των ειδικών θεμάτων (κίνδυνοι, κρίσιμοι παράγοντες) που σχετίζονται με το συγκεκριμένο έργο.

Ομάδα Β - ΠΡΟΔΙΑΓΡΑΦΕΣ ΥΠΗΡΕΣΙΩΝ

B1 Πολιτικές – Διαδικασίες και Μέτρα Αντιμετώπισης και Πρόληψης Κινδύνων

Το κριτήριο B1 αξιολογεί το βαθμό καταλληλότητας της προτεινόμενης μεθοδολογίας και το βαθμό συμβατότητας της μεθόδου παροχής των υπηρεσιών με τις συνθήκες λειτουργίας του φορέα και τους στόχους του έργου. Αξιολογείται η κάλυψη των προδιαγραφών του κεφαλαίου 7.1.4.2 του Παραρτήματος Ι της διακήρυξης.

B2 Λύση DDOS

Το κριτήριο B2 αξιολογεί το βαθμό καταλληλότητας της προτεινόμενης μεθοδολογίας και το βαθμό συμβατότητας της μεθόδου παροχής των υπηρεσιών με τις συνθήκες λειτουργίας του φορέα και τους στόχους του έργου. Αξιολογείται η κάλυψη των προδιαγραφών του κεφαλαίου 7.1.4.5 του Παραρτήματος Ι της διακήρυξης.

B3 Υπηρεσίες νεφοϋπολογιστικών υποδομών και υπηρεσιών

Το κριτήριο B3 αξιολογεί το βαθμό καταλληλότητας της προτεινόμενης μεθοδολογίας και το βαθμό συμβατότητας της μεθόδου παροχής των υπηρεσιών με τις συνθήκες λειτουργίας του φορέα και τους στόχους του έργου. Αξιολογείται η κάλυψη των προδιαγραφών του κεφαλαίου 7.1.4.4 του Παραρτήματος Ι της διακήρυξης.

B4 Εξειδικευμένες Λύσεις Ασφάλειας

Το κριτήριο B4 αξιολογεί το βαθμό καταλληλότητας της προτεινόμενης μεθοδολογίας και τα τεχνικά χαρακτηριστικά των προσφερόμενων λύσεων με τις συνθήκες λειτουργίας του φορέα και

τους στόχους του έργου. Αξιολογείται η κάλυψη των προδιαγραφών του κεφαλαίου 7.1.4.6 του Παραρτήματος Ι της διακήρυξης.

B5 Εξειδικευμένες Λύσεις Ασφάλειας Πληροφοριών και Εγγράφων

Το κριτήριο B5 αξιολογεί το βαθμό καταλληλότητας της προτεινόμενης μεθοδολογίας και τα τεχνικά χαρακτηριστικά των προσφερόμενων λύσεων με τις συνθήκες λειτουργίας του φορέα και τους στόχους του έργου. Αξιολογείται η κάλυψη των προδιαγραφών του κεφαλαίου 7.1.4.3 του Παραρτήματος Ι της διακήρυξης.

Ομάδα Γ – ΜΕΘΟΔΟΛΟΓΙΑ ΥΛΟΠΟΙΗΣΗΣ - ΔΙΟΙΚΗΣΗΣ

Γ1: Οργάνωση Υλοποίησης Έργου (Χρονοδιάγραμμα, Παραδοτέα)

Στα πλαίσια του κριτηρίου Γ1 αξιολογούνται:

- η σαφήνεια και πληρότητα ανάλυσης των προσφερόμενων υπηρεσιών του Υποψήφιου Αναδόχου, σε συνάρτηση με τον προσφερόμενο ανθρωποχρόνο,
- ο ρεαλιστικός χρονοπρογραμματισμός των παρεχόμενων εργασιών του υποψήφιου Αναδόχου με βάση τις επιχειρησιακές απαιτήσεις του Κυρίου του Έργου,
- η ορθολογική ανάλυση του αντικειμένου του έργου σε Ενότητες Εργασίας και επιμέρους δραστηριότητες / ενέργειες υλοποίησης του Έργου και των μεταξύ τους αλληλεξαρτήσεων, λαμβάνοντας υπόψη το φυσικό αντικείμενο και το χρονοδιάγραμμα υλοποίησής του,
- η ανάλυση, δομή και οργάνωση των παραδοτέων και η σύνδεσή τους με τις Ενότητες Εργασίας, σε σχέση με την προτεινόμενη Μεθοδολογία, τη ρεαλιστικότητα της προσέγγισης και την ολοκληρωμένη αντίληψη του υποψήφιου Αναδόχου για το Έργο,
- η λίστα με τα ορόσημα του Έργου, που αφορούν κρίσιμα σημεία/στιγμιότυπα του χρονοδιαγράμματος του Έργου, στα οποία το Έργο απομπλέκεται από κάποιο σημαντικό ρίσκο ή/και επιτυγχάνει κάποιο σημαντικό (ενδιάμεσο) στόχο.

Γ2: Μεθοδολογία Διοίκησης και Υλοποίησης Έργου - Προτεινόμενο σχήμα Διοίκησης Έργου

Στα πλαίσια του κριτηρίου Γ2 αξιολογούνται:

- ο βαθμός επάρκειας, σαφήνειας και αποτελεσματικότητας του τρόπου διακυβέρνησης του έργου. Ελέγχεται κατά πόσον από την προσφορά είναι ευδιάκριτα τα όρια λογοδοσίας όλων των ρόλων, καθ' όλον τον κύκλο ζωής του έργου και κατά πόσο ο τρόπος αξιοποίησης εξωτερικών συνεργατών, ή υπεργολάβων συντελεί στην ομαλή διακυβέρνηση χωρίς να αυξάνεται η πολυπλοκότητα,
- η καταλληλότητα και η επάρκεια των διαδικασιών και των μηχανισμών επικοινωνίας της Ομάδας Έργου με τα αρμόδια εμπλεκόμενα τμήματα/μονάδες, με στόχο τόσο τη μεταφορά τεχνογνωσίας όσο και την αποτελεσματικότερη υλοποίηση του έργου,
- η αποτελεσματικότητα της προτεινόμενης μεθοδολογίας διοίκησης και διασφάλισης ποιότητας.

Τμήμα 3

Κριτήριο	Περιγραφή	Συντελεστής Βαρύτητας	Παραπομπή σε παρ. απαίτησης της διακήρυξης
A	ΠΡΟΔΙΑΓΡΑΦΕΣ ΤΕΧΝΙΚΗΣ ΛΥΣΗΣ	5%	
A1	Αντίληψη και κατανόηση του έργου από τον υποψήφιο Ανάδοχο	5%	ΠΑΡΑΡΤΗΜΑ Ι ΚΕΦΑΛΑΙΑ 7.1.1 και 7.1.2
B	ΠΡΟΔΙΑΓΡΑΦΕΣ ΛΥΣΕΩΝ ΚΑΙ ΥΠΗΡΕΣΙΩΝ ΑΣΦΑΛΕΙΑΣ	90%	
B1	Πολιτικές – Διαδικασίες και Μέτρα Αντιμετώπισης και Πρόληψης Κινδύνων	9%	ΠΑΡΑΡΤΗΜΑ Ι ΚΕΦΑΛΑΙΟ 7.1.5.2
B2	Υπηρεσίες Soc & DDOS	30%	ΠΑΡΑΡΤΗΜΑ Ι ΚΕΦΑΛΑΙΟ 7.1.5.5
B3	Υπηρεσίες νεφοϋπολογιστικών υποδομών και υπηρεσιών	8%	ΠΑΡΑΡΤΗΜΑ Ι ΚΕΦΑΛΑΙΟ 7.1.5.4
B4	Εξειδικευμένες Λύσεις Ασφάλειας	14%	ΠΑΡΑΡΤΗΜΑ Ι ΚΕΦΑΛΑΙΟ 7.1.5.6
B5	Εξειδικευμένες Λύσεις Ασφάλειας Πληροφοριών και Εγγράφων	29%	ΠΑΡΑΡΤΗΜΑ Ι ΚΕΦΑΛΑΙΟ 7.1.5.3
Γ	ΜΕΘΟΔΟΛΟΓΙΑ ΥΛΟΠΟΙΗΣΗΣ - ΔΙΟΙΚΗΣΗΣ	5%	
Γ1	Οργάνωση Υλοποίησης Έργου (Χρονοδιάγραμμα, Παραδοτέα)	3%	ΠΑΡΑΡΤΗΜΑ Ι ΚΕΦΑΛΑΙΟ 7.1.7
Γ2	Μεθοδολογία Διοίκησης και Υλοποίησης Έργου - Προτεινόμενο σχήμα Διοίκησης Έργου	2%	ΠΑΡΑΡΤΗΜΑ Ι ΚΕΦΑΛΑΙΑ 7.1.9, 7.1.10, 7.1.11
ΣΥΝΟΛΟ		100%	

Επεξήγηση Κριτηρίων:

Ανά κατηγορία και κριτήριο αξιολογούνται:

Ομάδα Α - ΠΡΟΔΙΑΓΡΑΦΕΣ ΤΕΧΝΙΚΗΣ ΛΥΣΗΣ

A1: Αντίληψη και κατανόηση του έργου από τον υποψήφιο Ανάδοχο

Αντίληψη και κατανόηση του φυσικού αντικείμενου του έργου από τον υποψήφιο Ανάδοχο

Το κριτήριο A1 «Αντίληψη και κατανόηση του φυσικού αντικείμενου του έργου από τον υποψήφιο Ανάδοχο» αξιολογεί το βαθμό της κατανόησης των ειδικών απαιτήσεων του πλαισίου (context), τη στοχευμένη προσέγγιση στις ιδιαιτερότητες και την αναγνώριση-ανάλυση των ειδικών θεμάτων (κίνδυνοι, κρίσιμοι παράγοντες) που σχετίζονται με το συγκεκριμένο έργο.

Ομάδα Β - ΠΡΟΔΙΑΓΡΑΦΕΣ ΥΠΗΡΕΣΙΩΝ

B1 Πολιτικές – Διαδικασίες και Μέτρα Αντιμετώπισης και Πρόληψης Κινδύνων

Το κριτήριο B1 αξιολογεί το βαθμό καταλληλότητας της προτεινόμενης μεθοδολογίας και το βαθμό συμβατότητας της μεθόδου παροχής των υπηρεσιών με τις συνθήκες λειτουργίας του φορέα και τους στόχους του έργου. Αξιολογείται η κάλυψη των προδιαγραφών του κεφαλαίου 7.1.5.2 του Παραρτήματος Ι της διακήρυξης.

B2 Υπηρεσίες Soc & DDOS

Το κριτήριο B2 αξιολογεί το βαθμό καταλληλότητας της προτεινόμενης μεθοδολογίας και το βαθμό συμβατότητας της μεθόδου παροχής των υπηρεσιών με τις συνθήκες λειτουργίας του φορέα και τους στόχους του έργου. Αξιολογείται η κάλυψη των προδιαγραφών του κεφαλαίου 7.1.5.5 του Παραρτήματος Ι της διακήρυξης.

B3 Υπηρεσίες νεφροϋπολογιστικών υποδομών και υπηρεσιών

Το κριτήριο B3 αξιολογεί το βαθμό καταλληλότητας της προτεινόμενης μεθοδολογίας και το βαθμό συμβατότητας της μεθόδου παροχής των υπηρεσιών με τις συνθήκες λειτουργίας του φορέα και τους στόχους του έργου. Αξιολογείται η κάλυψη των προδιαγραφών του κεφαλαίου 7.1.5.4 του Παραρτήματος Ι της διακήρυξης.

B4 Εξειδικευμένες Λύσεις Ασφάλειας

Το κριτήριο B4 αξιολογεί το βαθμό καταλληλότητας της προτεινόμενης μεθοδολογίας και τα τεχνικά χαρακτηριστικά των προσφερόμενων λύσεων με τις συνθήκες λειτουργίας του φορέα και τους στόχους του έργου. Αξιολογείται η κάλυψη των προδιαγραφών του κεφαλαίου 7.1.5.6 του Παραρτήματος Ι της διακήρυξης.

B5 Εξειδικευμένες Λύσεις Ασφάλειας Πληροφοριών και Εγγράφων

Το κριτήριο B5 αξιολογεί το βαθμό καταλληλότητας της προτεινόμενης μεθοδολογίας και τα τεχνικά χαρακτηριστικά των προσφερόμενων λύσεων με τις συνθήκες λειτουργίας του φορέα και τους στόχους του έργου. Αξιολογείται η κάλυψη των προδιαγραφών του κεφαλαίου 7.1.5.3 του Παραρτήματος Ι της διακήρυξης.

Ομάδα Γ – ΜΕΘΟΔΟΛΟΓΙΑ ΥΛΟΠΟΙΗΣΗΣ - ΔΙΟΙΚΗΣΗΣ

Γ1: Οργάνωση Υλοποίησης Έργου (Χρονοδιάγραμμα, Παραδοτέα)

Στα πλαίσια του κριτηρίου Γ1 αξιολογούνται:

- η σαφήνεια και πληρότητα ανάλυσης των προσφερόμενων υπηρεσιών του Υποψήφιου Αναδόχου, σε συνάρτηση με τον προσφερόμενο ανθρωποχρόνο,
- ο ρεαλιστικός χρονοπρογραμματισμός των παρεχόμενων εργασιών του υποψήφιου Αναδόχου με βάση τις επιχειρησιακές απαιτήσεις του Κυρίου του Έργου,
- η ορθολογική ανάλυση του αντικειμένου του έργου σε Ενότητες Εργασίας και επιμέρους δραστηριότητες / ενέργειες υλοποίησης του Έργου και των μεταξύ τους αλληλεξαρτήσεων, λαμβάνοντας υπόψη το φυσικό αντικείμενο και το χρονοδιάγραμμα υλοποίησής του,
- η ανάλυση, δομή και οργάνωση των παραδοτέων και η σύνδεσή τους με τις Ενότητες Εργασίας, σε σχέση με την προτεινόμενη Μεθοδολογία, τη ρεαλιστικότητα της προσέγγισης και την ολοκληρωμένη αντίληψη του υποψήφιου Αναδόχου για το Έργο,
- η λίστα με τα ορόσημα του Έργου, που αφορούν κρίσιμα σημεία/στιγμιότυπα του χρονοδιαγράμματος του Έργου, στα οποία το Έργο απομπλέκεται από κάποιο σημαντικό ρίσκο ή/και επιτυγχάνει κάποιο σημαντικό (ενδιάμεσο) στόχο.

Γ2:Μεθοδολογία Διοίκησης και Υλοποίησης Έργου - Προτεινόμενο σχήμα Διοίκησης Έργου

Στα πλαίσια του κριτηρίου Γ2 αξιολογούνται:

- ο βαθμός επάρκειας, σαφήνειας και αποτελεσματικότητας του τρόπου διακυβέρνησης του έργου. Ελέγχεται κατά πόσον από την προσφορά είναι ευδιάκριτα τα όρια λογοδοσίας όλων των ρόλων, καθ' όλην τον κύκλο ζωής του έργου και κατά πόσο ο τρόπος αξιοποίησης εξωτερικών συνεργατών, ή υπεργολάβων συντελεί στην ομαλή διακυβέρνηση χωρίς να αυξάνεται η πολυπλοκότητα,
- η καταλληλότητα και η επάρκεια των διαδικασιών και των μηχανισμών επικοινωνίας της Ομάδας Έργου με τα αρμόδια εμπλεκόμενα τμήματα/μονάδες, με στόχο τόσο τη μεταφορά τεχνογνωσίας όσο και την αποτελεσματικότερη υλοποίηση του έργου,
- η αποτελεσματικότητα της προτεινόμενης μεθοδολογίας διοίκησης και διασφάλισης ποιότητας.

Τμήμα 4

Κριτήριο	Περιγραφή	Συνετελεστής Βαρύτητας	Παραπομπή σε παρ. απαίτησης της διακήρυξης
A	ΠΡΟΔΙΑΓΡΑΦΕΣ ΤΕΧΝΙΚΗΣ ΛΥΣΗΣ	5%	
A1	Αντίληψη και κατανόηση του έργου από τον υποψήφιο Ανάδοχο	5%	ΠΑΡΑΡΤΗΜΑ Ι ΚΕΦΑΛΑΙΑ 7.1.1 και 7.1.2

Κριτήριο	Περιγραφή	Συνετελεστής Βαρύτητας	Παραπομπή σε παρ. απαίτησης της διακήρυξης
B	ΠΡΟΔΙΑΓΡΑΦΕΣ ΛΥΣΕΩΝ ΚΑΙ ΥΠΗΡΕΣΙΩΝ ΑΣΦΑΛΕΙΑΣ	90%	
B1	Πολιτικές – Διαδικασίες και Μέτρα Αντιμετώπισης και Πρόληψης Κινδύνων	11%	ΠΑΡΑΡΤΗΜΑ Ι ΚΕΦΑΛΑΙΟ 7.1.6.2
B2	Υπηρεσίες Soc & DDOS	38%	ΠΑΡΑΡΤΗΜΑ Ι ΚΕΦΑΛΑΙΟ 7.1.6.5
B3	Υπηρεσίες νεφοϋπολογιστικών υποδομών και υπηρεσιών	9%	ΠΑΡΑΡΤΗΜΑ Ι ΚΕΦΑΛΑΙΟ 7.1.6.4
B4	Εξειδικευμένες Λύσεις Ασφάλειας	9%	ΠΑΡΑΡΤΗΜΑ Ι ΚΕΦΑΛΑΙΟ 7.1.6.6
B5	Εξειδικευμένες Λύσεις Ασφάλειας Πληροφοριών και Εγγράφων	23%	ΠΑΡΑΡΤΗΜΑ Ι ΚΕΦΑΛΑΙΟ 7.1.6.3
Γ	ΜΕΘΟΔΟΛΟΓΙΑ ΥΛΟΠΟΙΗΣΗΣ - ΔΙΟΙΚΗΣΗΣ	5%	
Γ1	Οργάνωση Υλοποίησης Έργου (Χρονοδιάγραμμα, Παραδοτέα)	3%	ΠΑΡΑΡΤΗΜΑ Ι ΚΕΦΑΛΑΙΟ 7.1.7
Γ2	Μεθοδολογία Διοίκησης και Υλοποίησης Έργου - Προτεινόμενο σχήμα Διοίκησης Έργου	2%	ΠΑΡΑΡΤΗΜΑ Ι ΚΕΦΑΛΑΙΑ 7.1.9, 7.1.10, 7.1.11
ΣΥΝΟΛΟ		100%	

Επεξήγηση Κριτηρίων:

Ανά κατηγορία και κριτήριο αξιολογούνται:

Ομάδα Α - ΠΡΟΔΙΑΓΡΑΦΕΣ ΤΕΧΝΙΚΗΣ ΛΥΣΗΣ

A1: Αντίληψη και κατανόηση του έργου από τον υποψήφιο Ανάδοχο

Αντίληψη και κατανόηση του φυσικού αντικείμενου του έργου από τον υποψήφιο Ανάδοχο

Το κριτήριο A1 «Αντίληψη και κατανόηση του φυσικού αντικείμενου του έργου από τον υποψήφιο Ανάδοχο» αξιολογεί το βαθμό της κατανόησης των ειδικών απαιτήσεων του πλαισίου (context), τη

στοχευμένη προσέγγιση στις ιδιαιτερότητες και την αναγνώριση-ανάλυση των ειδικών θεμάτων (κίνδυνοι, κρίσιμοι παράγοντες) που σχετίζονται με το συγκεκριμένο έργο.

Ομάδα Β - ΠΡΟΔΙΑΓΡΑΦΕΣ ΥΠΗΡΕΣΙΩΝ

B1 Πολιτικές – Διαδικασίες και Μέτρα Αντιμετώπισης και Πρόληψης Κινδύνων

Το κριτήριο B1 αξιολογεί το βαθμό καταλληλότητας της προτεινόμενης μεθοδολογίας και το βαθμό συμβατότητας της μεθόδου παροχής των υπηρεσιών με τις συνθήκες λειτουργίας του φορέα και τους στόχους του έργου. Αξιολογείται η κάλυψη των προδιαγραφών του κεφαλαίου 7.1.6.2 του Παραρτήματος Ι της διακήρυξης.

B2 Υπηρεσίες Soc & DDOS

Το κριτήριο B2 αξιολογεί το βαθμό καταλληλότητας της προτεινόμενης μεθοδολογίας και το βαθμό συμβατότητας της μεθόδου παροχής των υπηρεσιών με τις συνθήκες λειτουργίας του φορέα και τους στόχους του έργου. Αξιολογείται η κάλυψη των προδιαγραφών του κεφαλαίου 7.1.6.5 του Παραρτήματος Ι της διακήρυξης.

B3 Υπηρεσίες νεφοϋπολογιστικών υποδομών και υπηρεσιών

Το κριτήριο B3 αξιολογεί το βαθμό καταλληλότητας της προτεινόμενης μεθοδολογίας και το βαθμό συμβατότητας της μεθόδου παροχής των υπηρεσιών με τις συνθήκες λειτουργίας του φορέα και τους στόχους του έργου. Αξιολογείται η κάλυψη των προδιαγραφών του κεφαλαίου 7.1.6.4 του Παραρτήματος Ι της διακήρυξης.

B4 Εξειδικευμένες Λύσεις Ασφάλειας

Το κριτήριο B4 αξιολογεί το βαθμό καταλληλότητας της προτεινόμενης μεθοδολογίας και τα τεχνικά χαρακτηριστικά των προσφερόμενων λύσεων με τις συνθήκες λειτουργίας του φορέα και τους στόχους του έργου. Αξιολογείται η κάλυψη των προδιαγραφών του κεφαλαίου 7.1.6.6 του Παραρτήματος Ι της διακήρυξης.

B5 Εξειδικευμένες Λύσεις Ασφάλειας Πληροφοριών και Εγγράφων

Το κριτήριο B5 αξιολογεί το βαθμό καταλληλότητας της προτεινόμενης μεθοδολογίας και τα τεχνικά χαρακτηριστικά των προσφερόμενων λύσεων με τις συνθήκες λειτουργίας του φορέα και τους στόχους του έργου. Αξιολογείται η κάλυψη των προδιαγραφών του κεφαλαίου 7.1.6.3 του Παραρτήματος Ι της διακήρυξης.

Ομάδα Γ – ΜΕΘΟΔΟΛΟΓΙΑ ΥΛΟΠΟΙΗΣΗΣ - ΔΙΟΙΚΗΣΗΣ

Γ1: Οργάνωση Υλοποίησης Έργου (Χρονοδιάγραμμα, Παραδοτέα)

Στα πλαίσια του κριτηρίου Γ1 αξιολογούνται:

- η σαφήνεια και πληρότητα ανάλυσης των προσφερόμενων υπηρεσιών του Υποψήφιου Αναδόχου, σε συνάρτηση με τον προσφερόμενο ανθρωποχρόνο,
- ο ρεαλιστικός χρονοπρογραμματισμός των παρεχόμενων εργασιών του υποψήφιου Αναδόχου με βάση τις επιχειρησιακές απαιτήσεις του Κυρίου του Έργου,

- η ορθολογική ανάλυση του αντικειμένου του έργου σε Ενότητες Εργασίας και επιμέρους δραστηριότητες / ενέργειες υλοποίησης του Έργου και των μεταξύ τους αλληλεξαρτήσεων, λαμβάνοντας υπόψη το φυσικό αντικείμενο και το χρονοδιάγραμμα υλοποίησής του,
- η ανάλυση, δομή και οργάνωση των παραδοτέων και η σύνδεσή τους με τις Ενότητες Εργασίας, σε σχέση με την προτεινόμενη Μεθοδολογία, τη ρεαλιστικότητα της προσέγγισης και την ολοκληρωμένη αντίληψη του υποψήφιου Αναδόχου για το Έργο,
- η λίστα με τα ορόσημα του Έργου, που αφορούν κρίσιμα σημεία/στιγμιότυπα του χρονοδιαγράμματος του Έργου, στα οποία το Έργο απομπλέκεται από κάποιο σημαντικό ρίσκο ή/και επιτυγχάνει κάποιο σημαντικό (ενδιάμεσο) στόχο.

Γ2:Μεθοδολογία Διοίκησης και Υλοποίησης Έργου - Προτεινόμενο σχήμα Διοίκησης Έργου

Στα πλαίσια του κριτηρίου Γ2 αξιολογούνται:

- ο βαθμός επάρκειας, σαφήνειας και αποτελεσματικότητας του τρόπου διακυβέρνησης του έργου. Ελέγχεται κατά πόσον από την προσφορά είναι ευδιάκριτα τα όρια λογοδοσίας όλων των ρόλων, καθ' όλον τον κύκλο ζωής του έργου και κατά πόσο ο τρόπος αξιοποίησης εξωτερικών συνεργατών, ή υπεργολάβων συντελεί στην ομαλή διακυβέρνηση χωρίς να αυξάνεται η πολυπλοκότητα,
- η καταλληλότητα και η επάρκεια των διαδικασιών και των μηχανισμών επικοινωνίας της Ομάδας Έργου με τα αρμόδια εμπλεκόμενα τμήματα/μονάδες, με στόχο τόσο τη μεταφορά τεχνογνωσίας όσο και την αποτελεσματικότερη υλοποίηση του έργου,
- η αποτελεσματικότητα της προτεινόμενης μεθοδολογίας διοίκησης και διασφάλισης ποιότητας.

2.3.2 Βαθμολόγηση και κατάταξη προσφορών

2.3.2.1 Βαθμολόγηση Τεχνικών Προσφορών

Η Βαθμολόγηση των τεχνικών προσφορών θα γίνει σύμφωνα με τα "Κριτήρια Αξιολόγησης", όπως αυτά προσδιορίζονται στον πίνακα της παρ. 2.3.1.

Η βαθμολόγηση κάθε κριτηρίου αξιολόγησης κυμαίνεται από 100 βαθμούς στην περίπτωση που ικανοποιούνται ακριβώς όλοι οι όροι των τεχνικών προδιαγραφών, αυξάνεται δε μέχρι τους 150 βαθμούς όταν υπερκαλύπτονται οι απαιτήσεις του συγκεκριμένου κριτηρίου.

Κάθε κριτήριο αξιολόγησης βαθμολογείται αυτόνομα με βάση τα στοιχεία της προσφοράς.

Βαθμολογία μικρότερη από 100 βαθμούς (ήτοι προσφορά που δεν καλύπτει/παρουσιάζει αποκλίσεις από τις τεχνικές προδιαγραφές της παρούσας) επιφέρει την απόρριψη της προσφοράς.

Η σταθμισμένη βαθμολογία του κάθε κριτηρίου θα προκύπτει από το γινόμενο του επιμέρους συντελεστή βαρύτητας επί τη βαθμολογία του, η δε συνολική βαθμολογία της προσφοράς(B_i) θα προκύπτει από το άθροισμα των σταθμισμένων βαθμολογιών όλων των κριτηρίων.

Η συνολική βαθμολογία της τεχνικής προσφοράς υπολογίζεται με βάση τον παρακάτω τύπο :

$$B = \sigma_1 \chi K_1 + \sigma_2 \chi K_2 + \dots + \sigma_n \chi K_n$$

2.3.2.2 Α. Κατάταξη προσφορών

Πλέον συμφέρουσα από οικονομική άποψη προσφορά είναι εκείνη που παρουσιάζει το μεγαλύτερο Λ ο οποίος υπολογίζεται με βάση τον παρακάτω τύπο:

$$\Lambda_i = 80 * (B_i / B_{\max}) + 20 * (K_{\min} / K_i)$$

όπου:

B_{\max} η συνολική βαθμολογία που έλαβε η καλύτερη Τεχνική Προσφορά

B_i η συνολική βαθμολογία της Τεχνικής Προσφοράς i

K_{\min} το συνολικό συγκριτικό κόστος της Προσφοράς με τη μικρότερη τιμή

K_i το συνολικό συγκριτικό κόστος της Προσφοράς i

Λ_i το οποίο στρογγυλοποιείται στα 2 δεκαδικά ψηφία.

2.3.2.3 Διαμόρφωση συγκριτικού κόστους Προσφοράς

Το συγκριτικό κόστος K κάθε Προσφοράς περιλαμβάνει:

- το συνολικό κόστος για το Έργο, χωρίς ΦΠΑ {βλ. ΠΑΡΑΡΤΗΜΑ VI – Υπόδειγμα Οικονομικής Προσφοράς, Πίνακα 4}
- το κόστος συντήρησης του 1ου έτους {βλ. διευκρίνιση} μετά την προσφερόμενη εγγύηση, χωρίς ΦΠΑ {βλ. ΠΑΡΑΡΤΗΜΑ VI – Υπόδειγμα Οικονομικής Προσφοράς, Πίνακα 5}

όπως προκύπτει από τους Πίνακες Οικονομικής Προσφοράς του υποψηφίου Οικονομικού Φορέα.

Διευκρίνιση:

Τυχόν αναπροσαρμογή του ετήσιου κόστους συντήρησης που θα ορίζει ο υποψήφιος Ανάδοχος στην Προσφορά του, θα είναι σταθερή για το σύνολο των ετών συντήρησης και για κάθε έτος δεν θα υπερβαίνει το 5%.

2.4 Κατάρτιση - Περιεχόμενο Προσφορών

2.4.1 Γενικοί όροι υποβολής προσφορών

Οι προσφορές υποβάλλονται με βάση τις απαιτήσεις της παρούσας Διακήρυξης, για όλες τις περιγραφόμενες υπηρεσίες κάθε τμήματος

Δεν επιτρέπονται εναλλακτικές προσφορές.

Η ένωση οικονομικών φορέων υποβάλλει κοινή προσφορά, η οποία υπογράφεται υποχρεωτικά ηλεκτρονικά είτε από όλους τους οικονομικούς φορείς που αποτελούν την ένωση, είτε από εκπρόσωπο τους νομίμως εξουσιοδοτημένο. Στην προσφορά, απαραίτητως πρέπει να προσδιορίζεται η έκταση και το είδος της συμμετοχής του (συμπεριλαμβανομένης της κατανομής αμοιβής μεταξύ τους) κάθε μέλους της ένωσης, καθώς και ο εκπρόσωπος/συντονιστής αυτής.

Οι οικονομικοί φορείς μπορούν να αποσύρουν την προσφορά τους, πριν την καταληκτική ημερομηνία υποβολής προσφοράς, χωρίς να απαιτείται έγκριση εκ μέρους του αποφαινομένου οργάνου της αναθέτουσας αρχής, υποβάλλοντας έγγραφη ειδοποίηση προς την αναθέτουσα αρχή μέσω της λειτουργικότητας «Επικοινωνία» του ΕΣΗΔΗΣ.

2.4.2 Χρόνος και Τρόπος υποβολής προσφορών

2.4.2.1

Οι προσφορές υποβάλλονται από τους ενδιαφερόμενους ηλεκτρονικά, μέσω της διαδικτυακής πύλης www.promitheus.gov.gr του ΕΣΗΔΗΣ, μέχρι την καταληκτική ημερομηνία και ώρα που ορίζει η παρούσα διακήρυξη (άρθρο 1.5), στην Ελληνική Γλώσσα, σε ηλεκτρονικό φάκελο, σύμφωνα με τα αναφερόμενα στο ν.4412/2016, ιδίως στα άρθρα 36 και 37 και στην κατ' εξουσιοδότηση των διατάξεων της παρ. 5 του άρθρου 36 του ν.4412/2016 εκδοθείσα με αρ. 64233(ΦΕΚ Β' 2453/9-06-2021) Κοινή Απόφαση των Υπουργών Ανάπτυξης και Επενδύσεων και Ψηφιακής Διακυβέρνησης «Ρυθμίσεις τεχνικών ζητημάτων που αφορούν την ανάθεση και εκτέλεση των Δημοσίων Συμβάσεων Προμηθειών και Υπηρεσιών με χρήση των επιμέρους εργαλείων και διαδικασιών του Εθνικού Συστήματος Ηλεκτρονικών Δημοσίων Συμβάσεων (ΕΣΗΔΗΣ)» εφεξής «Κ.Υ.Α. ΕΣΗΔΗΣ Προμήθειες και Υπηρεσίες».

Για τη συμμετοχή στο διαγωνισμό οι ενδιαφερόμενοι οικονομικοί φορείς απαιτείται να διαθέτουν προηγμένη ηλεκτρονική υπογραφή που υποστηρίζεται τουλάχιστον από αναγνωρισμένο (εγκεκριμένο) πιστοποιητικό, το οποίο χορηγήθηκε από πάροχο υπηρεσιών πιστοποίησης, ο οποίος περιλαμβάνεται στον κατάλογο εμπιστευσης που προβλέπεται στην απόφαση 2009/767/ΕΚ και σύμφωνα με τα οριζόμενα στο Κανονισμό (ΕΕ) 910/2014 και να εγγραφούν στο ΕΣΗΔΗΣ, σύμφωνα με την περ. β της παρ. 2 του άρθρου 37 του ν. 4412/2016 και τις διατάξεις του άρθρου 6 της Κ.Υ.Α. ΕΣΗΔΗΣ Προμήθειες και Υπηρεσίες.

2.4.2.2

Ο χρόνος υποβολής της προσφοράς μέσω του ΕΣΗΔΗΣ βεβαιώνεται αυτόματα από το ΕΣΗΔΗΣ με υπηρεσίες χρονοσήμανσης, σύμφωνα με τα οριζόμενα στο άρθρο 37 του ν. 4412/2016 και τις διατάξεις του άρθρου 10 της ως άνω κοινής υπουργικής απόφασης.

Μετά την παρέλευση της καταληκτικής ημερομηνίας και ώρας, δεν υπάρχει η δυνατότητα υποβολής προσφοράς στο ΕΣΗΔΗΣ. Σε περιπτώσεις τεχνικής αδυναμίας λειτουργίας του ΕΣΗΔΗΣ, η αναθέτουσα αρχή ρυθμίζει τα της συνέχειας του διαγωνισμού με αιτιολογημένη απόφασή της.

2.4.2.3

Οι οικονομικοί φορείς υποβάλλουν με την προσφορά τους τα ακόλουθα σύμφωνα με τις διατάξεις του άρθρου 13 της Κ.Υ.Α. ΕΣΗΔΗΣ Προμήθειες και Υπηρεσίες:

(α) έναν ηλεκτρονικό (υπο)φάκελο με την ένδειξη «Δικαιολογητικά Συμμετοχής–Τεχνική Προσφορά», στον οποίο περιλαμβάνεται το σύνολο των κατά περίπτωση απαιτούμενων δικαιολογητικών και η τεχνική προσφορά, σύμφωνα με τις διατάξεις της κείμενης νομοθεσίας και την παρούσα.

(β) έναν ηλεκτρονικό (υπο)φάκελο με την ένδειξη «Οικονομική Προσφορά», στον οποίο περιλαμβάνεται η οικονομική προσφορά του οικονομικού φορέα και το σύνολο των κατά περίπτωση απαιτούμενων δικαιολογητικών.

Από τον Οικονομικό Φορέα σημαίνονται, με χρήση της σχετικής λειτουργικότητας του ΕΣΗΔΗΣ, τα στοιχεία εκείνα της προσφοράς του που έχουν εμπιστευτικό χαρακτήρα σύμφωνα με τα οριζόμενα στο άρθρο 21 του ν. 4412/2016. Εφόσον ένας οικονομικός φορέας χαρακτηρίζει πληροφορίες ως εμπιστευτικές, λόγω ύπαρξης τεχνικού ή εμπορικού απορρήτου, στη σχετική δήλωσή του, αναφέρει ρητά όλες τις σχετικές διατάξεις νόμου ή διοικητικές πράξεις που επιβάλλουν την εμπιστευτικότητα της συγκεκριμένης πληροφορίας.

Δεν χαρακτηρίζονται ως εμπιστευτικές, πληροφορίες σχετικά με τις τιμές μονάδας, τις προσφερόμενες ποσότητες, την οικονομική προσφορά και τα στοιχεία της τεχνικής προσφοράς που χρησιμοποιούνται για την αξιολόγησή της.

2.4.2.4

Εφόσον οι Οικονομικοί Φορείς καταχωρίσουν τα σχετικά στοιχεία, μεταδεδομένα και συνημμένα ηλεκτρονικά αρχεία που αφορούν δικαιολογητικά συμμετοχής-τεχνικής προσφοράς και οικονομικής προσφοράς στο ΕΣΗΔΗΣ, στην συνέχεια, μέσω σχετικής λειτουργικότητας, εξάγουν αναφορές (εκτυπώσεις) σε μορφή ηλεκτρονικών αρχείων με μορφότυπο PDF, τα οποία αποτελούν συνοπτική αποτύπωση των καταχωρισμένων στοιχείων. Τα ηλεκτρονικά αρχεία των εν λόγω αναφορών (εκτυπώσεων) υπογράφονται ψηφιακά, σύμφωνα με τις προβλεπόμενες διατάξεις (περ. β της παρ. 2 του άρθρου 37) και επισυνάπτονται από τον Οικονομικό Φορέα στους αντίστοιχους υποφακέλους. Επισημαίνεται ότι η εξαγωγή και η επισύναψη των προαναφερθέντων αναφορών (εκτυπώσεων) δύναται να πραγματοποιείται για κάθε υποφάκελο ξεχωριστά, από τη στιγμή που έχει ολοκληρωθεί η καταχώριση των στοιχείων σε αυτόν.

Εφόσον οι τεχνικές προδιαγραφές και οι οικονομικοί όροι δεν έχουν αποτυπωθεί στο σύνολό τους στις ειδικές ηλεκτρονικές φόρμες του συστήματος, επισυνάπτονται ηλεκτρονικά υπογεγραμμένα **τα** σχετικά ηλεκτρονικά αρχεία (ιδίως τεχνική και οικονομική προσφορά) παραπέμποντας, στα σχετικά άρθρα ή παραρτήματα της διακήρυξης.

2.4.2.5

Ειδικότερα, όσον αφορά τα συνημμένα ηλεκτρονικά αρχεία της προσφοράς, οι Οικονομικοί Φορείς τα καταχωρίζουν στους ανωτέρω (υπο)φακέλους μέσω του Υποσυστήματος, ως εξής :

Τα έγγραφα που καταχωρίζονται στην ηλεκτρονική προσφορά, και δεν απαιτείται να προσκομισθούν και σε έντυπη μορφή, γίνονται αποδεκτά κατά περίπτωση, σύμφωνα με τα προβλεπόμενα στις διατάξεις:

α) είτε των άρθρων 13, 14 και 28 του ν. 4727/2020 (Α' 184) περί ηλεκτρονικών δημοσίων εγγράφων που φέρουν ηλεκτρονική υπογραφή ή σφραγίδα και, εφόσον πρόκειται για αλλοδαπά δημόσια ηλεκτρονικά έγγραφα, εάν φέρουν επισημείωση e-Apostille

β) είτε των άρθρων 15 και 27 του ν. 4727/2020 (Α' 184) περί ηλεκτρονικών ιδιωτικών εγγράφων που φέρουν ηλεκτρονική υπογραφή ή σφραγίδα

γ) είτε του άρθρου 11 του ν. 2690/1999 (Α' 45),

δ) είτε της παρ. 2 του άρθρου 37 του ν. 4412/2016, περί χρήσης ηλεκτρονικών υπογραφών σε ηλεκτρονικές διαδικασίες δημοσίων συμβάσεων,

ε) είτε της παρ. 8 του άρθρου 92 του ν. 4412/2016, περί συνυποβολής υπεύθυνης δήλωσης στην περίπτωση απλής φωτοτυπίας ιδιωτικών εγγράφων.

Επιπλέον, δεν προσκομίζονται σε έντυπη μορφή τα ΦΕΚ και ενημερωτικά και τεχνικά φυλλάδια και άλλα έντυπα, εταιρικά ή μη, με ειδικό τεχνικό περιεχόμενο, δηλαδή έντυπα με αμιγώς τεχνικά χαρακτηριστικά, όπως αριθμούς, αποδόσεις σε διεθνείς μονάδες, μαθηματικούς τύπους και σχέδια.

Ειδικότερα, τα στοιχεία και δικαιολογητικά για τη συμμετοχή του Οικονομικού Φορέα στη διαδικασία καταχωρίζονται από αυτόν σε μορφή ηλεκτρονικών αρχείων με μορφότυπο PDF.

Έως την ημέρα και ώρα αποσφράγισης των προσφορών προσκομίζονται με ευθύνη του οικονομικού φορέα στην αναθέτουσα αρχή, σε έντυπη μορφή και σε κλειστό-ούς φάκελο-ους, στον οποίο αναγράφεται ο αποστολέας και ως παραλήπτης η Επιτροπή Διαγωνισμού του παρόντος διαγωνισμού, τα στοιχεία της ηλεκτρονικής προσφοράς του, τα οποία απαιτείται να προσκομισθούν σε πρωτότυπη μορφή. Τέτοια στοιχεία και δικαιολογητικά ενδεικτικά είναι :

α) η πρωτότυπη εγγυητική επιστολή συμμετοχής, πλην των περιπτώσεων που αυτή εκδίδεται ηλεκτρονικά, άλλως η προσφορά απορρίπτεται ως απαράδεκτη,

β) αυτά που δεν υπάγονται στις διατάξεις του άρθρου 11 παρ. 2 του ν. 2690/1999,

γ) ιδιωτικά έγγραφα τα οποία δεν έχουν επικυρωθεί από δικηγόρο ή δεν φέρουν θεώρηση από υπηρεσίες και φορείς της περίπτωσης α της παρ. 2 του άρθρου 11 του ν. 2690/1999 ή δεν συνοδεύονται από υπεύθυνη δήλωση για την ακρίβειά τους, καθώς και

δ) τα αλλοδαπά δημόσια έντυπα έγγραφα που φέρουν την επισημείωση της Χάγης (Apostille), ή προξενική θεώρηση και δεν έχουν επικυρωθεί από δικηγόρο.

Σε περίπτωση μη υποβολής ενός ή περισσότερων από τα ως άνω στοιχεία και δικαιολογητικά που υποβάλλονται σε έντυπη μορφή, πλην της πρωτότυπης εγγύησης συμμετοχής, η αναθέτουσα αρχή δύναται να ζητήσει τη συμπλήρωση και υποβολή τους, σύμφωνα με το άρθρο 102 του ν. 4412/2016.

Στα αλλοδαπά δημόσια έγγραφα και δικαιολογητικά εφαρμόζεται η Συνθήκη της Χάγης της 5ης.10.1961, που κυρώθηκε με το ν. 1497/1984 (Α' 188), εφόσον συντάσσονται σε κράτη που έχουν προσχωρήσει στην ως άνω Συνθήκη, άλλως φέρουν προξενική θεώρηση. Απαλλάσσονται από την απαίτηση επικύρωσης (με Apostille ή Προξενική Θεώρηση) αλλοδαπά δημόσια έγγραφα όταν καλύπτονται από διμερείς ή πολυμερείς συμφωνίες που έχει συνάψει η Ελλάδα (ενδεικτικά «Σύμβαση νομικής συνεργασίας μεταξύ Ελλάδας και Κύπρου – 05.03.1984» (κυρωτικός ν.1548/1985, «Σύμβαση περί απαλλαγής από την επικύρωση ορισμένων πράξεων και εγγράφων – 15.09.1977» (κυρωτικός ν.4231/2014)). Επίσης, απαλλάσσονται από την απαίτηση επικύρωσης ή παρόμοιας διατύπωσης δημόσια έγγραφα που εκδίδονται από τις αρχές κράτους μέλους που υπάγονται στον Καν ΕΕ 2016/1191 για την απλούστευση των απαιτήσεων για την υποβολή ορισμένων δημοσίων εγγράφων στην ΕΕ, όπως, ενδεικτικά, το λευκό ποινικό μητρώο, υπό τον όρο ότι τα σχετικά με το γεγονός αυτό δημόσια έγγραφα εκδίδονται για πολίτη της Ένωσης από τις αρχές του κράτους μέλους της ιθαγένειάς του.

Σημειώνεται ότι, γίνονται υποχρεωτικά αποδεκτά ευκρινή φωτοαντίγραφα εγγράφων που έχουν εκδοθεί από αλλοδαπές αρχές και έχουν επικυρωθεί από δικηγόρο, σύμφωνα με τα προβλεπόμενα στην παρ. 2 περ. β του άρθρου 11 του ν. 2690/1999 "Κώδικας Διοικητικής Διαδικασίας", όπως αντικαταστάθηκε ως άνω με το άρθρο 1 παρ.2 του ν.4250/2014.

Οι πρωτότυπες εγγυήσεις συμμετοχής, πλην των εγγυήσεων που εκδίδονται ηλεκτρονικά, προσκομίζονται με ευθύνη του οικονομικού φορέα, σε κλειστό φάκελο, στον οποίο αναγράφεται ο αποστολέας, τα στοιχεία του παρόντος διαγωνισμού και ως παραλήπτης η Επιτροπή Διαγωνισμού, το αργότερο πριν την ημερομηνία και ώρα αποσφράγισης των προσφορών που ορίζεται στην παρ. 3.1 της παρούσας, άλλως η προσφορά απορρίπτεται ως απαράδεκτη μετά από γνώμη της Επιτροπής Διαγωνισμού.

Η προσκόμιση των εγγυήσεων συμμετοχής πραγματοποιείται είτε με κατάθεση του ως άνω φακέλου στην υπηρεσία πρωτοκόλλου της αναθέτουσας αρχής, είτε με την αποστολή του ταχυδρομικώς, επί αποδείξει. Το βάρος απόδειξης της έγκαιρης προσκόμισης φέρει ο οικονομικός φορέας. Το εμπρόθεσμο αποδεικνύεται με την επίκληση του αριθμού πρωτοκόλλου ή την προσκόμιση του σχετικού αποδεικτικού αποστολής κατά περίπτωση.

Στην περίπτωση που επιλεγεί η αποστολή του φακέλου της εγγύησης συμμετοχής ταχυδρομικώς, ο οικονομικός φορέας αναρτά, εφόσον δεν διαθέτει αριθμό έγκαιρης εισαγωγής του φακέλου του στο πρωτόκολλο της αναθέτουσας αρχής, το αργότερο έως την ημερομηνία και ώρα αποσφράγισης των προσφορών, μέσω της λειτουργικότητας «Επικοινωνία», τα σχετικά αποδεικτικά στοιχεία προσκόμισης (αποδεικτικό κατάθεσης σε υπηρεσίες ταχυδρομείου- ταχυμεταφορών), προκειμένου να ενημερώσει την αναθέτουσα αρχή περί της τήρησης της υποχρέωσής του σχετικά με την (εμπρόθεσμη) προσκόμιση της εγγύησης συμμετοχής του στον παρόντα διαγωνισμό.

2.4.3 Περιεχόμενα Φακέλου «Δικαιολογητικά Συμμετοχής - Τεχνική Προσφορά»

2.4.3.1 Δικαιολογητικά Συμμετοχής

Τα στοιχεία και δικαιολογητικά για την συμμετοχή των προσφερόντων στη διαγωνιστική διαδικασία περιλαμβάνουν με ποινή αποκλεισμού τα ακόλουθα υπό α και β στοιχεία:

α) **το Ευρωπαϊκό Ενιαίο Έγγραφο Σύμβασης (ΕΕΕΣ)**, όπως προβλέπεται στις παρ. 1 και 3 του άρθρου 79 του ν. 4412/2016 και τη συνοδευτική υπεύθυνη δήλωση με την οποία ο οικονομικός φορέας δύναται να διευκρινίζει τις πληροφορίες που παρέχει με το ΕΕΕΣ σύμφωνα με την παρ. 9 του ίδιου άρθρου,

β) **την εγγύηση συμμετοχής**, όπως προβλέπεται στο άρθρο 72 του Ν.4412/2016 και τις παραγράφους 2.1.5 και 2.2.2 αντίστοιχα της παρούσας διακήρυξης.

Οι προσφέροντες συμπληρώνουν το σχετικό υπόδειγμα ΕΕΕΣ, το οποίο αποτελεί αναπόσπαστο μέρος της παρούσας διακήρυξης (**ΠΑΡΑΡΤΗΜΑ ΙΙΙ – ΕΥΡΩΠΑΙΚΟ ΕΝΙΑΙΟ ΕΓΓΡΑΦΟ ΣΥΜΒΑΣΗΣ (ΕΕΕΣ)**) ως Παράρτημα αυτής.

Η συμπλήρωσή του δύναται να πραγματοποιηθεί με χρήση του υποσυστήματος Promitheus ESPDint, προσβάσιμου μέσω της Διαδικτυακής Πύλης (www.promitheus.gov.gr) του ΟΠΣ ΕΣΗΔΗΣ, ή άλλης σχετικής συμβατής πλατφόρμας υπηρεσιών διαχείρισης ηλεκτρονικών ΕΕΕΣ. Οι Οικονομικοί Φορείς δύνανται για αυτό το σκοπό να αξιοποιήσουν το αντίστοιχο ηλεκτρονικό αρχείο με μορφότυπο XML που αποτελεί επικουρικό στοιχείο των εγγράφων της σύμβασης.

Το συμπληρωμένο από τον Οικονομικό Φορέα ΕΕΕΣ, καθώς και η τυχόν συνοδευτική αυτού υπεύθυνη δήλωση, υποβάλλονται σύμφωνα με την περίπτωση δ' της παραγράφου [2.4.2.5](#) της παρούσας, σε ψηφιακά υπογεγραμμένο ηλεκτρονικό αρχείο με μορφότυπο PDF.

Αναλυτικές οδηγίες και πληροφορίες για το θεσμικό πλαίσιο, τον τρόπο χρήσης και συμπλήρωσης ηλεκτρονικών ΕΕΕΣ και της χρήση του υποσυστήματος Promitheus ESPDint είναι αναρτημένες σε σχετική θεματική ενότητα στη Διαδικτυακή Πύλη (www.promitheus.gov.gr) του ΟΠΣ ΕΣΗΔΗΣ.

Οι ενώσεις οικονομικών φορέων που υποβάλλουν κοινή προσφορά, υποβάλλουν το ΕΕΕΣ για κάθε οικονομικό φορέα που συμμετέχει στην ένωση.

ΕΕΕΣ

Οι υποψήφιοι οικονομικοί υποβάλουν το ΕΕΕΣ, εντός του φακέλου των δικαιολογητικών συμμετοχής, ψηφιακά υπογεγραμμένο από τον κατά περίπτωση εκπρόσωπο του οικονομικού φορέα (ως εκπρόσωπος του οικονομικού φορέα, νοείται ο νόμιμος εκπρόσωπος αυτού, όπως προκύπτει από το ισχύον καταστατικό ή το πρακτικό εκπροσώπησης του κατά το χρόνο υποβολής της προσφοράς ή αίτησης συμμετοχής ή το αρμοδώς εξουσιοδοτημένο φυσικό πρόσωπο να εκπροσωπεί τον οικονομικό φορέα για διαδικασίες σύναψης συμβάσεων ή για συγκεκριμένη διαδικασία σύναψης σύμβασης).

Οι προσφέροντες συμπληρώνουν το σχετικό πρότυπο ΕΕΕΣ το οποίο έχει αναρτηθεί, σε μορφή αρχείων τύπου XML και PDF, στη διαδικτυακή πύλη www.promitheus.gov.gr του ΕΣΗΔΗΣ και

αποτελεί αναπόσπαστο τμήμα της διακήρυξης **ΠΑΡΑΡΤΗΜΑ ΙΙΙ – ΕΥΡΩΠΑΙΚΟ ΕΝΙΑΙΟ ΕΓΓΡΑΦΟ ΣΥΜΒΑΣΗΣ (ΕΕΕΣ)**.

Επισημαίνονται τα ακόλουθα, αναφορικά με την συμπλήρωση και υποβολή του ΕΕΕΣ:

α. ΕΕΕΣ –Οικονομικού Φορέα

Στην περίπτωση που ένας οικονομικός φορέας συμμετέχει μόνος του στο διαγωνισμό και δεν στηρίζεται στις ικανότητες άλλων οντοτήτων προκειμένου να ανταποκριθεί στα κριτήρια επιλογής, συμπληρώνεται υποβάλλει ένα (1) ΕΕΕΣ.

β. ΕΕΕΣ – Στήριξη Οικονομικού Φορέα στις ικανότητες άλλων φορέων

Στην περίπτωση που ένας οικονομικός φορέας στηρίζεται στις ικανότητες μίας ή περισσότερων άλλων οντοτήτων προκειμένου να ανταποκριθεί στα κριτήρια επιλογής, με την προσφορά υποβάλλεται χωριστό ΕΕΕΣ, που συμπληρώνεται και υπογράφεται ψηφιακά από τον τρίτο/ους, συμπληρώνοντας:

- τις ενότητες των Α και Β του Μέρους ΙΙ , το Μέρος ΙΙΙ , το Μέρος ΙV σχετικά με τις ικανότητες που δανείζει στον υποψήφιο οικονομικό φορέα καθώς και το Μέρος VI Τελικές Δηλώσεις

Για την υπογραφή του ΕΕΕΣ του τρίτου/ων ισχύουν τα ανωτέρω αναφερόμενα για την υπογραφή του ΕΕΕΣ του προσφέροντος.

γ. ΕΕΕΣ - Ενώσεις οικονομικών φορέων Κοινοπραξίες κλπ

Στην περίπτωση συμμετοχής στο διαγωνισμό από κοινού ομίλων οικονομικών φορέων (λ.χ ενώσεων, κοινοπραξιών, συνεταιρισμών κλπ), υποβάλλεται χωριστό ΕΕΕΣ για κάθε έναν συμμετέχοντα οικονομικό φορέα.

δ. ΕΕΕΣ - Υπεργολάβοι:

Σε περίπτωση που ο προσφέρων προτίθεται να αναθέσει υπό μορφή υπεργολαβίας σε τρίτο/ους (βλ. ΕΕΕΣ, μέρος ΙΙ, παράγραφος Δ «Πληροφορίες σχετικά με υπεργολάβους στην ικανότητα των οποίων δεν στηρίζεται ο οικονομικός φορέας») και το τμήμα του έργου που πρόκειται να ανατεθεί υπεργολαβικά υπερβαίνει το τριάντα τοις εκατό (30%) της συνολικής αξίας της σύμβασης, τότε ο υπεργολάβος συμπληρώνει και υπογράφει ψηφιακά χωριστό ΕΕΕΣ, το οποίο υποβάλλεται εντός του φακέλου δικαιολογητικών συμμετοχής, συμπληρώνοντας τα πεδία της ενότητας Α και Β του Μέρους ΙΙ και τα πεδία των ενότητων του Μέρους ΙΙΙ καθώς και το Μέρος VI Τελικές Δηλώσεις.

Για την υπογραφή του ΕΕΕΣ του υπεργολάβου ισχύουν και εφαρμόζονται τα ανωτέρω αναφερόμενα για την υπογραφή του ΕΕΕΣ του προσφέροντος.

2.4.3.2 Τεχνική Προσφορά

Η τεχνική προσφορά θα πρέπει να καλύπτει όλες τις απαιτήσεις και τις προδιαγραφές της παρούσας και συγκεκριμένα των Παραρτημάτων ΠΑΡΑΡΤΗΜΑ Ι και ΙΙ της παρούσας Διακήρυξης, περιγράφοντας ακριβώς πώς οι συγκεκριμένες απαιτήσεις και προδιαγραφές πληρούνται. Περιλαμβάνει ιδίως τα έγγραφα και δικαιολογητικά, βάσει των οποίων θα αξιολογηθεί η καταλληλότητα των προσφερόμενων υπηρεσιών, με βάση το κριτήριο ανάθεσης, σύμφωνα με τα αναλυτικώς αναφερόμενα στο ως άνω Παράρτημα.

Οι τεχνικές προδιαγραφές της παρούσας δεν έχουν αποτυπωθεί στις ειδικές ηλεκτρονικές φόρμες του ΕΣΗΔΗΣ, για αυτό οι υποψήφιοι Οικονομικοί Φορείς συντάσσουν την τεχνική προσφορά τους και υποβάλλουν ψηφιακά υπογεγραμμένα τα σχετικά ηλεκτρονικά αρχεία της Τεχνικής Προσφοράς σύμφωνα με το ΠΑΡΑΡΤΗΜΑ V – Υπόδειγμα Τεχνικής Προσφοράς της παρούσας διακήρυξης (σε συμπίεσμένη μορφή και κατά προτίμηση σε ένα (1) αρχείο pdf). Επιπλέον οι οικονομικοί φορείς αναφέρουν στην τεχνική προσφορά τους, ξεχωριστά για κάθε τμήμα της συμφωνίας – πλαίσιο για το οποίο υποβάλουν προσφορά, το τμήμα της σύμβασης που προτίθενται να αναθέσουν υπό μορφή υπεργολαβίας σε τρίτους, καθώς και τους υπεργολάβους που προτείνουν.

2.4.4 Περιεχόμενα Φακέλου «Οικονομική Προσφορά» / Τρόπος σύνταξης και υποβολής οικονομικών προσφορών

Η οικονομική προσφορά συντάσσεται με βάση το κριτήριο ανάθεσης και σύμφωνα με το υπόδειγμα που παρέχεται στο ΠΑΡΑΡΤΗΜΑ VI – Υπόδειγμα Οικονομικής Προσφοράς της παρούσας Διακήρυξης και υποβάλλεται ηλεκτρονικά σε μορφή αρχείου .pdf ψηφιακά υπογεγραμμένη, στον Υποφάκελο «Οικονομική Προσφορά».

Η τιμή δίνεται σε ευρώ ανά μονάδα μέτρησης.

Στην τιμή περιλαμβάνονται οι υπέρ τρίτων κρατήσεις, ως και κάθε άλλη επιβάρυνση, σύμφωνα με την κείμενη νομοθεσία, μη συμπεριλαμβανομένου Φ.Π.Α., για την παροχή των υπηρεσιών στον τόπο και με τον τρόπο που προβλέπεται στα της παρούσας.

Οι υπέρ τρίτων κρατήσεις υπόκεινται στο εκάστοτε ισχύον αναλογικό τέλος χαρτοσήμου και στην επ' αυτού εισφορά υπέρ ΟΓΑ.

Οι προσφερόμενες τιμές είναι σταθερές καθ' όλη τη διάρκεια της σύμβασης και δεν αναπροσαρμόζονται

Ως απαράδεκτες θα απορρίπτονται προσφορές στις οποίες:

- α) δεν δίνεται τιμή σε ΕΥΡΩ ή που καθορίζεται σχέση ΕΥΡΩ προς ξένο νόμισμα,
- β) δεν προκύπτει με σαφήνεια η προσφερόμενη τιμή, με την επιφύλαξη του άρθρου 102 του ν. 4412/2016 όπως τροποποιήθηκε με το άρθρο 42 του ν. 4782/Α36/9-3-2021 και
- γ) η τιμή υπερβαίνει τον προϋπολογισμό του αντίστοιχου τμήματος της συμφωνίας-πλαίσιο που καθορίζεται στην παρούσα διακήρυξη.

Στην οικονομική προσφορά θα πρέπει να επιλέγεται με σαφήνεια ένας από τους τρόπους πληρωμής που περιγράφονται στην παρ. 5.1 της παρούσας διακήρυξης.

2.4.5 Χρόνος ισχύος των προσφορών

Οι υποβαλλόμενες προσφορές ισχύουν και δεσμεύουν τους οικονομικούς φορείς για διάστημα δώδεκα (12) μηνών από την επόμενη της καταληκτικής ημερομηνίας υποβολής τους.

Προσφορά η οποία ορίζει χρόνο ισχύος μικρότερο από τον ανωτέρω προβλεπόμενο απορρίπτεται.

Η ισχύς της προσφοράς μπορεί να παρατείνεται εγγράφως, εφόσον τούτο ζητηθεί από την αναθέτουσα αρχή, πριν από τη λήξη της, με αντίστοιχη παράταση της εγγυητικής επιστολής

συμμετοχής σύμφωνα με τα οριζόμενα στο άρθρο 72 παρ. 1 α του ν. 4412/2016 και την παράγραφο 2.2.2 της παρούσας, κατ' ανώτατο όριο για χρονικό διάστημα ίσο με την προβλεπόμενη ως άνω αρχική διάρκεια. Σε περίπτωση αιτήματος της αναθέτουσας αρχής για παράταση της ισχύος της προσφοράς, για τους οικονομικούς φορείς, που αποδέχτηκαν την παράταση, πριν τη λήξη ισχύος των προσφορών τους, οι προσφορές ισχύουν και τους δεσμεύουν για το επιπλέον αυτό χρονικό διάστημα.

Μετά τη λήξη και του παραπάνω ανώτατου ορίου χρόνου παράτασης ισχύος της προσφοράς, τα αποτελέσματα της διαδικασίας ανάθεσης ματαιώνονται, εκτός αν η αναθέτουσα αρχή κρίνει, κατά περίπτωση, αιτιολογημένα, ότι η συνέχιση της διαδικασίας εξυπηρετεί το δημόσιο συμφέρον, οπότε οι οικονομικοί φορείς που συμμετέχουν στη διαδικασία μπορούν να επιλέξουν είτε να παρατείνουν την προσφορά και την εγγύηση συμμετοχής τους, εφόσον τους ζητηθεί πριν την πάροδο του ανωτέρω ανώτατου ορίου παράτασης της προσφοράς τους είτε όχι. Στην τελευταία περίπτωση, η διαδικασία συνεχίζεται με όσους παρέτειναν τις προσφορές τους και αποκλείονται οι λοιποί οικονομικοί φορείς. Σε περίπτωση που λήξει ο χρόνος ισχύος των προσφορών και δεν ζητηθεί παράταση της προσφοράς, η αναθέτουσα αρχή δύναται με αιτιολογημένη απόφασή της, εφόσον η εκτέλεση της σύμβασης εξυπηρετεί το δημόσιο συμφέρον, να ζητήσει εκ των υστέρων από τους οικονομικούς φορείς που συμμετέχουν στη διαδικασία είτε να παρατείνουν την προσφορά τους είτε όχι. Στην τελευταία περίπτωση, η διαδικασία συνεχίζεται με όσους παρέτειναν τις προσφορές τους.

2.4.6 Λόγοι απόρριψης προσφορών

Η αναθέτουσα αρχή με βάση τα αποτελέσματα του ελέγχου και της αξιολόγησης των προσφορών, απορρίπτει, σε κάθε περίπτωση, προσφορά:

- 1) η οποία αποκλίνει από अपαράβατους όρους περί σύνταξης και υποβολής της προσφοράς, ή δεν υποβάλλεται εμπρόθεσμα, με τον τρόπο και με το περιεχόμενο που ορίζεται στην παρούσα και συγκεκριμένα στις παραγράφους 2.4.1 (Γενικοί όροι υποβολής προσφορών), 2.4.2 (Χρόνος και τρόπος υποβολής προσφορών), 2.4.3 (Περιεχόμενο φακέλων δικαιολογητικών συμμετοχής, τεχνικής προσφοράς), 2.4.4 (Περιεχόμενο φακέλου οικονομικής προσφοράς, τρόπος σύνταξης και υποβολής οικονομικών προσφορών), 2.4.5 (Χρόνος ισχύος προσφορών), 3.1 (Αποσφράγιση και αξιολόγηση προσφορών), 3.2 (Πρόσκληση υποβολής δικαιολογητικών προσωρινού αναδόχου) της παρούσας,
 - 2) η οποία περιέχει ατελείς, ελλιπείς, ασαφείς ή λανθασμένες πληροφορίες ή τεκμηρίωση, συμπεριλαμβανομένων των πληροφοριών που περιέχονται στο ΕΕΕΣ, εφόσον αυτές δεν επιδέχονται συμπλήρωσης, διόρθωσης, αποσαφήνισης ή διευκρίνισης ή, εφόσον επιδέχονται, δεν έχουν αποκατασταθεί από τον προσφέροντα, εντός της προκαθορισμένης προθεσμίας, σύμφωνα το άρθρο 102 του ν. 4412/2016 και την παρ. [3.1.1](#) της παρούσας διακήρυξης,,
 - 3) για την οποία ο προσφέρων δεν παράσχει τις απαιτούμενες εξηγήσεις, εντός της προκαθορισμένης προθεσμίας ή η εξήγηση δεν είναι αποδεκτή από την αναθέτουσα αρχή σύμφωνα με την παράγραφο 3.1.1. της παρούσας και τα άρθρα 102 και 103 του ν. 4412/2016,
 - 4) η οποία είναι εναλλακτική προσφορά.
 - 5) η οποία υποβάλλεται από έναν προσφέροντα που έχει υποβάλλει δύο ή περισσότερες προσφορές
- Ο περιορισμός αυτός ισχύει, υπό τους όρους της παραγράφου 2.2.3.3 περ.γ της παρούσας (περ.

γ' της παρ. 4 του άρθρου 73 του ν. 4412/2016) και στην περίπτωση ενώσεων οικονομικών φορέων με κοινά μέλη, καθώς και στην περίπτωση οικονομικών φορέων που συμμετέχουν είτε αυτοτελώς είτε ως μέλη ενώσεων,

- 6) η οποία είναι υπό αίρεση,
- 7) η οποία θέτει όρο αναπροσαρμογής,
- 8) η οποία εμφανίζει οποιοδήποτε στοιχείο του προσφερομένου κόστους σε είδος, προϊόν ή υπηρεσία (εκτός εάν ρητά απαιτείται από τη διακήρυξη), ή σε μερικό ή γενικό σύνολο σε άλλο μέρος πλην της Οικονομικής Προσφοράς,
- 9) για την οποία ο προσφέρων δεν παράσχει, εντός αποκλειστικής προθεσμίας είκοσι (20) ημερών από την κοινοποίηση σε αυτόν σχετικής πρόσκλησης της αναθέτουσας αρχής, εξηγήσεις αναφορικά με την τιμή ή το κόστος που προτείνει σε αυτήν, στην περίπτωση που η προσφορά του φαίνεται ασυνήθιστα χαμηλή σε σχέση με τις υπηρεσίες, σύμφωνα με την παρ. 1 του άρθρου 88 του ν. 4412/2016,
- 10) εφόσον διαπιστωθεί ότι είναι ασυνήθιστα χαμηλή διότι δε συμμορφώνεται με τις ισχύουσες υποχρεώσεις της παρ. 2 του άρθρου 18 του ν. 4412/2016,
- 11) η οποία παρουσιάζει αποκλίσεις ως προς τους όρους και τις τεχνικές προδιαγραφές της σύμβασης,
- 12) η οποία παρουσιάζει ελλείψεις ως προς τα δικαιολογητικά που ζητούνται από τα έγγραφα της παρούσας διακήρυξης, εφόσον αυτές δεν θεραπευτούν από τον προσφέροντα με την υποβολή ή τη συμπλήρωσή τους, εντός της προκαθορισμένης προθεσμίας, σύμφωνα με τα άρθρα 102 και 103 του ν. 4412/2016,
- 13) εάν από τα δικαιολογητικά του άρθρου 103 του ν. 4412/2016, που προσκομίζονται από τον προσωρινό ανάδοχο, δεν αποδεικνύεται η μη συνδρομή των λόγων αποκλεισμού της παραγράφου 2.2.3 της παρούσας ή η πλήρωση μιας ή περισσότερων από τις απαιτήσεις των κριτηρίων ποιοτικής επιλογής, σύμφωνα με τις παραγράφους 2.2.4., περί κριτηρίων επιλογής,
- 14) εάν κατά τον έλεγχο των ως άνω δικαιολογητικών του άρθρου 103 του ν. 4412/2016, διαπιστωθεί ότι τα στοιχεία που δηλώθηκαν, σύμφωνα με το άρθρο 79 του ν. 4412/2016, είναι εκ προθέσεως απατηλά, ή ότι έχουν υποβληθεί πλαστά αποδεικτικά στοιχεία.
- 15) η οποία παρουσιάζει διαφορές μεταξύ των Πινάκων Οικονομικής Προσφοράς χωρίς τιμές και των αντιστοίχων Πινάκων Οικονομικής Προσφοράς με τιμές,
- 16) της οποίας το συνολικό τίμημα υπερβαίνει τον προϋπολογισμό του Έργου,
- 17) που η προσφερόμενη εγγύηση είναι μικρότερης χρονικής διάρκειας από την ελάχιστη ζητούμενη και δεν καλύπτει το σύνολο της προσφερόμενης λύσης.

3 ΔΙΕΝΕΡΓΕΙΑ ΔΙΑΔΙΚΑΣΙΑΣ - ΑΞΙΟΛΟΓΗΣΗ ΠΡΟΣΦΟΡΩΝ

3.1 Αποσφράγιση και αξιολόγηση προσφορών

3.1.1 Ηλεκτρονική αποσφράγιση προσφορών

Το πιστοποιημένο στο ΕΣΗΔΗΣ, για την αποσφράγιση των προσφορών αρμόδιο όργανο της Αναθέτουσας Αρχής (Επιτροπή Διαγωνισμού), προβαίνει στην έναρξη της διαδικασίας ηλεκτρονικής αποσφράγισης των φακέλων των προσφορών, κατά το άρθρο 100 του ν. 4412/2016, ακολουθώντας τα εξής στάδια:

- Ηλεκτρονική Αποσφράγιση του (υπό)φακέλου «Δικαιολογητικά Συμμετοχής-Τεχνική Προσφορά», την ημέρα και ώρα
- Ηλεκτρονική Αποσφράγιση του (υπό)φακέλου «Οικονομική Προσφορά», κατά την ημερομηνία και ώρα που θα ορίσει η Αναθέτουσα Αρχή

Σε κάθε στάδιο τα στοιχεία των προσφορών που αποσφραγίζονται είναι καταρχήν προσβάσιμα μόνο στα μέλη της Επιτροπής Διαγωνισμού και την Αναθέτουσα Αρχή.

3.1.2 Αξιολόγηση προσφορών

Μετά την ηλεκτρονική αποσφράγιση των προσφορών η Αναθέτουσα Αρχή προβαίνει στην αξιολόγηση αυτών μέσω των αρμόδιων πιστοποιημένων στο Σύστημα ΕΣΗΔΗΣ οργάνων της, εφαρμοζόμενων κατά τα λοιπά των κειμένων διατάξεων.

Η αναθέτουσα αρχή, τηρώντας τις αρχές της ίσης μεταχείρισης και της διαφάνειας, ζητά από τους προσφέροντες οικονομικούς φορείς, όταν οι πληροφορίες ή η τεκμηρίωση που πρέπει να υποβάλλονται είναι ή εμφανίζονται ελλιπείς ή λανθασμένες, συμπεριλαμβανομένων εκείνων στο ΕΕΕΣ, ή όταν λείπουν συγκεκριμένα έγγραφα, να υποβάλλουν, να συμπληρώνουν, να αποσαφηνίζουν ή να ολοκληρώνουν τις σχετικές πληροφορίες ή τεκμηρίωση, εντός προθεσμίας όχι μικρότερης των δέκα (10) ημερών και όχι μεγαλύτερης των είκοσι (20) ημερών από την ημερομηνία κοινοποίησης σε αυτούς της σχετικής πρόσκλησης. Η συμπλήρωση ή η αποσαφήνιση ζητείται και γίνεται αποδεκτή υπό την προϋπόθεση ότι δεν τροποποιείται η προσφορά του οικονομικού φορέα και ότι αφορά σε στοιχεία ή δεδομένα, των οποίων είναι αντικειμενικά εξακριβώσιμος ο προγενέστερος χαρακτήρας σε σχέση με το πέρας της καταληκτικής προθεσμίας παραλαβής προσφορών. Τα ανωτέρω ισχύουν κατ' αναλογία και για τυχόν ελλείπουσες δηλώσεις, υπό την προϋπόθεση ότι βεβαιώνουν γεγονότα αντικειμενικώς εξακριβώσιμα.

Ειδικότερα :

α) Η Επιτροπή Διαγωνισμού εξετάζει αρχικά την προσκόμιση της εγγύησης συμμετοχής, σύμφωνα με την παρ. 1 του άρθρου 72. Σε περίπτωση παράλειψης προσκόμισης, είτε της εγγύησης συμμετοχής ηλεκτρονικής έκδοσης, μέχρι την καταληκτική ημερομηνία υποβολής προσφορών, είτε του πρωτοτύπου της έντυπης εγγύησης συμμετοχής, μέχρι την ημερομηνία και ώρα αποσφράγισης, η Επιτροπή Διαγωνισμού συντάσσει πρακτικό στο οποίο εισηγείται την απόρριψη της προσφοράς ως απαράδεκτης.

Στη συνέχεια εκδίδεται από την αναθέτουσα αρχή απόφαση, με την οποία επικυρώνεται το ανωτέρω πρακτικό. Η απόφαση απόρριψης της προσφοράς του παρόντος εδαφίου εκδίδεται πριν από την έκδοση οποιασδήποτε άλλης απόφασης σχετικά με την αξιολόγηση των προσφορών της οικείας διαδικασίας ανάθεσης σύμβασης και κοινοποιείται σε όλους τους προσφέροντες με επιμέλεια αυτής μέσω της λειτουργικότητας της «Επικοινωνίας» του ηλεκτρονικού διαγωνισμού στο ΕΣΗΔΗΣ.

Κατά της εν λόγω απόφασης χωρεί προδικαστική προσφυγή, σύμφωνα με τα οριζόμενα στην παράγραφο [3.4](#) της παρούσας.

Η αναθέτουσα αρχή επικοινωνεί παράλληλα με τους φορείς που φέρονται να έχουν εκδώσει τις εγγυητικές επιστολές, προκειμένου να διαπιστώσει την εγκυρότητά τους.

β) Μετά την έκδοση της ανωτέρω απόφασης η Επιτροπή Διαγωνισμού προβαίνει αρχικά στον έλεγχο των δικαιολογητικών συμμετοχής και εν συνεχεία στην αξιολόγηση και βαθμολόγηση των τεχνικών προσφορών των προσφερόντων, των οποίων τα δικαιολογητικά συμμετοχής έκρινε πλήρη. Η αξιολόγηση και βαθμολόγηση γίνονται σύμφωνα με τα σχετικώς προβλεπόμενα στον ν.4412/2016 και τους όρους της παρούσας. Η διαδικασία αξιολόγησης ολοκληρώνεται με την καταχώριση πρακτικό των προσφερόντων, των αποτελεσμάτων του ελέγχου και της αξιολόγησης των δικαιολογητικών συμμετοχής, των αποτελεσμάτων της αξιολόγησης των τεχνικών προσφορών, της βαθμολόγησης των αποδεκτών τεχνικών προσφορών με βάση τα κριτήρια αξιολόγησης των παραγράφων 2.3.1 και 2.3.2 της παρούσας.

Τα αποτελέσματα των εν λόγω σταδίων («Δικαιολογητικά Συμμετοχής» & «Τεχνική Προσφορά» επικυρώνονται με απόφαση του αποφαινόμενου οργάνου της αναθέτουσας αρχής, η οποία κοινοποιείται στους προσφέροντες, εκτός από όσους αποκλείστηκαν οριστικά δυνάμει της παρ. 1 του άρθρου 72 του ν. 4412/2016, μέσω της λειτουργικότητας της «Επικοινωνίας» του ΕΣΗΔΗΣ. Μετά από την έκδοση και κοινοποίηση της ανωτέρω απόφασης, οι προσφέροντες λαμβάνουν γνώση των λοιπών συμμετεχόντων στη διαδικασία και των στοιχείων που υποβλήθηκαν από αυτούς.

Κατά της εν λόγω απόφασης χωρεί προδικαστική προσφυγή, σύμφωνα με τα οριζόμενα στην παράγραφο 3.4 της παρούσας.

γ) Μετά την ολοκλήρωση της αξιολόγησης, σύμφωνα με τα ανωτέρω, αποσφραγίζονται, κατά την ορισθείσα ημερομηνία και ώρα οι φάκελοι των οικονομικών προσφορών εκείνων των προσφερόντων που δεν έχουν απορριφθεί σύμφωνα με τα ανωτέρω.

δ) Η Επιτροπή Διαγωνισμού προβαίνει στην αξιολόγηση των οικονομικών προσφορών που αποσφραγίστηκαν και συντάσσει πρακτικό στο οποίο καταχωρούνται οι προσφορές κατά σειρά κατάταξης, με βάση τη συνολική βαθμολογία τους, καθώς και η αιτιολογημένη εισήγησή της για την αποδοχή ή απόρριψή τους και την ανάδειξη του προσωρινού αναδόχου.

Εάν οι προσφορές φαίνονται ασυνήθιστα χαμηλές σε σχέση με το αντικείμενο της σύμβασης, η αναθέτουσα αρχή απαιτεί από τους οικονομικούς φορείς, μέσω της λειτουργικότητας της «Επικοινωνίας» του ηλεκτρονικού διαγωνισμού στο ΕΣΗΔΗΣ, να εξηγήσουν την τιμή ή το κόστος που προτείνουν στην προσφορά τους, εντός αποκλειστικής προθεσμίας, κατά ανώτατο όριο είκοσι (20) ημερών από την κοινοποίηση της σχετικής πρόσκλησης. Στην περίπτωση αυτή εφαρμόζονται τα άρθρα 88 και 89 ν. 4412/2016. Εάν τα παρεχόμενα στοιχεία δεν εξηγούν κατά τρόπο ικανοποιητικό

το χαμηλό επίπεδο της τιμής ή του κόστους που προτείνεται, η προσφορά απορρίπτεται ως μη κανονική.

Στην περίπτωση ισοδύναμων προφορών, δηλαδή προσφορών με την ίδια συνολική τελική βαθμολογία μεταξύ δύο ή περισσότερων προσφερόντων, η ανάθεση γίνεται στην προσφορά με τη μεγαλύτερη βαθμολογία τεχνικής προσφοράς.

Αν οι ισοδύναμες προσφορές έχουν την ίδια βαθμολογία τεχνικής προσφοράς η αναθέτουσα αρχή επιλέγει τον ανάδοχο με κλήρωση μεταξύ των οικονομικών φορέων που υπέβαλαν τις ισοδύναμες προσφορές. Η κλήρωση γίνεται ενώπιον της Επιτροπής του Διαγωνισμού και παρουσία αυτών των οικονομικών φορέων.

Στη συνέχεια, εφόσον το αποφαινόμενο όργανο της αναθέτουσας αρχής εγκρίνει το ανωτέρω πρακτικό κατάταξης των προσφορών, εκδίδεται απόφαση για τα αποτελέσματα του εν λόγω σταδίου και η αναθέτουσα αρχή προσκαλεί εγγράφως, μέσω της λειτουργικότητας της «Επικοινωνίας» του ηλεκτρονικού διαγωνισμού στο ΕΣΗΔΗΣ, τον πρώτο σε κατάταξη προσφέροντα, στον οποίον πρόκειται να γίνει η κατακύρωση («προσωρινός ανάδοχος»), να υποβάλει τα δικαιολογητικά κατακύρωσης, σύμφωνα με όσα ορίζονται στο άρθρο 103 και την παρ. 3.2 της παρούσας, περί πρόσκλησης για υποβολή δικαιολογητικών. Η απόφαση έγκρισης του πρακτικού κατάταξης προσφορών δεν κοινοποιείται στους προσφέροντες και ενσωματώνεται στην απόφαση κατακύρωσης.

Σε κάθε περίπτωση, όταν εξ αρχής έχει υποβληθεί μία προσφορά, τα αποτελέσματα όλων των σταδίων της διαδικασίας ανάθεσης, ήτοι Δικαιολογητικών Συμμετοχής, Τεχνικής Προσφοράς και Οικονομικής Προσφοράς, επικυρώνονται με την απόφαση κατακύρωσης του άρθρου 105 του ν. 4412/2016, σύμφωνα με την παράγραφο 3.3 της παρούσας, που εκδίδεται μετά το πέρας και του τελευταίου σταδίου της διαδικασίας. Κατά της ανωτέρω απόφασης χωρεί προδικαστική προσφυγή ενώπιον της Ε.Α.ΔΗ.ΣΥ. σύμφωνα με όσα προβλέπονται στην παράγραφο 3.4 της παρούσας.

3.2 Πρόσκληση υποβολής δικαιολογητικών προσωρινού αναδόχου- Δικαιολογητικά προσωρινού αναδόχου

Μετά την αξιολόγηση των προσφορών, η αναθέτουσα αρχή αποστέλλει σχετική ηλεκτρονική πρόσκληση στον προσφέροντα, στον οποίο πρόκειται να γίνει η κατακύρωση («προσωρινό ανάδοχο»), μέσω της λειτουργικότητας της «Επικοινωνίας» του ηλεκτρονικού διαγωνισμού στο ΕΣΗΔΗΣ και τον καλεί να υποβάλει εντός προθεσμίας δέκα (10) ημερών από την κοινοποίηση της σχετικής έγγραφης ειδοποίησης σε αυτόν, τα αποδεικτικά έγγραφα νομιμοποίησης και τα πρωτότυπα ή αντίγραφα όλων των δικαιολογητικών που περιγράφονται στην παράγραφο [2.2.9.2](#) της παρούσας διακήρυξης, ως αποδεικτικά στοιχεία για τη μη συνδρομή των λόγων αποκλεισμού της παραγράφου [2.2.3](#) της διακήρυξης, καθώς και για την πλήρωση των κριτηρίων ποιοτικής επιλογής των παραγράφων [2.2.4](#) - [2.2.8](#) αυτής.

Ειδικότερα, το σύνολο των στοιχείων και δικαιολογητικών της ως άνω παραγράφου αποστέλλονται από αυτόν σε μορφή ηλεκτρονικών αρχείων με μορφότυπο PDF, σύμφωνα με τα ειδικώς οριζόμενα στην παράγραφο [2.4.2.5](#) της παρούσας.

Εντός της προθεσμίας υποβολής των δικαιολογητικών κατακύρωσης και το αργότερο έως την τρίτη εργάσιμη ημέρα από την καταληκτική ημερομηνία ηλεκτρονικής υποβολής των δικαιολογητικών κατακύρωσης, προσκομίζονται με ευθύνη του οικονομικού φορέα, στην αναθέτουσα αρχή, σε έντυπη μορφή και σε κλειστό φάκελο, στον οποίο αναγράφεται ο αποστολέας, τα στοιχεία του Διαγωνισμού και ως παραλήπτης η Επιτροπή Διαγωνισμού, τα στοιχεία και δικαιολογητικά, τα οποία απαιτείται να προσκομισθούν σε έντυπη μορφή (ως πρωτότυπα ή ακριβή αντίγραφα), σύμφωνα με τα προβλεπόμενα στις διατάξεις της ως άνω παραγράφου [2.4.2.5](#).

Αν δεν προσκομισθούν τα παραπάνω δικαιολογητικά ή υπάρχουν ελλείψεις σε αυτά που υποβλήθηκαν, η αναθέτουσα αρχή καλεί τον προσωρινό ανάδοχο να προσκομίσει τα ελλείποντα δικαιολογητικά ή να συμπληρώσει τα ήδη υποβληθέντα ή να παράσχει διευκρινήσεις, με την έννοια του άρθρου 102 του ν. 4412/2016, εντός δέκα (10) ημερών από την κοινοποίηση της σχετικής πρόσκλησης σε αυτόν.

Ο προσωρινός ανάδοχος δύναται να υποβάλει αίτημα, μέσω της λειτουργικότητας της «Επικοινωνίας» του ηλεκτρονικού διαγωνισμού στο ΕΣΗΔΗΣ, προς την αναθέτουσα αρχή, για παράταση της ως άνω προθεσμίας, συνοδευόμενο από αποδεικτικά έγγραφα περί αίτησης χορήγησης δικαιολογητικών προσωρινού αναδόχου. Στην περίπτωση αυτή η αναθέτουσα αρχή παρατείνει την προθεσμία υποβολής αυτών, για όσο χρόνο απαιτηθεί για τη χορήγησή τους από τις αρμόδιες δημόσιες αρχές. Ο προσωρινός ανάδοχος μπορεί να αξιοποιεί τη δυνατότητα αυτή τόσο εντός της αρχικής προθεσμίας για την υποβολή δικαιολογητικών όσο και εντός της προθεσμίας για την προσκόμιση ελλειπόντων ή τη συμπλήρωση ήδη υποβληθέντων δικαιολογητικών, κατά την έννοια του άρθρου 102 του ν. 4412/2016, ως ανωτέρω προβλέπεται. Η παρούσα ρύθμιση εφαρμόζεται αναλόγως και όταν η αναθέτουσα αρχή ζητήσει την προσκόμιση των δικαιολογητικών κατά τη διαδικασία αξιολόγησης των προσφορών ή αιτήσεων συμμετοχής και πριν από το στάδιο κατακύρωσης, κατ' εφαρμογή της διάταξης του πρώτου εδαφίου της παρ. 5 του άρθρου 79 του ν. 4412/2016, τηρουμένων των αρχών της ίσης μεταχείρισης και της διαφάνειας.

Απορρίπτεται η προσφορά του προσωρινού αναδόχου, καταπίπτει υπέρ της αναθέτουσας αρχής η εγγύηση συμμετοχής του και η κατακύρωση γίνεται στον προσφέροντα που υπέβαλε την αμέσως

επόμενη πλέον συμφέρουσα από οικονομική άποψη προσφορά, τηρουμένης της ανωτέρω διαδικασίας, εάν:

i) κατά τον έλεγχο των παραπάνω δικαιολογητικών διαπιστωθεί ότι τα στοιχεία που δηλώθηκαν με το Ευρωπαϊκό Ενιαίο Έγγραφο Σύμβασης (ΕΕΕΣ) είναι εκ προθέσεως απατηλά, ή έχουν υποβληθεί πλαστά αποδεικτικά στοιχεία, ή

ii) δεν υποβληθούν στο προκαθορισμένο χρονικό διάστημα τα απαιτούμενα πρωτότυπα ή αντίγραφα των παραπάνω δικαιολογητικών, ή

iii) από τα δικαιολογητικά που προσκομίσθηκαν νομίμως και εμπροθέσμως, δεν αποδεικνύεται η μη συνδρομή των λόγων αποκλεισμού σύμφωνα με την παράγραφο [2.2.3](#) (λόγοι αποκλεισμού) ή η πλήρωση μιας ή περισσότερων από τις απαιτήσεις των κριτηρίων ποιοτικής επιλογής σύμφωνα με τις παραγράφους [2.2.4](#) - [2.2.8](#) (κριτήρια ποιοτικής επιλογής) της παρούσας,

Σε περίπτωση έγκαιρης και προσήκουσας ενημέρωσης της αναθέτουσας αρχής για μεταβολές στις προϋποθέσεις, τις οποίες ο προσωρινός ανάδοχος είχε δηλώσει με το Ευρωπαϊκό Ενιαίο Έγγραφο Σύμβασης (ΕΕΕΣ) ότι πληροί, οι οποίες μεταβολές επήλθαν ή για τις οποίες μεταβολές έλαβε γνώση μετά την δήλωση και μέχρι την ημέρα της σύναψης της σύμβασης (οψιγενείς μεταβολές), δεν καταπίπτει υπέρ της Αναθέτουσας Αρχής η εγγύηση συμμετοχής του.

Αν κανένας από τους προσφέροντες δεν υποβάλλει αληθή ή ακριβή δήλωση ή δεν προσκομίσει ένα ή περισσότερα από τα απαιτούμενα έγγραφα και δικαιολογητικά ή δεν αποδείξει ότι: α) δεν βρίσκεται σε μία από τις καταστάσεις της παραγράφου [2.2.3](#) της παρούσας διακήρυξης και β) πληροί τα σχετικά κριτήρια ποιοτικής επιλογής τα οποία έχουν καθοριστεί σύμφωνα με τις παραγράφους [2.2.4](#) - [2.2.8](#) της παρούσας διακήρυξης, η διαδικασία ματαιώνεται.

Η διαδικασία ελέγχου των παραπάνω δικαιολογητικών ολοκληρώνεται με τη σύνταξη πρακτικού από την Επιτροπή του Διαγωνισμού, στο οποίο αναγράφεται η τυχόν συμπλήρωση δικαιολογητικών σύμφωνα με όσα ορίζονται ανωτέρω και τη διαβίβασή του στο αποφαινόμενο όργανο της αναθέτουσας αρχής για τη λήψη απόφασης είτε για την κατακύρωση της σύμβασης είτε για τη ματαίωση της διαδικασίας.

Επισημαίνεται ότι, η αναθέτουσα αρχή, αιτιολογημένα και κατόπιν γνώμης της αρμόδιας επιτροπής του διαγωνισμού, μπορεί να κατακυρώσει τη σύμβαση για ολόκληρη ή μεγαλύτερη ή μικρότερη ποσότητα των παρεχόμενων υπηρεσιών από αυτή που καθορίζεται στην παρούσα σε ποσοστό και ως εξής: εκατόν είκοσι τοις εκατό (120%) στην περίπτωση της μεγαλύτερης ποσότητας και ογδόντα τοις εκατό (80%) στην περίπτωση μικρότερης ποσότητας.

Τα αποτελέσματα του ελέγχου των παραπάνω δικαιολογητικών και της εισήγησης της Επιτροπής επικυρώνονται με την απόφαση κατακύρωσης.

Σε κάθε περίπτωση, όταν εξ αρχής έχει υποβληθεί μία προσφορά, τα αποτελέσματα όλων των σταδίων της διαδικασίας ανάθεσης, ήτοι Δικαιολογητικών Συμμετοχής, Τεχνικής Προσφοράς και Οικονομικής Προσφοράς, επικυρώνονται με την απόφαση κατακύρωσης του άρθρου 105 του ν. 4412/2016, σύμφωνα με την παράγραφο [3.3](#) της παρούσας, που εκδίδεται μετά το πέρας και του τελευταίου σταδίου της διαδικασίας. Κατά της ανωτέρω απόφασης χωρεί προδικαστική προσφυγή ενώπιον της Ε.Α.ΔΗ.ΣΥ. σύμφωνα με όσα προβλέπονται στην παράγραφο [3.4](#) της παρούσας.

3.3 Κατακύρωση - σύναψη σύμβασης

3.3.1 Τα αποτελέσματα του ελέγχου των παραπάνω δικαιολογητικών κατακύρωσης και της εισήγησης της Επιτροπής Διαγωνισμού επικυρώνονται με την απόφαση κατακύρωσης, στην οποία ενσωματώνεται η απόφαση έγκρισης του πρακτικού κατάταξης των προσφερόντων και ανάδειξης προσωρινού αναδόχου, σε συνέχεια της αξιολόγησης των οικονομικών προσφορών τους.

Η αναθέτουσα αρχή κοινοποιεί, μέσω της λειτουργικότητας της «Επικοινωνίας», σε όλους τους οικονομικούς φορείς που έλαβαν μέρος στη διαδικασία ανάθεσης, εκτός από όσους αποκλείστηκαν οριστικά, ιδίως δυνάμει της παρ. 1 του άρθρου 72 του ν. 4412/2016, την απόφαση κατακύρωσης, στην οποία αναφέρονται υποχρεωτικά οι προθεσμίες για την αναστολή της σύναψης σύμβασης, σύμφωνα με τα άρθρα 360 έως 372 του ν. 4412/2016, μαζί με αντίγραφο των πρακτικών κατάταξης των προσφερόντων και ανάδειξης προσωρινού αναδόχου, και, επιπλέον, αναρτά τα δικαιολογητικά του προσωρινού αναδόχου στα «Συνημμένα Ηλεκτρονικού Διαγωνισμού».

Μετά την έκδοση και κοινοποίηση της απόφασης κατακύρωσης οι προσφέροντες λαμβάνουν γνώση των οικονομικών προσφορών που αποσφραγίστηκαν, της κατάταξης των προσφορών και των υποβληθέντων δικαιολογητικών κατακύρωσης, με ενέργειες της αναθέτουσας αρχής. Κατά της απόφασης κατακύρωσης χωρεί προδικαστική προσφυγή ενώπιον της Ε.Α.ΔΗ.ΣΥ., σύμφωνα με την παράγραφο 3.4 της παρούσας. Δεν επιτρέπεται η άσκηση άλλης διοικητικής προσφυγής κατά της ανωτέρω απόφασης.

3.3.2 Η απόφαση κατακύρωσης καθίσταται οριστική, εφόσον συντρέξουν οι ακόλουθες προϋποθέσεις σωρευτικά:

- α) κοινοποιηθεί η απόφαση κατακύρωσης σε όλους τους οικονομικούς φορείς που δεν έχουν αποκλειστεί οριστικά,
- β) παρέλθει άπρακτη η προθεσμία άσκησης προδικαστικής προσφυγής ή σε περίπτωση άσκησης, παρέλθει άπρακτη η προθεσμία άσκησης αίτησης αναστολής κατά της απόφασης της Ε.Α.ΔΗ.ΣΥ. και σε περίπτωση άσκησης αίτησης αναστολής κατά της απόφασης της Ε.Α.ΔΗ.ΣΥ., εκδοθεί απόφαση επί της αίτησης, με την επιφύλαξη της χορήγησης προσωρινής διαταγής, σύμφωνα με όσα ορίζονται στο τελευταίο εδάφιο της παρ. 4 του άρθρου 372 του ν. 4412/2016,
- γ) ολοκληρωθεί επιτυχώς ο προσυμβατικός έλεγχος από το Ελεγκτικό Συνέδριο, σύμφωνα με τα άρθρα 324 έως 327 του ν. 4700/2020, εφόσον απαιτείται, και
- δ) ο προσωρινός ανάδοχος, υποβάλλει, στην περίπτωση που απαιτείται και έπειτα από σχετική πρόσκληση, υπεύθυνη δήλωση, που υπογράφεται σύμφωνα με όσα ορίζονται στο άρθρο 79Α του ν. 4412/2016, στην οποία δηλώνεται ότι, δεν έχουν επέλθει στο πρόσωπό του οψιγενείς μεταβολές κατά την έννοια του άρθρου 104 του ν. 4412/2016 και μόνον στην περίπτωση του προσυμβατικού ελέγχου ή της άσκησης προδικαστικής προσφυγής κατά της απόφασης κατακύρωσης. Η υπεύθυνη δήλωση ελέγχεται από την αναθέτουσα αρχή και μνημονεύεται στο συμφωνητικό. Εφόσον δηλωθούν οψιγενείς μεταβολές, η δήλωση ελέγχεται από την Επιτροπή Διαγωνισμού, η οποία εισηγείται προς το αρμόδιο αποφαινόμενο όργανο.

Μετά από την οριστικοποίηση της απόφασης κατακύρωσης η αναθέτουσα αρχή προσκαλεί τον ανάδοχο, μέσω της λειτουργικότητας της «Επικοινωνίας», να προσέλθει για υπογραφή του συμφωνητικού, θέτοντάς του προθεσμία δεκαπέντε (15) ημερών από την κοινοποίηση της σχετικής ειδικής πρόσκλησης. Η σύμβαση θεωρείται συναφθείσα με την κοινοποίηση της πρόσκλησης του προηγούμενου εδαφίου στον ανάδοχο.

Πριν την υπογραφή της σύμβασης υποβάλλεται η υπεύθυνη δήλωση της κοινής απόφασης των Υπουργών Ανάπτυξης και Επικρατείας 20977/23-8-2007 (Β' 1673) «*Δικαιολογητικά για την τήρηση των μητρώων του ν. 3310/2005 όπως τροποποιήθηκε με το ν. 3414/2005*».

Στην περίπτωση που ο ανάδοχος δεν προσέλθει να υπογράψει το ως άνω συμφωνητικό μέσα στην τεθείσα προθεσμία, με την επιφύλαξη αντικειμενικών λόγων ανωτέρας βίας, κηρύσσεται έκπτωτος, καταπίπτει υπέρ της αναθέτουσας αρχής η εγγυητική επιστολή συμμετοχής του και ακολουθείται η ίδια, ως άνω διαδικασία, για τον προσφέροντα που υπέβαλε την αμέσως επόμενη πλέον συμφέρουσα από οικονομική άποψη προσφορά. Αν κανένας από τους προσφέροντες δεν προσέλθει για την υπογραφή του συμφωνητικού, η διαδικασία ανάθεσης ματαιώνεται σύμφωνα με την παράγραφο 3.5 της παρούσας διακήρυξης. Στην περίπτωση αυτή, η αναθέτουσα αρχή μπορεί να αναζητήσει αποζημίωση, πέρα από την καταπίπτουσα εγγυητική επιστολή, ιδίως δυνάμει των άρθρων 197 και 198 ΑΚ.³

Εάν η αναθέτουσα αρχή δεν απευθύνει την ειδική πρόσκληση για την υπογραφή του συμφωνητικού εντός χρονικού διαστήματος εξήντα (60) ημερών από την οριστικοποίηση της απόφασης κατακύρωσης, με την επιφύλαξη της ύπαρξης επιτακτικού λόγου δημόσιου συμφέροντος ή αντικειμενικών λόγων ανωτέρας βίας, ο ανάδοχος δικαιούται να απέχει από την υπογραφή του συμφωνητικού, χωρίς να εκπέσει η εγγύηση συμμετοχής του, καθώς και να αναζητήσει αποζημίωση ιδίως δυνάμει των άρθρων 197 και 198 ΑΚ.

3.4 Προδικαστικές Προσφυγές - Προσωρινή και Οριστική Δικαστική Προστασία

Α. Κάθε ενδιαφερόμενος, ο οποίος έχει ή είχε συμφέρον να του ανατεθεί η συγκεκριμένη συμφωνία – πλαίσιο και έχει υποστεί ή ενδέχεται να υποστεί ζημία από εκτελεστή πράξη ή παράλειψη της αναθέτουσας αρχής κατά παράβαση της ευρωπαϊκής ενωσιακής ή εσωτερικής νομοθεσίας στον τομέα των δημοσίων συμβάσεων, έχει δικαίωμα να προσφύγει στην Ενιαία Αρχή Δημοσίων Συμβάσεων (Ε.Α.ΔΗ.ΣΥ.), σύμφωνα με τα ειδικότερα οριζόμενα στα άρθρα 345επ. ν. 4412/2016 και 1επ. π.δ. 39/2017, στρεφόμενος με προδικαστική προσφυγή, κατά πράξης ή παράλειψης της αναθέτουσας αρχής, προσδιορίζοντας ειδικώς τις νομικές και πραγματικές αιτιάσεις που δικαιολογούν το αίτημά του.

Σε περίπτωση προσφυγής κατά πράξης της αναθέτουσας αρχής, η προθεσμία για την άσκηση της προδικαστικής προσφυγής είναι:

(α) δέκα (10) ημέρες από την κοινοποίηση της προσβαλλόμενης πράξης στον ενδιαφερόμενο οικονομικό φορέα αν η πράξη κοινοποιήθηκε με ηλεκτρονικά μέσα ή τηλεομοιοτυπία ή

³ Άρθρο 105 παρ. 7 του ν. 4412/2016, όπως αντικαταστάθηκε από το άρθρο 45 του ν. 4782/2021.

(β) δεκαπέντε (15) ημέρες από την κοινοποίηση της προσβαλλόμενης πράξης σε αυτόν αν χρησιμοποιήθηκαν άλλα μέσα επικοινωνίας, άλλως

(γ) δέκα (10) ημέρες από την πλήρη, πραγματική ή τεκμαιρόμενη, γνώση της πράξης που βλάπτει τα συμφέροντα του ενδιαφερόμενου οικονομικού φορέα. Ειδικά για την άσκηση προσφυγής κατά προκήρυξης, η πλήρης γνώση αυτής τεκμαίρεται μετά την πάροδο δεκαπέντε (15) ημερών από τη δημοσίευση στο ΚΗΜΔΗΣ.

Σε περίπτωση παράλειψης που αποδίδεται στην αναθέτουσα αρχή, η προθεσμία για την άσκηση της προδικαστικής προσφυγής είναι δεκαπέντε (15) ημέρες από την επομένη της συντέλεσης της προσβαλλόμενης παράλειψης⁴.

Οι προθεσμίες ως προς την υποβολή των προδικαστικών προσφυγών και των παρεμβάσεων αρχίζουν την επομένη της ημέρας της προαναφερθείσας κατά περίπτωση κοινοποίησης ή γνώσης και λήγουν όταν περάσει ολόκληρη η τελευταία ημέρα και ώρα 23:59:59 και, αν αυτή είναι εξαιρετέα ή Σάββατο, όταν περάσει ολόκληρη η επομένη εργάσιμη ημέρα και ώρα 23:59:59⁵.

Η προδικαστική προσφυγή συντάσσεται υποχρεωτικά με τη χρήση του τυποποιημένου εντύπου του Παραρτήματος Ι του π.δ/τος 39/2017 και κατατίθεται ηλεκτρονικά μέσω της λειτουργικότητας «Επικοινωνία» στην ηλεκτρονική περιοχή του συγκεκριμένου διαγωνισμού, επιλέγοντας την ένδειξη «Προδικαστική Προσφυγή» σύμφωνα με το άρθρο 18 της Κ.Υ.Α. Προμήθειες και Υπηρεσίες.

Για το παραδεκτό της άσκησης της προδικαστικής προσφυγής κατατίθεται παράβολο από τον προσφεύγοντα υπέρ του Ελληνικού Δημοσίου, σύμφωνα με όσα ορίζονται στο άρθρο 363 Ν. 4412/2016 όπως τροποποιήθηκε με το άρθρο 135 Ν. 4782/2021. Η επιστροφή του παραβόλου στον προσφεύγοντα γίνεται: α) σε περίπτωση ολικής ή μερικής αποδοχής της προσφυγής του, β) όταν η αναθέτουσα αρχή ανακαλεί την προσβαλλόμενη πράξη ή προβαίνει στην οφειλόμενη ενέργεια πριν από την έκδοση της απόφασης της Ε.Α.ΔΗ.ΣΥ. επί της προσφυγής, γ) σε περίπτωση παραίτησης του προσφεύγοντα από την προσφυγή του έως και δέκα (10) ημέρες από την κατάθεση της προσφυγής.

Η προθεσμία για την άσκηση της προδικαστικής προσφυγής και η άσκησή της κωλύουν τη σύναψη της σύμβασης επί ποινή ακυρότητας, η οποία διαπιστώνεται με απόφαση της Ε.Α.ΔΗ.ΣΥ. μετά από άσκηση προδικαστικής προσφυγής, σύμφωνα με το άρθρο 368 του ν. 4412/2016 και 20 π.δ. 39/2017. Όμως, μόνη η άσκηση της προδικαστικής προσφυγής δεν κωλύει την πρόοδο της διαγωνιστικής διαδικασίας, υπό την επιφύλαξη χορήγησης από το Κλιμάκιο προσωρινής προστασίας σύμφωνα με το άρθρο 366 παρ. 1-2 ν. 4412/2016 και 15 παρ. 1-4 π.δ. 39/2017.

Η προηγούμενη παράγραφος δεν εφαρμόζεται στην περίπτωση που, κατά τη διαδικασία σύναψης της παρούσας σύμβασης, υποβληθεί μόνο μία (1) προσφορά.

Μετά την, κατά τα ως άνω, ηλεκτρονική κατάθεση της προδικαστικής προσφυγής η αναθέτουσα αρχή, μέσω της λειτουργίας «Επικοινωνία» :

α) Κοινοποιεί την προσφυγή το αργότερο έως την επομένη εργάσιμη ημέρα από την κατάθεσή της σε κάθε ενδιαφερόμενο τρίτο, ο οποίος μπορεί να θίγεται από την αποδοχή της προσφυγής, προκειμένου να ασκήσει το, προβλεπόμενο από τα άρθρα 362 παρ. 3 και 7 π.δ. 39/2017, δικαίωμα

⁴Άρθρο 361 του ν. 4412/2016 και 4 π.δ. 39/2017

⁵ Παρ. 2 του άρθρου 9 και άρθρο 18 της Κ.Υ.Α. ΕΣΗΔΗΣ Προμήθειες και Υπηρεσίες

παρέμβασής του στη διαδικασία εξέτασης της προσφυγής, για τη διατήρηση της ισχύος της προσβαλλόμενης πράξης, προσκομίζοντας όλα τα κρίσιμα έγγραφα που έχει στη διάθεσή του.

β) Διαβιβάζει στην Ε.Α.ΔΗ.ΣΥ., το αργότερο εντός δεκαπέντε (15) ημερών από την ημέρα κατάθεσης, τον πλήρη φάκελο της υπόθεσης, τα αποδεικτικά κοινοποίησης στους ενδιαφερόμενους τρίτους αλλά και την Έκθεση Απόψεων της επί της προσφυγής. Στην Έκθεση Απόψεων η αναθέτουσα αρχή μπορεί να παραθέσει αρχική ή συμπληρωματική αιτιολογία για την υποστήριξη της προσβαλλόμενης με την προδικαστική προσφυγή πράξης.

γ) Κοινοποιεί σε όλα τα μέρη την Έκθεση Απόψεων, τις Παρεμβάσεις και τα σχετικά έγγραφα που τυχόν τη συνοδεύουν, μέσω του ηλεκτρονικού τόπου του διαγωνισμού το αργότερο έως την επομένη εργάσιμη ημέρα από την κατάθεσή τους.

δ) Συμπληρωματικά υπομνήματα κατατίθενται από οποιοδήποτε από τα μέρη μέσω της πλατφόρμας του ΕΣΗΔΗΣ το αργότερο εντός πέντε (5) ημερών από την κοινοποίηση των απόψεων της αναθέτουσας αρχής.

Η άσκηση της προδικαστικής προσφυγής αποτελεί προϋπόθεση για την άσκηση των ένδικων βοηθημάτων της αίτησης αναστολής και της αίτησης ακύρωσης του άρθρου 372 ν. 4412/2016 κατά των εκτελεστών πράξεων ή παραλείψεων της αναθέτουσας αρχής.

Β. Όποιος έχει έννομο συμφέρον μπορεί να ζητήσει, με το ίδιο δικόγραφοεφαρμοζόμενων αναλογικά των διατάξεων του π.δ. 18/1989, την αναστολή εκτέλεσης της απόφασης της Ε.Α.ΔΗ.ΣΥ. και την ακύρωσή της ενώπιον του αρμοδίου Δικαστηρίου της παρ. 3 του αρθ. 372 Ν.4412/2016, όπως ισχύει. Το αυτό ισχύει και σε περίπτωση σιωπηρής απόρριψης της προδικαστικής προσφυγής από την Ε.Α.ΔΗ.ΣΥ.. Δικαίωμα άσκησης του ως άνω ένδικου βοηθήματος έχει και η αναθέτουσα αρχή αν η Ε.Α.ΔΗ.ΣΥ. κάνει δεκτή την προδικαστική προσφυγή, αλλά και αυτός του οποίου έχει γίνει εν μέρει δεκτή η προδικαστική προσφυγή.

Με την απόφαση της Ε.Α.ΔΗ.ΣΥ. λογίζονται ως συμπροσβαλλόμενες και όλες οι συναφείς προς την ανωτέρω απόφαση πράξεις ή παραλείψεις της αναθέτουσας αρχής, εφόσον έχουν εκδοθεί ή συντελεστεί αντιστοίχως έως τη συζήτηση της ως άνω αίτησης στο Δικαστήριο.

Η αίτηση αναστολής και ακύρωσης περιλαμβάνει μόνο αιτιάσεις που είχαν προταθεί με την προδικαστική προσφυγή ή αφορούν στη διαδικασία ενώπιον της Ε.Α.ΔΗ.ΣΥ. ή το περιεχόμενο των αποφάσεών της. Η αναθέτουσα αρχή, εφόσον ασκήσει την αίτηση της παρ. 1 του άρθρου 372 του ν. 4412/2016, μπορεί να προβάλει και οψιγενείς ισχυρισμούς αναφορικά με τους επιτακτικούς λόγους δημοσίου συμφέροντος, οι οποίοι καθιστούν αναγκαία την άμεση ανάθεση της σύμβασης.

Η ως άνω αίτηση κατατίθεται στο αρμόδιο δικαστήριο μέσα σε προθεσμία δέκα (10) ημερών από κοινοποίηση ή την πλήρη γνώση της απόφασης ή από την παρέλευση της προθεσμίας για την έκδοση της απόφασης επί της προδικαστικής προσφυγής, ενώ η δικάσιμος για την εκδίκαση της αίτησης ακύρωσης δεν πρέπει να απέχει πέραν των εξήντα (60) ημερών από την κατάθεση του δικογράφου.

Αντίγραφο της αίτησης με κλήση κοινοποιείται με τη φροντίδα του αιτούντος προς την Ε.Α.ΔΗ.ΣΥ., την αναθέτουσα αρχή, αν δεν έχει ασκήσει αυτή την αίτηση, και προς κάθε τρίτο ενδιαφερόμενο, την κλήτευση του οποίου διατάσσει με πράξη του ο Πρόεδρος ή ο προεδρεύων του αρμοδίου Δικαστηρίου ή Τμήματος έως την επόμενη ημέρα από την κατάθεση της αίτησης. Ο αιτών

υποχρεούνται επί ποινή απαραδέκτου του ενδίκου βοηθήματος να προβεί στις παραπάνω κοινοποιήσεις εντός αποκλειστικής προθεσμίας δύο (2) ημερών από την έκδοση και την παραλαβή της ως άνω πράξης, του Δικαστηρίου. Εντός αποκλειστικής προθεσμίας δέκα (10) ημερών από την ως άνω κοινοποίηση της αίτησης κατατίθεται η παρέμβαση και διαβιβάζονται ο φάκελος και οι απόψεις των παθητικώς νομιμοποιούμενων. Εντός της ίδιας προθεσμίας κατατίθενται στο Δικαστήριο και τα στοιχεία που υποστηρίζουν τους ισχυρισμούς των διαδίκων.

Επιπρόσθετα, η παρέμβαση κοινοποιείται με επιμέλεια του παρεμβαίνοντος στα λοιπά μέρη της δίκης εντός δύο (2) ημερών από την κατάθεσή της, αλλιώς λογίζεται ως अपараδέκτη. Το διατακτικό της δικαστικής απόφασης εκδίδεται εντός δεκαπέντε (15) ημερών από τη συζήτηση της αίτησης ή από την προθεσμία για την υποβολή υπομνημάτων.

Η προθεσμία για την άσκηση και η άσκηση της αίτησης ενώπιον του αρμοδίου δικαστηρίου κωλύουν τη σύναψη της σύμβασης μέχρι την έκδοση της οριστικής δικαστικής απόφασης, εκτός εάν με προσωρινή διαταγή ο αρμόδιος δικαστής αποφανθεί διαφορετικά. Επίσης, η προθεσμία για την άσκηση και η άσκηση της αίτησης κωλύουν την πρόοδο της διαδικασίας ανάθεσης για χρονικό διάστημα δεκαπέντε (15) ημερών από την άσκηση της αίτησης, εκτός εάν με την προσωρινή διαταγή ο αρμόδιος δικαστής αποφανθεί διαφορετικά. Για την άσκηση της αιτήσεως κατατίθεται παράβολο, σύμφωνα με τα ειδικότερα οριζόμενα στο άρθρο 372 παρ. 5 του Ν. 4412/2016.

Αν ο ενδιαφερόμενος δεν αιτήθηκε ή αιτήθηκε ανεπιτυχώς την αναστολή και η σύμβαση υπογράφηκε και η εκτέλεσή της ολοκληρώθηκε πριν από τη συζήτηση της αίτησης, εφαρμόζεται αναλόγως η παρ. 2 του άρθρου 32 του π.δ. 18/1989.

Αν το δικαστήριο ακυρώσει πράξη ή παράλειψη της αναθέτουσας αρχής μετά τη σύναψη της σύμβασης, το κύρος της τελευταίας δεν θίγεται, εκτός αν πριν από τη σύναψη αυτής είχε ανασταλεί η διαδικασία σύναψης της σύμβασης. Στην περίπτωση που η σύμβαση δεν είναι άκυρη, ο ενδιαφερόμενος δικαιούται να αξιώσει αποζημίωση, σύμφωνα με τα αναφερόμενα στο άρθρο 373 του ν. 4412/2016.

Με την επιφύλαξη των διατάξεων του ν. 4412/2016, για την εκδίκαση των διαφορών του παρόντος άρθρου εφαρμόζονται οι διατάξεις του π.δ. 18/1989.

3.5 Μатаίωση Διαδικασίας

Η αναθέτουσα αρχή ματαιώνει ή δύναται να ματαιώσει εν όλω ή εν μέρει, αιτιολογημένα, τη διαδικασία ανάθεσης, για τους λόγους και υπό τους όρους του άρθρου 106 του ν. 4412/2016, μετά από γνώμη της αρμόδιας Επιτροπής του Διαγωνισμού. Επίσης, αν διαπιστωθούν σφάλματα ή παραλείψεις σε οποιοδήποτε στάδιο της διαδικασίας ανάθεσης, μπορεί, μετά από γνώμη της ως άνω Επιτροπής, να ακυρώσει μερικώς τη διαδικασία ή να αναμορφώσει ανάλογα το αποτέλεσμα της ή να αποφασίσει την επανάληψή της από το σημείο που εμφοιλοχώρησε το σφάλμα ή η παράλειψη.

Ειδικότερα, η αναθέτουσα αρχή ματαιώνει τη διαδικασία σύναψης όταν αυτή αποβεί άγονη είτε λόγω μη υποβολής προσφοράς είτε λόγω απόρριψης όλων των προσφορών, καθώς και στην περίπτωση του δευτέρου εδαφίου της παρ. 7 του άρθρου 105, περί κατακύρωσης και σύναψης σύμβασης.

Επίσης μπορεί να ματαιώσει τη διαδικασία: α) λόγω παράτυπης διεξαγωγής της διαδικασίας ανάθεσης, εκτός εάν μπορεί να θεραπεύσει το σφάλμα ή την παράλειψη σύμφωνα με την παρ. 3 του άρθρου 106, β) αν οι οικονομικές και τεχνικές παράμετροι που σχετίζονται με τη διαδικασία ανάθεσης άλλαξαν ουσιωδώς και η εκτέλεση του συμβατικού αντικειμένου δεν ενδιαφέρει πλέον την αναθέτουσα αρχή ή τον φορέα για τον οποίο προορίζεται το υπό ανάθεση αντικείμενο, γ) αν λόγω ανωτέρας βίας, δεν είναι δυνατή η κανονική εκτέλεση της σύμβασης, δ) αν η επιλεγείσα προσφορά κριθεί ως μη συμφέρουσα από οικονομική άποψη, ε) στην περίπτωση των παρ. 3 και 4 του άρθρου 97, περί χρόνου ισχύος προσφορών, στ) για άλλους επιτακτικούς λόγους δημοσίου συμφέροντος, όπως ιδίως, δημόσιας υγείας ή προστασίας του περιβάλλοντος.

4 ΟΡΟΙ ΕΚΤΕΛΕΣΗΣ ΤΗΣ ΣΥΜΒΑΣΗΣ

4.1 Εγγυήσεις(καλής εκτέλεσης, προκαταβολής, καλής λειτουργίας)

4.1.1 Εγγύηση καλής εκτέλεσης συμφωνίας-πλαίσιο

Για την καλή εκτέλεση των όρων της συμφωνίας-πλαίσιο, οι συμβαλλόμενοι στη συμφωνία-πλαίσιο οικονομικοί φορείς υποχρεούνται να καταθέσουν πριν ή κατά την υπογραφή της συμφωνίας- πλαίσιο εγγύηση καλής εκτέλεσης, σύμφωνα με το άρθρο 72 παρ. 6 του ν. 4412/2016, το ύψος της οποίας ανέρχεται σε ποσοστό 0,5% επί της αξίας της συμφωνίας-πλαίσιο (δηλαδή του τμήματος που έχει ανατεθεί), χωρίς ΦΠΑ και χωρίς τα δικαιώματα προαίρεσης.

Ο χρόνος ισχύος της εγγύησης καλής εκτέλεσης της συμφωνίας-πλαίσιο είναι τρία (3) έτη από την υπογραφή της συμφωνίας – πλαίσιο και σε κάθε περίπτωση επιστρέφεται στο σύνολό της μετά από τη λήξη της ισχύος της συμφωνίας-πλαίσιο ή παρατάσεών της.

Η εγγύηση καλής εκτέλεσης της συμφωνίας-πλαίσιο καλύπτει συνολικά και χωρίς διακρίσεις την εφαρμογή όλων των όρων της συμφωνίας-πλαίσιο και κάθε απαίτηση της Αναθέτουσας Αρχής έναντι του οικονομικού φορέα που συμμετέχει στη συμφωνία-πλαίσιο.

Σε περίπτωση τροποποίησης της σύμβασης κατά την παράγραφο 4.5, η οποία συνεπάγεται αύξηση της συμβατικής αξίας, ο/οι ανάδοχος/οι είναι υποχρεωμένος να καταθέσει πριν την τροποποίηση, συμπληρωματική εγγύηση το ύψος της οποίας ανέρχεται σε ποσοστό 0,5% επί του ποσού της αύξησης, εκτός ΦΠΑ.

Η εγγύηση καλής εκτέλεσης καταπίπτει σε περίπτωση παράβασης των όρων της συμφωνίας-πλαίσιο, όπως αυτή ειδικότερα ορίζει.

4.1.2 Εγγύηση καλής εκτέλεσης εκτελεστικών συμβάσεων

Για την καλή εκτέλεση των όρων της εκτελεστικής σύμβασης, ο ανάδοχος υποχρεούται να καταθέσει μέχρι και την υπογραφή του συμφωνητικού εγγύηση καλής εκτέλεσης της σύμβασης αυτής, σύμφωνα με το άρθρο 72 παρ. 4 και 6 του ν. 4412/2016, το ύψος της οποίας ανέρχεται σε ποσοστό 4% επί της αξίας της εκτελεστικής σύμβασης χωρίς να συμπεριλαμβάνονται τα δικαιώματα προαίρεσης.

Η εγγύηση καλής εκτέλεσης, προκειμένου να γίνει αποδεκτή, πρέπει να περιλαμβάνει κατ'ελάχιστον τα αναφερόμενα στην παράγραφο 2.1.5. στοιχεία της παρούσας και επιπλέον τον αριθμό και τον τίτλο της σύμβασης και το περιεχόμενό της να είναι σύμφωνο με το υπόδειγμα που περιλαμβάνεται στο ΠΑΡΑΡΤΗΜΑ V – Υποδείγματα Εγγυητικών Επιστολών της Διακήρυξης και ταοριζόμενα στο άρθρο 72 του ν. 4412/2016.

Η εγγύηση καλής εκτέλεσης της εκτελεστικής σύμβασης καλύπτει συνολικά και χωρίς διακρίσεις την εφαρμογή όλων των όρων της σύμβασης και κάθε απαίτηση της Αναθέτουσας Αρχής έναντι του αναδόχου.

Ο χρόνος ισχύος της εγγύησης καλής εκτέλεσης της εκτελεστικής σύμβασης είναι ίσος με τη διάρκεια της εκτελεστικής σύμβασης πλέον 4 μηνών και παρατείνεται ανάλογα σε περίπτωση παράτασής του.

Σε περίπτωση τροποποίησης της σύμβασης κατά την παράγραφο 4.5, η οποία συνεπάγεται αύξησης συμβατικής αξίας, ο ανάδοχος είναι υποχρεωμένος να καταθέσει πριν την τροποποίηση, συμπληρωματική εγγύηση το ύψος της οποίας ανέρχεται σε ποσοστό 4% επί του ποσού της αύξησης, εκτός ΦΠΑ.

Η εγγύηση καλής εκτέλεσης καταπίπτει σε περίπτωση παράβασης των όρων της σύμβασης, όπως αυτή ειδικότερα ορίζει.

Στην περίπτωση χορήγησης προκαταβολής, σύμφωνα με την παράγραφο 5.1 Τρόπος Πληρωμής της παρούσας, απαιτείται από τον ανάδοχο «εγγύηση προκαταβολής» για ποσό ίσο με αυτό της προκαταβολής, σύμφωνα με το υπόδειγμα που περιλαμβάνεται στο ΠΑΡΑΡΤΗΜΑ VIII – Υποδείγματα Εγγυητικών Επιστολών της Διακήρυξης. Η προκαταβολή και η εγγύηση προκαταβολής μπορούν να χορηγούνται τμηματικά, σύμφωνα με την παράγραφο 5.1 της παρούσας (τρόπος πληρωμής).

Η απόσβεση της προκαταβολής πραγματοποιείται σύμφωνα με τα αναφερόμενα στην παρ. 5.1 Τρόπος Πληρωμής και η εγγύηση προκαταβολής επιστρέφεται μετά από την οριστική ποσοτική και ποιοτική παραλαβή των υπηρεσιών.

Η εγγύηση καλής εκτέλεσης και η εγγύηση προκαταβολής επιστρέφονται στο σύνολό τους [ή στην περίπτωση που οι υπηρεσίες είναι διαιρετές και η παράδοση γίνεται τμηματικά : αποδεσμεύονται τμηματικά, κατά το ποσό που αναλογεί στην αξία του μέρους του τμήματος της υπηρεσίας που παραλήφθηκε οριστικά] μετά την οριστική ποσοτική και ποιοτική παραλαβή του αντικειμένου της σύμβασης. Για τη σταδιακή αποδέσμευσή τους απαιτείται προηγούμενη γνωμοδότηση του αρμόδιου συλλογικού οργάνου. Εάν στο πρωτόκολλο παραλαβής αναφέρονται παρατηρήσεις ή υπάρχει εκπρόθεσμη παράδοση, η παραπάνω σταδιακή αποδέσμευση γίνεται μετά από την αντιμετώπιση, σύμφωνα με όσα προβλέπονται, των παρατηρήσεων και του εκπρόθεσμου.

Εγγύηση καλής Λειτουργίας :

Για την καλή λειτουργία του Έργου, μετά την οριστική παραλαβή του, ο Ανάδοχος υποχρεούται να καταθέσει **Εγγυητική Επιστολή Καλής Λειτουργίας** (βλ. ΠΑΡΑΡΤΗΜΑ VIII – Υποδείγματα Εγγυητικών Επιστολών), η αξία της οποίας θα ανέρχεται σε ποσοστό 2,5% του συμβατικού τιμήματος μη συμπεριλαμβανομένου ΦΠΑ.

Σε περίπτωση προσφοράς Περιόδου Εγγύησης μεγαλύτερης της ζητούμενης, το παραπάνω ποσοστό (2,5%) της Εγγυητικής Επιστολής προσαυξάνεται κατά μία (1) ποσοστιαία μονάδα για κάθε επί πλέον προσφερόμενο έτος εγγύησης. Κατά την Περίοδο Εγγύησης, ο Ανάδοχος ευθύνεται για την καλή λειτουργία του συνόλου του Έργου.

Η Εγγύηση Καλής Λειτουργίας επιστρέφεται μετά τη λήξη της περιόδου Εγγύησης, ύστερα από την εκκαθάριση των τυχόν απαιτήσεων από τους δύο συμβαλλόμενους.

4.2 Συμβατικό πλαίσιο – Εφαρμοστέα νομοθεσία

Κατά την εκτέλεση της σύμβασης εφαρμόζονται οι διατάξεις του ν. 4412/2016, οι όροι της παρούσας διακήρυξης και συμπληρωματικά ο Αστικός Κώδικας.

4.3 Όροι εκτέλεσης της συμφωνίας - πλαίσιο

Κατά την εκτέλεση της συμφωνίας – πλαίσιο και των εκτελεστικών συμβάσεων ο ανάδοχος τηρεί τις υποχρεώσεις στους τομείς του περιβαλλοντικού, κοινωνικοασφαλιστικού και εργατικού δικαίου, που έχουν θεσπιστεί με το δίκαιο της Ένωσης, το εθνικό δίκαιο, συλλογικές συμβάσεις ή διεθνείς διατάξεις περιβαλλοντικού, κοινωνικοασφαλιστικού και εργατικού δικαίου, οι οποίες απαριθμούνται στο Παράρτημα Χ του Προσαρτήματος Α του ν. 4412/2016.

Η τήρηση των εν λόγω υποχρεώσεων από τον ανάδοχο και τους υπεργολάβους του ελέγχεται και βεβαιώνεται από τα όργανα που επιβλέπουν την εκτέλεση της σύμβασης και τις αρμόδιες δημόσιες αρχές και υπηρεσίες που ενεργούν εντός των ορίων της ευθύνης και της αρμοδιότητάς τους.

Η σύναψη εκτελεστικών συμβάσεων κατά τη διάρκεια της συμφωνίας-πλαίσιο, θαπραγματοποιείται μόνο εφόσον κρίνεται σκόπιμο από την Αναθέτουσα Αρχή. Σε περίπτωση μισύναψης οποιασδήποτε εκτελεστικής σύμβασης, ο συμβαλλόμενος στη συμφωνία-πλαίσιο δενδικαιούνται αποζημίωσης. Επίσης ο συμβαλλόμενος στη συμφωνία-πλαίσιο δεν δικαιούνται αποζημίωσης, σε περίπτωση μη ανάθεσης του συνόλου του φυσικού αντικείμενου που καθορίζεται στηδιακήρυξη.

Ο ανάδοχος δεσμεύεται ότι:

α) σε όλα τα στάδια που προηγήθηκαν της σύμβασης δεν ενήργησε αθέμιτα, παράνομα ή καταχρηστικά και ότι θα εξακολουθήσει να μην ενεργεί κατ' αυτόν τον τρόπο κατά το στάδιο εκτέλεσης της σύμβασης,

β) ότι θα δηλώσει αμελλητί στην αναθέτουσα αρχή, από τη στιγμή που λάβει γνώση, οποιαδήποτε κατάσταση (ακόμη και ενδεχόμενη) σύγκρουσης συμφερόντων (προσωπικών, οικογενειακών, οικονομικών, πολιτικών ή άλλων κοινών συμφερόντων, συμπεριλαμβανομένων και αντικρουόμενων επαγγελματικών συμφερόντων) μεταξύ των νομίμων ή εξουσιοδοτημένων εκπροσώπων του καθώς και υπαλλήλων ή συνεργατών τους οποίους απασχολεί στην εκτέλεση της σύμβασης (π.χ. με σύμβαση υπεργολαβίας) και μελών του προσωπικού της αναθέτουσας αρχής που εμπλέκονται καθ' οιονδήποτε τρόπο στη διαδικασία εκτέλεσης της σύμβασης ή/και μπορούν να επηρεάσουν την έκβαση και τις αποφάσεις της αναθέτουσας αρχής περί την εκτέλεσή της, οποτεδήποτε και εάν η κατάσταση αυτή προκύψει κατά τη διάρκεια εκτέλεσης της σύμβασης.

Οι υποχρεώσεις και οι απαγορεύσεις της ρήτρας αυτής ισχύουν, αν ο ανάδοχος είναι ένωση, για όλα τα μέλη της ένωσης, καθώς και για τους υπεργολάβους που χρησιμοποιεί. Στο συμφωνητικό περιλαμβάνεται σχετική δεσμευτική δήλωση τόσο του αναδόχου όσο και των υπεργολάβων του.

Κατά την εκτέλεση της σύμβασης οανάδοχος δε δικαιούται να εκχωρεί το συμβατικό τίμημα σε οποιοδήποτε τρίτο, χωρίς την έγγραφη έγκριση της Αναθέτουσας Αρχής. Εάν το συμβατικό τίμημα εκχωρηθεί εν όλω ή εν μέρει σε Τράπεζα, κατά τα ως άνω αναφερόμενα, σε περίπτωση που, για λόγους που άπτονται στις συμβατικές σχέσεις μεταξύ των συμβαλλομένων μερών, δεν προκύψει εν όλω ή εν μέρει υπέρ της Τράπεζας το εκχωρούμενο τίμημα η Αναθέτουσα Αρχήδεν έχει καμία ευθύνη έναντι της εκδοχέως Τράπεζας.

Κατά την εκτέλεση της σύμβασηςοανάδοχος εγγυάται τη διάθεση του αναφερομένου στην Προσφορά του, επιστημονικού και λοιπού προσωπικού, καθώς επίσης και συνεργατών, που διαθέτουν την απαιτούμενη εμπειρία, τεχνογνωσία και ικανότητα, ώστε να ανταποκριθούν πλήρως

στις απαιτήσεις της Σύμβασης, υπόσχεται δε και βεβαιώνει ότι θα επιδεικνύουν πνεύμα συνεργασίας κατά τις επαφές τους με τις αρμόδιες υπηρεσίες και τα στελέχη της Αναθέτουσας Αρχής ή των εκάστοτε υποδεικνυομένων από αυτήν προσώπων. Σε αντίθετη περίπτωση, η Αναθέτουσα Αρχή δύναται να ζητήσει την αντικατάσταση μέλους της Ομάδας Έργου του αναδόχου, οπότε ο ανάδοχος οφείλει να προβεί σε αντικατάσταση με άλλο πρόσωπο, ανάλογης εμπειρίας και προσόντων. Αντικατάσταση μέλους της Ομάδας Έργου του Αναδόχου, κατόπιν αιτήματός του, κατά τη διάρκεια της εκτέλεσης του Έργου, δύναται να γίνει μετά από έγκριση της Αναθέτουσας Αρχής και μόνο με άλλο πρόσωπο αντιστοίχων προσόντων ή εμπειρίας. Ο Ανάδοχος υποχρεούται να ειδοποιήσει την ΚτΠ Α.Ε. εγγράφως δεκαπέντε (15) ημέρες πριν από την αντικατάσταση.

Σε περίπτωση που μέλη της Ομάδας Έργου του Αναδόχου αποχωρήσουν από αυτήν ή λύσουν τη συνεργασία τους μαζί του, ο Ανάδοχος υποχρεούται να εξασφαλίσει ότι κατά το χρονικό διάστημα, μέχρι την αποχώρησή τους, θα παρέχουν κανονικά τις υπηρεσίες τους και αφετέρου να αντικαταστήσει άμεσα τους αποχωρήσαντες συνεργάτες, με άλλα πρόσωπα που θα διαθέτουν τουλάχιστον ίση εμπειρία και ίσα προσόντα με τα αντικαθιστάμενα.

Σε περίπτωση λύσης, πτώχευσης, ή θέσης σε καθεστώς αναγκαστικής διαχείρισης ενός εκ των μελών που απαρτίζουν τον Ανάδοχο, η Σύμβαση εξακολουθεί να υφίσταται και οι απορρέουσες από τη Σύμβαση υποχρεώσεις βαρύνουν τα εναπομείναντα μέλη του Αναδόχου, μόνο εφόσον αυτά είναι σε θέση να τις εκπληρώσουν. Η κρίση για τη δυνατότητα εκπλήρωσης ή μη των όρων της Σύμβασης εναπόκειται στη διακριτική ευχέρεια του αρμοδίου οργάνου της Αναθέτουσας Αρχής. Σε αντίθετη περίπτωση, η Αναθέτουσα Αρχή δύναται να καταγγείλει τη Σύμβαση. Επίσης σε περίπτωση συγχώνευσης, εξαγοράς, μεταβίβασης της επιχείρησης κλπ. κάποιου εκ των μελών που απαρτίζουν τον Ανάδοχο, η συνέχιση ή όχι της Σύμβασης εναπόκειται στη διακριτική ευχέρεια της Αναθέτουσας Αρχής. Σε περίπτωση λύσης ή πτώχευσης του Αναδόχου, όταν αυτός αποτελείται από μία εταιρεία, ή θέσης της περιουσίας αυτού σε αναγκαστική διαχείριση, τότε η σύμβαση λύεται αυτοδίκαια από την ημέρα επέλευσης των ανωτέρω γεγονότων. Σε τέτοια περίπτωση καταπίπτουν υπέρ της Αναθέτουσας Αρχής και οι Εγγυητικές Επιστολές Προκαταβολής και Καλής Εκτέλεσης που προβλέπονται στη Σύμβαση.

Όλα τα έγγραφα, στοιχεία και πληροφορίες που λαμβάνει ο Ανάδοχος από την Εταιρεία στο πλαίσιο των συμβατικών του υποχρεώσεων ή υποπίπτουν στην αντίληψή του εξαιτίας της συμβατικής σχέσης του με την Εταιρεία, είναι εμπιστευτικά.

Ο Ανάδοχος δεν δικαιούται να δημοσιεύει ή αποκαλύπτει τέτοιες πληροφορίες και στοιχεία σε οποιονδήποτε τρίτο, παρά μόνο σε όσους εργοδοτούμενους από αυτόν ή συνεργαζόμενους με αυτόν ασχολούνται άμεσα με το περιεχόμενο της Σύμβασης και την εκτέλεση του Αντικειμένου

Σε περίπτωση αθέτησης από τον Ανάδοχο της ως άνω υποχρέωσής του, η Εταιρεία διατηρεί το δικαίωμα να καταγγείλει τη Σύμβαση κατά τα οριζόμενα στο άρθρο 13 ή/και να κοστολογήσει και απαιτήσει πληρωμή για όλες τις ζημιές που τυχόν έχει υποστεί εξαιτίας της διαρροής.

Ο Ανάδοχος δεν θα προβαίνει σε οποιεσδήποτε δημόσιες δηλώσεις αναφορικά με το Αντικείμενο της Σύμβασης ή τα Προϊόντα που παραδίδει ή τις Υπηρεσίες που παρέχει στην Εταιρεία δυνάμει της Σύμβασης χωρίς την προηγούμενη έγκριση της Εταιρείας, και δεν θα μετέχει σε οποιαδήποτε δραστηριότητα η οποία συγκρούεται με τις υποχρεώσεις του έναντι της Εταιρείας δυνάμει της

Σύμβασης. Δεν θα δεσμεύει την Εταιρεία με οποιοδήποτε τρόπο χωρίς την προηγούμενη γραπτή της συγκατάθεση και θα διευκρινίζει, όπου καθίσταται απαραίτητο, την υποχρέωσή του αυτή σε τρίτους.

Ο Ανάδοχος δεν υπόκειται στις υποχρεώσεις του παρόντος άρθρου σε ότι αφορά στην τεχνογνωσία που ενδεχομένως αποκτά εξαιτίας της εκτέλεσης του Αντικειμένου της Σύμβασης.

Όλα τα αποτελέσματα-μελέτες, στοιχεία και κάθε άλλο έγγραφο ή αρχείο σχετικό με το έργο καθώς και όλα τα υπόλοιπα παραδοτέα, που θα αποκτηθούν ή θα αναπτυχθούν από τον Ανάδοχο με δαπάνες του, θα αποτελούν αποκλειστική ιδιοκτησία της Εταιρείας (εκτός και εάν ήδη υπάρχουν κατοχυρωμένα πνευματικά δικαιώματα), η οποία θα μπορεί να τα διαχειρίζεται και να τα εκμεταλλεύεται.

Τα αποτελέσματα θα είναι πάντοτε στη διάθεση των νόμιμων εκπροσώπων της Εταιρείας κατά τη διάρκεια ισχύος της σύμβασης και εάν βρίσκονται στη κατοχή του Αναδόχου, θα παραδοθούν στην Εταιρεία κατά την καθ' όποιονδήποτε τρόπο λήξη ή λύση της σύμβασης. Σε περίπτωση αρχείων με στοιχεία σε ηλεκτρονική μορφή, ο Ανάδοχος υποχρεούται να συνοδεύσει την παράδοσή τους με έγγραφη τεκμηρίωση και με οδηγίες για την ανάκτηση /διαχείρισή τους.

Ο Ανάδοχος διαβεβαιώνει και εγγυάται ότι ουδείς τρίτος έχει ουδέν δικαίωμα επί του ως άνω έργου και σε κάθε περίπτωση αναλαμβάνει, δεσμεύεται και εγγυάται ότι θα αποκαταστήσει κάθε θετική και αποθετική ζημία και ηθική βλάβη που θα προκληθεί στην Εταιρεία.

Επίσης, δεσμεύεται ότι θα αναλάβει τα οποιαδήποτε έξοδα (συμπεριλαμβανομένης και της ενδεχόμενης αποζημίωσης) εναντίον τρίτου μέρους που ισχυρίζεται κυριότητα πνευματικών δικαιωμάτων μέρους ή όλου του έργου.

Επιπλέον ο ανάδοχος υποχρεούται να τηρεί τα αναφερόμενα στον Γενικό Κανονισμό Προστασίας Δεδομένων (Άρθρα 4, 9, 10 ΓΚΠΔ) και στο ν.4624/2019 (Α' 137/29-08-2019) (Άρθρα 44, 46)

Ειδικότερα :

α. Οι πληροφορίες της Εταιρείας οι οποίες θα τύχουν οποιασδήποτε μορφής επεξεργασία από τον Ανάδοχο, τους εργαζόμενους, τους συνεργάτες αυτού και τους τυχόν υπεργολάβους (οποιαδήποτε σχέση έχουν με τον Ανάδοχο) ενδέχεται να περιέχουν και δεδομένα προσωπικού χαρακτήρα, όπως ορίζονται (α) στον Γενικό Κανονισμό Προστασίας Δεδομένων (Άρθρα 4, 9, 10 ΓΚΠΔ) και (β) στο ν.4624/2019 (Α' 137/29-08-2019) (Άρθρα 44, 46).

β. Η επεξεργασία δεδομένων προσωπικού χαρακτήρα πραγματοποιείται αποκλειστικά για τον σκοπό που αφορά το αντικείμενο των υπηρεσιών που αναλαμβάνει να παράσχει ο Ανάδοχος στην Εταιρεία, δυνάμει της παρούσας Σύμβασης και μόνο στην έκταση που επιβάλλει ο σκοπός της επεξεργασίας σύμφωνα το αντικείμενο των υπηρεσιών που έχει αναλάβει να παρέχει.

γ. Η επεξεργασία των δεδομένων προσωπικού χαρακτήρα θα εκτελείται σύμφωνα με τους όρους και συμφωνίες της παρούσας Σύμβασης και τις Οδηγίες της Εταιρείας. Ο Ανάδοχος δεσμεύεται ως προς την εφαρμογή και συμμόρφωση προς την ισχύουσα νομοθεσία για την προστασία δεδομένων προσωπικού χαρακτήρα (ιδίως Γενικός Κανονισμός Προστασίας Δεδομένων – 2016/679/ΕΕ), όπως ερμηνεύεται ιδίως από τις Αποφάσεις ή Γνωμοδοτήσεις της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα - ΑΠΔΠΧ) και του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων.

δ. Τα αρχεία που δημιουργούνται με την συλλογή, επεξεργασία και αποθήκευση των πληροφοριών που ενδέχεται να περιέχουν και προσωπικά δεδομένα, και γενικότερα όλων των ανάλογων μορφών αρχείων και πληροφοριών της Εταιρείας, από τον Ανάδοχο, ανήκουν κατ' αποκλειστικότητα στην Εταιρεία.

ε. Ο Ανάδοχος βεβαιώνει και εγγυάται στην Εταιρεία ότι θα λαμβάνει όλα τα απαραίτητα οργανωτικά και τεχνικά μέτρα για την ασφάλεια των πληροφοριών που ενδέχεται να περιέχουν και προσωπικά δεδομένα, και γενικότερα όλων των ανάλογων μορφών αρχείων και πληροφοριών της Εταιρείας, καθώς και για την προστασία τους από τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση και κάθε άλλη μορφή αθέμιτης επεξεργασίας, στο πλαίσιο των καθηκόντων του που πηγάζουν από την παρούσα Σύμβαση.

Εάν μετά την κατακύρωση του Διαγωνισμού και πριν από την παράδοση εξοπλισμού/έτοιμου λογισμικού βάσει του αντικειμένου της σύμβασης, στο πλαίσιο πρότασης επικαιροποίησης, έχουν ανακοινωθεί νεότερα μοντέλα/ εκδόσεις, αποδεδειγμένα ισχυρότερα και καλύτερα από εκείνα που προσφέρθηκαν και αξιολογήθηκαν, τότε ο Ανάδοχος υποχρεούται, και η ΚτΠ Α.Ε. δύναται να αποδεχθεί, να τα προμηθεύσει αντί των προσφερθέντων, με την προϋπόθεση ότι δεν επέρχεται οποιαδήποτε πρόσθετη οικονομική επιβάρυνση.

4.4 Υπεργολαβία

4.4.1. Ο συμβαλλόμενος στη συμφωνία-πλαίσιο ανάδοχος της εκτελεστικής σύμβασης δεν απαλλάσσεται από τις συμβατικές του υποχρεώσεις και ευθύνες λόγω ανάθεσης της εκτέλεσης τμήματος/τμημάτων της σύμβασης σε υπεργολάβους. Η τήρηση των υποχρεώσεων της παρ. 2 του άρθρου 18 του ν. 4412/2016 από υπεργολάβους δεν αίρει την ευθύνη του κυρίου αναδόχου.

4.4.2. Κατά την υπογραφή της συμφωνίας-πλαίσιο /της εκτελεστικής σύμβασης ο κύριος ανάδοχος υποχρεούται να αναφέρει στην αναθέτουσα αρχή το όνομα, τα στοιχεία επικοινωνίας και τους νόμιμους εκπροσώπους των υπεργολάβων του, οι οποίοι συμμετέχουν στην εκτέλεση αυτής, εφόσον είναι γνωστά τη συγκεκριμένη χρονική στιγμή. Επιπλέον, υποχρεούται να γνωστοποιεί στην αναθέτουσα αρχή κάθε αλλαγή των πληροφοριών αυτών, κατά τη διάρκεια της σύμβασης, καθώς και τις απαιτούμενες πληροφορίες σχετικά με κάθε νέο υπεργολάβο, τον οποίο ο κύριος ανάδοχος χρησιμοποιεί εν συνεχεία στην εν λόγω σύμβαση, προσκομίζοντας τα σχετικά συμφωνητικά/δηλώσεις συνεργασίας. Σε περίπτωση διακοπής της συνεργασίας του Αναδόχου με υπεργολάβο/ υπεργολάβους της σύμβασης, αυτός υποχρεούται σε άμεση γνωστοποίηση της διακοπής αυτής στην Αναθέτουσα Αρχή, οφείλει δε να διασφαλίσει την ομαλή εκτέλεση του τμήματος/ των τμημάτων της σύμβασης είτε από τον ίδιο, είτε από νέο υπεργολάβο τον οποίο θα γνωστοποιήσει στην αναθέτουσα αρχή κατά την ως άνω διαδικασία. Σε περίπτωση που ο ανάδοχος έχει στηριχθεί στις ικανότητες του υπεργολάβου όσον αφορά τη χρηματοοικονομική επάρκεια-τεχνική και επαγγελματική ικανότητα, σύμφωνα με τις απαιτήσεις της διακήρυξης, υποχρεούται να προτείνει αντικαταστάτη. Για τον έλεγχο της συνδρομής των προϋποθέσεων στο πρόσωπο του νέου υπεργολάβου εφαρμόζονται αναλόγως οι διατάξεις της παρούσας για τον έλεγχο της συνδρομής των λόγων αποκλεισμού και των κριτηρίων επιλογής του.

4.4.3. Η αναθέτουσα αρχή επαληθεύει τη συνδρομή των λόγων αποκλεισμού για τους υπεργολάβους, όπως αυτοί περιγράφονται στην παράγραφο 2.2.3 και με τα αποδεικτικά μέσα της παραγράφου

2.2.9.2 της παρούσας, εφόσον το(α) τμήμα(τα) της σύμβασης, το(α) οποίο(α) ο ανάδοχος προτίθεται να αναθέσει υπό μορφή υπεργολαβίας σε τρίτους, υπερβαίνουν σωρευτικά ποσοστό του τριάντα τοις εκατό (30%) της συνολικής αξίας της σύμβασης. Επιπλέον, προκειμένου να μην αθετούνται οι υποχρεώσεις της παρ. 2 του άρθρου 18 του ν. 4412/2016, δύναται να επαληθεύσει τους ως άνω λόγους και για τμήμα ή τμήματα της σύμβασης που υπολείπονται του ως άνω ποσοστού.

Όταν από την ως άνω επαλήθευση προκύπτει ότι συντρέχουν λόγοι αποκλεισμού απαιτεί την αντικατάστασή του, κατά τα ειδικότερα αναφερόμενα στις παρ. 5 και 6 του άρθρου 131 του ν. 4412/2016.

4.5 Τροποποίηση συμφωνίας-πλαίσιο ή της εκτελεστικής σύμβασης κατά τη διάρκεια της

Επιφυλασσομένων των ρητρών προαίρεσης που αναφέρεται ανωτέρω στην παρούσα, η συμφωνία-πλαίσιο μπορεί να τροποποιείται κατά τη διάρκειά της, χωρίς να απαιτείται νέα διαδικασία σύναψης σύμβασης, μόνο σύμφωνα με τους όρους και τις προϋποθέσεις του άρθρου 132 του ν. 4412/2016 και κατόπιν γνωμοδότησης του αρμοδίου οργάνου.

4.6 Δικαίωμα μονομερούς λύσης της σύμβασης

4.6.1. Η αναθέτουσα αρχή μπορεί, με τις προϋποθέσεις που ορίζουν οι κείμενες διατάξεις, να καταγγείλει τη συμφωνία-πλαίσιο κατά τη διάρκεια της εκτέλεσής της, εφόσον:

α) η συμφωνία-πλαίσιο έχει υποστεί ουσιώδη τροποποίηση, κατά την έννοια της παρ. 4 του άρθρου 132 του ν. 4412/2016, που θα απαιτούσε νέα διαδικασία σύναψης σύμβασης

β) ο ανάδοχος, κατά το χρόνο της ανάθεσης της σύμβασης, τελούσε σε μια από τις καταστάσεις που αναφέρονται στην παράγραφο 2.2.3.1 και, ως εκ τούτου, θα έπρεπε να έχει αποκλειστεί από τη διαδικασία σύναψης της σύμβασης,

γ) η συμφωνία-πλαίσιο δεν έπρεπε να ανατεθεί στον ανάδοχο λόγω σοβαρής παραβίασης των υποχρεώσεων που υπέχει από τις Συνθήκες και την Οδηγία 2014/24/ΕΕ, η οποία έχει αναγνωριστεί με απόφαση του Δικαστηρίου της Ένωσης στο πλαίσιο διαδικασίας δυνάμει του άρθρου 258 της ΣΛΕΕ.

δ) ο ανάδοχος καταδικαστεί αμετάκλητα, κατά τη διάρκεια εκτέλεσης της σύμβασης, για ένα από τα αδικήματα που αναφέρονται στην παρ. **Error! Reference source not found.** της παρούσας,

ε) ο ανάδοχος πτωχεύσει ή υπαχθεί σε διαδικασία ειδικής εκκαθάρισης ή τεθεί υπό αναγκαστική διαχείριση από εκκαθαριστή ή από το δικαστήριο ή υπαχθεί σε διαδικασία πτωχευτικού συμβιβασμού ή αναστείλει τις επιχειρηματικές του δραστηριότητες ή υπαχθεί σε διαδικασία εξυγίανσης και δεν τηρεί τους όρους αυτής ή εάν βρεθεί σε οποιαδήποτε ανάλογη κατάσταση, προκύπτουσα από παρόμοια διαδικασία, προβλεπόμενη σε εθνικές διατάξεις νόμου. Η αναθέτουσα αρχή μπορεί να μην καταγγείλει τη σύμβαση, υπό την προϋπόθεση ότι ο ανάδοχος ο οποίος θα βρεθεί σε μία εκ των καταστάσεων που αναφέρονται στην περίπτωση αυτή αποδεικνύει ότι είναι σε θέση να εκτελέσει τη σύμβαση, λαμβάνοντας υπόψη τις ισχύουσες διατάξεις και τα μέτρα για τη συνέχιση της επιχειρηματικής του λειτουργίας.



5 ΕΙΔΙΚΟΙ ΟΡΟΙ ΕΚΤΕΛΕΣΗΣ ΕΚΤΕΛΕΣΤΙΚΩΝ ΣΥΜΒΑΣΕΩΝ

5.1 Τρόπος πληρωμής

5.1.1. Η πληρωμή του αναδόχου θα πραγματοποιηθεί με ένα από τους παρακάτω τρόπους πληρωμής που θα δηλώσει ο υποψήφιος οικονομικός φορέας στον υποφάκελο της οικονομικής προσφοράς του.

Στην περίπτωση που δεν έχει επιλεγεί με σαφήνεια ένας από τους κάτωθι τρόπους πληρωμής, θεωρείται ότι ο υποψήφιος Ανάδοχος αποδέχεται τον τρόπο πληρωμής που θα επιλέξει η Αναθέτουσα Αρχή.

Τρόποι Πληρωμής:

1)	Το 100% της συμβατικής αξίας μετά την οριστική παραλαβή της Σύμβασης
2)	<p>1) Χορήγηση έντοκης προκαταβολής μέχρι ποσοστού τριάντα τοις εκατό (30%) του συμβατικού τιμήματος χωρίς Φ.Π.Α., με την κατάθεση ισόποσης εγγύησης, σύμφωνα με τα οριζόμενα στο άρθρο 72§7 του ν. 4412/2016 και της Παρ.4.1 της παρούσας. Η παραπάνω προκαταβολή θα είναι έντοκη. Κατά την εξόφληση θα παρακρατείται τόκος επί της εισπραχθείσας προκαταβολής και για το χρονικό διάστημα υπολογιζόμενου από την ημερομηνία λήψεως μέχρι την ημερομηνία οριστικής και ποιοτικής παραλαβής. Για τον υπολογισμό του τόκου θα λαμβάνεται υπόψη το ύψος του επιτοκίου των εντόκων γραμματίων του Δημοσίου 12μηνιας διάρκειας που θα ισχύει κατά την ημερομηνία λήψης της προκαταβολής προσαυξημένο κατά 0,25 ποσοστιαίες μονάδες το οποίο θα παραμένει σταθερό μέχρι την εξάντληση του ποσού της χορηγηθείσας προκαταβολής.</p> <p>2) Τμηματικές απολογιστικές πληρωμές του φυσικού αντικείμενου που έχει παραληφθεί, έπειτα από τον ποσοτικό και ποιοτικό έλεγχο, ανά χρονικό διάστημα τριών (3) μηνών, αφού παρακρατηθεί τόκος επί της απομειωμένης από την προηγούμενη πληρωμή προκαταβολής και για το χρονικό διάστημα από την ημερομηνία του υπολογισμού τόκου της προηγούμενης τμηματικής πληρωμής μέχρι την οριστική ποιοτική και ποσοτική παραλαβή της σύμβασης. Η πληρωμή του συμβατικού τιμήματος θα γίνεται με την προσκόμιση των νομίμων παραστατικών και δικαιολογητικών που προβλέπονται από τις διατάξεις του άρθρου 200 παρ. 4 του ν. 4412/2016, καθώς και κάθε άλλου δικαιολογητικού που τυχόν ήθελε ζητηθεί από τις αρμόδιες υπηρεσίες που διενεργούν τον έλεγχο και την πληρωμή.</p>

Επισημαίνεται ότι η παραπάνω προκαταβολή δύναται να χορηγηθεί και τμηματικά.

Η πληρωμή του συμβατικού τιμήματος θα γίνεται με την προσκόμιση των νόμιμων παραστατικών και δικαιολογητικών που προβλέπονται από τις διατάξεις του άρθρου 200 παρ. 5 του ν. 4412/2016,

καθώς και κάθε άλλου δικαιολογητικού που τυχόν ήθελε ζητηθεί από τις αρμόδιες υπηρεσίες που διενεργούν τον έλεγχο και την πληρωμή.

5.1.2. Τον Ανάδοχο βαρύνουν οι υπέρ τρίτων κρατήσεις, ως και κάθε άλλη επιβάρυνση, σύμφωνα με την κείμενη νομοθεσία, μη συμπεριλαμβανομένου Φ.Π.Α., για την παροχή των υπηρεσιών στον τόπο και με τον τρόπο που προβλέπεται στα έγγραφα της σύμβασης.

Ιδίως βαρύνεται με τις ακόλουθες κρατήσεις:

α) Κράτηση 0,10% η οποία υπολογίζεται επί της αξίας κάθε πληρωμής προ φόρων και κρατήσεων της αρχικής, καθώς και κάθε συμπληρωματικής σύμβασης υπέρ της Ενιαίας Ανεξάρτητης Αρχής Δημοσίων Συμβάσεων σύμφωνα με το άρθρο 12 του ν. 4912/2022

β) Κράτηση ύψους 0,02% υπέρ της ανάπτυξης και συντήρησης του ΟΠΣ ΕΣΗΔΗΣ, η οποία υπολογίζεται επί της αξίας, εκτός ΦΠΑ, της αρχικής, καθώς και κάθε συμπληρωματικής σύμβασης. Το ποσό αυτό παρακρατείται σε κάθε πληρωμή από την αναθέτουσα αρχή στο όνομα και για λογαριασμό του Υπουργείου Ψηφιακής Διακυβέρνησης, σύμφωνα με την παρ. 6 του άρθρου 36 του ν. 4412/2016.

Οι υπέρ τρίτων κρατήσεις υπόκεινται στο εκάστοτε ισχύον αναλογικό τέλος χαρτοσήμου και στην επ' αυτού εισφορά υπέρ ΟΓΑ.

5.2 Αναπροσαρμογή τιμής

Δεν επιτρέπεται η αναπροσαρμογή τιμών στη Συμφωνία Πλαίσιο και στις εκτελεστικές αυτής συμβάσεις.

5.3 Παρακολούθηση των Εκτελεστικών Συμβάσεων

5.3.1 Η παρακολούθηση της εκτέλεσης κάθε Σύμβασης και η διοίκηση αυτής θα διενεργηθεί από την καθ' ύλην αρμόδια υπηρεσία ή άλλως από την υπηρεσία η οποία ορίζεται με απόφαση της αναθέτουσας αρχής ή επιτροπή που συγκροτείται επίσης με απόφαση της αναθέτουσας αρχής η οποία και θα εισηγείται στο αρμόδιο αποφαινόμενο όργανο για όλα τα ζητήματα που αφορούν στην προσήκουσα εκτέλεση όλων των όρων της σύμβασης και στην εκπλήρωση των υποχρεώσεων του αναδόχου, στη λήψη των επιβεβλημένων μέτρων λόγω μη τήρησης των ως άνω όρων και ιδίως για ζητήματα που αφορούν σε τροποποίηση του αντικειμένου και παράταση της διάρκειας της σύμβασης, με την επιφύλαξη του άρθρου 132 του ν. 4412/2016. Την καθ' ύλην αρμόδια υπηρεσία ή επιτροπή που θα είναι αρμόδια για την παρακολούθηση και εισήγηση στο αρμόδιο αποφαινόμενο όργανο, όπως περιγράφεται ανωτέρω, θα υποστηρίζει στο έργο της ο σύμβουλος τεχνικής υποστήριξης (ΣΤΥ).

5.3.2. Η αρμόδια υπηρεσία μπορεί, με απόφασή της να ορίζει για την παρακολούθηση της σύμβασης ως επόπτη με καθήκοντα εισηγητή υπάλληλο της υπηρεσίας. Με την ίδια απόφαση δύνανται να ορίζονται και άλλοι υπάλληλοι της αρμόδιας υπηρεσίας ή των εξυπηρετούμενων από την σύμβαση φορέων, στους οποίους ανατίθενται επιμέρους καθήκοντα για την παρακολούθηση της σύμβασης. Σε αυτή την περίπτωση ο επόπτης λειτουργεί ως συντονιστής.

Τα καθήκοντα του επόπτη είναι, ενδεικτικά, η πιστοποίηση της εκτέλεσης του αντικειμένου της σύμβασης, καθώς και ο έλεγχος της συμμόρφωσης του αναδόχου με τους όρους της σύμβασης. Με

εισήγηση του επόπτη η υπηρεσία που διοικεί τη σύμβαση μπορεί να απευθύνει έγγραφα με οδηγίες και εντολές προς τον ανάδοχο που αφορούν στην εκτέλεση της σύμβασης.

5.4 Παραλαβή των εκτελεστικών συμβάσεων

Η παραλαβή των παρεχόμενων υπηρεσιών ή/και παραδοτέων γίνεται από επιτροπή παραλαβής που συγκροτείται, σύμφωνα με την παράγραφο 11 εδάφιο δ' του άρθρου 221 του ν. 4412/2016. Κατά τη διαδικασία παραλαβής (εφαρμόζεται και σε τμηματικές παραλαβές) διενεργείται ο απαιτούμενος έλεγχος σύμφωνα με τα οριζόμενα στη σύμβαση, μπορεί δε να καλείται να παραστεί και ο ανάδοχος.

Μετά την ολοκλήρωση της διαδικασίας, η επιτροπή παραλαβής:

α) είτε παραλαμβάνει τις σχετικές υπηρεσίες ή παραδοτέα, εφόσον καλύπτονται οι απαιτήσεις της σύμβασης χωρίς έγκριση ή απόφαση του αποφαινόμενου οργάνου,
β) είτε εισηγείται για την παραλαβή με παρατηρήσεις ή την απόρριψη των παρεχόμενων υπηρεσιών ή παραδοτέων σύμφωνα με τα κατωτέρω:

- Αν η επιτροπή παραλαβής κρίνει ότι οι παρεχόμενες υπηρεσίες ή/και τα παραδοτέα δεν ανταποκρίνονται πλήρως στους όρους της σύμβασης, συντάσσεται πρωτόκολλο προσωρινής παραλαβής, που αναφέρει τις παρεκκλίσεις που διαπιστώθηκαν από τους όρους της σύμβασης και γνωμοδοτεί αν οι αναφερόμενες παρεκκλίσεις επηρεάζουν την καταλληλότητα των παρεχόμενων υπηρεσιών ή/και παραδοτέων και συνεπώς αν μπορούν οι τελευταίες να καλύψουν τις σχετικές ανάγκες.
Στην περίπτωση που διαπιστωθεί ότι δεν επηρεάζεται η καταλληλότητα, με αιτιολογημένη απόφαση του αρμόδιου αποφαινόμενου οργάνου, μπορεί να εγκριθεί η παραλαβή των εν λόγω παρεχόμενων υπηρεσιών ή/και παραδοτέων, με έκπτωση επί της συμβατικής αξίας, η οποία θα πρέπει να είναι ανάλογη προς τις διαπιστωθείσες παρεκκλίσεις. Μετά την έκδοση της ως άνω απόφασης, η επιτροπή παραλαβής υποχρεούται να προβεί στην οριστική παραλαβή των παρεχόμενων υπηρεσιών ή/και παραδοτέων της σύμβασης και να συντάξει σχετικό πρωτόκολλο οριστικής παραλαβής, σύμφωνα με τα αναφερόμενα στην απόφαση.
- Αν διαπιστωθεί ότι επηρεάζεται η καταλληλότητα, με αιτιολογημένη απόφαση του αρμόδιου αποφαινόμενου οργάνου απορρίπτονται οι παρεχόμενες υπηρεσίες ή τα παραδοτέα, με την επιφύλαξη των οριζόμενων στο άρθρο 5.5 της παρούσας.

Αν παρέλθει χρονικό διάστημα μεγαλύτερο των 30 ημερών από την ημερομηνία υποβολής του και δεν έχει εκδοθεί πρωτόκολλο παραλαβής ή πρωτόκολλο με παρατηρήσεις, θεωρείται ότι η παραλαβή έχει συντελεστεί αυτοδίκαια.

Ανεξάρτητα από την, κατά τα ανωτέρω, αυτοδίκαιη παραλαβή και την πληρωμή του αναδόχου, πραγματοποιούνται οι προβλεπόμενοι από τη σύμβαση έλεγχοι από επιτροπή που συγκροτείται με απόφαση του Διοικητικού Συμβουλίου, στην οποία δεν μπορεί να συμμετέχουν ο πρόεδρος και τα μέλη της επιτροπής της παραγράφου 1. Η παραπάνω επιτροπή παραλαβής προβαίνει σε όλες τις διαδικασίες παραλαβής που προβλέπονται από την σύμβαση και συντάσσει τα σχετικά πρωτόκολλα. Οι εγγυητικές επιστολές προκαταβολής και καλής εκτέλεσης δεν επιστρέφονται πριν την ολοκλήρωση όλων των προβλεπομένων από τη σύμβαση ελέγχων και τη σύνταξη των σχετικών πρωτοκόλλων. Οποιαδήποτε ενέργεια που έγινε από την αρχική επιτροπή παραλαβής, δεν λαμβάνεται υπόψη.

5.5 Απόρριψη Παραδοτέων – Αντικατάσταση

Σε περίπτωση οριστικής απόρριψης ολόκληρου ή μέρους των παρεχόμενων υπηρεσιών ή /και παραδοτέων, με έκπτωση επί της συμβατικής αξίας, με απόφαση της αναθέτουσας αρχής μπορεί να εγκρίνεται αντικατάσταση των υπηρεσιών ή/και παραδοτέων αυτών με άλλα, που να είναι σύμφωνα με τους όρους της σύμβασης.

Αν η αντικατάσταση γίνεται μετά τη λήξη της συνολικής διάρκειας της σύμβασης, η προθεσμία που ορίζεται για την αντικατάσταση δεν μπορεί να είναι μεγαλύτερη του 25% της συνολικής διάρκειας της σύμβασης, ο δε ανάδοχος υπόκειται σε ποινικές ρήτρες, σύμφωνα με το άρθρο 218 του ν. 4412/2016 και την παράγραφο 5.6 της παρούσας, λόγω εκπρόθεσμης παράδοσης.

Αν ο ανάδοχος δεν αντικαταστήσει τις υπηρεσίες ή/και τα παραδοτέα που απορρίφθηκαν μέσα στην προθεσμία που του τάχθηκε και εφόσον έχει λήξει η συνολική διάρκεια, κηρύσσεται έκπτωτος και υπόκειται στις προβλεπόμενες κυρώσεις.

5.6 Κήρυξη οικονομικού φορέα έκπτωτου - Κυρώσεις

5.6.1. Ο ανάδοχος, με την επιφύλαξη της συνδρομής λόγων ανωτέρας βίας, κηρύσσεται υποχρεωτικά έκπτωτος από τη συμφωνία-πλαίσιο ή και της εκτελεστικής σύμβασης που έχει υπογράψει και από κάθε δικαίωμα που απορρέει από αυτήν με απόφαση της Αναθέτουσας Αρχής, ύστερα από γνωμοδότηση του αρμόδιου οργάνου :

α) στην περίπτωση της παρ. 7 του άρθρου 105 του ν. 4412/2016 περί κατακύρωσης και σύναψης σύμβασης

β) στην περίπτωση που δεν εκπληρώσει τις υποχρεώσεις του που απορρέουν από τη σύμβαση ή/και δεν συμμορφωθεί με τις σχετικές γραπτές εντολές της υπηρεσίας, που είναι σύμφωνες με τη σύμβαση ή τις κείμενες διατάξεις, εντός του συμφωνημένου χρόνου εκτέλεσης της σύμβασης,

γ) εφόσον δεν παράσχει τις υπηρεσίες ή δεν υποβάλει τα παραδοτέα ή δεν προβεί στην αντικατάστασή τους μέσα στον συμβατικό χρόνο ή στον χρόνο παράτασης που του δοθεί, σύμφωνα με τα όσα προβλέπονται στο άρθρο 217 του ν. 4412/2016 περί διάρκειας σύμβασης παροχής υπηρεσίας, με την επιφύλαξη των παρ. 2 και 3 του άρθρου 203 του ν. 4412/2016.

Στην περίπτωση συνδρομής λόγου έκπτωσης του αναδόχου από τη σύμβαση κατά την ως άνω περίπτωση (γ), η αναθέτουσα αρχή κοινοποιεί στον ανάδοχο ειδική όχληση, η οποία μνημονεύει τις διατάξεις του άρθρου 203 του ν. 4412/2016 και περιλαμβάνει συγκεκριμένη περιγραφή των ενεργειών στις οποίες οφείλει να προβεί ο ανάδοχος, προκειμένου να συμμορφωθεί, μέσα σε προθεσμία που καθορίζεται με απόφαση της Αναθέτουσας Αρχής η οποία δεν μπορεί να είναι μικρότερη των δεκαπέντε (15) ημερών από την κοινοποίηση της ανωτέρω όχλησης. Αν η προθεσμία, που τεθεί με την ειδική όχληση, παρέλθει, χωρίς ο ανάδοχος να συμμορφωθεί, κηρύσσεται έκπτωτος μέσα σε προθεσμία τριάντα (30) ημερών από την άπρακτη πάροδο της προθεσμίας συμμόρφωσης.

Ο ανάδοχος δεν κηρύσσεται έκπτωτος για λόγους που αφορούν σε υπαιτιότητα του φορέα εκτέλεσης της σύμβασης ή αν συντρέχουν λόγοι ανωτέρας βίας.

Στον ανάδοχο που κηρύσσεται έκπτωτος από τη σύμβαση, επιβάλλονται, με απόφαση του αποφαινόμενου οργάνου, ύστερα από γνωμοδότηση του αρμόδιου οργάνου, το οποίο

υποχρεωτικά καλεί τον ενδιαφερόμενο προς παροχή εξηγήσεων, αθροιστικά οι παρακάτω κυρώσεις:

α) ολική κατάπτωση της εγγύησης καλής εκτέλεσης της σύμβασης,

β) είσπραξη εντόκως της προκαταβολής που χορηγήθηκε στον έκπτωτο από τη σύμβαση ανάδοχο είτε από ποσόν που δικαιούται να λάβει είτε με κατάθεση του ποσού από τον ίδιο είτε με κατάπτωση της εγγύησης προκαταβολής. Ο υπολογισμός των τόκων γίνεται από την ημερομηνία λήψης της προκαταβολής από τον ανάδοχο μέχρι την ημερομηνία έκδοσης της απόφασης κήρυξής του ως εκπτώτου, με το ισχύον κάθε φορά ανώτατο όριο επιτοκίου για τόκο από δικαιοπραξία, από την ημερομηνία δε αυτή και μέχρι της επιστροφής της, με το ισχύον κάθε φορά επιτόκιο για τόκο υπερημερίας εφόσον προβλέπεται προκαταβολή.

5.6.2. Αν οι υπηρεσίες παρασχεθούν από υπαιτιότητα του αναδόχου μετά τη λήξη της διάρκειας της σύμβασης και μέχρι λήξης του χρόνου της παράτασης που χορηγήθηκε, επιβάλλονται εις βάρος του ποινικές ρήτρες, με αιτιολογημένη απόφαση της αναθέτουσας αρχής. Ποινικές ρήτρες δύναται να επιβάλλονται και για πλημμελή εκτέλεση των όρων της σύμβασης ⁶.

Οι ποινικές ρήτρες υπολογίζονται ως εξής:

α) για καθυστέρηση που περιορίζεται σε χρονικό διάστημα που δεν υπερβαίνει το 50% της προβλεπόμενης συνολικής διάρκειας της σύμβασης ή σε περίπτωση τμηματικών/ενδιαμέσων προθεσμιών της αντίστοιχης προθεσμίας επιβάλλεται ποινική ρήτρα 2,5% επί της συμβατικής αξίας χωρίς ΦΠΑ των υπηρεσιών που παρασχέθηκαν εκπρόθεσμα,

β) για καθυστέρηση που υπερβαίνει το 50% επιβάλλεται ποινική ρήτρα 5% χωρίς ΦΠΑ επί της συμβατικής αξίας των υπηρεσιών που παρασχέθηκαν εκπρόθεσμα,

γ) οι ποινικές ρήτρες για υπέρβαση των τμηματικών προθεσμιών είναι ανεξάρτητες από τις επιβαλλόμενες για υπέρβαση της συνολικής διάρκειας της σύμβασης και δύνανται να ανακαλούνται με αιτιολογημένη απόφαση της αναθέτουσας αρχής, αν οι υπηρεσίες που αφορούν στις ως άνω τμηματικές προθεσμίες παρασχεθούν μέσα στη συνολική της διάρκεια και τις εγκεκριμένες παρατάσεις αυτής και με την προϋπόθεση ότι το σύνολο της σύμβασης έχει εκτελεστεί πλήρως.

Το ποσό των ποινικών ρητρών αφαιρείται/συμψηφίζεται από/με την αμοιβή του αναδόχου.

Η επιβολή ποινικών ρητρών δεν στερεί από την αναθέτουσα αρχή το δικαίωμα να κηρύξει τον ανάδοχο έκπτωτο.

5.7 Διοικητικές προσφυγές κατά τη διαδικασία εκτέλεσης

Ο ανάδοχος μπορεί κατά των αποφάσεων που επιβάλλουν σε βάρος του κυρώσεις, δυνάμει των όρων των άρθρων 5.6 (Κήρυξη οικονομικού φορέα εκπτώτου - Κυρώσεις), 5.5. (Απόρριψη παραδοτέων – Αντικατάσταση) και 5.4(Παραλαβή των εκτελεστικών συμβάσεων), καθώς και κατ' εφαρμογή των συμβατικών όρων να ασκήσει προσφυγή για λόγους νομιμότητας και ουσίας ενώπιον του φορέα που εκτελεί τη σύμβαση μέσα σε ανατρεπτική προθεσμία (30) ημερών από την ημερομηνία της

⁶ Πρβλ. άρθρο 218 του ν.4412/2016, όπως τροποποιήθηκε με το άρθρο 43 παρ. 25, υποπαρ. α του ν. 4605/2019.

κοινοποίησης ή της πλήρους γνώσης της σχετικής απόφασης. Η εμπρόθεσμη άσκηση της προσφυγής αναστέλλει τις επιβαλλόμενες κυρώσεις.

Επί της προσφυγής αποφασίζει το αρμοδίως αποφαινόμενο όργανο, ύστερα από γνωμοδότηση του προβλεπόμενου της περίπτωσης δ' της παραγράφου 11 του άρθρου 221 του ν.4412/2016 οργάνου, εντός προθεσμίας τριάντα (30) ημερών από την άσκησή της, άλλως θεωρείται ως σιωπηρώς απορριφθείσα. Κατά της απόφασης αυτής δεν χωρεί η άσκηση άλλης οποιασδήποτε φύσης διοικητικής προσφυγής. Αν κατά της απόφασης που επιβάλλει κυρώσεις δεν ασκηθεί εμπρόθεσμα η προσφυγή ή αν απορριφθεί αυτή από το αποφαινόμενο αρμοδίως όργανο, η απόφαση καθίσταται οριστική. Αν ασκηθεί εμπρόθεσμα προσφυγή, αναστέλλονται οι συνέπειες της απόφασης μέχρι αυτή να οριστικοποιηθεί.

5.8 Δικαστική επίλυση διαφορών

Κάθε διαφορά μεταξύ των συμβαλλόμενων μερών που προκύπτει από τις συμβάσεις που συνάπτονται στο πλαίσιο της παρούσας διακήρυξης, επιλύεται με την άσκηση προσφυγής ή αγωγής στο Διοικητικό Εφετείο της Περιφέρειας, στην οποία εκτελείται εκάστη σύμβαση, κατά τα ειδικότερα οριζόμενα στις παρ. 1 έως και 6 του άρθρου 205Α του ν. 4412/2016. Πριν από την άσκηση της προσφυγής στο Διοικητικό Εφετείο προηγείται υποχρεωτικά η τήρηση της ενδικοφανούς διαδικασίας που προβλέπεται στο άρθρο 205 του ν. 4412/2016 και την παράγραφο 5.7 της παρούσας, διαφορετικά η προσφυγή απορρίπτεται ως απαράδεκτη. Αν ο ανάδοχος της σύμβασης είναι κοινοπραξία, η προσφυγή ασκείται είτε από την ίδια είτε από όλα τα μέλη της. Δεν απαιτείται η τήρηση ενδικοφανούς διαδικασίας αν ασκείται από τον ενδιαφερόμενο αγωγή, στο δικόγραφο της οποίας δεν σωρεύεται αίτημα ακύρωσης ή τροποποίησης διοικητικής πράξης ή παράλειψης.

6 ΕΚΤΕΛΕΣΤΙΚΕΣ ΣΥΜΒΑΣΕΙΣ

6.1 Λειτουργία της Συμφωνίας Πλαίσιο - Ανάθεση των Εκτελεστικών Συμβάσεων

Κατόπιν της σύναψης της Συμφωνίας Πλαισίου με τους Αντισυμβαλλόμενους, το Έργο θα χωριστεί σε επιμέρους εκτελεστικές συμβάσεις, ανάλογα με τις εκάστοτε ανάγκες της Αναθέτουσας Αρχής, των οποίων το συνολικό τίμημα καθώς και τα χρονοδιαγράμματα εκτέλεσης δεν είναι γνωστά εκ των προτέρων, αλλά θα καθορίζονται με την κάθε Εκτελεστική Σύμβαση που θα υπογράφεται μεταξύ της Αναθέτουσας Αρχής και του Αναδόχου, ο οποίος θα καλείται προς υπογραφή, ύστερα από σχετική διαδικασία, όπως προβλέπεται αμέσως κατωτέρω.

Ειδικότερα επισημαίνεται ότι Ο Ανάδοχος οφείλει να ανταποκρίνεται σε κάθε Πρόσκληση της Αναθέτουσας Αρχής για υλοποίηση μιας εκτελεστικής Σύμβασης ως ανωτέρω.

6.2 Υπογραφή εκτελεστικών συμβάσεων

6.2.1 Κάθε Εκτελεστική Σύμβαση συνάπτεται μετά από πρόκληση της αναθέτουσας αρχής προς τον αντισυμβαλλόμενο της αντίστοιχης Συμφωνίας – Πλαίσιο. Στην πρόσκληση θα καθορίζεται το αντικείμενο εργασιών, ο τρόπος εκτέλεσης, τα παραδοτέα καθώς και το χρονοδιάγραμμα ολοκλήρωσης, σύμφωνα με τη σχετική Πρόσκληση της Αναθέτουσας Αρχής και την αντίστοιχη εξατομικευμένη προσφορά του Αναδόχου της Εκτελεστικής Σύμβασης. Σημειώνεται ότι η Αναθέτουσα αρχή κατά τη διάρκεια της Εκτελεστικής Σύμβασης θα μεριμνήσει ώστε να υπάρχει η απαραίτητη συνεργασία μεταξύ του αντισυμβαλλόμενου και των εμπλεκόμενων που σχετίζονται με τις εργασίες της.

6.2.2 Σε κάθε πρόσκληση Εκτελεστικής Σύμβασης θα προσδιορίζονται επακριβώς τα προφίλ των στελεχών που απαιτούνται.

Ο αντισυμβαλλόμενος θα μπορεί να ορίζει στελέχη για την κάλυψη των απαιτήσεων της εκάστοτε εκτελεστικής τα οποία μπορεί να είναι μέλη εξ' όσων συμπεριέλαβε στην προσφορά του για τη Συμφωνία Πλαίσιο ή άλλα αλλά με κατ' ελάχιστο τα προσόντα των μελών της προσφοράς.

6.2.3 Στο Σχήμα Υλοποίησης και Διοίκησης Έργου θα γίνεται αναφορά στα εξής:

- στους ρόλους που θα ανατεθούν στο προσωπικό του Αναδόχου στο πλαίσιο του Έργου
- στον αριθμό των ατόμων, ανά ρόλο, που θα συμμετέχουν στην Ομάδα Υλοποίησης και Διοίκησης του Έργου και θα είναι υπεύθυνα για το σύνολο των ενεργειών στο πλαίσιο του Έργου
- στα στελέχη που θα αναλάβουν τους ρόλους του Υπεύθυνου Έργου και του αναπληρωτή Υπεύθυνου Έργου
- στο γνωστικό αντικείμενο που θα καλύψει το προσωπικό του Αναδόχου (με ειδική αναφορά σε αυτό του Υπεύθυνου Έργου και του αναπληρωτή Υπεύθυνου Έργου)

6.3 Κατάρτιση και Υποβολή Προσφορών

ΔΕΝ ΕΦΑΡΜΟΖΕΤΑΙ

6.4 Παραλαβή – Αποσφράγιση Προσφορών

ΔΕΝ ΕΦΑΡΜΟΖΕΤΑΙ

6.5 Δικαιολογητικά του αντισυμβαλλόμενου στον οποίο πρόκειται να γίνει η κατακύρωση της εκτελεστικής σύμβασης

6.5.1 Ο υποψήφιος ανάδοχος στον οποίο πρόκειται να γίνει η κατακύρωση της εκτελεστικής σύμβασης, ειδοποιείται μέσω ΕΣΗΔΗΣ από τον Αναθέτουσα Αρχή να υποβάλει στον δικτυακό τόπο του συγκεκριμένου διαγωνισμού ενημερωμένα τα σχετικά δικαιολογητικά σύμφωνα με τα άρθρα 79 και 80, και κατά περίπτωση του άρθρου 82 του Ν.4412/16.

6.6 Αξιολόγηση δικαιολογητικών προσωρινού αναδόχου

6.6.1 Η αξιολόγηση των δικαιολογητικών προσωρινού αναδόχου θα διενεργηθεί σύμφωνα με τα αναφερόμενα στο άρθρο 3.2 «Πρόσκληση υποβολής δικαιολογητικών προσωρινού αναδόχου – Δικαιολογητικά προσωρινού αναδόχου» της παρούσας διακήρυξης.

6.6.2 Εφόσον συντρέχουν οι περιπτώσεις έκπτωσης του άρθρου 3.2 «Πρόσκληση υποβολής δικαιολογητικών προσωρινού αναδόχου – Δικαιολογητικά προσωρινού αναδόχου» της διακήρυξης, ο προσωρινός ανάδοχος κηρύσσεται έκπτωτος, καταπίπτει υπέρ της Αναθέτουσας Αρχής η εγγύηση καλής εκτέλεσης της Συμφωνίας πλαίσιο του προσωρινού αναδόχου και η κατακύρωση γίνεται στον οικονομικό φορέα που υπέβαλε την αμέσως επόμενη πλέον συμφέρουσα από οικονομική άποψη προσφορά βάσει του κριτηρίου ανάθεσης της παρούσας χωρίς να λαμβάνεται υπόψη η προσφορά του προσφέροντος που απορρίφθηκε.

6.6.3 Οι οικονομικοί φορείς σύμφωνα με την παρ. 6 του άρθρου 79 του Ν. 4412/16 δεν υποχρεούνται να υποβάλουν δικαιολογητικά, όταν η Αναθέτουσα Αρχή που έχει αναθέσει τη σύμβαση ή συνάψει τη συμφωνία-πλαίσιο, διαθέτει ήδη τα δικαιολογητικά αυτά.

6.7 Κατακύρωση – σύναψη εκτελεστικής σύμβασης

6.7.1 Η Αναθέτουσα Αρχή αποστέλλει ηλεκτρονικά ανακοίνωση της απόφασης κατακύρωσης στον αντισυμβαλλόμενο με τον οποίο πρόκειται να υπογραφεί η εκτελεστική σύμβαση και τον καλεί να προσέλθει για την υπογραφή της σύμβασης σε καθορισμένη ημερομηνία και ώρα. Από την ως άνω ανακοίνωση η εκτελεστική σύμβαση θεωρείται συναφθείσα, το δε έγγραφο της σύμβασης έχει αποδεικτικό χαρακτήρα.

Η απόφαση κατακύρωσης καθίσταται οριστική εφόσον:

- Κοινοποιηθεί στον ανάδοχο
- Ολοκληρωθεί επιτυχώς ο προσυμβατικός έλεγχος από το Ελεγκτικό Συνέδριο (εφόσον απαιτείται) σύμφωνα με τα άρθρα 324-327 του ν. 4700/2020 (ΦΕΚ Α' 127)
- Ο ανάδοχος έχει υποβάλλει υπεύθυνη δήλωση στην οποία δηλώνεται ότι δεν έχουν επέλθει στο πρόσωπό του οψιγενείς μεταβολές κατά την έννοια του άρθρου 104 του ν. 4412/2016

6.7.2 Για την καλή εκτέλεση των όρων της εκτελεστικής σύμβασης, ο ανάδοχος παρέχει πριν ή κατά την υπογραφή της σύμβασης εγγύηση καλής εκτέλεσης, το ύψος της καθορίζεται σε ποσοστό 4% της αξίας της εκτελεστικής σύμβασης.

6.8 Εκτέλεση εκτελεστικής σύμβασης

6.8.1 Η εκτελεστική σύμβαση θεωρείται ότι εκτελέστηκε όταν:

6.8.1.1 Παραδόθηκαν και παραλήφθηκαν οριστικά (ποσοτικά και ποιοτικά) οι υπηρεσίες και τα υπό προμήθεια είδη.

6.8.1.2 Έγινε η αποπληρωμή του συμβατικού τιμήματος αφού, προηγουμένως επιβλήθηκαν τυχόν κυρώσεις ή εκπτώσεις.

6.8.1.3 Εκπληρώθηκαν και οι τυχόν λοιπές συμβατικές υποχρεώσεις και από τα δύο συμβαλλόμενα μέρη και αποδεσμεύθηκαν οι σχετικές εγγυήσεις κατά τα προβλεπόμενα από την εκτελεστική σύμβαση.

Για την εκτέλεση των εκτελεστικών συμβάσεων, την παρακολούθηση και παραλαβή τους, ισχύουν οι σχετικές προβλέψεις του Ν. 4412/2016 όπως εκάστοτε ισχύει.

7 ΠΑΡΑΡΤΗΜΑΤΑ

7.1 ΠΑΡΑΡΤΗΜΑ Ι – Αναλυτική Περιγραφή Φυσικού και Οικονομικού Αντικειμένου της συμφωνίας - πλαίσιο

7.1.1 Περιβάλλον της συμφωνίας - πλαίσιο

7.1.1.1 Εμπλεκόμενοι στην υλοποίηση του Έργου

Για την υλοποίηση του Έργου της παρούσας Διακήρυξης εμπλέκονται οι ακόλουθοι:

Φορέας Υλοποίησης	Κοινωνία της Πληροφορίας Μ.Α.Ε	Βλ. Παρ. 7.1.1.2 Error! Unknown switch argument. του Παραρτήματος Ι
Φορέας Χρηματοδότησης	Υπουργείο Ψηφιακής Διακυβέρνησης	Βλ. Παρ. 7.1.1.3 του Παραρτήματος Ι
Κύριος του Έργου	Υπουργείο Ψηφιακής Διακυβέρνησης	Βλ. Παρ. 7.1.1.4 του Παραρτήματος Ι
Φορέας Λειτουργίας του Έργου	Υπουργείο Ψηφιακής Διακυβέρνησης	Βλ. Παρ. 7.1.1.4 του Παραρτήματος Ι
Όργανα & Επιτροπές Παρακολούθησης, Διακυβέρνησης και Ελέγχου του Έργου	-	Βλ. Παρ. Error! Reference source not found. του Παραρτήματος Ι

7.1.1.2 Φορέας Υλοποίησης – Αναθέτουσα Αρχή

Η «Κοινωνία της Πληροφορίας Μ.Α.Ε.», είναι εταιρεία η οποία λειτουργεί χάριν του δημοσίου συμφέροντος και έχει ως κύρια αποστολή την ανάπτυξη δράσεων και την υποστήριξη των αρμόδιων φορέων για τη βελτίωση της διοικητικής ικανότητας της Δημόσιας Διοίκησης, καθώς και την εκτέλεση και διαχείριση έργων στον τομέα της πληροφορικής, επικοινωνίας και νέων τεχνολογιών για τη Δημόσια Διοίκηση. Η Εταιρεία λειτουργεί με τους κανόνες της ιδιωτικής οικονομίας του Ν. 3429/2005 στο πλαίσιο των διατάξεων του Ν. 3614/2007 (ΦΕΚ 267/Α), και του καταστατικού της όπως αυτό τροποποιήθηκε και ισχύει (ΦΕΚ 343/Β/07-02-2020) και εποπτεύεται από το Υπουργείο Ψηφιακής Διακυβέρνησης.

Βασικός σκοπός της Εταιρείας, όπως ορίζεται στην τελευταία τροποποίηση του καταστατικού αυτής (ΦΕΚ 343/Β/07-02-2020), είναι:

α) Η εκτέλεση δράσεων και έργων βελτίωσης της διοικητικής ικανότητας της δημόσιας διοίκησης στο πλαίσιο εφαρμογής οποιουδήποτε επιχειρησιακού προγράμματος, απ' όπου κι εάν αυτό χρηματοδοτείται (λ.χ. από ενωσιακούς ή/και από εθνικούς πόρους ή/και μέσω του Προγράμματος Δημοσίων Επενδύσεων), και η υποστήριξη της για την εκτέλεση όμοιων δράσεων και έργων με στόχο την ενδυνάμωση της διοικητικής αποτελεσματικότητάς της.

β) Η εκτέλεση έργων στον τομέα της πληροφορικής, της επικοινωνίας και των νέων τεχνολογιών για τη βελτίωση της δημόσιας διοίκησης στο πλαίσιο εφαρμογής των επιχειρησιακών προγραμμάτων του ΕΣΠΑ ή άλλων ευρωπαϊκών συγχρηματοδοτούμενων προγραμμάτων, ή/και εθνικών προγραμμάτων, απ' όπου κι εάν αυτά χρηματοδοτούνται (λ.χ. από ενωσιακούς ή/και από εθνικούς πόρους ή/και μέσω του Προγράμματος Δημοσίων Επενδύσεων), και η υποστήριξη της δημόσιας διοίκησης για την εκτέλεση σχετικών έργων.

γ) Η υποστήριξη του Υπουργείου Ψηφιακής Διακυβέρνησης ως βασικός επιτελικός βραχίονας υλοποίησης της στρατηγικής, των έργων και δράσεων του Υπουργείου στο πλαίσιο του Ψηφιακού Μετασχηματισμού της Δημόσιας Διοίκησης της χώρας.

δ) Η υποστήριξη ή/και διαχείριση της λειτουργίας συστημάτων πληροφορικής και επικοινωνίας της δημόσιας διοίκησης, όπως προβλέπεται ήδη στο ν. 2860/2000 (άρθρο 24 παράγραφος 6γ).

ε) Η ανάληψη της εκτέλεσης πράξεων και ενεργειών τεχνικής υποστήριξης, που χρηματοδοτούνται από επιχειρησιακά προγράμματα του ΕΣΠΑ ή από άλλα συγχρηματοδοτούμενα ευρωπαϊκά προγράμματα, ή/και εθνικά προγράμματα με χρηματοδότηση μέσω του Προγράμματος Δημοσίων Επενδύσεων ή/και μέσω του τακτικού προϋπολογισμού.

στ) Η χωρίς αντάλλαγμα υποστήριξη των ενδιαμέσων φορέων διαχείρισης για δράσεις κρατικών ενισχύσεων στο πλαίσιο του ΕΣΠΑ, ή/και άλλων συγχρηματοδοτούμενων προγραμμάτων, ή/και εθνικών προγραμμάτων δράσεων κρατικών ενισχύσεων χρηματοδοτούμενα από κάθε πηγή χρηματοδότησης (λ.χ. ενωσιακή ή/και εθνική) ύστερα από αίτηση του φορέα και υπογραφή σχετικής προγραμματικής συμφωνίας με την εταιρεία.

ζ) Η ανάληψη ως δικαιούχου ή ενδιάμεσου φορέα της υλοποίησης πράξεων σχετικών με Τεχνολογίες Πληροφορικής και Επικοινωνιών που απευθύνονται σε πολίτες ή σε επιχειρήσεις (κρατικές ενισχύσεις) και χρηματοδοτούνται από συγχρηματοδοτούμενα προγράμματα ή/ και εθνικά προγράμματα χρηματοδοτούμενα από το Πρόγραμμα Δημοσίων Επενδύσεων ή/και από κάθε άλλη πηγή.

η) Η ανάληψη της υλοποίησης ενεργειών τεχνικής βοήθειας που χρηματοδοτούνται από επιχειρησιακά προγράμματα του ΕΣΠΑ ή/και από άλλα συγχρηματοδοτούμενα προγράμματα ή/και εθνικά προγράμματα με πηγή χρηματοδότησης ενωσιακούς ή/και εθνικούς πόρους ή/ και μέσω του Προγράμματος Δημοσίων Επενδύσεων.

θ) Η συστηματική τεκμηρίωση και παρακολούθηση των χαρακτηριστικών, των προβλημάτων και της εξέλιξης της διοικητικής ικανότητας της δημόσιας διοίκησης, την αξιολόγηση των αποτελεσμάτων των προγραμμάτων και δράσεων που αποσκοπούν στη βελτίωση της και τη διευκόλυνση της μεταφοράς και προσαρμογής ξένης εμπειρίας και καλών πρακτικών στο ελληνικό διοικητικό περιβάλλον.

ι) Η συλλογή και επεξεργασία ποιοτικών και ποσοτικών στοιχείων για τα θέματα που σχετίζονται με την πρόοδο της Ελλάδας σε θέματα κοινωνίας της πληροφορίας και ψηφιακής σύγκλισης στους τομείς των τεχνολογιών πληροφορικής και ηλεκτρονικών επικοινωνιών, καθώς και σε άλλους τομείς, η εξέλιξη των οποίων διέπεται από τεχνολογίες πληροφορικής και ηλεκτρονικών επικοινωνιών.

ια) Η διάχυση βέλτιστων πρακτικών και η συμμετοχή σε διεθνείς οργανισμούς και έργα, που σχετίζονται με τους παραπάνω τομείς, καθώς και η κατάρτιση σχετικών μελετών και προτάσεων προς την πολιτεία και κάθε άλλο ενδιαφερόμενο.

7.1.1.3 Φορέας Χρηματοδότησης

Φορέας χρηματοδότησης είναι το Υπουργείο Ψηφιακής Διακυβέρνησης.

7.1.1.4 Κύριος του Έργου – Φορέας Λειτουργίας

Κύριος του Έργου είναι το Υπουργείο Ψηφιακής Διακυβέρνησης.

7.1.2 Σκοπός και στόχοι του Έργου

Ως βασική συνιστώσα της στρατηγικής για τη διαμόρφωση του ψηφιακού μέλλοντος της Ευρώπης, του σχεδίου ανάκαμψης για την Ευρώπη και της στρατηγικής της ΕΕ για την Ασφάλεια, η στρατηγική για την κυβερνοασφάλεια θα ενισχύσει τη συλλογική ανθεκτικότητα της Ευρώπης έναντι των κυβερνοαπειλών και θα διασφαλίσει ότι όλοι οι πολίτες και οι επιχειρήσεις θα μπορούν να επωφεληθούν πλήρως από αξιόπιστες υπηρεσίες και αξιόπιστα ψηφιακά εργαλεία. Είτε πρόκειται για τις συνδεδεμένες συσκευές και το δίκτυο ηλεκτρικής ενέργειας είτε για τις τράπεζες, τα αεροπλάνα, τις δημόσιες διοικήσεις και τα νοσοκομεία που χρησιμοποιούν ή από τα οποία εξυπηρετούνται οι Ευρωπαίοι, τους αξίζει να το πράττουν έχοντας τη βεβαιότητα ότι θα προστατεύονται από τις κυβερνοαπειλές.

Στο πλαίσιο αυτό εκπονήθηκε η στρατηγική της ΕΕ για την κυβερνοασφάλεια που δίνει στην ΕΕ τη δυνατότητα να ενισχύσει τον ηγετικό της ρόλο όσον αφορά τους διεθνείς κανόνες και τα διεθνή πρότυπα στον κυβερνοχώρο και να εντείνει τη συνεργασία με εταίρους σε ολόκληρο τον κόσμο για την προώθηση ενός παγκόσμιου, ανοικτού, σταθερού και ασφαλούς κυβερνοχώρου, βασισμένου στο κράτος δικαίου, τα ανθρώπινα δικαιώματα, τις θεμελιώδεις ελευθερίες και τις δημοκρατικές αξίες.

Αντίστοιχα το Υπουργείο Ψηφιακής Διακυβέρνησης διαμόρφωσε την Εθνική Στρατηγική για την Κυβερνοασφάλεια οριοθετώντας :

- Τις αρχές και το όραμα ανάπτυξης της Εθνικής Στρατηγικής για την Κυβερνοασφάλειας
- Τη Μεθοδολογία ανάπτυξης της Στρατηγικής
- Τη λειτουργία της Εθνικής Αρχής Κυβερνοασφάλειας
- Το σύστημα διακυβέρνησης
- Τη θωράκιση των κρίσιμων υποδομών
- Τη βελτιστοποίηση της αντιμετώπισης περιστατικών
- Την ανάπτυξη ικανοτήτων και την προαγωγή της ενημέρωσης και ευαισθητοποίησης του συνόλου των εμπλεκομένων

Στην παραπάνω κατεύθυνση και δεδομένου ότι Το Υπουργείο Ψηφιακής Διακυβέρνησης και οι εποπτευόμενοι φορείς του, διαχειρίζονται και λειτουργούν κρίσιμες υποδομές και οντότητες όπως ενδεικτικά :

- Την Εθνική Κυβερνητική Πύλη gov.gr για την εξυπηρέτηση πολιτών και επιχειρήσεων
- Κρίσιμα πληροφοριακά συστήματα στο χώρο της υγείας και της Κοινωνικής Ασφάλισης (Μητρώο ΑΜΚΑ, Ηλεκτρονική Συνταγογράφηση, ΠΣ Προνοιακών επιδομάτων, Σύστημα ασφαλιστικής ιστορίας ΑΤΛΑΣ, ΠΣ ασφαλιστικών εισφορών μη μισθωτών κα)

- Κρίσιμα Πληροφοριακά Συστήματα στο χώρο της φορολογίας και της Δημοσιονομικής Πολιτικής (Taxis, IcisNet, mydata, ΠΣ Δημοσιονομικής Πολιτικής κα)
- Κρίσιμα Πληροφοριακά Συστήματα στο χώρο της χωροταξίας και της κτηματογράφησης (ΠΣ Κτηματολογίου, Ψηφιακός Χάρτης κα)

Κρίνεται εξαιρετικά επείγουσα και επιτακτική η υλοποίηση Δράσης για την ενίσχυση της κυβερνοανθεκτικότητας των κρίσιμων οντοτήτων και των υποδομών του ΥΨΗΔ και των εποπτευόμενων φορέων του, στο πλαίσιο μιας ολιστικής προσέγγισης που αφορά όλες τις βασικές συνιστώσες της Κυβερνοαφάλειας (Ανθρώπινο δυναμικό, Διαδικασίες και συστήματα Λογισμικού και Υλισμικού).

Στο πλαίσιο διαχείρισης κινδύνων στον κυβερνοχώρο που τίθεται από τις ευρωπαϊκές πρωτοβουλίες και το περιβάλλον κυβερνοασφάλειας, η Δράση για την ενίσχυση της Κυβερνοανθεκτικότητας των κρίσιμων οντοτήτων του ΥΨΗΔ και των εποπτευόμενων φορέων του εστιάζει σε ένα πλέγμα δράσεων που αφορά στο σύνολο των κρίσιμων παραγόντων και αναλύεται στα παρακάτω υποκεφάλαια.

Η σύμβαση υποδιαιρείται σε τέσσερα (4) τμήματα, ως εξής:

1. Τμήμα 1 «Υπηρεσίες εξασφάλισης επιχειρησιακής συνέχειας, ασφάλειας διακίνησης δεδομένων και μέτρα και πολιτικές πρόληψης και αντιμετώπισης κινδύνων για τη Γ.Γ.Π.Σ.Δ.Δ.»
2. Τμήμα 2 «Εξειδικευμένες λύσεις και υπηρεσίες ασφάλειας για την Η.ΔΙ.Κ.Α. Α.Ε.»
3. Τμήμα 3 «Εξειδικευμένες λύσεις και υπηρεσίες ασφάλειας για το Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο»»
4. Τμήμα 4 «Εξειδικευμένες λύσεις και υπηρεσίες ασφάλειας για την Ε.Δ.Υ.Τ.Ε. Α.Ε.»

Παρακάτω περιγράφεται το φυσικό αντικείμενο ανά τμήμα.

7.1.3 Φυσικό αντικείμενο Τμήματος 1 «Υπηρεσίες εξασφάλισης επιχειρησιακής συνέχειας, ασφάλειας διακίνησης δεδομένων και μέτρα και πολιτικές πρόληψης και αντιμετώπισης κινδύνων για τη Γ.Γ.Π.Σ.Δ.Δ.»

7.1.3.1 Διαστασιολόγηση λογισμικού, εξοπλισμού και υπηρεσιών

Κατηγορία	Μονάδα διαστασιολόγησης	Ελάχιστο μέγεθος
Ransomware Readiness Assessment	A/M	16
Εκπόνηση Μελέτης Ανάλυσης και Αξιολόγησης Κινδύνων	A/M	22
διενέργεια δράσεων ενημέρωσης για τη μεταφορά τεχνογνωσίας και την διαμόρφωση κουλτούρας ενεργούς ευαισθητοποίησης για τους κινδύνους κυβερνοασφάλειας	A/M	22
διαμόρφωση πλάνου ανάκαμψης από καταστροφές για κρίσιμες οντότητες	A/M	22
Εκπόνηση Μελέτης εξωτερικού και εσωτερικού περιβάλλοντος και την ανάδειξη βέλτιστων πρακτικών	A/M	22
διενέργεια ελέγχων διεύθυνσης εξωτερικών δικτύων, εφαρμογών Ιστού, φυσικής ασφάλειας και διαρροής	A/M	16

Κατηγορία	Μονάδα διαστασιολόγησης	Ελάχιστο μέγεθος
δεδομένων για τον εντοπισμό των ευπαθειών σε υποδομές, συσκευές και διακομιστές που είναι προσβάσιμοι από το διαδίκτυο		
Αξιοποίηση τεχνολογικής καινοτομίας και ερευνητικής πρωτοπορίας	A/M	46
Παροχή υπηρεσιών ανάκαμψης από καταστροφή & λήψης αντιγράφων ασφαλείας (disaster recovery as a service & data backup as a service)	CREDITS €	1.500.000,00
Υπηρεσίες εγκατάστασης/παραμετροποίησης υπηρεσιών ανάκαμψης από καταστροφή & λήψης αντιγράφων ασφαλείας (disaster recovery as a service & data backup as a service)	A/M	100
Backup σε tape 1,960PB χωρητικότητα	PB	1.960
Backup σε disk για το 50% της χωρητικότητας (800 TB ωφέλιμης χωρητικότητας)	PB	1,840 ⁷
MailSecurity (αφορά 20000 σταθμούς εργασίας)	Σταθμοί εργασίας	20.000
Endpoint Security User level (αφορά 20000 σταθμούς εργασίας)	Σταθμοί εργασίας	20.000
Managed services security endpoint & mail (αφορά 20000 σταθμούς εργασίας)	Σταθμοί εργασίας	20.000
Λύση που αφορά τον έλεγχο της πρόσβασης των εσωτερικών χρηστών στο Διαδίκτυο και την ανάλυση των επικοινωνιών τους – Firewalls	Τεμάχια	3
Λύση Ασφαλείας και προστασίας των χρηστών από απειλές του διαδικτύου (WebSecurityGateway)	Τεμάχια	3
Μηχανισμός ελέγχου πρόσβασης χρηστών πολλαπλών παραγόντων (Multi Factor Authentication MFA)	Χρήστες	10.000

7.1.3.2 Πολιτικές – Διαδικασίες και Μέτρα Αντιμετώπισης και Πρόληψης

7.1.3.2.1 Υπηρεσίες Ransomware readiness assessment

Η Υπηρεσία Αξιολόγησης Ετοιμότητας Ransomware θα επιτρέπει στην ΓΓΠΣΔΔ να αξιολογήσει την ετοιμότητά της να ανταποκριθεί και να ανακτήσει από επιθέσεις ransomware, να εντοπίσει κενά ελέγχου και να παρέχει πρακτικές συστάσεις για τη βελτίωση των δυνατοτήτων απόκρισης συμβάντων.

⁷Εκτιμάται ότι για την κάλυψη των 800 TB ωφέλιμης χωρητικότητας απαιτείται χωρητικότητα δίσκου 1.840 TB.

Τα κριτήρια αξιολόγησης της υπηρεσίας θα βασίζονται στις βέλτιστες πρακτικές του κλάδου και στην πρακτική εμπειρία των συμβούλων του Αναδόχου.

Η υπηρεσία θα πρέπει να παράσχει συγκεκριμένα κριτήρια αξιολόγησης που θα έχουν προκαθοριστεί για να παρέχουν μια αμερόληπτη αξιολόγηση των δυνατοτήτων μας. Το πεδίο εφαρμογής καλύπτει την τεχνική ετοιμότητα, τη διαχείριση περιστατικών και τις δυνατότητες που είναι απαραίτητες για την απόκριση σε σημαντικά περιστατικά ransomware. Οι στόχοι της υπηρεσίας περιλαμβάνουν:

- Αξιολόγηση στους τομείς της διαδικασίας αντιμετώπισης συμβάντων.
- Παροχή μιας βαθμολογίας ωριμότητας για κάθε τομέα διαδικασίας.
- Παροχή συστάσεων βελτίωσης με βάση τα ευρήματα της αξιολόγησης.
- Παροχή έκθεσης αξιολόγησης και διεξαγωγή απολογισμού σε εκτελεστικό επίπεδο.

7.1.3.2.2 Εκπόνηση Μελέτης Ανάλυσης και Αξιολόγησης Κινδύνων

Ο Ανάδοχος θα πραγματοποιήσει μελέτη ανάλυσης κινδύνου και αποτίμησης επικινδυνότητας, προκειμένου να αναγνωρίσει και αναλύσει τις ενδεχόμενες απειλές στην ακεραιότητα των υποδομών.

Στο πλαίσιο της εργασίας αυτής, ο Ανάδοχος κατ' ελάχιστον:

- Θα μελετήσει και καταγράψει όλες τις απειλές και κινδύνους που πιθανά αντιμετωπίζει ή αναμένεται να αντιμετωπίσουν οι υποδομές.
- Θα κατηγοριοποιήσει και εξετάσει τις απειλές που θα αναγνωρίσει σε (α) ενδογενείς, οι οποίες προέρχονται από το εσωτερικό του συστήματος και εξαρτώνται από το επίπεδο της εσωτερικής αξιοπιστίας, ασφάλειας και ανθεκτικότητας, σε (β) εξωγενείς, οι οποίες προέρχονται από το εξωτερικό περιβάλλον, όπως καιρικές συνθήκες, φυσικές καταστροφές κλπ και (γ) σε απειλές που προέρχονται από άλλα διασυνδεδεμένα συστήματα ή δίκτυα. Παράλληλα, θα διενεργηθεί εκτίμηση της σοβαρότητας κάθε απειλής.
- Θα διενεργήσει μια συσχέτιση μεταξύ των διαθέσιμων πόρων (πληροφοριακά συστήματα, δίκτυα, εγκαταστάσεις, ανθρώπινο δυναμικό) και των εκτιμώμενων απειλών που δύναται να τους επηρεάσουν εφόσον εκδηλωθούν.
- Θα καταγράψει τα ευάλωτα σημεία και τις αδυναμίες των πόρων που απαιτούνται για τη συνέχιση κάθε επιχειρησιακής λειτουργίας. Στη συνέχεια θα αξιολογήσει την πιθανότητα εκδήλωσης των απειλών που έχει ήδη αναγνωρίσει και θα εκτιμήσει την επίδραση τους στη λειτουργία συστημάτων και υποδομών και τη διάθεση των παρεχόμενων υπηρεσιών.
- Θα αναλύσει τις ανάγκες και απαιτήσεις προστασίας.
- Θα προσδιορίσει και προτείνει τη διαδικασία που θα ακολουθήσει καθώς και τα μέτρα που θα λάβει, προκειμένου να αντιμετωπίσει κάθε ενδεχόμενη απειλή
- Θα προτείνει διαδικασίες αξιολόγησης της αποτελεσματικότητας των μέτρων που προτείνει να εφαρμοσθούν κατά περίπτωση απειλής.

7.1.3.2.3 Διενέργεια δράσεων ενημέρωσης για τη μεταφορά τεχνογνωσίας και την διαμόρφωση κουλτούρας ενεργούς ευαισθητοποίησης για τους κινδύνους κυβερνοασφάλειας

Ο Ανάδοχος καλείται να παράσχει υπηρεσίες σχεδιασμού και υλοποίησης δράσεων ενημέρωσης προς τις αρμόδιες υπηρεσίες της ΓΓΠΣΔΔ κατά την υλοποίηση του έργου, στις ακόλουθες θεματικές ενότητες:

- Εισαγωγή στην Ασφάλεια Πληροφοριών
- Οι κυβερνοαπειλές (Cyber Threats)
- Υλική Ασφάλεια Αρχείων και Μηχανημάτων
- Ασφάλεια Επιφάνειας Εργασίας
- Αποθήκευση αρχείων και δεδομένων
- Αποστολή και διαμοιρασμός αρχείων
- Ασφάλεια κωδικών πρόσβασης
- Ασύρματα δίκτυα και κινητή επικοινωνία
- Διαδικτυακή Ασφάλεια
- Συστήματα Κοινωνικής Μηχανικής (Social Engineering)
- Ασφάλεια ηλεκτρονικού ταχυδρομείου
- Κακόβουλο λογισμικό (Ioί, Worms, Trojans, Spyware, Adware)
- Ηλεκτρονικό «ψάρεμα» (Phishing)
- Μέσα Κοινωνικής Δικτύωσης

Οι συμμετέχοντες μόλις ολοκληρώσουν την εκπαίδευση θα έχουν κατανοήσει τα θέματα των νέων τεχνολογιών και διαδικτύου, ασφάλειας υπολογιστικών συστημάτων και υποδομών, ασφαλής χρήσης του διαδικτύου αλλά και χειρισμού διαδικτυακών προγραμμάτων και προγραμμάτων ηλεκτρονικού υπολογιστή. Επιπλέον, θα μπορούν να αναγνωρίσουν τα διάφορα είδη κυβερνοαπειλών και θα έχουν μάθει βασικούς κανόνες ασφαλείας για την αποτροπή τους.

Πιο ειδικά ο Ανάδοχος καλείται να παρέχει τις παρακάτω υπηρεσίες:

Ι. Μεθοδολογία εκπαίδευσης, εκπαιδευτικό υλικό και εισαγωγή των δεδομένων στην εκπαιδευτική πλατφόρμα

Ο Ανάδοχος θα πρέπει να τεκμηριώσει και να παραδώσει τη μεθοδολογία εκπαίδευσης που θα ακολουθήσει πριν την έναρξη του προγράμματος. Η μεθοδολογία θα πρέπει να επιδιώκει την επίτευξη των παρακάτω εκπαιδευτικών στόχων για τους εκπαιδευόμενους:

- Ανάκληση γνώσεων
- Κατανόηση εκπαιδευτικού υλικού
- Εφαρμογή γνώσεων στην πράξη και σε περιβάλλον προσομοίωσης ή/και σε μελέτες περίπτωσης
- Ανάλυση και σύνθεση γνώσεων
- Η θεωρία και οι ασκήσεις αξιολόγησης/εξέτασης να αποδίδονται μέσω σύγχρονων authoring tools (όπως Articulate, Captivate κ.α.), εξειδικευμένων στην εκπαίδευση ενηλίκων.

- Ενσωμάτωση μηχανισμών παιχνιδιού στην εκπαιδευτική διαδικασία, με δυνατότητες επιβράβευσης (π.χ. πόντοι, σήματα, εικονικά νομίσματα κ.ά.)

Ο Ανάδοχος θα αναλάβει τον σχεδιασμό των εκπαιδευτικών προγραμμάτων λαμβάνοντας υπόψη συγκεκριμένες παραμέτρους. Οι παράμετροι αυτοί αφορούν τη διαφοροποιημένη προσέγγιση ανάλογα με την ομάδα-στόχο, τον τρόπο εκπαίδευσης και τα μέσα που θα χρησιμοποιηθούν.

Ο Ανάδοχος καλείται να μελετήσει τα μοντέλα που έχουν ακολουθήσει άλλες ευρωπαϊκές χώρες για σχετικά προγράμματα εκπαίδευσης, ενημέρωσης και ευαισθητοποίησης εταιρειών και οργανισμών. Ο στόχος της μελέτης είναι να μπορεί ο Ανάδοχος να παρέχει τις κατάλληλες κατευθύνσεις και να αντλήσει καλές πρακτικές στο πεδίο της κατάρτισης και ευαισθητοποίησης εργαζόμενων σε θέματα Κυβερνοασφάλειας.

Ο Ανάδοχος, καλείται να παραδώσει για κάθε εκπαιδευτική ενότητα του προγράμματος, τους εκπαιδευτικούς στόχους, τα εκπαιδευτικά αποτελέσματα, τη διάρκεια αλλά και πιθανές ασκήσεις/ερωτήσεις προς πρακτική εξάσκηση των γνώσεων. Ο σχεδιασμός του εκπαιδευτικού προγράμματος πρέπει να υποστηρίζεται από μια πολυμεσική υλοποίηση, η οποία θα περιλαμβάνει διάφορα οπτικοακουστικά μέσα (π.χ. ήχος, εικόνες, βίντεο, mini games, gamification, quizzes, learning modalities, slideshow κ.α).

Για την ασύγχρονη εκπαίδευση απαιτείται ένα σύγχρονο και πλήρως φιλικό προς το χρήστη σύστημα Learning Management (Learning Management System, LMS), το οποίο να βασίζεται σε εφαρμογή PWA (Progressive Web Application) έτσι ώστε να μην απαιτείται εγκατάσταση της μέσω Google/Apple Store καθώς και όλες οι απαραίτητες ενημερώσεις (updates) να γίνονται κεντρικά και να ενημερώνονται αυτόματα όλοι οι χρήστες, χωρίς να χρειάζεται να προβούν σε καμία ενέργεια αναβάθμισης. Επιπλέον, το LMS θα πρέπει να είναι μία απόλυτα εξατομικευμένη λύση που θα παραμετροποιηθεί, προσαρμοστεί και ενσωματωθεί πλήρως τόσο στα μηχανογραφικά συστήματα όσο και στους μηχανισμούς ασφαλείας της ΓΓΠΣΔΔ. Θα πρέπει να καλύπτει τις ανάγκες στο σύνολο των εκπαιδευόμενων (ιδιωτικός και δημόσιος τομέας), να παρέχει στενή διασύνδεση (integration) με όλα τα εργαλεία του MS Office και να αποτελεί συμβατή πλατφόρμα με διεθνή πρότυπα ηλεκτρονικής μάθησης όπως SCORM με τα οποία εξασφαλίζεται η επαναχρησιμοποίηση, η προσβασιμότητα και η ανθεκτικότητα του εκπαιδευτικού υλικού στις τεχνολογικές μεταβολές, καθώς και η διαλειτουργικότητα μεταξύ συστημάτων ηλεκτρονικής μάθησης. Η αρχιτεκτονική της πλατφόρμας (πλατφορμών) θα δίνει τη δυνατότητα στον χρήστη να αλληλεπιδρά δυναμικά με όλο το εκπαιδευτικό υλικό. Επιπλέον, ο Ανάδοχος θα πρέπει να παρακολουθεί με αναφορές το πλήθος των χρηστών που θα παρακολουθούν ή/και ολοκληρώνουν το εκπαιδευτικό ασύγχρονο πρόγραμμα κατάρτισης καθώς και να καταγράφονται αναλυτικά όλα τα ερωτηματολόγια με τις απαντήσεις στα τελικά διαδικτυακά (ψηφιακά) τεστ όλων των χρηστών σε αναλυτική καρτέλα προφίλ.

Για τον σχεδιασμό του εκπαιδευτικού υλικού πρέπει να ακολουθούνται με ακρίβεια τα πρότυπα σχεδιασμού εκπαιδευτικού υλικού, όπως περιγράφονται:

- Ο εκπαιδευτικός σχεδιασμός ψηφιακού υλικού ("instructional design") θα πρέπει να βασίζεται στη σαφή και αιτιολογημένη κατάτμηση του υλικού ενοτήτων σε υποενότητες μάθησης, με ορισμένη μέγιστη διάρκεια. Παράλληλα για την πλήρη κατανόηση της κατάτμησης των ενοτήτων σε υποενότητες μάθησης ο Ανάδοχος οφείλει να συνδέσει κάθε ενότητα/υποένότητα με διακριτούς εκπαιδευτικούς στόχους.
- Ο χρήστης θα πρέπει να ακολουθεί σαφή εκπαιδευτικά μονοπάτια (Θεωρία, Αυτοαξιολόγηση, Εξέταση, Πιστοποίηση), για τα οποία να δύναται να έχουν υποχρεωτική σειριακή ακολουθία παρακολούθηση, ανάλογα με τους σκοπούς της εκπαίδευσης.

- Η διάδραση με το περιεχόμενο και η ενεργητική μάθηση των καταρτιζόμενων πρέπει με σαφή τρόπο να επιτυγχάνεται μέσω σύνθετων εργαλείων, εξειδικευμένων στην εκπαίδευση ενηλίκων, όπως business case studies, role playing, psychometric analysis κ.ά.
- Ο πρακτικός προσανατολισμός: μέθοδος «μαθαίνω κάνοντας» (learning by doing) θα επιτυγχάνεται με προσομοίωση πραγματικών συνθηκών (μελέτες περίπτωσης, επίλυση προβλήματος) και άλλες τεχνικές που ο ανάδοχος μπορεί να επιλέξει ώστε να ενθαρρύνει τη μάθηση μέσα από την επαφή των καταρτιζόμενων με πραγματικές συνθήκες λήψης απόφασης, συμπεριφορικές δραστηριότητες και ανάλυση επιλογών.
- Η πολυμεσική μάθηση είναι ο βασικός στόχος αυτού του έργου. Προκειμένου ο Ανάδοχος να διασφαλίσει ένα πολυμεσικό περιβάλλον μάθησης, οι παρουσιάσεις, τα βίντεο και η δόμηση του υλικού σε διαφορετικά εκπαιδευτικά μέσα και εκπαιδευτικά εργαλεία θα πρέπει να τηρεί προδιαγραφές της πολυμεσικής μάθησης και να διευκολύνει την επεξεργασία, κατανόηση και αφομοίωση των πληροφοριών και της παρεχόμενης γνώσης και την εύκολη και διαδραστική πλοήγηση.
- Οι προδιαγραφές αξιολόγησης της κατανόησης και αφομοίωσης της γνώσης από τους καταρτιζόμενους θα πρέπει να γίνεται με τη μέθοδο αξιολόγησης βάσει μετρήσιμων μαθησιακών αποτελεσμάτων – ταξινομία ADDIE και να απεικονίζεται σε ανάλογες αναφορές.
- Κάθε ενότητα ή/ και υποενότητα μάθησης θα ακολουθείται από αξιολόγηση με quiz πολλαπλής ή μοναδικής επιλογής, ερωτήσεις σωστό λάθος. Προτεινόμενο μοντέλο είναι η αξιολόγηση να αποτελείται από ένα quiz αυτοαξιολόγησης και ένα βαθμολογούμενο, ανά υποενότητα μάθησης, ενώ οι ερωτήσεις θα πρέπει να αναφέρονται κυρίως σε συμπεριφορικά στοιχεία, επιλογές και αποκρίσεις σε πιθανά σενάρια σχετικά με το περιεχόμενο του εκπαιδευτικού προγράμματος και τους εκπαιδευτικούς στόχους.

Ο Ανάδοχος θα αναλάβει τον σχεδιασμό της μεθοδολογίας αξιολόγησης των αποτελεσμάτων γνώσεων, ο οποίος θα προκύπτει από σχετικά κριτήρια αξιολόγησης όπου θα συμμετέχουν οι εκπαιδευόμενοι με το πέρας της εκπαίδευσης. Πιο συγκεκριμένα, οι συμμετέχοντες θα πρέπει να συμμετάσχουν στην παραπάνω διαδικασία, η οποία θα τους αξιολογεί αυτόματα και άμεσα. Τα αποτελέσματα αυτά θα πρέπει να είναι άμεσα συγκρίσιμα και να παράγουν αναφορές με συνέπεια και συνεκτικότητα. Οι αναφορές θα απεικονίζονται και με ιεραρχικό επίπεδο της θέσης εργασίας που κατέχει κάθε υπάλληλος και ανά τμήμα όπου θα προκύπτουν συγκεντρωτικά ή ατομικά γνωστικά αποτελέσματα.

Το εκπαιδευτικό υλικό, για το οποίο ο Ανάδοχος θα έχει την επιμέλεια και επίβλεψη, σύμφωνα με τις ανάγκες και τον σχεδιασμό, θα είναι διαθέσιμο στην εκπαιδευτική πλατφόρμα και θα πρέπει να κατατεθεί ως ένα από τα παραδοτέα του έργου αυτού.

II. Σχεδιασμός και ανάπτυξη της ψηφιακής πλατφόρμας για την ασύγχρονη εξ' αποστάσεως εκπαίδευση

Το σύστημα τηλεεκπαίδευσης (E-Learning platform) θα είναι εύκολα προσβάσιμο και θα εξυπηρετεί τις ανάγκες του έργου. Το σύστημα ηλεκτρονικής εκπαίδευσης θα αποτελείται από μία πλατφόρμα ασύγχρονης τηλε-εκπαίδευσης (Learning Management System) για διαχείριση και παράδοση ασύγχρονων προγραμμάτων ηλεκτρονικής (ψηφιακής) μάθησης (e-learning). Ο Ανάδοχος θα πρέπει να διασφαλίσει ότι θα παρεμετροποιήσει και θα διαμορφώσει την αρχιτεκτονική της πλατφόρμας ώστε να μπορεί να φιλοξενήσει την εκπαιδευτική διαδικασία καθώς και τη φόρτωση και διαχείριση κάθε είδους εκπαιδευτικού υλικού, την ανταλλαγή και διάχυση πληροφορίας και την υποστήριξη κάθε είδους διεργασίας ανταλλαγής πληροφοριών. Το σύστημα θα πρέπει να μπορεί να χρησιμοποιηθεί προκειμένου να διαχειρίζονται και χρονοπρογραμματίζονται τα εκπαιδευτικά προγράμματα ασύγχρονης μορφής, οι μαθησιακές διαδικασίες καθώς η δυνατότητα διενέργειας δοκιμασιών (test)

αξιολόγησης της επίτευξης των εκπαιδευτικών στόχων και αξιολόγησης του εκπαιδευτικού προγράμματος από τους συμμετέχοντες.

Ο Ανάδοχος πριν από τον σχεδιασμό της αρχιτεκτονικής και την ανάπτυξη της εκπαιδευτικής πλατφόρμας (ή πλατφορμών), καλείται να παρουσιάσει μια ενδελεχή ανάλυση των στοιχείων που θα παρακολουθούνται δυναμικά εντός της πλατφόρμας και να ορίσει ένα σαφές, ρεαλιστικό και περιγραφικό σύστημα δεικτών για την καταγραφή του εκπαιδευτικού και επιμορφωτικού κέρδους.

Η πρόσβαση στο σύστημα τηλεκπαίδευσης θα πρέπει να μπορεί να πραγματοποιείται μέσα από δημοφιλείς φυλλομετρητές διαδικτύου που πληρούν τα διεθνή standards, όπως οι: Google Chrome, Mozilla Firefox, Microsoft Edge, από οποιοδήποτε σημείο του κόσμου, οποιαδήποτε στιγμή της ημέρας και από οποιαδήποτε συσκευή (desktop, laptop, tablet, smartphone). Δεν θα πρέπει να απαιτείται κανένα άλλο, πρόσθετο λογισμικό στη συσκευή που θα επιλέξει ο χρήστης καθώς και καμία εγκατάσταση. Όλες οι λειτουργίες και τα υποσυστήματα της εφαρμογής μπορούν να συνδυαστούν ελεύθερα. Ο σχεδιασμός και η ανάπτυξη της ψηφιακής πλατφόρμας θα πρέπει να διασφαλίζει ότι το σύστημα θα είναι άμεσα προσιτό και εύκολο στην πλοήγηση και χρήση από τους συμμετέχοντες, όπου αυτός επιθυμεί, και να υποστηρίζει τη διαχείριση μεγάλου αριθμού ενεργών χρηστών. Το σύστημα το οποίο θα διαμορφώσει ο Ανάδοχος θα πρέπει να επιτρέπει τη δημιουργία προσωπικού λογαριασμού για κάθε εκπαιδευόμενο, στον οποίο θα καταγράφεται όλη του η δραστηριότητα όπως επίσης και τα αποτελέσματα της εξέτασης/ αξιολόγησης.

Γενικές κατευθύνσεις που πρέπει να ακολουθούνται για το σύστημα τηλεκπαίδευσης:

- Το λογισμικό ασύγχρονης εκπαίδευσης θα πρέπει να παρέχει χρήσιμα εργαλεία, όπως:
 - Βαθμολόγιο
 - Ημερολόγιο
 - Helpdesk
 - Ερωτηματολόγια (Review) για τη συλλογή δεδομένων από τους καταρτιζόμενους
 - Ηλεκτρονικά τεστ (online quiz)
 - Άμεσα μηνύματα (Forum/chat) με βαθμολόγηση απαντήσεων
 - Βιβλιοθήκη περιεχομένου
 - Μικροεκπαιδεύσεις – Microlearnings
 - Αιτήματα εγγραφής εκπαιδευόμενων σε νέες εκπαιδεύσεις
 - Ενσωματωμένο σύστημα ερωτηματολογίων (survey) ανά ομάδες χρηστών
- Πολύγλωσσο περιβάλλον και περιεχόμενο.
- Δημιουργία οργανογράμματος για οργάνωση των χρηστών ανά τομέα / διεύθυνση / γεωγραφική τοποθεσία κ.ά. σε γραφικό περιβάλλον
- Δημιουργία απεριόριστων χρηστών και ομάδων χρηστών.
- Δημιουργία απεριόριστων εκπαιδεύσεων με τελική πιστοποίηση.
- Δημιουργία εκπαιδευτικών μονοπατιών.
- Υποστήριξη διαφορετικών επιπέδων διαχείρισης, χρήσης, ρόλων και ομάδων χρηστών υποστηρίζοντας τα Azure, Microsoft Active Directory ,LDAP και Google Business.

- Υποστήριξη κατάλληλων μέτρων για την προστασία των προσωπικών δεδομένων τόσο των χειριστών της εφαρμογής, όσο και ευαίσθητων πληροφοριών στο υλικό παρουσίασης, σύμφωνα με τον κανονισμό GDPR. Πιο συγκεκριμένα:
 - ο Αποδοχή/Συναίνεση συλλογής δεδομένων: Το σύστημα υποστηρίζει λειτουργικότητες καταχώρησης και καταγραφής της συναίνεσης του χρήστη αναφορικά με τη συλλογή και διαχείριση των δεδομένων που έχουν ήδη καταχωρηθεί στο σύστημα ή των δεδομένων που θα συλλεχθούν κατά τη διάρκεια των διαδικασιών κατάρτισης κρυπτογραφημένα.
 - ο Ενημέρωση περί συλλεγόμενων δεδομένων. Ο χρήστης μπορεί να ενημερωθεί αναλυτικά και με σαφή τρόπο για το ποια δεδομένα συλλέγονται, τους λόγους για τους οποίους γίνεται η συλλογή τους, τον τρόπο χρήσης τους, καθώς επίσης και για τη διάρκεια διατήρησης αυτών των δεδομένων στα συστήματα. Επίσης, μπορεί να ενημερωθεί αναλυτικά για τους όρους χρήσης του συστήματος και τις εκπαιδευτικές διαδικασίες στις οποίες θα συμμετάσχει.
- Λειτουργία αυτόματης δημιουργίας και εισαγωγής εκπαιδευτικού περιεχομένου με εφαρμογές MS Office για την θεωρία και τα ερωτηματολόγια με online editor.
- Πλήρης συμμόρφωση με την τρέχουσα έκδοση του διεθνούς προτύπου SCORM.
- Λειτουργία μέσω Web Browser και είναι συμβατό με τα διεθνή πρότυπα του W3C.
- Λειτουργία σε περιβάλλον HTTPS. Όλες οι επιμέρους λειτουργίες να παρέχονται εντός πρωτοκόλλου HTTPS και πάνω από secure channel SSL/TLS.
- Πολιτική ασφάλειας κωδικών πρόσβασης. Το σύστημα να υποστηρίζει:
 - ο Πολιτική πολυπλοκότητας κωδικών (ελάχιστο πλήθος χαρακτήρων, συμπερίληψη special characters, συμπερίληψη χαρακτήρων με κεφαλαία, συμπερίληψη αριθμητικών χαρακτήρων, αποτροπή χρήσης ακολουθίας π.χ. 1234, αποτροπή χρήσης κοινών κωδικών π.χ. qwerty).
 - ο Παραγωγή κωδικών με τυχαίο τρόπο και σύμφωνα με την πολιτική πολυπλοκότητας χωρίς την επέμβαση φυσικού προσώπου (διαχειριστή) > Διαδικασίες επαναφοράς κωδικού χωρίς ενημέρωση και χωρίς την επέμβαση φυσικού προσώπου (διαχειριστή) > Διαδικασίες υποχρεωτικής αλλαγής κωδικού (π.χ. κατά την 1η είσοδο στο σύστημα).
 - ο Διατήρηση ιστορικού κωδικών πρόσβασης και αποτροπή επαναχρησιμοποίησης παλιού κωδικού.
- Υποστήριξη αρθρωτής (modular) και ανοικτής αρχιτεκτονικής, ώστε να επιτρέπονται επεκτάσεις/αναβαθμίσεις.
- Δυνατότητα δημιουργίας πολλαπλών Portals με βάση τον ρόλο του Χρήστη (Δημόσιος τομέας, Ιδιωτικός Τομέας, Ομάδες Διεύθυνσης, Εκπαιδευτές, Εκπαιδευόμενοι, κ.ά.).
- Δυνατότητα καταγραφής της πορείας και των ενεργειών του καταρτιζόμενου (tracking-timeline) καθ' όλη τη διάρκεια εκάστου εκπαιδευτικού προγράμματος.
- Μηχανισμό χρονοπρογραμματισμού και αποστολής αυτοματοποιημένων ειδοποιήσεων μέσω e-Mail ή/και SMS, in app notifications, έτσι ώστε να παρέχονται όλες οι κατάλληλες πληροφορίες για την επιλογή της βέλτιστης διαδικασίας αποστολής σε όλες τις λειτουργίες της πλατφόρμας δυνατότητα:

- Αποστολή σε όλους: Θα γίνει αποστολή σε όσους έχουν ενεργές τις ειδοποιήσεις, και έχουν αποδεχθεί τους όρους.
- Εξαίρεση: Ο διαχειριστής μπορεί να επιλέξει ποιοι θα εξαιρεθούν της αποστολής
- Ατομική Αποστολή: Ο διαχειριστής μπορεί να επιλέξει συγκεκριμένα άτομα που θα γίνει η αποστολή
- Δεν έχουν λάβει ειδοποίηση: Ο διαχειριστής μπορεί να επιλέξει τους όσους δεν έχουν λάβει τη συγκεκριμένη ειδοποίηση από προηγούμενη αποστολή.

Το σύστημα επιπλέον θα πρέπει να διαθέτει σύστημα αναφορών έτσι ώστε να μπορούν να παράγονται αναφορές για τις ενέργειες που υποστηρίζονται από το σύστημα. Ενδεικτικά:

- Αναφορές για το σύνολο των χρηστών / ομάδα / χρήστη
- Αναφορές ανά θεματικό πεδίο / μάθημα / εξέταση / πιστοποίηση.

Που θα περιλαμβάνουν τουλάχιστον τα παρακάτω δεδομένα:

- Ποσοστό συμμετοχής (δλδ πόσοι έχουν ξεκινήσει ή ολοκληρώσει)
- Χρόνους κατανάλωσης περιεχομένου (μέσο όρο, σύνολο)
- Μέσο χρόνο ολοκλήρωσης ανά εκπαιδευτικό πρόγραμμα
- Αποτελέσματα εξετάσεων / μάθημα, αξιολόγηση, πιστοποίηση και Top 10 /100
- Ποιες ερωτήσεις εμφανίζουν συχνά λάθη ανά θεματικό πεδίο, μάθημα
- Προσωποποιημένες αναφορές επίδοσης με στατιστικά ανά γνωστικό αντικείμενο
- Αναλυτικά αποτελέσματα ερευνών
- Big data analytics για ανάλυση δεξιοτήτων που αναπτύχθηκαν με συγκεκριμένους δείκτες (KPI's)

Το σύστημα τηλεκπαίδευσης θα πρέπει να υποστηρίζει τουλάχιστον τις εξής κατηγορίες χρηστών και σχετικά δικαιώματα:

- Εκπαιδευομένους
- Εκπαιδευτές
- Διαχειριστές της πλατφόρμας εξ αποστάσεως εκπαίδευσης

Οι δυνατότητες του συστήματος σε σχέση με τον χρήστη/εκπαιδευόμενο αναφέρονται συνοπτικά παρακάτω:

- Εγγραφή στο εκπαιδευτικό πρόγραμμα
- Προβολή και παρακολούθηση εκπαιδευτικού υλικού
- Συμμετοχή σε τυποποιημένες έρευνες (αξιολόγηση εκπαιδευτικού προγράμματος) με σκοπό την έκφραση των απόψεων του εκπαιδευμένου σχετικά με το εκπαιδευτικό υλικό ή τη διαδικασία εκπαίδευσης
- Συμμετοχή σε μη υποχρεωτικά μαθήματα μικρής διάρκειας, μεγάλης ποικιλίας με συνδυασμό πολλαπλών μορφών περιεχομένου και δυνατότητα αναζήτησης με λέξεις κλειδιά.
- Συμμετοχή σε εξέταση (test αξιολόγησης) που μπορεί να έχει διάφορες μορφές ερωτήσεων όπως πολλαπλής επιλογής, σωστό-λάθος και ερωτήσεις με σύντομες απαντήσεις κ.λ.π.

- Προβολή και εκτύπωση βεβαίωσης της ολοκλήρωσης της συμμετοχής στο εκπαιδευτικό πρόγραμμα μετά την επιτυχή ολοκλήρωση του τεστ αξιολόγησης

Οι δυνατότητες του συστήματος σε σχέση με τον χρήστη Διαχειριστή αναφέρονται συνοπτικά παρακάτω.

Ως Διαχειριστής ορίζεται το στέλεχος το οποίο θα παρακολουθεί την υλοποίηση του έργου και θα είναι υπεύθυνος για τα παρακάτω (ενδεικτική και όχι εξαντλητική λίστα):

- Προσθήκη έτοιμου εκπαιδευτικού υλικού ή δημιουργίας μέσω Online editor σε ιδιαίτερα φιλικό περιβάλλον πλοήγησης και με λίγες οθόνες (wizards).
- Δημιουργία ερωτηματολογίων (Test Bank) με αυτόματη εισαγωγή από συγκεκριμένα πρότυπα MS Office.
- Δημιουργία και χρονοπρογραμματισμό του εκπαιδευτικού προγράμματος με τις απαραίτητες αυτόματες ειδοποιήσεις (SMS,email,In-app notification)
- Διαχείριση δραστηριοτήτων (quiz, αξιολογήσεις, τεστ κ.ο.κ.)
- Δημιουργία επεξεργασία και διαγραφή χρηστών οποιασδήποτε μορφής στο σύστημα και απόδοση ρόλων
- Προβολή λίστας συνδεδεμένων χρηστών στην LMS
- Διαχείριση αιτήσεων που υποβάλλονται για συμμετοχή στην εκπαίδευση
- Επικοινωνία με όλους τους χρήστες του συστήματος
- Δυνατότητα επαναφοράς της εκπαίδευσης σε μια προηγούμενη κατάσταση
- Εξαγωγή των αποτελεσμάτων όλων των εκπαιδευόμενων σε αρχεία Excel ή PDF με βάση αν ολοκλήρωσαν ή όχι το πρόγραμμα κατάρτισης και αν πέρασαν την τελική αξιολόγηση/εξέταση

Δυνατότητες του συστήματος σε σχέση με τη δημιουργία αναφορών:

Το σύστημα πρέπει να υποστηρίζει την αποτύπωση live αναφορών με κατ' ελάχιστον τις ακόλουθες κατηγορίες:

- Αναφορές αποδοχής όρων χρήσης
- Αναφορές επισκέψεων (ημερήσιες, μηνιαίες, ετήσιες)
- Αναφορές πρόσβασης κάθε κατηγορίας χρηστών με επιλογή της επιθυμητής χρονικής περιόδου
- Αποτελέσματα αξιολογήσεων, εξετάσεων, τελικών Πιστοποιήσεων.
- Καρτέλα εκπαιδευόμενου με όλα τα στοιχεία που σχετίζονται με τον συγκεκριμένο εκπαιδευόμενο και τη συμμετοχή του στο εκπαιδευτικό πρόγραμμα
- Αξιολόγηση/ εξέταση εκπαιδευόμενου, αποτελέσματα και βεβαίωση συμμετοχής του εκπαιδευόμενου

«Επικοινωνιακή Διαχείριση Κρίσεων στον Κυβερνοχώρο»

Η υιοθέτηση νέων τεχνολογιών, η συλλογή, επεξεργασία και αποθήκευση τεράστιου όγκου δεδομένων, έχουν δημιουργήσει νέους κινδύνους που απαιτούν ειδικό σχεδιασμό, προετοιμασία και αντιμετώπιση. Ακόμα και μικρής έκτασης κυβερνοεπιθέσεις, μπορούν να προκαλέσουν σοβαρά προβλήματα στην φήμη, την παραγωγικότητα και την ομαλή λειτουργία ενός οργανισμού.

Το αντικείμενο του παρόντος αφορά στον σχεδιασμό και υλοποίηση ενός εκπαιδευτικού προγράμματος με στόχο την έγκαιρη προετοιμασία και την αποτελεσματική αντίδραση της Ομάδας Διαχείρισης Κρίσεων σε περίπτωση κρίσεων στον κυβερνοχώρο.

Στόχος του προγράμματος είναι:

- α) η δημιουργία ισχυρής εταιρικής συναντίληψης σχετικά με τους κινδύνους τόσο στο «παραδοσιακό» περιβάλλον όσο και στον κυβερνοχώρο
- β) η συγκρότηση & εκπαίδευση της Ομάδας Διαχείρισης Κρίσεων στον Κυβερνοχώρο ώστε να λειτουργεί αποτελεσματικά κατά την αντιμετώπιση τέτοιων κρίσεων
- γ) η επεξεργασία των εσωτερικών διαδικασιών που πρέπει να ακολουθούνται σε περίπτωση κρίσεων στον κυβερνοχώρο και
- δ) η ανάπτυξη ειδικών δεξιοτήτων για την ορθή επικοινωνιακή διαχείριση των κρίσεων

Στο εκπαιδευτικό πρόγραμμα θα παρουσιαστούν και θα αναλυθούν στα μέλη της Ομάδας Διαχείρισης Κρίσεων τα ακόλουθα:

A. Εκτίμηση της υφιστάμενης κατάστασης/ Communication Cyber Crisis Preparedness Assessment

- Αξιολόγηση του υφιστάμενου σχεδίου επικοινωνιακής διαχείρισης κρίσεων στον κυβερνοχώρο και του βαθμού ετοιμότητας του οργανισμού
- Αξιολόγηση του επιπέδου awareness υπαλλήλων και στελεχών σχετικά με ζητήματα ασφάλειας στον κυβερνοχώρο

Β. Συγκρότηση της Ομάδας Διαχείρισης Κρίσεων στον Κυβερνοχώρο

Συγκρότηση ή αναδιάρθρωση της υφιστάμενης Ομάδας Διαχείρισης Κρίσεων με την προσθήκη νέων μελών, ανακατανομή αρμοδιοτήτων, καθορισμός ρόλων και διαδικασιών επικοινωνίας και συνεργασίας των μελών της κατά την διάρκεια μιας κρίσης στον κυβερνοχώρο.

Γ. Crisis Management Basics & Cyber Security Basics

- Οριοθέτηση cyber incident και cyber crisis
- Cyber threats landscape

Δ. Case studies

- Παρουσίαση και ανάλυση σημαντικών και περίπλοκων case studies. Αξιολόγηση της ετοιμότητας των εταιρειών που έπεσαν θύματα κυβερνοεπίθεσης, παρουσίαση και αξιολόγηση της δημόσιας αντίδρασής τους, της επικοινωνίας τους με stakeholders και κοινό κατά την διάρκεια της κρίσης.

Ε. Σχεδιασμός Σεναρίων & Ανάπτυξη της Αντίδρασης της Ομάδας Διαχείρισης Κρίσεων στον Κυβερνοχώρο (Tabletop exercise)

- Σχεδιασμός και συνδιαμόρφωση των πιθανότερων, για τον οργανισμό, σεναρίων κρίσεων στον κυβερνοχώρο
- Παρουσίαση και εξάσκηση στις τεχνικές πρόληψης και διαχείρισης κρίσεων στον κυβερνοχώρο με βάση τα προεπιλεγμένα σενάρια. Προσομοίωση σε round table περιβάλλον

ΣΤ. Διαπραγματεύσεις

Workshop στις τεχνικές διαπραγμάτευσης που πρέπει να ακολουθηθούν σε περίπτωση κρίσης στον κυβερνοχώρο με hackers, media ή άλλους stakeholders.

Ζ. Media Training

- α) Εκπαίδευση των στελεχών της Ομάδας Διαχείρισης Κρίσεων στον Κυβερνοχώρο στις τεχνικές πρόληψης και διαχείρισης επικοινωνιακών κρίσεων στον κυβερνοχώρο,
- β) Οδηγίες για σύνταξη δελτίων τύπου, δηλώσεων, non papers,
- γ) Επιλογή των κατάλληλων καναλιών επικοινωνίας και τεχνικές παρέμβασης.

Η. Παραδοτέο

Δημιουργία εξειδικευμένου οδηγού Επικοινωνιακής Διαχείρισης Κρίσεων στον Κυβερνοχώρο.

7.1.3.2.4 Διαμόρφωση πλάνου ανάκαμψης από καταστροφές για κρίσιμες οντότητες

Ο κύριος στόχος του παρόντος είναι η εκπόνηση Πλάνου Ανάκαμψης από Καταστροφές (DRP) για τις κρίσιμες υποδομές. Επιμέρους στόχοι του Σχεδίου Ανάκαμψης από Καταστροφή αφορούν τα εξής:

- καθορισμός των υποδομών και των συστημάτων με προτεραιοποίησή τους, όσον αφορά στην ετοιμότητα ανάκαμψης από καταστροφή,
- καθορισμός των παραμέτρων και των εξαρτήσεων των υποδομών και των συστημάτων, σε σχέση και με την υποδομή εφεδρείας ανάκαμψης από καταστροφή
- καθορισμός των αποδεκτών διαστημάτων απώλειας πληροφοριών από τον προηγούμενο συγχρονισμό δεδομένων (RecoveryPointObjective "RPO") και των αναγκών και αποδεκτών χρόνων ενεργοποίησης εκάστου υποσυστήματος (RecoveryTimeObjective "RTO")
- καθορισμός των αναγκών σε υποδομές εξυπηρετητών φιλοξενίας με όλα τα τεχνικά χαρακτηριστικά λειτουργίας τους και των απαραίτητων δικτυακών υποδομών
- καθορισμός του τρόπου – μεθόδου λειτουργίας των νέων συστημάτων ανάκαμψης από καταστροφή και της τεχνολογίας που θα επιλεγεί για τη συχνότητα συγχρονισμού – ενημέρωσης
- καθορισμός των αναγκών τροποποιήσεων ή αναβαθμίσεων που θα πρέπει να υλοποιηθούν στο υφιστάμενο DataCenter, για τη συνεργασία και συγχρονισμό με το DisasterRecoverySite
- καθορισμός τυχόν αναγκών για επέκταση συμβολαίων υποστήριξης των Αναδόχων των υφιστάμενων συστημάτων και υποδομών ή για υπογραφή νέων SLAs.

Για την επίτευξη των ανωτέρω στόχων, ο Ανάδοχος θα βασιστεί στις κατευθύνσεις και καλές πρακτικές του διεθνούς προτύπου ISO 22301:2012, το οποίο αποτελεί ένα πρότυπο που θεσπίζει καλές πρακτικές, ώστε:

- να συνταχθεί Πλάνο Ανάκαμψης από Καταστροφή (DRP) για τις εφαρμογές και τα συστήματα
- να αναπτυχθούν οι απαραίτητες διοικητικές και υποστηρικτικές διαδικασίες για τη συντήρηση και επικαιροποίηση τουDRP.

Επίσης θα ληφθούν υπόψη καλές πρακτικές που προκύπτουν από τα πρότυπα ISOPAS 22399:2007 και ISO/ IEC 27001:2013.

7.1.3.2.5 Εκπόνηση Μελέτης εξωτερικού και εσωτερικού περιβάλλοντος και την ανάδειξη βέλτιστων πρακτικών

Απαραίτητο συστατικό για τον αποτελεσματικό έλεγχο ασφάλειας των υποδομών και συστημάτων είναι η αντίληψη και η αξιολόγηση του ευρύτερου περιβάλλοντος στους τομείς της ασφάλειας των δικτύων / πληροφοριακών συστημάτων και της διασφάλισης του απορρήτου των επικοινωνιών.

Επομένως, θα πρέπει να διενεργηθεί μια μελέτη της κατάστασης που επικρατεί και των πρακτικών που εφαρμόζονται στον τομέα ασφάλειας σε παρεμφερή συστήματα τόσο εντός της χώρας όσο και σε διεθνές επίπεδο. Σκοπός της μελέτης αυτής είναι να δημιουργηθεί μια ολοκληρωμένη βάση γνώσης για το πλήρες ιστορικό που αφορά την ασφάλεια και στη συνέχεια να εξαχθούν χρήσιμα συμπεράσματα, τα οποία θα αξιοποιηθούν από τον Ανάδοχο για να φέρει εις πέρας τις υπόλοιπες εργασίες που απαιτούνται.

Στο πλαίσιο της εργασίας αυτής, θα συλλεχθούν και στη συνέχεια επεξεργασθούν και αναλυθούν πληροφορίες και δεδομένα που αφορούν στην ασφάλεια παρόμοιων υποδομών και συστημάτων τόσο εντός της χώρας όσο και σε άλλες χώρες. Τα δεδομένα θα εστιάσουν κατ' ελάχιστον:

- Στα υιοθετημένα Συστήματα Διαχείρισης της Ασφάλειας των Πληροφοριών (ΣΔΑΠ) και τις υποκείμενες σε αυτά διαδικασίες, πολιτικές και πρακτικές
- Στους κινδύνους ασφάλειας, στις ευπάθειες ανάλογων συστημάτων και στις μεθόδους αποτίμησης της επικινδυνότητας που συνήθως εμφανίζονται ή εφαρμόζονται αντίστοιχα
- Στις αποτελεσματικές μεθόδους παρακολούθησης της ασφάλειας ανάλογων υποδομών και συστημάτων
- Στα καταξιωμένα εργαλεία και μηχανισμούς ΤΠΕ που χρησιμοποιούνται για τον επιτυχή έλεγχο ασφάλειας ανάλογων υποδομών και συστημάτων
- Στο ιστορικό περιστατικών ασφάλειας και στις μεθόδους αντιμετώπισης αυτών, από τα οποία να μπορεί να εξαχθεί χρήσιμη γνώση για την καλύτερη διασφάλιση της ασφάλειας

Τα συστήματα που θα αποτελέσουν αντικείμενο της παρούσας μελέτης, θα μπορούν να είναι είτε δημόσια είτε ιδιωτικά, αλλά θα πρέπει να παρουσιάζουν ανάλογα επιχειρησιακά χαρακτηριστικά με αυτά της ΓΓΠΣΔΔ, ώστε να μπορούν στη συνέχεια να πραγματοποιηθούν οι ενέργειες παραλληλισμού μεταξύ τους και εξαγωγής χρήσιμων συμπερασμάτων. Για τη συλλογή των δεδομένων και τη δημιουργία μιας πλήρους και αντιπροσωπευτικής βάσης γνώσης ασφάλειας συστημάτων, απαιτείται όπως μελετηθούν τουλάχιστον τρεις (3) περιπτώσεις (businesscases) ανάλογων δικτύων, εκ των οποίων τουλάχιστον οι δύο (2) θα είναι οπωσδήποτε στο εξωτερικό, η καθεμία σε διαφορετική χώρα, τεχνολογικά προηγμένη όπως συγκεκριμένα είναι τα πλέον ανεπτυγμένα κράτη μέλη της Ευρωπαϊκής Ένωσης, οι ΗΠΑ, το Ισραήλ, η Ιαπωνία, η Νότια Κορέα, κλπ.

Παράλληλα με τη διερεύνηση της ασφάλειας των προαναφερθέντων έτερων συστημάτων, η παρούσα εργασία θα λάβει υπόψη και τις πλέον επιστημονικά καταξιωμένες μεθόδους και πρακτικές που εφαρμόζονται στην πρόληψη, αντιμετώπιση, και εν γένει διαχείριση της ασφάλειας παρόμοιων συστημάτων. Η πληροφορία αυτή θα αποτελέσει επίσης τμήμα της ολοκληρωμένης βάσης

7.1.3.2.6 Διενέργεια ελέγχων διείσδυσης εξωτερικών δικτύων, εφαρμογών Ιστού, φυσικής ασφάλειας και διαρροής δεδομένων

Έλεγχοι διείσδυσης εξωτερικών δικτύων

Στο σύγχρονο περιβάλλον κυβερνοαπειλών κάθε ευπάθεια μπορεί να αποτελέσει αντικείμενο εκμετάλλευσης με καταστροφικές συνέπειες. Οι έλεγχοι διείσδυσης εξωτερικών δικτύων (external network penetration test) εντοπίζουν ευπάθειες σε υποδομές, συσκευές και διακομιστές που είναι προσβάσιμες από το διαδίκτυο.

Οι έλεγχοι προσομοιάζουν τις επιθέσεις κακόβουλων εισβολέων, οι οποίοι έχουν ως στόχο τη ναπόκτηση πρόσβαση σε συστήματα και τις εφαρμογές της περιμέτρου. Η μέθοδος εκτέλεσης των ελέγχων θα πρέπει να εξασφαλίζουν ότι δεν θα προκληθούν φθορές ή οποιουδήποτε τύπου προβλήματα στη λειτουργία υποδομών και συστημάτων.

Έλεγχοι διείσδυσης εφαρμογών ιστού

Οι δοκιμές διείσδυσης διαδικτυακών εφαρμογών στοχεύουν στον εντοπισμό τρωτών σημείων ασφαλείας που προκύπτουν από ανασφαλείς πρακτικές ανάπτυξης στη δημιουργία τη σχεδίαση και τη διαχείριση του λογισμικού ή ιστότοπου. Οι διαδικτυακές εφαρμογές χρησιμοποιούνται όλο και περισσότερο και αποτελούν κατεξοχήν στόχο κακόβουλων επιθέσεων. Στα πλαίσια των ελέγχων θα πρέπει να πραγματοποιηθεί μια σειρά προσομοιωμένων επιθέσεων, οι οποίες προσομοιάζουν κακόβουλες επιθέσεις, με σκοπό την αποτύπωση κάθε ευπάθειας και τη συνολική αποτίμηση του βαθμού ασφάλειας μιας εφαρμογής.

Έλεγχοι Φυσικής Ασφάλειας

Ο έλεγχος φυσικής ασφάλειας αξιολογεί τα μέτρα ασφαλείας που προστατεύουν τα περιουσιακά στοιχεία του οργανισμού από απειλές και στοχεύει σε προτάσεις για τυχόν βελτιώσεις. Οι έλεγχοι πρέπει να σχεδιάζονται με στόχο την παραβίαση της φυσικής ασφάλειας μίας ή περισσότερων τοποθεσιών. Τα σενάρια θα πρέπει να καθοριστούν βάσει ανάλυσης των υποδομών, με στόχο τη μη εξουσιοδοτημένη πρόσβαση σε φυσικές τοποθεσίες και πρόσβαση στο εσωτερικό δίκτυο με τη χρήση ειδικών συσκευών.

Ο υποψήφιος ανάδοχος καλείται να περιγράψει στην τεχνική του προσφορά τη μεθοδολογία εκτέλεσης των ελέγχων.

Έλεγχοι Διαρροής Δεδομένων

Οι έλεγχοι διαρροής δεδομένων αφορούν στη συγκέντρωση, ανάλυση και αξιολόγηση της βαρύτητας και του βαθμού ευαισθησίας πληροφοριών του οργανισμού από διάφορες πηγές (συμπεριλαμβανομένου του σκοτεινού διαδικτύου).

Ο έλεγχος θα πρέπει να αφορά πληθώρα δεδομένων, όπως ενδεικτικά ονόματα χρήστη και κωδικοί χρηστών, μηνύματα ηλεκτρονικού ταχυδρομείου κλπ. Στη συνέχεια θα πρέπει να προτείνονται μέτρα για την αντιμετώπιση ή το μετριασμό των συνεπειών της διαρροής και την αποφυγή της επανάληψής της.

Ο υποψήφιος ανάδοχος καλείται να περιγράψει στην τεχνική του προσφορά τη μεθοδολογία εκτέλεσης του συνόλου των παραπάνω ελέγχων.

7.1.3.2.7 Αξιοποίηση τεχνολογικής καινοτομίας και ερευνητικής πρωτοπορίας

Η διασφάλιση επαρκούς Επιχειρησιακής Συνέχειας, ειδικά απέναντι στο ενδεχόμενο κυβερνοεπιθέσεων, προϋποθέτει συνδυαστικές δράσεις πολλαπλής στόχευσης. Από τη μια πλευρά πρέπει να υπάρχει συστηματική μέριμνα για την αντιμετώπιση ήδη γνωστών τύπων κυβερνοαπειλών, με χρήση βέλτιστων πρακτικών και διαθέσιμων αποτελεσματικών τεχνολογιών. Από την άλλη, πρέπει να υπάρχει επίσης μέριμνα για την αντιμετώπιση καινοφανών κυβερνοεπιθέσεων, με αξιοποίηση προηγμένων μεθοδολογιών και τεχνολογικών λύσεων, όπως αυτές προκύπτουν, προδιαγράφονται και αξιολογούνται σε εξειδικευμένα ακαδημαϊκά ερευνητικά περιβάλλοντα.

Δεδομένων των ρηξικέλευθων εξελίξεων σε θέματα Κυβερνοασφάλειας, ο συνδυασμός βέλτιστων πρακτικών, δοκιμασμένων λύσεων και προηγμένων (state-of-the-art) μεθοδολογιών και τεχνολογιών αποτελεί το επαρκέστερο μέσο διασφάλισης της Επιχειρησιακής Συνέχειας. Συνεπώς, τα ζητούμενα πληροφοριακά συστήματα, τεχνολογικά προϊόντα και εξειδικευμένες υπηρεσίες θα πρέπει να παρέχονται με τρόπο που εγγυάται ότι όχι μόνο τα καταλληλότερα διαθέσιμα συστήματα της αγοράς, αλλά και πρωτότυπες μεθοδολογίες και τεχνολογίες.

Επιπρόσθετα, οι δόκιμες μεθοδολογίες και τεχνολογίες διασφάλισης της Επιχειρησιακής Συνέχειας προϋποθέτουν τακτικούς και συστηματικούς ελέγχους (penetration tests), αξιολογήσεις (audits), πιστοποιήσεις (certifications), μελέτες ανάλυσης και διαχείρισης επικινδυνότητας (risk analysis and management) κλπ., οι οποίες πρέπει να εκπονούνται σύμφωνα με διεθνή πρότυπα και αντίστοιχες καλές πρακτικές. Οι αδιαμφισβήτητες αυτές αναγκαιότητες, με τη σειρά τους, προϋποθέτουν συνθήκες λειτουργικής ανεξαρτησίας και αβίαστων επιστημονικών αποτιμήσεων.

Ο Ανάδοχος καλείται να παρουσιάσει περιοδική καταγραφή και πλάνο αξιολόγησης των καινοτόμων τεχνολογιών και ερευνητικών επιτευγμάτων.

7.1.3.3 Εξειδικευμένες Λύσεις Ασφάλειας Πληροφοριών, Εγγράφων και εφαρμογών

7.1.3.3.1 Μηχανισμός Ελέγχου Πρόσβασης Χρηστών Πολλαπλών Παραγόντων (MFA)

Η λύση αυτή αφορά 10.000 διαχειριστές η οποία θα εξασφαλίζει τον έλεγχο πρόσβασης χρηστών πολλαπλών σημείων. Η λύση βοηθά στην απλοποίηση και τη διαχείριση της πρόσβασης των χρηστών ενός οργανισμού. Η επαλήθευση πρόσβασης βοηθά στην επίτευξη μιας ισορροπίας μεταξύ χρηστικότητας και ασφάλειας μέσω της χρήσης πρόσβασης πολλαπλών παραγόντων (MFA: Multi-factor Authentication). Η λύση θα διασφαλίζει ισχυρό έλεγχο ταυτότητας μέσω του μηχανισμού MFA και υποστηρίζει μια ευρεία γκάμα μηχανισμών ελέγχου ταυτότητας πολλαπλών παραγόντων για την επαλήθευση των χρηστών κατά τον έλεγχο ταυτότητας από εφαρμογές web, επιτραπέζιους υπολογιστές, κινητά και διακομιστές. Ο έλεγχος ταυτότητας πολλαπλών παραγόντων διασφαλίζει ότι ο χρήστης που έχει πρόσβαση σε εφαρμογές και διακομιστές είναι πραγματικά το σωστό άτομο.

Ο έλεγχος ταυτότητας πολλαπλών παραγόντων (MFA, που περιλαμβάνει έλεγχο ταυτότητας) είναι μια ηλεκτρονική μέθοδος ελέγχου ταυτότητας κατά την οποία παρέχεται σε έναν χρήστη πρόσβαση σε μια εφαρμογή μόνο αφού παρουσιάσει επιτυχώς δύο ή περισσότερα αποδεικτικά στοιχεία (ή παράγοντες) στον μηχανισμό ελέγχου ταυτότητας: γνώση (κάτι που γνωρίζει μόνο ο χρήστης), κατοχή (κάτι που έχει μόνο ο χρήστης) και εγγενής (κάτι που είναι μόνο ο χρήστης).

Υπάρχουν διαφορετικοί τρόποι υλοποίησης ενός τέτοιου μηχανισμού. Στα πλαίσια του παρόντος έργου θα υλοποιηθεί λύση on-premise χρησιμοποιώντας υποδομή του Φορέα υπό τη μορφή virtual appliance και θα πρέπει να γίνει εκτενής περιγραφή των αναγκών σε hardware resources. Η χρήση πολλαπλών παραγόντων ελέγχου ταυτότητας για την απόδειξη της ταυτότητάς κάποιου βασίζεται στην προϋπόθεση ότι ένας μη εξουσιοδοτημένος φορέας είναι απίθανο να είναι σε θέση να παρέχει όλους τους παράγοντες που απαιτούνται για την πρόσβαση.

Εάν, σε μια προσπάθεια ελέγχου ταυτότητας, τουλάχιστον ένα από τα στοιχεία λείπει ή παρέχεται λανθασμένα, η ταυτότητα του χρήστη δεν διαπιστώνεται με επαρκή βεβαιότητα και η πρόσβαση στο στοιχείο που προστατεύεται από έλεγχο ταυτότητας πολλαπλών παραγόντων, τότε παραμένει αποκλεισμένη. Οι παράγοντες ελέγχου ταυτότητας ενός συστήματος ελέγχου ταυτότητας πολλαπλών παραγόντων μπορεί να περιλαμβάνουν:

- Κάτι που έχει ο χρήστης: Οποιοδήποτε φυσικό αντικείμενο έχει στην κατοχή του ο χρήστης, όπως ένα διακριτικό ασφαλείας, ένα κλειδί κ.λπ.
- Κάτι που γνωρίζει ο χρήστης: Ορισμένες γνώσεις που είναι γνωστές μόνο στον χρήστη, όπως κωδικός πρόσβασης, PIN κ.λπ.
- Κάτι που είναι ο χρήστης: Κάποια φυσικά χαρακτηριστικά του χρήστη (βιομετρικά), όπως δακτυλικό αποτύπωμα, ίριδα ματιών, φωνή, ταχύτητα πληκτρολόγησης, μοτίβο στα διαστήματα πατήματος πληκτρων κ.λπ.

7.1.3.4 Υπηρεσίες νεφοϋπολογιστικών υποδομών και υπηρεσιών

7.1.3.4.1 Υπηρεσίες ανάκαμψης από καταστροφή και λήψης αντιγράφων ασφαλείας

Μεσκοπώ την ενίσχυση της επιχειρησιακής συνέχειας, απαιτείται η παροχή υπηρεσιών λήψης Αντιγράφων ασφαλείας (Backup) και ανάκαμψης από καταστροφή (Επαναφοράς (Recovery)). Απαιτείται να λαμβάνονται αντίγραφα ασφαλείας σε υπολογιστικούς πόρους που βρίσκονται εγκατεστημένοι είτε τοπικά (On-premises) είτε στον πάροχο του Νέφους (Cloud). Ως προστατευόμενοι υπολογιστικοί πόροι δύναται να θεωρηθούν στοιχεία όπως [VMs, DBs, Folders/Files]. Επίσης, θα υπάρχει η δυνατότητα επιλογής επαναφοράς των προστατευμένων υποδομών είτε τοπικά (On-premises) είτε στον πάροχο του Νέφους (Cloud). Θα υπάρχουν επιλογές της υπηρεσίας αυτής με βάση τον όγκο των προστατευόμενων πόρων/δεδομένων ώστε να καλύπτονται διαφορετικού τύπου ανάγκες.

Ο ανάδοχος είναι υπεύθυνος και για την Εγκατάσταση / παραμετροποίηση υπηρεσιών ανάκαμψης από καταστροφή και λήψης αντιγράφων ασφαλείας ανάλογα με τις ανάγκες.

7.1.3.5 Εξειδικευμένες λύσεις ασφαλείας

7.1.3.5.1 Λύση δημιουργίας αντιγράφων ασφαλείας σε ταινίες με PhysicalAirGap – TrueAirGap 1.960PB χωρητικότητα

Τα οφέλη από την υλοποίηση μίας λύσης Air Gap με physical isolation είναι η δημιουργία ενός "κενού αέρα" μεταξύ των δεδομένων παραγωγής και της λύσης προστασίας αντιγράφων ασφαλείας. Αυτό εξασφαλίζεται με τις κασέτες ταινίας και ο λόγος είναι ότι οι βιβλιοθήκες ταινιών είναι ένα σύστημα που βρίσκεται «εκτός σύνδεσης».

Σε περίπτωση μιας προσπάθειας επίθεσης από χάκερ τα δεδομένα είναι εξασφαλισμένα γιατί δεν μπορούν να αλλοιώσουν δεδομένα που δεν μπορούν να φτάσουν. Αυτή είναι μια πολύ αποτελεσματική άμυνα ενάντια σε ένα ευρύ φάσμα απειλών στον κυβερνοχώρο.

Οι λύσεις προστασίας δεδομένων διαθέτουν εγγενώς τη λειτουργικότητα και τα χαρακτηριστικά που απαιτεί ένας οργανισμός για την υλοποίηση λύσης τύπου Tape Air Gap. Με απλά βήματα μπορεί να προστεθεί επιπλέον πολιτική προστασίας δεδομένων για δημιουργία επιπλέον αντιγράφων προστασίας δεδομένων σε σύστημα αποθήκευσης που βασίζονται σε ταινίες που διαθέτει και σήμερα ο οργανισμός σας. Προαπαιτούμενα είναι η δημιουργία του συστήματος που θα διαχειρίζεται τους οδηγούς ταινιών που θα αποθηκεύονται τα επιπλέον αντίγραφα. Πρόκειται για μία αυτοματοποιημένη λύση και ένα ισχυρό εργαλείο ενάντια σε διαφόρων τύπων κυβερνοεπιθέσεων.

7.1.3.5.2 Λύση δημιουργίας αντιγράφων ασφαλείας σε δίσκο Backup με LogicalAirGap για το 50% της χωρητικότητας

Ο στόχος είναι η λύση να μπορεί να υλοποιηθεί με τέτοιο τρόπο ώστε χρησιμοποιώντας εγγενή λειτουργικότητα των υφιστάμενων κεντρικών συστημάτων αποθήκευσης να είναι δυνατό να προστατευθούν τα volumes που φιλοξενούν συστήματα όπως εικονικές μηχανές, βάσεις δεδομένων κλπ. Η προστασία των παραγωγικών volumes θέλουμε να γίνεται μέσω αμετάβλητων χρονικά αντιγράφων εικόνων. Τα προστατευμένα αντίγραφα, αποθηκεύονται σε απομονωμένο λογικό κενό αέρος το οποίο είναι εκτός σύνδεσης (offline by design). Με τον τρόπο αυτό μπορεί να επιτευχθεί απόλυτη προστασία από κάθε κακόβουλη εισβολή αφού τα volumes είναι απροσπέλαστα. Μέσα από

το γραφικό περιβάλλον της λύσης ο διαχειριστής ορίζει τα volumes που θέλει να προστατεύσει και στη συνέχεια παραμετροποιεί τη συχνότητα και τη διάρκεια (retention) των προστατευμένων αντιγράφων.

7.1.3.5.3 Λύση προστασίας ηλεκτρονικού ταχυδρομείου MailSecurity - 20.000 σταθμούς εργασίας

Η λύση προστασίας ηλεκτρονικού ταχυδρομείου αποτελεί μια ακόμα γραμμή άμυνας για το ηλεκτρονικό ταχυδρομείο των χρηστών. Ο στόχος της λύσης είναι να προστατεύει τα εισερχόμενα, εξερχόμενα και εσωτερικά email από επιθέσεις phishing. Η λύση θα επιθεωρεί τα μεταδεδομένα, τα συνημμένα (attachments), τους συνδέσμους και τη γλώσσα επικοινωνίας, καθώς και όλες τις ιστορικές επικοινωνίες, για να προσδιορίσει τις σχέσεις μεταξύ του αποστολέα και του παραλήπτη, αυξάνοντας την πιθανότητα αναγνώρισης πλαστοπροσωπίας χρήστη ή δόλιων μηνυμάτων. Επίσης επιθεωρεί εσωτερική επικοινωνία σε πραγματικό χρόνο προκειμένου να αποφευχθούν πλευρικές επιθέσεις και εσωτερικές απειλές.

7.1.3.5.4 Λύση Endpoint Detection and Response - 20.000 σταθμούς εργασίας

Η λύση EDR είναι απαραίτητη για την προστασία των συστημάτων από κακόβουλα λογισμικά. Η λύση EDR πρέπει να είναι ικανή να ανιχνεύει απειλές χρησιμοποιώντας δυναμική ανάλυση συμπεριφοράς για τον εντοπισμό γνωστών και άγνωστων απειλών. Ο οργανισμός μπορεί να αποκτήσει πλήρη ορατότητα στα τελικά σημεία, να εντοπίζει και να ανταποκρίνεται σε απειλές αυτόνομα, χωρίς να απαιτείται πρόσθετο προσωπικό υψηλής εξειδίκευσης. Η λύση πρέπει να διαθέτει εγγενείς δυνατότητες χρήσης τεχνητής νοημοσύνης στην ανίχνευση απειλών στα τερματικά.

Οι βασικές δυνατότητες της πλατφόρμας πρέπει να περιλαμβάνουν:

- Λεπτομερείς πληροφορίες σχετικά με διαδικασίες και εφαρμογές που εκτελούνται σε τελικά σημεία
- Πλήρη ορατότητα στα τελικά σημεία, χαρτογράφηση απειλών με βάση το MITRE ATT&CK και οπτικοποίηση των απειλών.
- Ανίχνευση απειλών βασισμένων σε υπογραφές (signature based) αλλά και σε νέες απειλές που εντοπίζονται με ανάλυση της συμπεριφοράς του τελικού σημείου (behavioral based).
- Ταχεία αυτόνομη απόκριση σε συμβάντα.
- Δυνατότητα υλοποίησης και λειτουργίας χωρίς internet (air-gapped).
- agent να έχει χαμηλές απαιτήσεις σε resources (<1% CPU) και να μην επηρεάζει την ομαλή λειτουργία των τελικών σημείων.
- Ο agent να υποστηρίζει τη δυνατότητα παρακολούθησης του λειτουργικού συστήματος από το επίπεδο του hypervisor (όπου υποστηρίζεται).
- Δυνατότητες Threat Hunting που επιτρέπει στους αναλυτές να αναζητούν την παρουσία συγκεκριμένων δεικτών κινδύνου – indicators of compromise

7.1.3.5.5 Managed services security endpoint & mail (αφορά 20.000 σταθμούς εργασίας)

Η υπηρεσία θα πρέπει να παρέχει παρακολούθηση και έλεγχο των endpoints του πελάτη με άμεση ενημέρωση για περιστατικά ασφάλειας, δυνατότητα ανίχνευσης απειλών και γρήγορης απόκρισης 24 ώρες το 24ωρο, 7 ημέρες την εβδομάδα. Η υπηρεσία θα πρέπει να παρέχει 24ωρη παρακολούθηση των endpoints (Managed Detection and Response) με στόχο τον εντοπισμό περιστατικών ασφάλειας

και ενημέρωση του πελάτη μέσω τηλεφώνου/e-mail για περιστατικά ασφάλειας βάση SLA. Επίσης θα πρέπει να περιλαμβάνει παροχή συμβουλών για τη διερεύνηση και την αντιμετώπιση του περιστατικού.

7.1.3.5.6 Λύση που αφορά τον έλεγχο της πρόσβασης των εσωτερικών χρηστών στο Διαδίκτυο

Απαιτείται η υλοποίηση λύσης για τον έλεγχο της πρόσβασης των εσωτερικών χρηστών στο Διαδίκτυο, σύμφωνα με τις προδιαγραφές του υπίνακα συμμόρφωσης 7.2.1.8

7.1.3.5.7 Λύση Ασφαλείας και προστασίας των χρηστών από απειλές του διαδικτύου (WebSecurityGateway)

Η συγκεκριμένη λύση ασφαλείας πρόκειται να καλύψει την ανάγκη προστασίας του εταιρικού δικτύου από επιθέσεις και απειλές στο περιεχόμενο της υπηρεσίας ηλεκτρονικής αλληλογραφίας.

Πιο συγκεκριμένα ο ρόλος της εν λόγω λύσης ασφαλείας στην υποδομή θα πρέπει να καλύπτει τουλάχιστον τα ακόλουθα:

- Δυνατότητα ελέγχων ασφαλείας στο περιεχόμενο HTTP, HTTPS και FTP βασισμένων σε συγκεκριμένους κανόνες (πολιτικές ασφαλείας) οι οποίοι θα εφαρμόζονται ανά χρήστη ή ομάδα χρηστών (user ή group) οι λογαριασμοί των οποίων λαμβάνονται από κάποια υπηρεσία καταλόγου (π.χ. AD, LDAP service).
- Υποστήριξη μηχανισμού caching.
- Ενσωματωμένος μηχανισμός Antivirus για την ανίχνευση και καταστολή ιών και άλλων ειδών κακόβουλου λογισμικού στο περιεχόμενο της ηλεκτρονικής αλληλογραφίας. Να αναφερθούν οι υποστηριζόμενοι κατασκευαστές.
- URL Filtering – έλεγχος της πρόσβασης των χρηστών σε συγκεκριμένες κατηγορίες ιστοσελίδων με δυνατότητα εφαρμογής διαφορετικών πολιτικών ανά domain user/group.
- Application Identification & Control – αναγνώριση και έλεγχος των εφαρμογών HTTP & HTTPS. Δυνατότητα εφαρμογής πολιτικών ελέγχου πρόσβασης βάσει της εφαρμογής που χρησιμοποιεί ο χρήστης σε συνδυασμό με το Source/Destination IP address, το πρωτόκολλο και τον χρήστη (domain user/group).

Η λύση ασφαλείας θα πρέπει να αποστέλλει δεδομένα καταγραφής (logs) σε λύση διαχείρισης περιστατικών ασφαλείας (SIEM) & συλλογής αρχείων καταγραφής.

7.1.4 Φυσικό αντικείμενο Τμήματος 2 «Εξειδικευμένες λύσεις και υπηρεσίες ασφαλείας για την Η.ΔΙ.Κ.Α. Α.Ε.»

7.1.4.1 Διαστασιολόγηση λογισμικού, εξοπλισμού και υπηρεσιών

Κατηγορία	Μονάδα διαστασιολόγησης	Ελάχιστο μέγεθος
Διαμόρφωση πολιτικών ασφαλείας κρίσιμων οντοτήτων με στόχο την ανάδειξη τεχνικών και οργανωτικών μέτρων για την προστασία τους από Κυβερνοαπειλές	A/M	14
Διαμόρφωση πολιτικών ορθής χρήσης Πληροφοριακών συστημάτων και εφαρμογών	A/M	14

Κατηγορία	Μονάδα διαστασιολόγησης	Ελάχιστο μέγεθος
Διενέργεια δράσεων ενημέρωσης για τη μεταφορά τεχνογνωσίας και την διαμόρφωση κουλτούρας ενεργούς ευαισθητοποίησης για τους κινδύνους κυβερνοασφάλειας	A/M	14
Διαμόρφωση πλάνου ανάκαμψης από καταστροφές για κρίσιμες οντότητες	A/M	14
Εκπόνηση Μελέτης εξωτερικού και εσωτερικού περιβάλλοντος και την ανάδειξη βέλτιστων πρακτικών	A/M	14
Διαμόρφωση πολιτικής αντιγράφων ασφαλείας, που θα περιγράφει σκοπό, πεδίο εφαρμογής, ρόλους και ευθύνες	A/M	14
Διαμόρφωση Συστήματος Διαχείρισης της Ασφάλειας των Πληροφοριών (ΣΔΑΠ) με βάση το πρότυπο ISO 27001 & Εκπόνηση Μελέτης Ανάλυσης και Αξιολόγησης Κινδύνων	A/M	14
Διενέργεια ελέγχων διείσδυσης εξωτερικών δικτύων, εφαρμογών Ιστού, φυσικής ασφάλειας και διαρροής δεδομένων για τον εντοπισμό των ευπαθειών σε υποδομές, συσκευές και διακομιστές που είναι προσβάσιμοι από το διαδίκτυο	A/M	16
Αξιοποίηση τεχνολογικής καινοτομίας και ερευνητικής πρωτοπορίας	A/M	46
Λύση DDOS	Τεμάχια	1
Παροχή υπηρεσιών ανάκαμψης από καταστροφή & λήψης αντιγράφων ασφαλείας (disaster recovery as a service & data backup as a service)	CREDITS €	500.000,00
Υπηρεσίες εγκατάστασης/παραμετροποίησης υπηρεσιών ανάκαμψης από καταστροφή & λήψης αντιγράφων ασφαλείας (disaster recovery as a service & data backup as a service)	A/M	40
NGFW για το DataCenter, για την πρόσβαση των εσωτερικών χρηστών στο Διαδίκτυο και την ανάλυση των επικοινωνιών τους και για την απομακρυσμένη πρόσβαση. Άδειες για προστασία IPS, antimalware, Application Control. Διαχειριστικό εργαλείο για τα firewall	Τεμάχια	2
Switches για τη διασύνδεση των firewalls	Τεμάχια	2
Virtual firewall Για 10 tenants με High availability Και άδειες IPS και antimalware	Μήνες	30
Λύση Microsegmentation	Endpoints	500

Κατηγορία	Μονάδα διαστασιολόγησης	Ελάχιστο μέγεθος
	Εικονικές μηχανές	600
Λύση Ασφαλείας και προστασίας των χρηστών από απειλές του διαδικτύου (WebSecurityGateway) - 250 χρήστες και Συσκευές υλικού (HWappliances)	Χρήστες Συσκευές	250 2
Λύση Αυστηρής πιστοποίησης για την απομακρυσμένη πρόσβαση (MFA, ZeroTrust)	Μήνες	30
Λύση CloudProxy προστασίας απομακρυσμένων χρηστών	Μήνες	30
Λύση Antimalware απομακρυσμένων χρηστών (AV, EDR, XDR)	Μήνες	30
Λύση εκπαίδευσης για 250 χρήστες σε phishing campaigns και cyberattacks	Χρήστες	250
Λύση Ασφαλούς Πρόσβασης χρηστών στο εταιρικό δίκτυο	Ταυτόχρονα συνδεδεμένες συσκευές	500
Λύση Πλατφόρμας Ενορχήστρωσης Ασφαλείας, Αυτοματοποίησης	Μήνες	30
Πλατφόρμα Κυβερνοασφάλειας – Εκτεταμένης Ανίχνευσης & Απόκρισης (CyberSecurity)	Assets GB log files/ημέρα	3.000 100
Λύση Προστασίας Βάσεων Δεδομένων	Βάσεις δεδομένων	20
Λογισμικό κυβερνοασφάλειας ΑΙ, συμπεριλαμβανομένης εγκατάστασης, εκπαίδευσης και υποστήριξης 24/7. 1000 Άδειες	Μήνες	30
Υπηρεσίες Επιχειρησιακής Λειτουργίας	Α/Μ	20
Λύση Διαβάθμισης και Σήμανσης Εγγράφων	Σταθμοί εργασίας	1.000
Λύση Προστασίας Δεδομένων από Διαρροή	Σταθμοί εργασίας	1.000
Λύση Διαχείρισης Δικαιωμάτων Εγγράφων	Χρήστες	1.000
Λύση Διαχείρισης Λογαριασμών και Δικαιωμάτων Πρόσβασης Χρηστών	Λογαριασμοί	1.000
Λύση Διαχείρισης Προνομιούχων Λογαριασμών Πρόσβασης	Λογαριασμοί διαχειριστών Λογαριασμοί συνεργατών (named users)	100 50
Λύση μηχανισμών ισχυρής ταυτοποίησης	Λογαριασμοί	500

7.1.4.2 Πολιτικές – Διαδικασίες και Μέτρα Αντιμετώπισης και Πρόληψης

7.1.4.2.1 Διαμόρφωση πολιτικών ορθής χρήσης Πληροφοριακών συστημάτων και εφαρμογών

Ο Ανάδοχος θα εκπονήσει μελέτη πολιτικής ορθής χρήσης πληροφοριακών συστημάτων και εφαρμογών, προκειμένου να καθοριστούν οι υποχρεώσεις όλων των χρηστών, καθώς και οι αρχές, οι κανόνες και οι συνέπειες για το σύνολο των προσώπων στα οποία εκχωρείται το δικαίωμα πρόσβασης στα πληροφοριακά συστήματα και τις εφαρμογές. Η πολιτική ορθής χρήσης αποβλέπει στην αποτροπή καταχρηστικής άσκησης των δικαιωμάτων των χρηστών και της τέλεσης πράξεων που συνιστούν κίνδυνο παραβίασης του απορρήτου των δεδομένων / πληροφοριών, ή διακύβευσης της ασφάλειας των πληροφοριακών συστημάτων και εφαρμογών ή της ακεραιότητας και διαθεσιμότητας των υποδομών.

Στο πλαίσιο της εργασίας αυτής, ο Ανάδοχος κατ' ελάχιστον:

- Θα διενεργήσει κατάλληλη κατηγοριοποίηση του συνόλου των υφιστάμενων και δυνητικών χρηστών, προκειμένου να προτείνει στη συνέχεια μια διαφοροποιημένη πολιτική ορθής χρήσης προσαρμοσμένη σε κάθε κατηγορία.
- Θα διενεργήσει μια κατηγοριοποίηση των πληροφοριακών συστημάτων και εφαρμογών, προκειμένου να προσδιορίσει στη συνέχεια τα συστήματα εκείνα που είναι ευάλωτα σε ένα περιστατικό ανάρμοστης χρήσης.
- Θα αναλύσει τα ιδιαίτερα χαρακτηριστικά κάθε κατηγορίας χρηστών, που θα προκύψουν από τη σχετική έρευνα και κατηγοριοποίηση που θα έχει ήδη κάνει και στη συνέχεια θα προσδιορίσει τις ανάγκες και υποχρεώσεις χρήσης κάθε κατηγορίας
- Θα προσδιορίσει τις διαδικασίες που πρέπει να εφαρμόζονται, τις ενέργειες που συνιστώνται και τα μέτρα που πρέπει να παίρνονται, προκειμένου να διασφαλιστεί η ορθή χρήση του δικτύου
- Θα προσδιορίσει τις ενέργειες που απαγορεύονται ή πρέπει να αποφεύγονται και οι οποίες συνιστούν μια ανάρμοστη χρήση πληροφοριακών συστημάτων και εφαρμογών.
- Θα προτείνει τις διαδικασίες και τα διορθωτικά και/ή αποτρεπτικά μέτρα που πρέπει να εφαρμόζονται σε περίπτωση που διαπιστωθεί κάποιο περιστατικό ανάρμοστης χρήσης πληροφοριακών συστημάτων και εφαρμογών
- Θα συντάξει σχέδια συμφωνητικών ορθής χρήσης, τα οποία θα υπογράφονται από τους δυνητικούς χρήστες πληροφοριακών συστημάτων και εφαρμογών, κατόπιν επιθυμίας της ΗΔΙΚΑ. Το ελάχιστο περιεχόμενο των συμφωνητικών αυτών περιλαμβάνει μια σύνοψη των δικαιωμάτων και υποχρεώσεων κάθε κατηγορίας χρήστη
- Θα μεριμνήσει για την κατάλληλη ενημέρωση όλων των χρηστών (φτάνοντας μέχρι το επίπεδο τελικού χρήστη) επί της πολιτικής ορθής χρήσης που θα εφαρμοσθεί, αφού εγκριθεί από την ΗΔΙΚΑ
- Θα προσδιορίσει τις διαδικασίες που πρέπει να εφαρμοστούν και τις ενέργειες που πρέπει να πραγματοποιηθούν, προκειμένου να καταστεί δυνατός ο τακτικός έλεγχος και παρακολούθηση της εφαρμογής ή όχι της πολιτικής ορθής χρήσης.

7.1.4.2.2 Διενέργεια δράσεων ενημέρωσης για τη μεταφορά τεχνογνωσίας και την διαμόρφωση κουλτούρας ενεργούς ευαισθητοποίησης για τους κινδύνους κυβερνοασφάλειας

Ο Ανάδοχος καλείται να παράσχει υπηρεσίες σχεδιασμού και υλοποίησης δράσεων ενημέρωσης προς τις αρμόδιες υπηρεσίες της ΗΔΙΚΑ κατά την υλοποίηση του έργου, στις ακόλουθες θεματικές ενότητες:

- Εισαγωγή στην Ασφάλεια Πληροφοριών
- Οι κυβερνοαπειλές (Cyber Threats)
- Υλική Ασφάλεια Αρχείων και Μηχανημάτων
- Ασφάλεια Επιφάνειας Εργασίας
- Αποθήκευση αρχείων και δεδομένων
- Αποστολή και διαμοιρασμός αρχείων
- Ασφάλεια κωδικών πρόσβασης
- Ασύρματα δίκτυα και κινητή επικοινωνία
- Διαδικτυακή Ασφάλεια
- Συστήματα Κοινωνικής Μηχανικής (Social Engineering)
- Ασφάλεια ηλεκτρονικού ταχυδρομείου
- Κακόβουλο λογισμικό (Ιοί, Worms, Trojans, Spyware, Adware)
- Ηλεκτρονικό «ψάρεμα» (Phishing)
- Μέσα Κοινωνικής Δικτύωσης

Οι συμμετέχοντες μόλις ολοκληρώσουν την εκπαίδευση θα έχουν κατανοήσει τα θέματα των νέων τεχνολογιών και διαδικτύου, ασφάλειας υπολογιστικών συστημάτων και υποδομών, ασφαλής χρήσης του διαδικτύου αλλά και χειρισμού διαδικτυακών προγραμμάτων και προγραμμάτων ηλεκτρονικού υπολογιστή. Επιπλέον, θα μπορούν να αναγνωρίσουν τα διάφορα είδη κυβερνοαπειλών και θα έχουν μάθει βασικούς κανόνες ασφαλείας για την αποτροπή τους.

Πιο ειδικά ο Ανάδοχος καλείται να παρέχει τις παρακάτω υπηρεσίες:

Ι. Μεθοδολογία εκπαίδευσης, εκπαιδευτικό υλικό και εισαγωγή των δεδομένων στην εκπαιδευτική πλατφόρμα

Ο Ανάδοχος θα πρέπει να τεκμηριώσει και να παραδώσει τη μεθοδολογία εκπαίδευσης που θα ακολουθήσει πριν την έναρξη του προγράμματος. Η μεθοδολογία θα πρέπει να επιδιώκει την επίτευξη των παρακάτω εκπαιδευτικών στόχων για τους εκπαιδευόμενους:

- Ανάκληση γνώσεων
- Κατανόηση εκπαιδευτικού υλικού
- Εφαρμογή γνώσεων στην πράξη και σε περιβάλλον προσομοίωσης ή/και σε μελέτες περίπτωσης
- Ανάλυση και σύνθεση γνώσεων

- Η θεωρία και οι ασκήσεις αξιολόγησης/εξέτασης να αποδίδονται μέσω σύγχρονων authoring tools (όπως Articulate, Captivate κ.α.), εξειδικευμένων στην εκπαίδευση ενηλίκων.
- Ενσωμάτωση μηχανισμών παιχνιδιού στην εκπαιδευτική διαδικασία, με δυνατότητες επιβράβευσης (π.χ. πόντοι, σήματα, εικονικά νομίσματα κ.ά.)

Ο Ανάδοχος θα αναλάβει τον σχεδιασμό των εκπαιδευτικών προγραμμάτων λαμβάνοντας υπόψη συγκεκριμένες παραμέτρους. Οι παράμετροι αυτοί αφορούν τη διαφοροποιημένη προσέγγιση ανάλογα με την ομάδα-στόχο, τον τρόπο εκπαίδευσης και τα μέσα που θα χρησιμοποιηθούν.

Ο Ανάδοχος καλείται να μελετήσει τα μοντέλα που έχουν ακολουθήσει άλλες ευρωπαϊκές χώρες για σχετικά προγράμματα εκπαίδευσης, ενημέρωσης και ευαισθητοποίησης εταιρειών και οργανισμών. Ο στόχος της μελέτης είναι να μπορεί ο Ανάδοχος να παρέχει τις κατάλληλες κατευθύνσεις και να αντλήσει καλές πρακτικές στο πεδίο της κατάρτισης και ευαισθητοποίησης εργαζομένων σε θέματα Κυβερνοασφάλειας.

Ο Ανάδοχος, καλείται να παραδώσει για κάθε εκπαιδευτική ενότητα του προγράμματος, τους εκπαιδευτικούς στόχους, τα εκπαιδευτικά αποτελέσματα, τη διάρκεια αλλά και πιθανές ασκήσεις/ερωτήσεις προς πρακτική εξάσκηση των γνώσεων. Ο σχεδιασμός του εκπαιδευτικού προγράμματος πρέπει να υποστηρίζεται από μια πολυμεσική υλοποίηση, η οποία θα περιλαμβάνει διάφορα οπτικοακουστικά μέσα (π.χ. ήχος, εικόνες, βίντεο, mini games, gamification, quizzes, learning modalities, slideshow κ.α).

Για την ασύγχρονη εκπαίδευση απαιτείται ένα σύγχρονο και πλήρως φιλικό προς το χρήστη σύστημα Learning Management (Learning Management System, LMS), το οποίο να βασίζεται σε εφαρμογή PWA (Progressive Web Application) έτσι ώστε να μην απαιτείται εγκατάσταση της μέσω Google/Apple Store καθώς και όλες οι απαραίτητες ενημερώσεις (updates) να γίνονται κεντρικά και να ενημερώνονται αυτόματα όλοι οι χρήστες, χωρίς να χρειάζεται να προβούν σε καμία ενέργεια αναβάθμισης. Επιπλέον, το LMS θα πρέπει να είναι μία απόλυτα εξατομικευμένη λύση που θα παραμετροποιηθεί, προσαρμοστεί και ενσωματωθεί πλήρως τόσο στα μηχανογραφικά συστήματα όσο και στους μηχανισμούς ασφαλείας της ΗΔΙΚΑ. Θα πρέπει να καλύπτει τις ανάγκες στο σύνολο των εκπαιδευόμενων (ιδιωτικός και δημόσιος τομέας), να παρέχει στενή διασύνδεση (integration) με όλα τα εργαλεία του MS Office και να αποτελεί συμβατή πλατφόρμα με διεθνή πρότυπα ηλεκτρονικής μάθησης όπως SCORM με τα οποία εξασφαλίζεται η επαναχρησιμοποίηση, η προσβασιμότητα και η ανθεκτικότητα του εκπαιδευτικού υλικού στις τεχνολογικές μεταβολές, καθώς και η διαλειτουργικότητα μεταξύ συστημάτων ηλεκτρονικής μάθησης. Η αρχιτεκτονική της πλατφόρμας (πλατφορμών) θα δίνει τη δυνατότητα στον χρήστη να αλληλεπιδρά δυναμικά με όλο το εκπαιδευτικό υλικό. Επιπλέον, ο Ανάδοχος θα πρέπει να παρακολουθεί με αναφορές το πλήθος των χρηστών που θα παρακολουθούν ή/και ολοκληρώνουν το εκπαιδευτικό ασύγχρονο πρόγραμμα κατάρτισης καθώς και να καταγράφονται αναλυτικά όλα τα ερωτηματολόγια με τις απαντήσεις στα τελικά διαδικτυακά (ψηφιακά) τεστ όλων των χρηστών σε αναλυτική καρτέλα προφίλ.

Για τον σχεδιασμό του εκπαιδευτικού υλικού πρέπει να ακολουθούνται με ακρίβεια τα πρότυπα σχεδιασμού εκπαιδευτικού υλικού, όπως περιγράφονται:

- Ο εκπαιδευτικός σχεδιασμός ψηφιακού υλικού ("instructional design") θα πρέπει να βασίζεται στη σαφή και αιτιολογημένη κατάτμηση του υλικού ενοτήτων σε υποενότητες μάθησης, με ορισμένη μέγιστη διάρκεια. Παράλληλα για την πλήρη κατανόηση της κατάτμησης των ενοτήτων σε υποενότητες μάθησης ο Ανάδοχος οφείλει να συνδέσει κάθε ενότητα/υποένότητα με διακριτούς εκπαιδευτικούς στόχους.
- Ο χρήστης θα πρέπει να ακολουθεί σαφή εκπαιδευτικά μονοπάτια (Θεωρία, Αυτοαξιολόγηση, Εξέταση, Πιστοποίηση), για τα οποία να δύναται να έχουν υποχρεωτική σειριακή ακολουθία παρακολούθησης, ανάλογα με τους σκοπούς της εκπαίδευσης.

- Η διάδραση με το περιεχόμενο και η ενεργητική μάθηση των καταρτιζόμενων πρέπει με σαφή τρόπο να επιτυγχάνεται μέσω σύνθετων εργαλείων, εξειδικευμένων στην εκπαίδευση ενηλίκων, όπως business case studies, role playing, psychometric analysis κ.ά.
- Ο πρακτικός προσανατολισμός: μέθοδος «μαθαίνω κάνοντας» (learning by doing) θα επιτυγχάνεται με προσομοίωση πραγματικών συνθηκών (μελέτες περίπτωσης, επίλυση προβλήματος) και άλλες τεχνικές που ο ανάδοχος μπορεί να επιλέξει ώστε να ενθαρρύνει τη μάθηση μέσα από την επαφή των καταρτιζόμενων με πραγματικές συνθήκες λήψης απόφασης, συμπεριφορικές δραστηριότητες και ανάλυση επιλογών.
- Η πολυμεσική μάθηση είναι ο βασικός στόχος αυτού του έργου. Προκειμένου ο Ανάδοχος να διασφαλίσει ένα πολυμεσικό περιβάλλον μάθησης, οι παρουσιάσεις, τα βίντεο και η δόμηση του υλικού σε διαφορετικά εκπαιδευτικά μέσα και εκπαιδευτικά εργαλεία θα πρέπει να τηρεί προδιαγραφές της πολυμεσικής μάθησης και να διευκολύνει την επεξεργασία, κατανόηση και αφομοίωση των πληροφοριών και της παρεχόμενης γνώσης και την εύκολη και διαδραστική πλοήγηση.
- Οι προδιαγραφές αξιολόγησης της κατανόησης και αφομοίωσης της γνώσης από τους καταρτιζόμενους θα πρέπει να γίνεται με τη μέθοδο αξιολόγησης βάσει μετρήσιμων μαθησιακών αποτελεσμάτων – ταξινόμια ADDIE και να απεικονίζεται σε ανάλογες αναφορές.
- Κάθε ενότητα ή/ και υποενότητα μάθησης θα ακολουθείται από αξιολόγηση με quiz πολλαπλής ή μοναδικής επιλογής, ερωτήσεις σωστό λάθος. Προτεινόμενο μοντέλο είναι η αξιολόγηση να αποτελείται από ένα quiz αυτοαξιολόγησης και ένα βαθμολογούμενο, ανά υποενότητα μάθησης, ενώ οι ερωτήσεις θα πρέπει να αναφέρονται κυρίως σε συμπεριφορικά στοιχεία, επιλογές και αποκρίσεις σε πιθανά σενάρια σχετικά με το περιεχόμενο του εκπαιδευτικού προγράμματος και τους εκπαιδευτικούς στόχους.

Ο Ανάδοχος θα αναλάβει τον σχεδιασμό της μεθοδολογίας αξιολόγησης των αποτελεσμάτων γνώσεων, ο οποίος θα προκύπτει από σχετικά κριτήρια αξιολόγησης όπου θα συμμετέχουν οι εκπαιδευόμενοι με το πέρας της εκπαίδευσης. Πιο συγκεκριμένα, οι συμμετέχοντες θα πρέπει να συμμετάσχουν στην παραπάνω διαδικασία, η οποία θα τους αξιολογεί αυτόματα και άμεσα. Τα αποτελέσματα αυτά θα πρέπει να είναι άμεσα συγκρίσιμα και να παράγουν αναφορές με συνέπεια και συνεκτικότητα. Οι αναφορές θα απεικονίζονται και με ιεραρχικό επίπεδο της θέσης εργασίας που κατέχει κάθε υπάλληλος και ανά τμήμα όπου θα προκύπτουν συγκεντρωτικά ή ατομικά γνωστικά αποτελέσματα.

Το εκπαιδευτικό υλικό, για το οποίο ο Ανάδοχος θα έχει την επιμέλεια και επίβλεψη, σύμφωνα με τις ανάγκες και τον σχεδιασμό, θα είναι διαθέσιμο στην εκπαιδευτική πλατφόρμα και θα πρέπει να κατατεθεί ως ένα από τα παραδοτέα του έργου αυτού.

II. Σχεδιασμός και ανάπτυξη της ψηφιακής πλατφόρμας για την ασύγχρονη εξ' αποστάσεως εκπαίδευση

Το σύστημα τηλεεκπαίδευσης (E-Learning platform) θα είναι εύκολα προσβάσιμο και θα εξυπηρετεί τις ανάγκες του έργου. Το σύστημα ηλεκτρονικής εκπαίδευσης θα αποτελείται από μία πλατφόρμα ασύγχρονης τηλε-εκπαίδευσης (Learning Management System) για διαχείριση και παράδοση ασύγχρονων προγραμμάτων ηλεκτρονικής (ψηφιακής) μάθησης (e-learning). Ο Ανάδοχος θα πρέπει να διασφαλίσει ότι θα παρεμετροποιήσει και θα διαμορφώσει την αρχιτεκτονική της πλατφόρμας ώστε να μπορεί να φιλοξενήσει την εκπαιδευτική διαδικασία καθώς και τη φόρτωση και διαχείριση κάθε είδους εκπαιδευτικού υλικού, την ανταλλαγή και διάχυση πληροφορίας και την υποστήριξη κάθε είδους διεργασίας ανταλλαγής πληροφοριών. Το σύστημα θα πρέπει να μπορεί να χρησιμοποιηθεί προκειμένου να διαχειρίζονται και χρονοπρογραμματίζονται τα εκπαιδευτικά προγράμματα ασύγχρονης μορφής, οι μαθησιακές διαδικασίες καθώς η δυνατότητα διενέργειας δοκιμασιών (test)

αξιολόγησης της επίτευξης των εκπαιδευτικών στόχων και αξιολόγησης του εκπαιδευτικού προγράμματος από τους συμμετέχοντες.

Ο Ανάδοχος πριν από τον σχεδιασμό της αρχιτεκτονικής και την ανάπτυξη της εκπαιδευτικής πλατφόρμας (ή πλατφορμών), καλείται να παρουσιάσει μια ενδελεχή ανάλυση των στοιχείων που θα παρακολουθούνται δυναμικά εντός της πλατφόρμας και να ορίσει ένα σαφές, ρεαλιστικό και περιγραφικό σύστημα δεικτών για την καταγραφή του εκπαιδευτικού και επιμορφωτικού κέρδους.

Η πρόσβαση στο σύστημα τηλεκπαίδευσης θα πρέπει να μπορεί να πραγματοποιείται μέσα από δημοφιλείς φυλλομετρητές διαδικτύου που πληρούν τα διεθνή standards, όπως οι: Google Chrome, Mozilla Firefox, Microsoft Edge, από οποιοδήποτε σημείο του κόσμου, οποιαδήποτε στιγμή της ημέρας και από οποιαδήποτε συσκευή (desktop, laptop, tablet, smartphone). Δεν θα πρέπει να απαιτείται κανένα άλλο, πρόσθετο λογισμικό στη συσκευή που θα επιλέξει ο χρήστης καθώς και καμία εγκατάσταση. Όλες οι λειτουργίες και τα υποσυστήματα της εφαρμογής μπορούν να συνδυαστούν ελεύθερα. Ο σχεδιασμός και η ανάπτυξη της ψηφιακής πλατφόρμας θα πρέπει να διασφαλίζει ότι το σύστημα θα είναι άμεσα προσιτό και εύκολο στην πλοήγηση και χρήση από τους συμμετέχοντες, όπου αυτός επιθυμεί, και να υποστηρίζει τη διαχείριση μεγάλου αριθμού ενεργών χρηστών. Το σύστημα το οποίο θα διαμορφώσει ο Ανάδοχος θα πρέπει να επιτρέπει τη δημιουργία προσωπικού λογαριασμού για κάθε εκπαιδευόμενο, στον οποίο θα καταγράφεται όλη του η δραστηριότητα όπως επίσης και τα αποτελέσματα της εξέτασης/ αξιολόγησης.

Γενικές κατευθύνσεις που πρέπει να ακολουθούνται για το σύστημα τηλεκπαίδευσης:

- Το λογισμικό ασύγχρονης εκπαίδευσης θα πρέπει να παρέχει χρήσιμα εργαλεία, όπως:
 - Βαθμολόγιο
 - Ημερολόγιο
 - Helpdesk
 - Ερωτηματολόγια (Review) για τη συλλογή δεδομένων από τους καταρτιζόμενους
 - Ηλεκτρονικά τεστ (online quiz)
 - Άμεσα μηνύματα (Forum/chat) με βαθμολόγηση απαντήσεων
 - Βιβλιοθήκη περιεχομένου
 - Μικροεκπαιδεύσεις – Microlearnings
 - Αιτήματα εγγραφής εκπαιδευόμενων σε νέες εκπαιδεύσεις
 - Ενσωματωμένο σύστημα ερωτηματολογίων (survey) ανά ομάδες χρηστών
- Πολύγλωσσο περιβάλλον και περιεχόμενο.
- Δημιουργία οργανογράμματος για οργάνωση των χρηστών ανά τομέα / διεύθυνση / γεωγραφική τοποθεσία κ.ά. σε γραφικό περιβάλλον
- Δημιουργία απεριόριστων χρηστών και ομάδων χρηστών.
- Δημιουργία απεριόριστων εκπαιδεύσεων με τελική πιστοποίηση.
- Δημιουργία εκπαιδευτικών μονοπατιών.
- Υποστήριξη διαφορετικών επιπέδων διαχείρισης, χρήσης, ρόλων και ομάδων χρηστών υποστηρίζοντας τα Azure, Microsoft Active Directory ,LDAP και Google Business.

- Υποστήριξη κατάλληλων μέτρων για την προστασία των προσωπικών δεδομένων τόσο των χειριστών της εφαρμογής, όσο και ευαίσθητων πληροφοριών στο υλικό παρουσίασης, σύμφωνα με τον κανονισμό GDPR. Πιο συγκεκριμένα:
 - ο Αποδοχή/Συναίνεση συλλογής δεδομένων: Το σύστημα υποστηρίζει λειτουργικότητες καταχώρησης και καταγραφής της συναίνεσης του χρήστη αναφορικά με τη συλλογή και διαχείριση των δεδομένων που έχουν ήδη καταχωρηθεί στο σύστημα ή των δεδομένων που θα συλλεχθούν κατά τη διάρκεια των διαδικασιών κατάρτισης κρυπτογραφημένα.
 - ο Ενημέρωση περί συλλεγόμενων δεδομένων. Ο χρήστης μπορεί να ενημερωθεί αναλυτικά και με σαφή τρόπο για το ποια δεδομένα συλλέγονται, τους λόγους για τους οποίους γίνεται η συλλογή τους, τον τρόπο χρήσης τους, καθώς επίσης και για τη διάρκεια διατήρησης αυτών των δεδομένων στα συστήματα. Επίσης, μπορεί να ενημερωθεί αναλυτικά για τους όρους χρήσης του συστήματος και τις εκπαιδευτικές διαδικασίες στις οποίες θα συμμετάσχει.
- Λειτουργία αυτόματης δημιουργίας και εισαγωγής εκπαιδευτικού περιεχομένου με εφαρμογές MS Office για την θεωρία και τα ερωτηματολόγια με online editor.
- Πλήρης συμμόρφωση με την τρέχουσα έκδοση του διεθνούς προτύπου SCORM.
- Λειτουργία μέσω Web Browser και είναι συμβατό με τα διεθνή πρότυπα του W3C.
- Λειτουργία σε περιβάλλον HTTPS. Όλες οι επιμέρους λειτουργίες να παρέχονται εντός πρωτοκόλλου HTTPS και πάνω από secure channel SSL/TLS.
- Πολιτική ασφάλειας κωδικών πρόσβασης. Το σύστημα να υποστηρίζει:
 - ο Πολιτική πολυπλοκότητας κωδικών (ελάχιστο πλήθος χαρακτήρων, συμπερίληψη special characters, συμπερίληψη χαρακτήρων με κεφαλαία, συμπερίληψη αριθμητικών χαρακτήρων, αποτροπή χρήσης ακολουθίας π.χ. 1234, αποτροπή χρήσης κοινών κωδικών π.χ. qwerty).
 - ο Παραγωγή κωδικών με τυχαίο τρόπο και σύμφωνα με την πολιτική πολυπλοκότητας χωρίς την επέμβαση φυσικού προσώπου (διαχειριστή) > Διαδικασίες επαναφοράς κωδικού χωρίς ενημέρωση και χωρίς την επέμβαση φυσικού προσώπου (διαχειριστή) > Διαδικασίες υποχρεωτικής αλλαγής κωδικού (π.χ. κατά την 1η είσοδο στο σύστημα).
 - ο Διατήρηση ιστορικού κωδικών πρόσβασης και αποτροπή επαναχρησιμοποίησης παλιού κωδικού.
- Υποστήριξη αρθρωτής (modular) και ανοικτής αρχιτεκτονικής, ώστε να επιτρέπονται επεκτάσεις/αναβαθμίσεις.
- Δυνατότητα δημιουργίας πολλαπλών Portals με βάση τον ρόλο του Χρήστη (Δημόσιος τομέας, Ιδιωτικός Τομέας, Ομάδες Διεύθυνσης, Εκπαιδευτές, Εκπαιδευόμενοι, κ.ά.).
- Δυνατότητα καταγραφής της πορείας και των ενεργειών του καταρτιζόμενου (tracking-timeline) καθ' όλη τη διάρκεια εκάστου εκπαιδευτικού προγράμματος.
- Μηχανισμό χρονοπρογραμματισμού και αποστολής αυτοματοποιημένων ειδοποιήσεων μέσω e-Mail ή/και SMS, in app notifications, έτσι ώστε να παρέχονται όλες οι κατάλληλες πληροφορίες για την επιλογή της βέλτιστης διαδικασίας αποστολής σε όλες τις λειτουργίες της πλατφόρμας δυνατότητα:

- Αποστολή σε όλους: Θα γίνει αποστολή σε όσους έχουν ενεργές τις ειδοποιήσεις, και έχουν αποδεχθεί τους όρους.
- Εξαίρεση: Ο διαχειριστής μπορεί να επιλέξει ποιοι θα εξαιρεθούν της αποστολής
- Ατομική Αποστολή: Ο διαχειριστής μπορεί να επιλέξει συγκεκριμένα άτομα που θα γίνει η αποστολή
- Δεν έχουν λάβει ειδοποίηση: Ο διαχειριστής μπορεί να επιλέξει τους όσους δεν έχουν λάβει τη συγκεκριμένη ειδοποίηση από προηγούμενη αποστολή.

Το σύστημα επιπλέον θα πρέπει να διαθέτει σύστημα αναφορών έτσι ώστε να μπορούν να παράγονται αναφορές για τις ενέργειες που υποστηρίζονται από το σύστημα. Ενδεικτικά:

- Αναφορές για το σύνολο των χρηστών / ομάδα / χρήστη
- Αναφορές ανά θεματικό πεδίο / μάθημα / εξέταση / πιστοποίηση.

Που θα περιλαμβάνουν τουλάχιστον τα παρακάτω δεδομένα:

- Ποσοστό συμμετοχής (δλδ πόσοι έχουν ξεκινήσει ή ολοκληρώσει)
- Χρόνους κατανάλωσης περιεχομένου (μέσο όρο, σύνολο)
- Μέσο χρόνο ολοκλήρωσης ανά εκπαιδευτικό πρόγραμμα
- Αποτελέσματα εξετάσεων / μάθημα, αξιολόγηση, πιστοποίηση και Top 10 /100
- Ποιες ερωτήσεις εμφανίζουν συχνά λάθη ανά θεματικό πεδίο, μάθημα
- Προσωποποιημένες αναφορές επίδοσης με στατιστικά ανά γνωστικό αντικείμενο
- Αναλυτικά αποτελέσματα ερευνών
- Big data analytics για ανάλυση δεξιοτήτων που αναπτύχθηκαν με συγκεκριμένους δείκτες (KPI's)

Το σύστημα τηλεκπαίδευσης θα πρέπει να υποστηρίζει τουλάχιστον τις εξής κατηγορίες χρηστών και σχετικά δικαιώματα:

- Εκπαιδευομένους
- Εκπαιδευτές
- Διαχειριστές της πλατφόρμας εξ αποστάσεως εκπαίδευσης

Οι δυνατότητες του συστήματος σε σχέση με τον χρήστη/εκπαιδευόμενο αναφέρονται συνοπτικά παρακάτω:

- Εγγραφή στο εκπαιδευτικό πρόγραμμα
- Προβολή και παρακολούθηση εκπαιδευτικού υλικού
- Συμμετοχή σε τυποποιημένες έρευνες (αξιολόγηση εκπαιδευτικού προγράμματος) με σκοπό την έκφραση των απόψεων του εκπαιδευομένου σχετικά με το εκπαιδευτικό υλικό ή τη διαδικασία εκπαίδευσης
- Συμμετοχή σε μη υποχρεωτικά μαθήματα μικρής διάρκειας, μεγάλης ποικιλίας με συνδυασμό πολλαπλών μορφών περιεχομένου και δυνατότητα αναζήτησης με λέξεις κλειδιά.
- Συμμετοχή σε εξέταση (test αξιολόγησης) που μπορεί να έχει διάφορες μορφές ερωτήσεων όπως πολλαπλής επιλογής, σωστό-λάθος και ερωτήσεις με σύντομες απαντήσεις κ.λ.π.

- Προβολή και εκτύπωση βεβαίωσης της ολοκλήρωσης της συμμετοχής στο εκπαιδευτικό πρόγραμμα μετά την επιτυχή ολοκλήρωση του τεστ αξιολόγησης

Οι δυνατότητες του συστήματος σε σχέση με τον χρήστη Διαχειριστή αναφέρονται συνοπτικά παρακάτω.

Ως Διαχειριστής ορίζεται το στέλεχος το οποίο θα παρακολουθεί την υλοποίηση του έργου και θα είναι υπεύθυνος για τα παρακάτω (ενδεικτική και όχι εξαντλητική λίστα):

- Προσθήκη έτοιμου εκπαιδευτικού υλικού ή δημιουργίας μέσω Online editor σε ιδιαίτερα φιλικό περιβάλλον πλοήγησης και με λίγες οθόνες (wizards).
- Δημιουργία ερωτηματολογίων (Test Bank) με αυτόματη εισαγωγή από συγκεκριμένα πρότυπα MS Office.
- Δημιουργία και χρονοπρογραμματισμό του εκπαιδευτικού προγράμματος με τις απαραίτητες αυτόματες ειδοποιήσεις (SMS,email,In-app notification)
- Διαχείριση δραστηριοτήτων (quiz, αξιολογήσεις, τεστ κ.ο.κ.)
- Δημιουργία επεξεργασία και διαγραφή χρηστών οποιασδήποτε μορφής στο σύστημα και απόδοση ρόλων
- Προβολή λίστας συνδεδεμένων χρηστών στην LMS
- Διαχείριση αιτήσεων που υποβάλλονται για συμμετοχή στην εκπαίδευση
- Επικοινωνία με όλους τους χρήστες του συστήματος
- Δυνατότητα επαναφοράς της εκπαίδευσης σε μια προηγούμενη κατάσταση
- Εξαγωγή των αποτελεσμάτων όλων των εκπαιδευόμενων σε αρχεία Excel ή PDF με βάση αν ολοκλήρωσαν ή όχι το πρόγραμμα κατάρτισης και αν πέρασαν την τελική αξιολόγηση/εξέταση

Δυνατότητες του συστήματος σε σχέση με τη δημιουργία αναφορών:

Το σύστημα πρέπει να υποστηρίζει την αποτύπωση live αναφορών με κατ' ελάχιστον τις ακόλουθες κατηγορίες:

- Αναφορές αποδοχής όρων χρήσης
- Αναφορές επισκέψεων (ημερήσιες, μηνιαίες, ετήσιες)
- Αναφορές πρόσβασης κάθε κατηγορίας χρηστών με επιλογή της επιθυμητής χρονικής περιόδου
- Αποτελέσματα αξιολογήσεων, εξετάσεων, τελικών Πιστοποιήσεων.
- Καρτέλα εκπαιδευόμενου με όλα τα στοιχεία που σχετίζονται με τον συγκεκριμένο εκπαιδευόμενο και τη συμμετοχή του στο εκπαιδευτικό πρόγραμμα
- Αξιολόγηση/ εξέταση εκπαιδευόμενου, αποτελέσματα και βεβαίωση συμμετοχής του εκπαιδευόμενου

«Επικοινωνιακή Διαχείριση Κρίσεων στον Κυβερνοχώρο»

Η υιοθέτηση νέων τεχνολογιών, η συλλογή, επεξεργασία και αποθήκευση τεράστιου όγκου δεδομένων, έχουν δημιουργήσει νέους κινδύνους που απαιτούν ειδικό σχεδιασμό, προετοιμασία και αντιμετώπιση. Ακόμα και μικρής έκτασης κυβερνοεπιθέσεις, μπορούν να προκαλέσουν σοβαρά προβλήματα στην φήμη, την παραγωγικότητα και την ομαλή λειτουργία ενός οργανισμού.

Το αντικείμενο του παρόντος αφορά στον σχεδιασμό και υλοποίηση ενός εκπαιδευτικού προγράμματος με στόχο την έγκαιρη προετοιμασία και την αποτελεσματική αντίδραση της Ομάδας Διαχείρισης Κρίσεων σε περίπτωση κρίσεων στον κυβερνοχώρο.

Στόχος του προγράμματος είναι:

- α) η δημιουργία ισχυρής εταιρικής συναντίληψης σχετικά με τους κινδύνους τόσο στο «παραδοσιακό» περιβάλλον όσο και στον κυβερνοχώρο
- β) η συγκρότηση & εκπαίδευση της Ομάδας Διαχείρισης Κρίσεων στον Κυβερνοχώρο ώστε να λειτουργεί αποτελεσματικά κατά την αντιμετώπιση τέτοιων κρίσεων
- γ) η επεξεργασία των εσωτερικών διαδικασιών που πρέπει να ακολουθούνται σε περίπτωση κρίσεων στον κυβερνοχώρο και
- δ) η ανάπτυξη ειδικών δεξιοτήτων για την ορθή επικοινωνιακή διαχείριση των κρίσεων

Στο εκπαιδευτικό πρόγραμμα θα παρουσιαστούν και θα αναλυθούν στα μέλη της Ομάδας Διαχείρισης Κρίσεων τα ακόλουθα:

A. Εκτίμηση της υφιστάμενης κατάστασης/ Communication Cyber Crisis Preparedness Assessment

- Αξιολόγηση του υφιστάμενου σχεδίου επικοινωνιακής διαχείρισης κρίσεων στον κυβερνοχώρο και του βαθμού ετοιμότητας του οργανισμού
- Αξιολόγηση του επιπέδου awareness υπαλλήλων και στελεχών σχετικά με ζητήματα ασφάλειας στον κυβερνοχώρο

Β. Συγκρότηση της Ομάδας Διαχείρισης Κρίσεων στον Κυβερνοχώρο

Συγκρότηση ή αναδιάρθρωση της υφιστάμενης Ομάδας Διαχείρισης Κρίσεων με την προσθήκη νέων μελών, ανακατανομή αρμοδιοτήτων, καθορισμός ρόλων και διαδικασιών επικοινωνίας και συνεργασίας των μελών της κατά την διάρκεια μιας κρίσης στον κυβερνοχώρο.

Γ. Crisis Management Basics & Cyber Security Basics

- Οριοθέτηση cyber incident και cyber crisis
- Cyber threats landscape

Δ. Case studies

- Παρουσίαση και ανάλυση σημαντικών και περίπλοκων case studies. Αξιολόγηση της ετοιμότητας των εταιρειών που έπεσαν θύματα κυβερνοεπίθεσης, παρουσίαση και αξιολόγηση της δημόσιας αντίδρασής τους, της επικοινωνίας τους με stakeholders και κοινό κατά την διάρκεια της κρίσης.

Ε. Σχεδιασμός Σεναρίων & Ανάπτυξη της Αντίδρασης της Ομάδας Διαχείρισης Κρίσεων στον Κυβερνοχώρο (Tabletop exercise)

- Σχεδιασμός και συνδιαμόρφωση των πιθανότερων, για τον οργανισμό, σεναρίων κρίσεων στον κυβερνοχώρο
- Παρουσίαση και εξάσκηση στις τεχνικές πρόληψης και διαχείρισης κρίσεων στον κυβερνοχώρο με βάση τα προεπιλεγμένα σενάρια. Προσομοίωση σε round table περιβάλλον

ΣΤ. Διαπραγματεύσεις

Workshop στις τεχνικές διαπραγμάτευσης που πρέπει να ακολουθηθούν σε περίπτωση κρίσης στον κυβερνοχώρο με hackers, media ή άλλους stakeholders.

Ζ. Media Training

- α) Εκπαίδευση των στελεχών της Ομάδας Διαχείρισης Κρίσεων στον Κυβερνοχώρο στις τεχνικές πρόληψης και διαχείρισης επικοινωνιακών κρίσεων στον κυβερνοχώρο,
- β) Οδηγίες για σύνταξη δελτίων τύπου, δηλώσεων, non papers,
- γ) Επιλογή των κατάλληλων καναλιών επικοινωνίας και τεχνικές παρέμβασης.

Η. Παραδοτέο

Δημιουργία εξειδικευμένου οδηγού Επικοινωνιακής Διαχείρισης Κρίσεων στον Κυβερνοχώρο.

7.1.4.2.3 Διαμόρφωση πλάνου ανάκαμψης από καταστροφές για κρίσιμες οντότητες

Ο κύριος στόχος του παρόντος είναι η εκπόνηση Πλάνου Ανάκαμψης από Καταστροφές (DRP) για τις κρίσιμες υποδομές. Επιμέρους στόχοι του Σχεδίου Ανάκαμψης από Καταστροφή αφορούν τα εξής:

- καθορισμός των υποδομών και των συστημάτων με προτεραιοποίησή τους, όσον αφορά στην ετοιμότητα ανάκαμψης από καταστροφή,
- καθορισμός των παραμέτρων και των εξαρτήσεων των υποδομών και των συστημάτων, σε σχέση και με την υποδομή εφεδρείας ανάκαμψης από καταστροφή
- καθορισμός των αποδεκτών διαστημάτων απώλειας πληροφοριών από τον προηγούμενο συγχρονισμό δεδομένων (RecoveryPointObjective "RPO") και των αναγκών και αποδεκτών χρόνων ενεργοποίησης εκάστου υποσυστήματος (RecoveryTimeObjective "RTO")
- καθορισμός των αναγκών σε υποδομές εξυπηρετητών φιλοξενίας με όλα τα τεχνικά χαρακτηριστικά λειτουργίας τους και των απαραίτητων δικτυακών υποδομών
- καθορισμός του τρόπου – μεθόδου λειτουργίας των νέων συστημάτων ανάκαμψης από καταστροφή και της τεχνολογίας που θα επιλεγεί για τη συχνότητα συγχρονισμού – ενημέρωσης
- καθορισμός των αναγκών τροποποιήσεων ή αναβαθμίσεων που θα πρέπει να υλοποιηθούν στο υφιστάμενο DataCenter, για τη συνεργασία και συγχρονισμό με το DisasterRecoverySite
- καθορισμός τυχόν αναγκών για επέκταση συμβολαίων υποστήριξης των Αναδόχων των υφιστάμενων συστημάτων και υποδομών ή για υπογραφή νέων SLAs.

Για την επίτευξη των ανωτέρω στόχων, ο Ανάδοχος θα βασιστεί στις κατευθύνσεις και καλές πρακτικές του διεθνούς προτύπου ISO 22301:2012, το οποίο αποτελεί ένα πρότυπο που θεσπίζει καλές πρακτικές, ώστε:

- να συνταχθεί Πλάνο Ανάκαμψης από Καταστροφή (DRP) για τις εφαρμογές και τα συστήματα
- να αναπτυχθούν οι απαραίτητες διοικητικές και υποστηρικτικές διαδικασίες για τη συντήρηση και επικαιροποίηση τουDRP.

Επίσης θα ληφθούν υπόψη καλές πρακτικές που προκύπτουν από τα πρότυπα ISOPAS 22399:2007 και ISO/ IEC 27001:2013.

7.1.4.2.4 Εκπόνηση Μελέτης εξωτερικού και εσωτερικού περιβάλλοντος και την ανάδειξη βέλτιστων πρακτικών

Απαραίτητο συστατικό για τον αποτελεσματικό έλεγχο ασφάλειας των υποδομών και συστημάτων είναι η αντίληψη και η αξιολόγηση του ευρύτερου περιβάλλοντος στους τομείς της ασφάλειας των δικτύων / πληροφοριακών συστημάτων και της διασφάλισης του απορρήτου των επικοινωνιών.

Επομένως, θα πρέπει να διενεργηθεί μια μελέτη της κατάστασης που επικρατεί και των πρακτικών που εφαρμόζονται στον τομέα ασφάλειας σε παρεμφερή συστήματα τόσο εντός της χώρας όσο και σε διεθνές επίπεδο. Σκοπός της μελέτης αυτής είναι να δημιουργηθεί μια ολοκληρωμένη βάση γνώσης για το πλήρες ιστορικό που αφορά την ασφάλεια και στη συνέχεια να εξαχθούν χρήσιμα συμπεράσματα, τα οποία θα αξιοποιηθούν από τον Ανάδοχο για να φέρει εις πέρας τις υπόλοιπες εργασίες που απαιτούνται.

Στο πλαίσιο της εργασίας αυτής, θα συλλεχθούν και στη συνέχεια επεξεργασθούν και αναλυθούν πληροφορίες και δεδομένα που αφορούν στην ασφάλεια παρόμοιων υποδομών και συστημάτων τόσο εντός της χώρας όσο και σε άλλες χώρες. Τα δεδομένα θα εστιάσουν κατ' ελάχιστον:

- Στα υιοθετημένα Συστήματα Διαχείρισης της Ασφάλειας των Πληροφοριών (ΣΔΑΠ) και τις υποκείμενες σε αυτά διαδικασίες, πολιτικές και πρακτικές
- Στους κινδύνους ασφάλειας, στις ευπάθειες ανάλογων συστημάτων και στις μεθόδους αποτίμησης της επικινδυνότητας που συνήθως εμφανίζονται ή εφαρμόζονται αντίστοιχα
- Στις αποτελεσματικές μεθόδους παρακολούθησης της ασφάλειας ανάλογων υποδομών και συστημάτων
- Στα καταξιωμένα εργαλεία και μηχανισμούς ΤΠΕ που χρησιμοποιούνται για τον επιτυχή έλεγχο ασφάλειας ανάλογων υποδομών και συστημάτων
- Στο ιστορικό περιστατικών ασφάλειας και στις μεθόδους αντιμετώπισης αυτών, από τα οποία να μπορεί να εξαχθεί χρήσιμη γνώση για την καλύτερη διασφάλιση της ασφάλειας

Τα συστήματα που θα αποτελέσουν αντικείμενο της παρούσας μελέτης, θα μπορούν να είναι είτε δημόσια είτε ιδιωτικά, αλλά θα πρέπει να παρουσιάζουν ανάλογα επιχειρησιακά χαρακτηριστικά με αυτά της ΗΔΙΚΑ, ώστε να μπορούν στη συνέχεια να πραγματοποιηθούν οι ενέργειες παραλληλισμού μεταξύ τους και εξαγωγής χρήσιμων συμπερασμάτων. Για τη συλλογή των δεδομένων και τη δημιουργία μιας πλήρους και αντιπροσωπευτικής βάσης γνώσης ασφάλειας συστημάτων, απαιτείται όπως μελετηθούν τουλάχιστον τρεις (3) περιπτώσεις (businesscases) ανάλογων δικτύων, εκ των οποίων τουλάχιστον οι δύο (2) θα είναι οπωσδήποτε στο εξωτερικό, η καθεμία σε διαφορετική χώρα, τεχνολογικά προηγμένη όπως συγκεκριμένα είναι τα πλέον ανεπτυγμένα κράτη μέλη της Ευρωπαϊκής Ένωσης, οι ΗΠΑ, το Ισραήλ, η Ιαπωνία, η Νότια Κορέα, κλπ.

Παράλληλα με τη διερεύνηση της ασφάλειας των προαναφερθέντων έτερων συστημάτων, η παρούσα εργασία θα λάβει υπόψη και τις πλέον επιστημονικά καταξιωμένες μεθόδους και πρακτικές που εφαρμόζονται στην πρόληψη, αντιμετώπιση, και εν γένει διαχείριση της ασφάλειας παρόμοιων συστημάτων. Η πληροφορία αυτή θα αποτελέσει επίσης τμήμα της ολοκληρωμένης βάσης

7.1.4.2.5 Διαμόρφωση πολιτικής αντιγράφων ασφαλείας

Η πολιτική αντιγράφων ασφαλείας αποτελεί κρίσιμο παράγοντα για την επιχειρησιακή συνέχεια και τη δυνατότητα ανάκαμψης από καταστροφή.

Ο Ανάδοχος καλείται να διαμορφώσει πολιτική αντιγράφων ασφαλείας για τις υποδομές και τα πληροφοριακά συστήματα της ΗΔΙΚΑ, η οποία θα περιλαμβάνει κατ' ελάχιστο τα εξής:

- Συχνότητα λήψης αντιγράφων ασφαλείας
- Τύπος δεδομένων / αρχείων τα οποία θα αφορά
- Τοποθεσία και μέσο λήψης αντιγράφων
- Χρόνος διατήρησης αντιγράφων
- Αρμοδιότητες προσωπικού και προμηθευτών σχετικά με τη λήψη αντιγράφων ασφαλείας
- Διαδικασίες και κανόνες ελέγχου της ακεραιότητας των αντιγράφων

- Διαδικασία ανάκτησης δεδομένων από τα αντίγραφα ασφαλείας

7.1.4.2.6 Διαμόρφωση Συστήματος Διαχείρισης της Ασφάλειας των Πληροφοριών (ΣΔΑΠ) με βάση το πρότυπο ISO 27001 & Εκπόνηση Μελέτης Ανάλυσης και Αξιολόγησης Κινδύνων

Για τη διαμόρφωση ενός ολοκληρωμένου ΣΔΑΠ για την ΗΔΙΚΑ, ο Ανάδοχος θα πραγματοποιήσει τις ενέργειες που αναφέρονται στο πρότυπο ISO 27001 συμπεριλαμβανομένου του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR) και αφορούν στη Φάση "Plan" που αναφέρεται στο πρότυπο, όπως κατ' ελάχιστον αναφέρονται οι ακόλουθες:

- Θα ορίσει το Πεδίο Εφαρμογής του ΣΔΑΠ (scope and boundaries of the ISMS), όσον αφορά τα επιχειρησιακά χαρακτηριστικά της ΗΔΙΚΑ και τα αγαθά που πρέπει να προστατευθούν. Παράλληλα, θα καταγράψει τις συνιστώσες εκείνες του περιβάλλοντος που δεν θα περιλαμβάνονται στο πεδίο εφαρμογής, συνοδευμένες από κατάλληλη τεκμηρίωση για την εξαίρεση τους
- Θα ορίσει την πολιτική του ΣΔΑΠ, όσον αφορά το ευρύτερο περιβάλλον λειτουργίας
- Θα ορίσει τη μεθοδολογία αποτίμησης της επικινδυνότητας που θα εφαρμοστεί
- Θα προσδιορίσει τους κινδύνους που ενέχονται στη λειτουργία του Δικτύου
- Θα αναλύσει και θα εκτιμήσει τους κινδύνους αυτούς
- Θα προσδιορίσει και υπολογίσει μεθόδους για την αντιμετώπιση των κινδύνων
- Θα επιλέξει κατάλληλα σημεία ελέγχου (controls) αντιμετώπισης των κινδύνων
- Θα μεριμνήσει για να λάβει την έγκριση της Διοίκησης της ΗΔΙΚΑ όσον αφορά τους προτεινόμενους υπολειμματικούς κινδύνους
- Θα μεριμνήσει για να λάβει την έγκριση της Διοίκησης της ΗΔΙΚΑ για να υλοποιήσει και να λειτουργήσει το υιοθετημένο ΣΔΑΠ
- Θα προετοιμάσει μια Δήλωση Εφαρμοσιμότητας (Statement of Applicability), η οποία θα περιλαμβάνει τα προβλεπόμενα στο πρότυπο ISO 27001.

Στο πλαίσιο των ενεργειών διαμόρφωσης του ΣΔΑΠ, θα πραγματοποιήσει κατ' ελάχιστον τις παρακάτω εργασίες, τα αποτελέσματα των οποίων θα συμπεριληφθούν κατά περίπτωση στις πολιτικές, διαδικασίες σχέδια και λοιπά έγγραφα του ΣΔΑΠ.

Ανάλυση επιχειρησιακών επιπτώσεων

Ο Ανάδοχος θα εκπονήσει ανάλυση επιχειρησιακών επιπτώσεων, με την οποία θα εντοπίσει και καταγράψει τις επιχειρησιακές λειτουργίες και τους πόρους που υποστηρίζουν τις λειτουργίες αυτές και σχετίζονται ή μπορεί να επηρεάσουν την ακεραιότητα των υποδομών της ΗΔΙΚΑ και τη διαθεσιμότητα των παρεχόμενων από αυτήν υπηρεσιών.

Ανάλυση κινδύνου και αποτίμηση επικινδυνότητας

Ο Ανάδοχος θα πραγματοποιήσει μελέτη ανάλυσης κινδύνου και αποτίμησης επικινδυνότητας, προκειμένου να αναγνωρίσει και αναλύσει τις ενδεχόμενες απειλές στην ακεραιότητα των υποδομών.

Στο πλαίσιο της εργασίας αυτής, ο Ανάδοχος κατ' ελάχιστον:

- Θα μελετήσει και καταγράψει όλες τις απειλές και κινδύνους που πιθανά αντιμετωπίζει ή αναμένεται να αντιμετωπίσουν οι υποδομές.
- Θα κατηγοριοποιήσει και εξετάσει τις απειλές που θα αναγνωρίσει σε (α) ενδογενείς, οι οποίες προέρχονται από το εσωτερικό του συστήματος και εξαρτώνται από το επίπεδο της εσωτερικής αξιοπιστίας, ασφάλειας και ανθεκτικότητας, σε (β) εξωγενείς, οι οποίες προέρχονται από το εξωτερικό περιβάλλον, όπως καιρικές συνθήκες, φυσικές καταστροφές κλπ και (γ) σε απειλές που προέρχονται από άλλα διασυνδεδεμένα συστήματα ή δίκτυα. Παράλληλα, θα διενεργηθεί εκτίμηση της σοβαρότητας κάθε απειλής.
- Θα διενεργήσει μια συσχέτιση μεταξύ των διαθέσιμων πόρων (πληροφοριακά συστήματα, δίκτυα, εγκαταστάσεις, ανθρώπινο δυναμικό) και των εκτιμώμενων απειλών που δύναται να τους επηρεάσουν εφόσον εκδηλωθούν.
- Θα καταγράψει τα ευάλωτα σημεία και τις αδυναμίες των πόρων που απαιτούνται για τη συνέχιση κάθε επιχειρησιακής λειτουργίας. Στη συνέχεια θα αξιολογήσει την πιθανότητα εκδήλωσης των απειλών που έχει ήδη αναγνωρίσει και θα εκτιμήσει την επίδραση τους στη λειτουργία συστημάτων και υποδομών και τη διάθεση των παρεχόμενων υπηρεσιών.
- Θα αναλύσει τις ανάγκες και απαιτήσεις προστασίας.
- Θα προσδιορίσει και προτείνει τη διαδικασία που θα ακολουθήσει καθώς και τα μέτρα που θα λάβει, προκειμένου να αντιμετωπίσει κάθε ενδεχόμενη απειλή
- Θα προτείνει διαδικασίες αξιολόγησης της αποτελεσματικότητας των μέτρων που προτείνει να εφαρμοσθούν κατά περίπτωση απειλής.

Διαμόρφωση πολιτικών ασφάλειας κρίσιμων οντοτήτων με στόχο την ανάδειξη τεχνικών και οργανωτικών μέτρων για την προστασία τους από Κυβερνοαπειλές

Η διαμόρφωση πολιτικών θα πρέπει να είναι κατάλληλα δομημένη, ώστε να καλύπτει όλες τις παραμέτρους / συνιστώσες λειτουργίας των κρίσιμων υποδομών της ΗΔΙΚΑ. Ειδικότερα, θα γίνει σαφής αναφορά και ανάλυση στα ακόλουθα:

- Εύρος των πολιτικών. Αρχικά θα προσδιοριστεί το σύνολο των αγαθών των κρίσιμων υποδομών της ΗΔΙΚΑ, για τα οποία θα διαμορφωθούν οι πολιτικές και στη συνέχεια θα προσδιοριστούν και αναλυθούν οι απειλές που αντιμετωπίζουν τα αγαθά αυτά
- Ασφάλεια των υποδομών, των πληροφοριακών συστημάτων και των υποκείμενων δεδομένων
 - ο Φυσική ασφάλεια (μέθοδοι υλοποίησης, κανόνες προστασίας, κλπ)
 - ο Ασφάλεια δικτύου (VPNs, ασφάλεια συνδέσεων, συνδέσεις εξωτερικών συνεργατών, κανόνες πρόσβασης στο δικτυακό εξοπλισμό, κανόνες χρησιμοποίησης δικτύου, κλπ)
 - ο Ασφάλεια εξυπηρετητών (Διαχείριση, πρόσβαση, λογισμικό, δικτυακές υπηρεσίες, αναβάθμιση, προσθήκη νέου συστήματος, κλπ)
 - ο Συστήματα χρηστών (κανόνες ασφάλειας, διαχείριση χρηστών, λογισμικό χρηστών, πολιτικών κωδικών πρόσβασης (passwords))
 - ο Κακόβουλο λογισμικό
- Προστασία πληροφοριών (έλεγχος διασποράς στοιχείων, κρυπτογράφηση δεδομένων, διαχείριση στοιχείων που δίνονται σε τρίτους, κλπ)

Υλοποίηση και λειτουργία του ΣΔΑΠ

Για την υλοποίηση και λειτουργία του υιοθετημένου ΣΔΑΠ, ο Ανάδοχος θα πραγματοποιήσει τις ενέργειες που αναφέρονται στο πρότυπο ISO 27001 συμπεριλαμβανομένου του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR) και αφορούν στη Φάση "Do" που αναφέρεται στο πρότυπο, όπως κατ' ελάχιστον αναφέρονται οι ακόλουθες:

- Θα αναπτύξει ένα σχέδιο αντιμετώπισης των κινδύνων (risk treatment plan), το οποίο προσδιορίζει τις κατάλληλες ενέργειες που πρέπει να γίνουν για την ορθή διαχείριση των κινδύνων ασφάλειας
- Θα υλοποιήσει το σχέδιο αντιμετώπισης κινδύνων, ώστε να επιτύχει τους αντίστοιχους στόχους που έχουν τεθεί
- Θα υλοποιήσει τα σημεία ελέγχου (controls) για την αντιμετώπιση των κινδύνων, που έχουν επιλεγεί κατά τη φάση διαμόρφωσης του ΣΔΑΠ, ώστε να επιτευχθούν οι αντίστοιχοι στόχοι
- Θα ορίσει τους δείκτες με τους οποίους θα μετριέται η αποτελεσματικότητα των επιλεγθέντων μέτρων αντιμετώπισης και στη συνέχεια θα προσδιορίσει την αποτελεσματικότητα των δεικτών αυτών στην παραγωγή συγκρίσιμων και αναπαραγωγίμων αποτελεσμάτων
- Θα υλοποιήσει προγράμματα εκπαίδευσης και ευαισθητοποίησης
- Θα διαχειριστεί τη λειτουργία του ΣΔΑΠ
- Θα διαχειριστεί τους απαιτούμενους πόρους για τη λειτουργία του ΣΔΑΠ
- Θα υλοποιήσει διαδικασίες και όποια άλλα μέτρα κρίνει, ώστε να καταστεί δυνατή η έγκαιρη ανίχνευση περιστατικών ασφάλειας και η αποτελεσματική ανταπόκριση σε αυτά
- Θα προσδιορίσει και στη συνέχεια μεριμνήσει να διαθέσει τους πόρους που απαιτούνται:
 - ο για την ορθή διαμόρφωση, υλοποίηση, παρακολούθηση, ανασκόπηση, συντήρηση και βελτίωση του ΣΔΑΠ
 - ο ώστε να διασφαλιστεί ότι οι υιοθετημένες διαδικασίες ασφάλειας των πληροφοριών υποστηρίζουν τις επιχειρησιακές απαιτήσεις
 - ο για να προσδιοριστούν και αντιμετωπιστούν οι απαιτήσεις που προέρχονται από το υφιστάμενο νομικό ή ρυθμιστικό πλαίσιο καθώς και οι ενδεχόμενες συμβατικές υποχρεώσεις
 - ο Διατηρήσει ένα επαρκές επίπεδο ασφάλειας, εφαρμόζοντας κατάλληλα τα επιλεγμένα μέτρα ελέγχου για την αντιμετώπιση των κινδύνων
 - ο Εκπονεί ανασκοπήσεις του ΣΔΑΠ, όποτε κριθεί απαραίτητο και στη συνέχεια να ανταποκρίνεται κατάλληλα, ανάλογα με τα πορίσματα των ανασκοπήσεων αυτών
 - ο Να βελτιώνει την αποτελεσματικότητα του ΣΔΑΠ, όπου κριθεί απαραίτητο
- Θα εκπονήσει προγράμματα εκπαίδευσης και ευαισθητοποίησης σε όλα τα στελέχη της Αναθέτουσας Αρχής και του Φορέα Λειτουργίας, στα οποία τους έχουν ανατεθεί αρμοδιότητες που ορίζονται στο υιοθετημένο ΣΔΑΠ, ώστε αυτά να καταστούν ικανά να προβούν στην επιτυχή άσκηση των καθηκόντων τους.

Παρακολούθηση και ανασκόπηση του ΣΔΑΠ

Για την παρακολούθηση και ανασκόπηση του υιοθετημένου ΣΔΑΠ, ο Ανάδοχος θα πραγματοποιήσει τις ενέργειες που αναφέρονται στο πρότυπο ISO 27001 συμπεριλαμβανομένου του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR) και αφορούν στη Φάση "Check" που αναφέρεται στο πρότυπο, όπως κατ' ελάχιστον αναφέρονται οι ακόλουθες:

- Θα πραγματοποιήσει κατάλληλες διαδικασίες και ενέργειες παρακολούθησης και ανασκόπησης του ΣΔΑΠ
- Θα πραγματοποιεί τακτικές ανασκοπήσεις της αποτελεσματικότητας του ΣΔΑΠ, λαμβάνοντας υπόψη τα ευρήματα των εσωτερικών ελέγχων που θα πραγματοποιεί, τα συμπεράσματα που

θα προκύπτουν από τα περιστατικά ασφάλειας που έχουν συμβεί, καθώς και τις προτάσεις άλλων εμπλεκόμενων φορέων

- Θα μετρήσει την αποτελεσματικότητα των μέτρων αντιμετώπισης των κινδύνων, ώστε να επιβεβαιώσει ότι ικανοποιούνται οι απαιτήσεις ασφάλειας
- Θα προβεί σε ανασκόπηση της αποτίμησης επικινδυνότητας σε τακτά χρονικά διαστήματα και των υπολειμματικών κινδύνων (residual risks) καθώς και τα επίπεδα κινδύνου που θεωρήθηκαν αποδεκτά, λαμβάνοντα υπόψη τα πλέον πρόσφατα δεδομένα
- Θα διενεργεί εσωτερικούς ελέγχους ασφάλειας σε τακτά χρονικά διαστήματα (που θα οριστούν επακριβώς κατά την Φάση ανάλυσης απαιτήσεων του έργου)
- Θα μεριμνήσει για την ανασκόπηση του υιοθετημένου ΣΔΑΠ από το αρμόδιο όργανο σε τακτά χρονικά διαστήματα
- Θα επικαιροποιεί τα σχέδια ασφάλειας, λαμβάνοντας υπόψη τα ευρήματα από τις ενέργειες παρακολούθησης και ανασκόπησης του ΣΔΑΠ
- Θα καταγράφει τις ενέργειες και τα γεγονότα, που θα μπορούσαν να έχουν επίπτωση στην αποτελεσματικότητα ή στην απόδοση του υιοθετημένου ΣΔΑΠ.

Συντήρηση και βελτίωση του ΣΔΑΠ

Για τη συντήρηση και βελτίωση του υιοθετημένου ΣΔΑΠ, ο Ανάδοχος θα πραγματοποιήσει τις ενέργειες που αναφέρονται στο πρότυπο ISO 27001 συμπεριλαμβανομένου του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR) και αφορούν στη Φάση "Act" που αναφέρεται στο πρότυπο, όπως κατ' ελάχιστον αναφέρονται οι ακόλουθες:

- Θα πραγματοποιήσει τις βελτιώσεις στο ΣΔΑΠ, που έχουν προσδιοριστεί
- Θα προβεί σε κατάλληλες διορθωτικές και προληπτικές ενέργειες, εφαρμόζοντας τα ευρήματα της αποτύπωσης κατάστασης και ειδικότερα τις βέλτιστες πρακτικές της Παρ. 1.3.1 και των υποπαραγράφων αυτής.
- Θα επικοινωνήσει τις ενέργειες βελτίωσης σε όλα τα εμπλεκόμενα μέρη, με όλα τα απαραίτητα στοιχεία και λεπτομέρειες
- Θα διασφαλίσει ότι οι πραγματοποιημένες βελτιώσεις επιτυγχάνουν το σχετικό στόχο τους.

7.1.4.2.7 Διενέργεια ελέγχων διεξόδους εξωτερικών δικτύων, εφαρμογών Ιστού, φυσικής ασφάλειας και διαρροής δεδομένων

Έλεγχοι διεξόδους εξωτερικών δικτύων

Στο σύγχρονο περιβάλλον κυβερνοαπειλών κάθε ευπάθεια μπορεί να αποτελέσει αντικείμενο εκμετάλλευσης με καταστροφικές συνέπειες. Οι έλεγχοι διεξόδους εξωτερικών δικτύων (external network penetration test) εντοπίζουν ευπάθειες σε υποδομές, συσκευές και διακομιστές που είναι προσβάσιμες από το διαδίκτυο.

Οι έλεγχοι προσομοιάζουν τις επιθέσεις κακόβουλων εισβολέων, οι οποίοι έχουν ως στόχο τη ναπόκτηση πρόσβαση σε συστήματα και τις εφαρμογές της περιμέτρου. Η μέθοδοι εκτέλεσης των ελέγχων θα πρέπει να εξασφαλίζουν ότι δεν θα προκληθούν φθορές ή οποιουδήποτε τύπου προβλήματα στη λειτουργία υποδομών και συστημάτων.

Έλεγχοι διεξόδους εφαρμογών ιστού

Οι δοκιμές διεξόδους διαδικτυακών εφαρμογών στοχεύουν στον εντοπισμό τρωτών σημείων ασφαλείας που προκύπτουν από ανασφαλείς πρακτικές ανάπτυξης στη δημιουργία τη σχεδίαση και τη διαχείριση του λογισμικού ή ιστότοπου. Οι διαδικτυακές εφαρμογές χρησιμοποιούνται όλο και περισσότερο και αποτελούν κατεξοχήν στόχο κακόβουλων επιθέσεων. Στα πλαίσια των ελέγχων θα

πρέπει να πραγματοποιηθεί μια σειρά προσομοιωμένων επιθέσεων, οι οποίες προσομοιάζουν κακόβουλες επιθέσεις, με σκοπό την αποτύπωση κάθε ευπάθειας και τη συνολική αποτίμηση του βαθμού ασφάλειας μιας εφαρμογής.

Έλεγχοι Φυσικής Ασφάλειας

Ο έλεγχος φυσικής ασφάλειας αξιολογεί τα μέτρα ασφαλείας που προστατεύουν τα περιουσιακά στοιχεία του οργανισμού από απειλές και στοχεύει σε προτάσεις για τυχόν βελτιώσεις. Οι έλεγχοι πρέπει να σχεδιάζονται με στόχο την παραβίαση της φυσικής ασφάλειας μίας ή περισσότερων τοποθεσιών. Τα σενάρια θα πρέπει να καθοριστούν βάσει ανάλυσης των υποδομών, με στόχο τη μη εξουσιοδοτημένη πρόσβαση σε φυσικές τοποθεσίες και πρόσβαση στο εσωτερικό δίκτυο με τη χρήση ειδικών συσκευών.

Ο υποψήφιος ανάδοχος καλείται να περιγράψει στην τεχνική του προσφορά τη μεθοδολογία εκτέλεσης των ελέγχων.

Έλεγχοι Διαρροής Δεδομένων

Οι έλεγχοι διαρροής δεδομένων αφορούν στη συγκέντρωση, ανάλυση και αξιολόγηση της βαρύτητας και του βαθμού ευαισθησίας πληροφοριών του οργανισμού από διάφορες πηγές (συμπεριλαμβανομένου του σκοτεινού διαδικτύου).

Ο έλεγχος θα πρέπει να αφορά πληθώρα δεδομένων, όπως ενδεικτικά ονόματα χρήστη και κωδικοί χρηστών, μηνύματα ηλεκτρονικού ταχυδρομείου κλπ. Στη συνέχεια θα πρέπει να προτείνονται μέτρα για την αντιμετώπιση ή το μετριασμό των συνεπειών της διαρροής και την αποφυγή της επανάληψής της.

Ο υποψήφιος ανάδοχος καλείται να περιγράψει στην τεχνική του προσφορά τη μεθοδολογία εκτέλεσης των ελέγχων.

Ο υποψήφιος ανάδοχος καλείται να περιγράψει στην τεχνική του προσφορά τη μεθοδολογία εκτέλεσης του συνόλου των παραπάνω ελέγχων.

7.1.4.2.8 Αξιοποίηση τεχνολογικής καινοτομίας και ερευνητικής πρωτοπορίας

Η διασφάλιση επαρκούς Επιχειρησιακής Συνέχειας, ειδικά απέναντι στο ενδεχόμενο κυβερνοεπιθέσεων, προϋποθέτει συνδυαστικές δράσεις πολλαπλής στόχευσης. Από τη μια πλευρά πρέπει να υπάρχει συστηματική μέριμνα για την αντιμετώπιση ήδη γνωστών τύπων κυβερνοαπειλών, με χρήση βέλτιστων πρακτικών και διαθέσιμων αποτελεσματικών τεχνολογιών. Από την άλλη, πρέπει να υπάρχει επίσης μέριμνα για την αντιμετώπιση καινοφανών κυβερνοεπιθέσεων, με αξιοποίηση προηγμένων μεθοδολογιών και τεχνολογικών λύσεων, όπως αυτές προκύπτουν, προδιαγράφονται και αξιολογούνται σε εξειδικευμένα ακαδημαϊκά ερευνητικά περιβάλλοντα.

Δεδομένων των ρηξικέλευθων εξελίξεων σε θέματα Κυβερνοασφάλειας, ο συνδυασμός βέλτιστων πρακτικών, δοκιμασμένων λύσεων και προηγμένων (state-of-the-art) μεθοδολογιών και τεχνολογιών αποτελεί το επαρκέστερο μέσο διασφάλισης της Επιχειρησιακής Συνέχειας. Συνεπώς, τα ζητούμενα πληροφοριακά συστήματα, τεχνολογικά προϊόντα και εξειδικευμένες υπηρεσίες θα πρέπει να παρέχονται με τρόπο που εγγυάται ότι όχι μόνο τα καταλληλότερα διαθέσιμα συστήματα της Αγοράς, αλλά και οι πρωτότυπες μεθοδολογίες και τεχνολογίες που παρέχει ο σχετικά εξειδικευμένος ακαδημαϊκός τομέας θα αξιοποιούνται συνδυαστικά.

Επιπρόσθετα, οι δόκιμες μεθοδολογίες και τεχνολογίες διασφάλισης της Επιχειρησιακής Συνέχειας προϋποθέτουν τακτικούς και συστηματικούς ελέγχους (penetration tests), αξιολογήσεις (audits), πιστοποιήσεις (certifications), μελέτες ανάλυσης και διαχείρισης επικινδυνότητας (risk analysis and management) κλπ., οι οποίες πρέπει να εκπονούνται σύμφωνα με διεθνή πρότυπα και αντίστοιχες καλές πρακτικές. Οι αδιαμφισβήτητες αυτές αναγκαιότητες, με τη σειρά τους, προϋποθέτουν συνθήκες λειτουργικής ανεξαρτησίας και αβίαστων επιστημονικών αποτιμήσεων, κάτι που μπορεί να εξυπηρετηθεί αποτελεσματικά με τη συνδρομή του εξειδικευμένου ακαδημαϊκού τομέα.

7.1.4.3 Εξειδικευμένες Λύσεις Ασφάλειας Πληροφοριών, Εγγράφων και εφαρμογών

7.1.4.3.1 Λύση Διαβάθμισης και Σήμανσης Εγγράφων

Η λύση Διαβάθμισης εγγράφων (Documents Classification) θα πρέπει να δίνει τη δυνατότητα στον χρήστη να επιλέξει και να αποδώσει με απλές κινήσεις, το κατάλληλο επίπεδο διαβάθμισης σε ένα έγγραφο, με βάση την Πολιτική Ασφάλειας του Φορέα. Το επιλεγμένο επίπεδο διαβάθμισης θα πρέπει να συνοδεύει το έγγραφο μέσω κατάλληλης σήμανσης στα μεταδεδομένα (metadata), αλλά και στην εμφάνιση του εγγράφου, ώστε να καθίσταται ορατό στους χρήστες, να εντείνεται η εγρήγορση του χρήστη (awareness) και να αποφεύγεται η κακή χρήση του εγγράφου λόγω αμέλειας. Η λύση Διαβάθμισης εγγράφων θα πρέπει να συμπληρώνει και να αναδεικνύει της δυνατότητες του συστήματος DLP.

7.1.4.3.2 Λύση Προστασίας Δεδομένων από Διαρροή

Η επέκταση της ψηφιακής διαχείρισης εγγράφων σε συνδυασμό με τη διαθεσιμότητα πληθώρας διαφορετικών μεθόδων για την αποστολή και γενικά τη διακίνηση εγγράφων, έχει δημιουργήσει επιπλέον κινδύνους για τη διαρροή κρίσιμων εγγράφων εκτός του οργανισμού. Η λύση αποτροπής διαρροής πληροφοριών θα πρέπει να ανιχνεύει και να προλαμβάνει τη διακίνηση ευαίσθητων και εμπιστευτικών εγγράφων μέσω κάθε δυνατής οδού πχ μέσω αποσπώμενων αποθηκευτικών μέσων (usb), μέσω αλληλογραφίας (email), μέσω δικτυακής μεταφοράς αρχείων (ftp), μέσω internetupload, κλπ.

Η λύση θα πρέπει να εκμεταλλεύεται τη σήμανση των εγγράφων από λύσεις διαβάθμισης εγγράφων, για τον εντοπισμό ευαίσθητων και εμπιστευτικών εγγράφων.

7.1.4.3.3 Λύση Διαχείρισης Δικαιωμάτων Εγγράφων

Για την αποτελεσματική προστασία των εγγράφων του οργανισμού τα οποία πρέπει να υποστούν επεξεργασία από απομακρυσμένους χρήστες ή να διατηρηθούν σε υποδομές εκτός της περιμέτρου του οργανισμού, απαιτείται μία λύση διαχείρισης των δικαιωμάτων χρήσης των εγγράφων αυτών η οποία να επιτρέπει τον καθορισμό των δικαιωμάτων πρόσβασης στα έγγραφα αυτά και τον απομακρυσμένο έλεγχο τους (IRM - Information Rights Management). Η λύση πρέπει να προστατεύει τον οργανισμό από επιχειρηματικούς και κανονιστικούς κινδύνους που σχετίζονται με την μη αποδεκτή χρήση των εγγράφων του οργανισμού από εξωτερικούς συνεργάτες ή την χρήση τους για σκοπούς μη συμβατούς με τους σκοπούς επεξεργασίας που θέτει ο οργανισμός.

Η λύση πρέπει να είναι εύχρηστη ώστε οι κανόνες και οι πολιτικές προστασίας των εγγράφων να καθορίζονται από τους ίδιους τους χρήστες χωρίς να απαιτείται πάντα η εμπλοκή του τμήματος Πληροφορικής (IT). Οι κανόνες και οι πολιτικές προστασίας εγγράφων πρέπει να εφαρμόζονται είτε σε μεμονωμένους χρήστες είτε σε ομάδες χρηστών και να δίνουν την δυνατότητα στους ιδιοκτήτες των εγγράφων όχι μόνο να καθορίζουν τους χρήστες που έχουν δικαίωμα πρόσβασης στα έγγραφα, αλλά και να εποπτεύουν την χρήση των εγγράφων ή να ανακαλούν τα δικαιώματα πρόσβασης. Η λύση πρέπει να δίνει τη δυνατότητα εφαρμογής πολιτικών και κανόνων προστασίας είτε σε μεμονωμένα έγγραφα είτε σε ομάδες εγγράφων που διατηρούνται σε φακέλους, **filesystems**, κλπ.

Αναλυτικότερα η λύση πρέπει να έχει τα χαρακτηριστικά που περιγράφονται στις επόμενες παραγράφους.

Καθορισμός δικαιωμάτων χρήσης και απομακρυσμένος έλεγχος επί των εγγράφων

- Η λύση πρέπει να επιτρέπει τον καθορισμό του είδους των δικαιωμάτων που έχει κάθε χρήστης επί του εγγράφου (πχ μόνο ανάγνωση, επεξεργασία, ορισμός δικαιούχων, κλπ)
- Η λύση πρέπει να δίνει την δυνατότητα εξ αποστάσεως αναίρεσης των δικαιωμάτων που έχουν παραχωρηθεί σε χρήστες ή διαγραφής ενός εγγράφου
- Η λύση πρέπει να δίνει την δυνατότητα ορισμού ημερομηνιών λήξης της ισχύος των δικαιωμάτων πρόσβασης.
- Η λύση πρέπει να δίνει την δυνατότητα σε διαχειριστές να καθορίζουν πολιτικές πρόσβασης και σε χρήστες να εφαρμόζουν αυτές τις πολιτικές πρόσβασης σε έγγραφα.

Απόδοση δικαιωμάτων σε χρήστες

- Η λύση πρέπει να έχει την δυνατότητα να αποδίδει συγκεκριμένα δικαιώματα πρόσβασης είτε σε μεμονωμένους χρήστες είτε σε ομάδες χρηστών.
- Η λύση πρέπει να δίνει την δυνατότητα καθορισμού των διαδικτυακών διευθύνσεων από τις οποίες επιτρέπεται η πρόσβαση στα έγγραφα.
- Η λύση πρέπει να αναγνωρίζει και να αυθεντικοποιεί τους χρήστες του οργανισμού μέσω πλήρους λειτουργικής διασύνδεσης με το AD του οργανισμού.
- Η λύση πρέπει να έχει την δυνατότητα απόδοσης συγκεκριμένων δικαιωμάτων πρόσβασης σε χρήστες που ανήκουν σε συγκεκριμένες ομάδες του οργανισμού (ActiveDirectorygroups).
- Η λύση πρέπει να δίνει την δυνατότητα να καθορίζονται ονομαστικά οι χρήστες (εσωτερικοί ή εξωτερικοί) στους οποίους επιτρέπεται η πρόσβαση στα έγγραφα του οργανισμού καθώς και το είδος της πρόσβασης που παρέχεται.
- Η λύση πρέπει να έχει την δυνατότητα αποστολής ειδοποιήσεων/προσκλήσεων (invitations) σε εξωτερικούς χρήστες στους οποίους παραχωρείται πρόσβαση σε ένα έγγραφο.
- Οι χρήστες στους οποίους αποδίδεται δικαίωμα πρόσβασης πρέπει να μπορούν να διαχειρίζονται το έγγραφο χωρίς την χρήση ειδικών προγραμμάτων (transparency).

Είδη εγγράφων φάκελοι και μέσα αποθήκευσης

- Η λύση πρέπει να δίνει την δυνατότητα καθορισμού δικαιωμάτων πρόσβασης είτε σε διακριτά έγγραφα είτε σε όλα τα έγγραφα που διατηρούνται σε συγκεκριμένα διακριτά σημεία διατήρησης (φακέλους ή μέσα αποθήκευσης).
- Η λύση πρέπει να δίνει δυνατότητα καθορισμού δικαιωμάτων πρόσβασης σε αρχεία που διατηρούνται είτε σε τοπικούς servers είτε σε εφαρμογές νέφους (Office365, Dropbox, Sharepoint, κλπ).
- Ο τρόπος διαχείρισης των δικαιωμάτων πρόσβασης θα πρέπει να είναι ίδιος ανεξάρτητα από το μέσο διατήρησης των αρχείων (πχ. τοπικοί servers, ή εφαρμογές cloud).

Συμβατότητα και αλληλεπίδραση με εφαρμογές τρίτων κατασκευαστών

- Η λύση πρέπει να έχει πλήρη συμβατότητα με τις εφαρμογές του MicrosoftOffice και να δίνει δυνατότητα στους χρήστες των εφαρμογών να καθορίζουν τα δικαιώματα επί των εγγράφων μέσα από το περιβάλλον των ίδιων των εφαρμογών.
- Η λύση πρέπει να έχει πλήρη συμβατότητα με τις εφαρμογές Outlook και Exchange.
- Η λύση πρέπει να έχει δυνατότητα καθορισμού δικαιωμάτων και σε αρχεία pdf.
- Η λύση πρέπει να έχει την δυνατότητα λειτουργικής διασύνδεσης με λύση DLP (DataLossPrevention).
- Η λύση να έχει πλήρη συμβατότητα με την εφαρμογή SIEM

7.1.4.3.4 Λύση Διαχείρισης Λογαριασμών και Δικαιωμάτων Πρόσβασης Χρηστών

Η λύση Διαχείρισης Λογαριασμών και Δικαιωμάτων πρόσβασης χρηστών (Identity & Access Rights Management - IAM) θα πρέπει να διασυνδέεται και να επικοινωνεί με τα Πληροφοριακά Συστήματα του Οργανισμού (πιο συγκεκριμένα να διατεθούν adapters με τον ActiveDirectory και με μία βάση (Oracle ή MSSQL) του Φορέα , ώστε να ενημερώνεται σε πραγματικό χρόνο για τα accounts και τα δικαιώματα που διατηρούνται σε κάθε πληροφοριακό σύστημα. Επιπρόσθετα, η λύση IAM θα πρέπει να διασυνδέεται με το πληροφοριακό σύστημα στο οποίο διατηρείται το μητρώο των εργαζομένων και συνεργατών του Οργανισμού, ώστε να ενημερώνεται σε πραγματικό χρόνο για τα φυσικά πρόσωπα που εργάζονται για τον Οργανισμό, την θέση και τον ρόλο τους, καθώς και για οποιαδήποτε σχετική αλλαγή.

Βασική λειτουργικότητα της λύσης IAM θα πρέπει να είναι η αντιστοίχιση κάθε λογαριασμού (Account) σε φυσικό πρόσωπο, ώστε να μην υπάρχουν λογαριασμοί με άγνωστο ιδιοκτήτη, αλλά και ο εντοπισμός οποιουδήποτε λογαριασμού δημιουργείται από ανώνυμο εισβολέα. Με τον τρόπο αυτό, θα πρέπει να εξασφαλίζεται ότι για κάθε λογαριασμό υπάρχει κάποιο φυσικό πρόσωπο που φέρει την ευθύνη του, και ότι για κάθε εξουσιοδοτημένο χρήστη υπάρχει πλήρης εικόνα για τα δικαιώματα πρόσβασης που του έχουν αποδοθεί. Η λύση IAM θα πρέπει να έχει τη δυνατότητα να αυτοματοποιεί τις ροές εργασιών μέσω από τις οποίες δημιουργούνται ή αναιρούνται λογαριασμοί και δικαιώματα πρόσβασης, να αποφεύγονται ανθρώπινα λάθη και παραλείψεις κατά την απόδοση ή αναίρεση λογαριασμών και δικαιωμάτων πρόσβασης.

7.1.4.3.5 Λύση Διαχείρισης Προνομιούχων Λογαριασμών Πρόσβασης

Ορισμένοι χρήστες έχουν πρόσθετα δικαιώματα, λόγω της φύσης του ρόλου που επιτελούν εντός του οργανισμού. Για τον λόγο αυτό, απαιτείται η ύπαρξη επιπλέον μηχανισμών που θα προστατεύουν από μη εξουσιοδοτημένη χρήση των λογαριασμών των εν λόγω χρηστών. Η λύση θα πρέπει να περιλαμβάνει κατ' ελάχιστο:

- Ασφαλή διαχείριση των κωδικών πρόσβασης των διαχειριστών συστημάτων και εφαρμογών, συμπεριλαμβανομένου ασφαλούς αποθετηρίου των κωδικών πρόσβασης.
- Μηχανισμούς επιβολής κανόνων συνθετότητας και αποφυγής ανακύκλωσης των κωδικών πρόσβασης και προσωποποίησης των κοινόχρηστων (Shared) accounts
- Μηχανισμούς λογοδοσίας για τη χρήση των λογαριασμών
- Καταγραφή των ενεργειών των διαχειριστών σε κρίσιμα συστήματα και εφαρμογές

7.1.4.3.6 Λύση μηχανισμών ισχυρής ταυτοποίησης

Η λύση αυτή αφορά 500 χρήστες διαχειριστές η οποία θα εξασφαλίζει τον έλεγχο πρόσβασης χρηστών πολλαπλών σημείων. Η λύση βοηθά στην απλοποίηση και τη διαχείριση της πρόσβασης των χρηστών ενός οργανισμού. Η επαλήθευση πρόσβασης βοηθά στην επίτευξη μιας ισορροπίας μεταξύ χρηστικότητας και ασφάλειας μέσω της χρήσης πρόσβασης πολλαπλών παραγόντων (MFA: Multi-factor Authentication). Η λύση θα διασφαλίζει ισχυρό έλεγχο ταυτότητας μέσω του μηχανισμού MFA και υποστηρίζει μια ευρεία γκάμα μηχανισμών ελέγχου ταυτότητας πολλαπλών παραγόντων για την επαλήθευση των χρηστών κατά τον έλεγχο ταυτότητας από εφαρμογές web, επιτραπέζιους υπολογιστές, κινητά και διακομιστές. Ο έλεγχος ταυτότητας πολλαπλών παραγόντων διασφαλίζει ότι ο χρήστης που έχει πρόσβαση σε εφαρμογές και διακομιστές είναι πραγματικά το σωστό άτομο.

Ο έλεγχος ταυτότητας πολλαπλών παραγόντων (MFA, που περιλαμβάνει έλεγχο ταυτότητας) είναι μια ηλεκτρονική μέθοδος ελέγχου ταυτότητας κατά την οποία παρέχεται σε έναν χρήστη πρόσβαση σε μια εφαρμογή μόνο αφού παρουσιάσει επιτυχώς δύο ή περισσότερα αποδεικτικά στοιχεία (ή παράγοντες) στον μηχανισμό ελέγχου ταυτότητας: γνώση (κάτι που γνωρίζει μόνο ο χρήστης), κατοχή (κάτι που έχει μόνο ο χρήστης) και εγγενής (κάτι που είναι μόνο ο χρήστης).

Υπάρχουν διαφορετικοί τρόποι υλοποίησης ενός τέτοιου μηχανισμού. Στα πλαίσια του παρόντος έργου θα υλοποιηθεί λύση on-premise χρησιμοποιώντας υποδομή του Φορέα υπό τη μορφή virtual appliance και να γίνει εκτενής περιγραφή των αναγκών σε hardware resources. Η χρήση πολλαπλών παραγόντων ελέγχου ταυτότητας για την απόδειξη της ταυτότητάς κάποιου βασίζεται στην προϋπόθεση ότι ένας μη εξουσιοδοτημένος φορέας είναι απίθανο να είναι σε θέση να παρέχει όλους τους παράγοντες που απαιτούνται για την πρόσβαση.

Εάν, σε μια προσπάθεια ελέγχου ταυτότητας, τουλάχιστον ένα από τα στοιχεία λείπει ή παρέχεται λανθασμένα, η ταυτότητα του χρήστη δεν διαπιστώνεται με επαρκή βεβαιότητα και η πρόσβαση στο στοιχείο που προστατεύεται από έλεγχο ταυτότητας πολλαπλών παραγόντων, τότε παραμένει αποκλεισμένη. Οι παράγοντες ελέγχου ταυτότητας ενός συστήματος ελέγχου ταυτότητας πολλαπλών παραγόντων μπορεί να περιλαμβάνουν:

- Κάτι που έχει ο χρήστης: Οποιοδήποτε φυσικό αντικείμενο έχει στην κατοχή του ο χρήστης, όπως ένα διακριτικό ασφαλείας, ένα κλειδί κ.λπ.
- Κάτι που γνωρίζει ο χρήστης: Ορισμένες γνώσεις που είναι γνωστές μόνο στον χρήστη, όπως κωδικός πρόσβασης, PIN κ.λπ.
- Κάτι που είναι ο χρήστης: Κάποια φυσικά χαρακτηριστικά του χρήστη (βιομετρικά), όπως δακτυλικό αποτύπωμα, ίριδα ματιών, φωνή, ταχύτητα πληκτρολόγησης, μοτίβο στα διαστήματα πατήματος πληκτρων κ.λπ.

7.1.4.4 Υπηρεσίες νεφροϋπολογιστικών υποδομών και υπηρεσιών

7.1.4.4.1 Υπηρεσίες ανάκαμψης από καταστροφή και λήψης αντιγράφων ασφαλείας

Μεσκοπό την ενίσχυση της επιχειρησιακής συνέχειας, απαιτείται η παροχή υπηρεσιών λήψης Αντιγράφων ασφαλείας (Backup) και ανάκαμψης από καταστροφή (Επαναφοράς (Recovery)). Απαιτείται να λαμβάνονται αντίγραφα ασφαλείας σε υπολογιστικούς πόρους που βρίσκονται εγκατεστημένοι είτε τοπικά (On-premises) είτε στον πάροχο του Νέφους (Cloud). Ως προστατευόμενοι υπολογιστικοί πόροι δύνανται να θεωρηθούν στοιχεία όπως [VMs, DBs, Folders/Files]. Επίσης, θα υπάρχει η δυνατότητα επιλογής επαναφοράς των προστατευμένων υποδομών είτε τοπικά (On-premises) είτε στον πάροχο του Νέφους (Cloud). Θα υπάρχουν επιλογές της υπηρεσίας αυτής με βάση τον όγκο των προστατευόμενων πόρων/δεδομένων ώστε να καλύπτονται διαφορετικού τύπου ανάγκες.

Ο ανάδοχος είναι υπεύθυνος και για την Εγκατάσταση / παραμετροποίηση υπηρεσιών ανάκαμψης από καταστροφή και λήψης αντιγράφων ασφάλειας ανάλογα με τις ανάγκες.

7.1.4.5 Λύση Ddos

Η πρωτοβουλία στοχεύει στην ενδυνάμωση του επιπέδου ασφάλειας για τις υποδομές της ΗΔΙΚΑ και η πλήρης συμμόρφωση της με τις κανονιστικές απαιτήσεις (όπως ο νόμος ν. 4577/2018 «Ενσωμάτωση στην ελληνική νομοθεσία της Οδηγίας 2016/1148/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση και άλλες διατάξεις», ο Γενικός Κανονισμός Προσωπικών Δεδομένων, κλπ.).

Η προσφερόμενη λύση ασφάλειας θα πρέπει να παρέχει προστασία του εταιρικού δικτύου από επιθέσεις τύπου άρνησης υπηρεσιών και κατανεμημένης άρνησης υπηρεσιών. Οι επιθέσεις αυτές συχνά είναι σύνθετες (multi-vector), συνδυάζοντας – πολλές φορές ταυτόχρονα – ογκομετρικές (volumetric) επιθέσεις μεγάλης κλίμακας, επιθέσεις στους διαθέσιμους πόρους της υπάρχουσας υποδομής (π.χ. firewall/συσκευές IPS) και επιθέσεις εναντίον συγκεκριμένων εφαρμογών (application layer attacks).

Η προσφερόμενη λύση θα πρέπει να βασίζεται σε εξειδικευμένη συσκευή προστασίας από επιθέσεις τύπου DoS/DDoS η οποία έχει σχεδιαστεί ειδικά για να παρέχει on-premise προστασία της διαθεσιμότητας των δικτυακών πόρων από μια συνεχώς επεκτεινόμενη γκάμα απειλών σε επίπεδο εφαρμογής (application-level), διασφαλίζοντας έτσι την αξιόπιστη πρόσβαση σε δικτυακές υπηρεσίες ζωτικής σημασίας και την επιχειρησιακή συνέχεια της Αναθέτουσας Αρχής. Η συσκευή αυτή θα πρέπει να διαθέτει την κατάλληλη stateless τεχνολογία ανίχνευσης και φιλτραρίσματος, η οποία θα της επιτρέψει να παραμείνει σε λειτουργία κατά την διάρκεια εκδήλωσης επιθέσεων μικρού όγκου (low volume attacks), οι οποίες έχουν σχεδιαστεί με στόχο να θέτουν εκτός λειτουργίας μηχανισμούς όπως τα firewalls και τα IPS.

Η προσφερόμενη λύση θα πρέπει κατ' ελάχιστο να περιλαμβάνει τις παρακάτω λειτουργίες:

- Προστασία από γνωστές και άγνωστες επιθέσεις – Η προσφερόμενη λύση θα πρέπει να ανιχνεύει επιθέσεις τύπου DoS/ DDoS βάση υπογραφών και συμπεριφοράς
- Προστασία από επιθέσεις βασιζόμενες στον δικτυακό όγκο - Η προσφερόμενη λύση θα πρέπει να διαχειρίζεται επιθέσεις τύπου DoS/ DDoS μεγάλου όγκου δικτυακής κίνησης.
- Προστασία από επιθέσεις σε επίπεδο εφαρμογών – Η προσφερόμενη λύση θα πρέπει να προστατεύει εφαρμογές όπως IIS, Apache, κ.λπ. από επιθέσεις τύπου DoS/ DDoS.
- Προστατεύει από επιθέσεις σε επίπεδο πρωτοκόλλου - Η προσφερόμενη λύση θα πρέπει να διαχειρίζεται επιθέσεις τύπου DoS/ DDoS σε πρωτόκολλα όπως HTTP, SMTP κ.λπ.
- Προώθηση των συμβάντων ασφαλείας στην υφιστάμενη λύση SIEM - Η λύση αυτή θα πρέπει να προωθεί τα συμβάντα ασφαλείας στην υφιστάμενη λύση SIEM

7.1.4.6 Εξειδικευμένες λύσεις ασφάλειας

7.1.4.6.1 NGFW για το Data Center, για την πρόσβαση των εσωτερικών χρηστών στο Διαδίκτυο και την ανάλυση των επικοινωνιών τους και για την απομακρυσμένη πρόσβαση. Αδειες για προστασία IPS, antimalware, Application Control. Διαχειριστικό εργαλείο για τα firewall

Απαιτείται η προμήθεια και εγκατάσταση NextGenerationfirewalls, σύμφωνα με τις προδιαγραφές του πίνακα συμμόρφωσης 7.2.2.9.

7.1.4.6.2 Δικτυακός εξοπλισμός (switches) για τη διασύνδεση των firewalls

Απαιτείται η προμήθεια και εγκατάσταση δικτυακού εξοπλισμού για τη διασύνδεση των firewalls, σύμφωνα με τις προδιαγραφές του πίνακα συμμόρφωσης 7.2.2.10.

7.1.4.6.3 Λύση Virtual Firewalls

Η λύσηπεριλαμβάνει Virtual Next Generation Firewall και Next Generation Intrusion Prevention System Platform.

Οι προδιαγραφές παρατίθενται στον πίνακα συμμόρφωσης7.2.2.11.

7.1.4.6.4 Microsegmentation με χρήση Agent στο Data Center

Η προσφερόμενη λύση θα παρέχει προστασία στους εξυπηρετητές της Αναθέτουσας Αρχής με χρήση λογισμικού (agent). Η εν λόγω λύση, ενσωματώνοντας μια σειρά πρωτοποριακών δυνατοτήτων και χαρακτηριστικών όπως συμπεριφορά διαδικασιών, ανίχνευση ανωμαλιών σε επίπεδο επικοινωνίας, ανίχνευση τρωτών σημείων κ.λπ. θα παρέχει την έγκαιρη ανίχνευση κακόβουλης δραστηριότητας ή/και απρόσμενης συμπεριφοράς στους εξυπηρετητές.

Η προσφερόμενη λύση θα πρέπει κατ' ελάχιστο να περιλαμβάνει τις παρακάτω λειτουργίες:

- Υποστήριξη microsegmentation σεεπίπεδο workload (VM ή baremetal server ή container)
- Παρακολούθηση της συμπεριφοράς των διαδικασιών (process behavior)
- Ανίχνευση των τρωτών σημείων του λογισμικού (software vulnerabilities)
- Ανίχνευση ανωμαλιών επικοινωνίας σε επίπεδο δικτύου
- Αναγνώριση της ανοικτής επιφάνειας επίθεσης, συνδιάζοντας πληροφορία σχετική με θύρες επικοινωνίας, διαδικασίες και στοιχεία κίνησης (traffic volume)
- Υποστήριξη όλων των λειτουργιών ενός εικονικού περιβάλλοντος ανεξάρτητα από το περιβάλλον hypervisor.
- Δυνατότητα συλλογής της τηλεμετρίας με εναλλακτικές επιλογές όπου δεν είναι δυνατή η εγκατάσταση agent λογισμικού.
- Αυτόματη δημιουργία πολιτικής whitelist για τμηματοποίηση (segmentation), με βάση χάρτες εξάρτησης εφαρμογών χωρίς τη χρήση προτύπων (με εστίαση σε περιβάλλοντα Brownfield)
- Παρακολούθηση της γενεαλογίας ενός δέντρου διεργασίας και διατήρηση ιστορικών καταγραφών με την πάροδο του χρόνου

Η λύση ασφαλείας θα πρέπει να αποστέλλει δεδομένα καταγραφής (logs) σε σύστημα διαχείρισης περιστατικών ασφαλείας (SIEM) & συλλογής αρχείων καταγραφής.

7.1.4.6.5 Λύση Ασφαλείας και προστασίας των χρηστών από απειλές του διαδικτύου (WebSecurityGateway)

Η συγκεκριμένη λύση ασφάλειας πρόκειται να καλύψει την ανάγκη προστασίας του εταιρικού δικτύου από επιθέσεις και απειλές στο περιεχόμενο της υπηρεσίας ηλεκτρονικής αλληλογραφίας.

Πιο συγκεκριμένα ο ρόλος της εν λόγω λύσης ασφαλείας στην υποδομή της εταιρίας θα πρέπει να καλύπτει τουλάχιστον τα ακόλουθα:

- Δυνατότητα ελέγχων ασφαλείας στο περιεχόμενο HTTP, HTTPS και FTP βασισμένων σε συγκεκριμένους κανόνες (πολιτικές ασφάλειας) οι οποίοι θα εφαρμόζονται ανά χρήστη ή ομάδα χρηστών (user ή group) οι λογαριασμοί των οποίων λαμβάνονται από κάποια υπηρεσία καταλόγου (π.χ. AD, LDAP service).
- Υποστήριξη μηχανισμού caching.
- Ενσωματωμένος μηχανισμός Antivirus για την ανίχνευση και καταστολή ιών και άλλων ειδών κακόβουλου λογισμικού στο περιεχόμενο της ηλεκτρονικής αλληλογραφίας. Να αναφερθούν οι υποστηριζόμενοι κατασκευαστές.
- URL Filtering – έλεγχος της πρόσβασης των χρηστών σε συγκεκριμένες κατηγορίες ιστοσελίδων με δυνατότητα εφαρμογής διαφορετικών πολιτικών ανά domain user/group.
- Application Identification & Control – αναγνώριση και έλεγχος των εφαρμογών HTTP & HTTPS. Δυνατότητα εφαρμογής πολιτικών ελέγχου πρόσβασης βάσει της εφαρμογής που χρησιμοποιεί ο χρήστης σε συνδυασμό με το Source/Destination IP address, το πρωτόκολλο και τον χρήστη (domain user/group).

Η λύση ασφαλείας θα πρέπει να αποστέλλει δεδομένα καταγραφής (logs) στην υφιστάμενη λύση διαχείρισης περιστατικών ασφαλείας (SIEM) & συλλογής αρχείων καταγραφής.

7.1.4.6.6 Λύση Αυστηρής πιστοποίησης για την απομακρυσμένη πρόσβαση (MFA, Zero Trust)

Οι προδιαγραφές παρατίθενται στον πίνακα συμμόρφωσης 7.2.2.14.

7.1.4.6.7 Λύση Cloud Proxy προστασίας απομακρυσμένων χρηστών

Η λύση Cloud Proxy παρέχει την πρώτη γραμμή άμυνας στην πρόσβαση στο Διαδίκτυο, ανεξάρτητα από τη θέση των χρηστών. Η λύση πρέπει να βασίζεται στο cloud και να υποστηρίζεται από ένα παγκόσμιο δίκτυο κέντρων δεδομένων.

Οι προδιαγραφές παρατίθενται στον πίνακα συμμόρφωσης 7.2.2.15.

7.1.4.6.8 Λύση Antimalware απομακρυσμένων χρηστών (AV, EDR, XDR)

Η λύση αφορά σε εξειδικευμένο λογισμικό προστασίας τερματικού και ανάλυσης επιθέσεων.

Οι προδιαγραφές παρατίθενται στον πίνακα συμμόρφωσης 7.2.2.16.

7.1.4.6.9 Λύση εκπαίδευσης για 250 χρήστες σε phishing campaigns και cyberattacks

Η λύση επιτρέπει την εκπαίδευση χρηστών για τους διάφορους τύπους επιθέσεων ώστε να εργάζονται πιο έξυπνα και ασφαλέστερα μέσω ηλεκτρονικής πλατφόρμας Security Awareness που παρέχει περιεχόμενο εκπαίδευσης με τη μορφή video και ερωτήσεων αλλά και με τη δυνατότητα διεξαγωγής phishing campaigns για την αποδοτικότερη και συνεχή εκπαίδευση των χρηστών.

7.1.4.6.10 Λύση Ασφαλούς Πρόσβασης χρηστών στο εταιρικό δίκτυο

Η προσφερόμενη λύση θα πρέπει να παρέχει υπηρεσίες πιστοποίησης, εξουσιοδότησης και λογιστικής (AAA) με βάση την ταυτότητα των χρηστών τους, συμμόρφωση με την πολιτική της ΗΔΙΚΑ και τον τύπο της συσκευής.

Οι προδιαγραφές παρατίθενται στον πίνακα συμμόρφωσης 7.2.2.18.

7.1.4.6.11 Λύση Πλατφόρμας Ενορχήστρωσης Ασφαλείας, Αυτοματοποίησης

Η προσφερόμενη λύση θα πρέπει να συλλέγει τα συμβάντα από την κεντρική πλατφόρμα διαχείρισης των προσφερόμενων λύσεων ασφαλείας και να τα συνδυάζει με ευφυής πληροφορίες απειλών (Threat Intelligence) για τον άμεσο και αποτελεσματικό των απειλών.

Η προσφερόμενη λύση θα πρέπει κατ' ελάχιστο να περιλαμβάνει τις παρακάτω λειτουργίες:

- Να λειτουργεί στο νέφος (cloud based solution)
- Το κέντρο δεδομένων, που φιλοξενεί την προτεινόμενη λύση cloud, πρέπει να βρίσκεται σε χώρα που ανήκει στην Ευρωπαϊκή Ένωση
- Η ενσωμάτωση της λύσης με την προτεινόμενη λύση ασφάλειας να είναι άμεση χωρίς ιδιαίτερες προσαρμογές
- Δυνατότητα ενοποίησης του μηχανισμού ειδοποίησης (alerting) με email και πλατφόρμες ανταλλαγής μηνυμάτων και επικοινωνίας, όπως οι Cisco Webex teams, Microsoft Teams με άμεσα διαθέσιμα workflows
- Δυνατότητα αυτοματοποίησης δημιουργίας ticket μέσω του εργαλείου SOAR σε συστήματα ticketing, όπως το ServiceNow με άμεσα διαθέσιμα Workflows.
- Δυνατότητα threat hunting επιτρέποντας τη συλλογή παρατηρήσιμων (observables) όπως IPs, domain, hash αρχείων) από τη πλατφόρμα διαχείρισης των NGFWs και διερεύνηση ενάντια σε πληροφορίες από το Threat Intelligence του προμηθευτή ή άλλες πηγές threat intelligence
- Μέσω της ενορχήστρωσης να επιτρέπεται η αυτοματοποίηση επαναλαμβανόμενων και κρίσιμων εργασιών ασφαλείας, όπως η έρευνα απειλών και οι περιπτώσεις αποκατάστασης. Η πλατφόρμα να παρέχει προκατασκευασμένες ροές εργασίας και δυνατότητες απόκρισης ή δημιουργίας νέων από τον διαχειριστή μέσω απλού κώδικα ή λειτουργιών τύπου drag-drop.
- Να επιτρέπει ενσωματώσεις με εργαλεία ασφαλείας τρίτων κατασκευαστών μέσω ανοιχτού API

7.1.4.6.12 Πλατφόρμα Κυβερνοασφάλειας – Εκτεταμένης Ανίχνευσης & Απόκρισης (Cyber Security)

Η πλατφόρμα πρέπει να αποτελεί μια ολοκληρωμένη λύση open XDR (Extended Detection & Response) με χαρακτηριστικά και λειτουργίες Next Gen SOC (Security Operation Center), η οποία να εξασφαλίζει την κεντρική παρακολούθηση και διαχείριση, αποφεύγοντας παλαιού τύπου τεχνικές με την εγκατάσταση διαφορετικών ξεχωριστών απλών εργαλείων SIEM (Security Information & Events Management) και άλλων που εγκαθίσταται και διαχειρίζονται ξεχωριστά ή απαιτείται χειροκίνητη ξεχωριστή διαδικασία ενσωμάτωσής του.

Η πλατφόρμα πρέπει να έχει τη δυνατότητα συλλογής και επεξεργασίας από πολλαπλών τύπων πηγές δεδομένων και όχι μόνο αρχείων καταγραφής, κινούμενη στη φιλοσοφία του big data security analytics. Συνδυάζοντας πληροφορίες από δικτυακή κίνηση (network traffic), user data, cloud data, file data στόχος είναι η εξάλειψη πιθανών τυφλών σημείων και ο συσχετισμός όλων των δεδομένων για την παραγωγή καλύτερων αποτελεσμάτων. Μέσα από αυτοματοποιημένες διαδικασίες εμπλουτισμού και συσχετισμών, τα δεδομένα θα βελτιστοποιούνται για αξιοποίηση από μηχανισμούς έρευνας και εντοπισμού. Ειδικότερα με την εκμετάλλευση αυτοματοποιημένης επεξεργασίας και μηχανικής μάθησης, το σύστημα θα πρέπει να μπορεί να λειτουργεί αποτελεσματικά ως ένα ολοκληρωμένο κέντρο αναφοράς και αυτόματης πρότασης και λήψης αντιμέτρων. Το σύστημα θα πρέπει κατ' ελάχιστον να συνοδεύεται από τεχνολογίες SIEM, NTA και Threat Intelligence και να μην απαιτείται η ξεχωριστή προμήθεια λογισμικού.

Το προσφερόμενο σύστημα θα πρέπει να έχει τη δυνατότητα να υποστηρίζει και το μοντέλο MDR (Managed Detection & Response) και στο σύνολό του θα πρέπει να υποστηρίζει όλο τον κύκλο ζωής αναγνώρισης και αντιμετώπισης απειλών, που αναλύεται στα στάδια:

- Συλλογή (Collect)
- Εντοπισμός (Detect)
- Έρευνα (Investigate)
- Απόκριση (Respond)

Το υπο προμήθεια σύστημα θα πρέπει να περιλαμβάνει την προμήθεια, εγκατάσταση και παραμετροποίηση αισθητήρων ασφαλείας (φυσικών ή εικονικών), οι οποίοι θα εφαρμόζουν λειτουργίες ML-IDS, antivirus, sandboxing και NTA.

Χαρακτηριστικά Next Gen Soc

- Μοντέρνο περιβάλλον χρήσης (GUI) που ενσωματώνει απαραίτητες λειτουργίες παρακολούθησης και διαχείρισης.
- Πρόσβαση με χρήση ρόλων χρηστών (RBAC – Role Based Access) για την διαχείριση δικαιωμάτων (user privilege management)
- Υποστήριξη πολλαπλών ενοίκων (multi-tenant) για την ξεχωριστή διαχείριση οντοτήτων, φυσικών δικτύων κτλ
- Εφαρμογή ξεχωριστού μοντέλου μηχανικής μάθησης ανά tenant για τη βελτίωση ακρίβειας των αποτελεσμάτων και τη μείωση των εσφαλμένων θετικών συμβάντων (false positives), εφαρμόζοντας ξεχωριστά συμπεριφορικά μοντέλα.
- Εξελεξιμένες δυνατότητες μηχανικής μάθησης Δυνατότητες ενσωμάτωσης με εργαλεία και τεχνολογίες ασφαλείας Firewalls, WAF, EDR, SOAR κτλ
- Υποστήριξη API για ενσωμάτωση με τεχνολογίες HoneyPots, εργαλεία OSINT κτλ.
- Μία ενοποιημένη, υψηλής απόδοσης, αποθήκη δεδομένων ("Big Data" High Speed Lake)
- Δυνατότητα εγκατάστασης τόσο σε φυσικό εξοπλισμό, όσο και σε εικονικό ή περιβάλλον cloud
- Κατανεμημένη και επεκτάσιμη αρχιτεκτονική που να υποστηρίζει ωστόσο και "All In One" σενάρια.
- Υψηλή διαθεσιμότητας με τη χρήση clusters και ευέλικτη τήρηση και αποθήκευση δεδομένων.
- Μηχανισμοί Συλλογής που να μπορούν να εγκατασταθούν τόσο σε φυσικό όσο και σε εικονικό περιβάλλον
- Το σύστημα θα πρέπει να ακολουθεί ανοιχτή αρχιτεκτονική που να επιτρέπει την εισαγωγή δεδομένων από οποιαδήποτε συσκευή με τη χρήση Integration APIS.
- Κεντροποιημένη διαχείριση

- Απλό ενοποιημένο μοντέλο αδειών χωρίς επιπλέον κόστη

Next-Generation SIEM

Η πλατφόρμα θα πρέπει να βασίζεται σε μια ενοποιημένη αποθήκη δεδομένων βασισμένη στην αρχιτεκτονική του big data lake. Τα δεδομένα θα πρέπει κατ' ελάχιστον να μπορούν να εισαχθούν μέσω syslog. Όπου είναι εφικτό θα πρέπει να παρέχεται η δυνατότητα χρήσης parsers για κυριότερες και δημοφιλέστερες λύσεις δικτύων και ασφαλείας ώστε οι πληροφορίες να κανονικοποιούνται και να συσχετίζονται με αυτοματοποιημένο τρόπο. Θα πρέπει να παρέχονται οι παρακάτω ελάχιστες λειτουργικότητες:

- Απλός όσο και εξεζητημένος μηχανισμός αναζήτησης που να βασίζεται σε λογικούς τελεστές (Boolean modifiers)
- Οι αναζητήσεις να μπορούν να εφαρμοστούν ως μόνιμα φίλτρα σε όλο το περιβάλλον για ταχύτερη διερεύνηση και ανάλυση περιστατικών.
- Υψηλής απόδοσης και άμεσες ανταποκρίσεις στην αναζήτηση και το φιλτράρισμα στο big data
- Πρόσβαση σε πηγές δεδομένων και όχι μόνο σε syslog δεδομένα
- Συλλογή δεδομένων από δικτυακή κίνηση (μέσω TAP ή Mirror Traffic). Τα πακέτα θα πρέπει να γίνονται reduce, να κανονικοποιούνται και να μετατρέπονται σε αξιοποιήσιμα μετα-δεδομένα για την ενσωμάτωση στο big data lake.
- Συλλογή δεδομένων από user sources όπως το Microsoft AD μέσω API Connector
- Συλλογή δεδομένων από πηγές νέφους (cloud) Office365 μέσω Connectors
- Τα δεδομένα από πηγές πρέπει να κανονικοποιούνται, να εμπλουτίζονται και να συσχετίζονται αυτόματα από το σύστημα
- Πηγές εμπλουτισμού πρέπει να περιλαμβάνονται γεωγραφικού προσδιορισμού (Geo-Awareness), IP Reputation, Threat Intelligence και DPI Application awareness.
- Μοντέρνο περιβάλλον χρήστη με λειτουργίες SIEM που περιλαμβάνουν ερωτήματα και δημιουργίες κανόνων.
- Πρόσθετο για παραδοσιακή απεικόνιση SIEM (π.χ. Kibana)

Εντοπισμός KillChain (KillChain Detections)

(συμπεριλαμβάνοντας IDS/Exploit, Malware και APT Sandboxing, Anti-Phishing κτλ.)

- Το σύστημα πρέπει να έχει ενσωματωμένους μηχανισμούς εντοπισμών σε κάθε φάση του CyberSecurity KillChain, συμπεριλαμβάνοντας Reconnaissance, Delivery, Exploitation, Installation, Command & Control, and Actions & Exfiltrations
- Το σύστημα πρέπει να περιλαμβάνει ενσωματωμένη βάση υπογραφών IDS, ενισχυμένη από ανάλυση μηχανικής μάθησης (ML-IDS)
- Η πλατφόρμα πρέπει να υποστηρίζει πολλαπλά Threat Intelligence Feeds, συμπεριλαμβάνοντας εμπορικές πηγές, open-source, anti-phishing κ.α.
- Η πλατφόρμα πρέπει να επιτρέπει ενσωμάτωση με 3rd party feeds μέσω STIX/TAXII και/η MISP
- Η πλατφόρμα πρέπει να έχει ενσωματωμένες δυνατότητες APT Sandboxing για να αναγνωρίζει και να περιορίζει άγνωστα αρχεία, και για εντοπισμό ransomware, spyware.

Ανάλυση Δικτύου (Network Traffic Analysis)

Με την επιθεώρηση δικτυακής κίνησης σε πραγματικό χρόνο, η πλατφόρμα πρέπει να μπορεί να μοντελοποιήσει την κίνηση για αναγνώριση παράτυπων συμπεριφορών και ειδοποιήσεων.

- Η πλατφόρμα πρέπει να ενσωματώνει λειτουργικότητα Deep Packet Inspection (DPI) για την αναγνώριση τουλάχιστον 4000 εφαρμογών και να δομεί σχετικά συμπεριφορικά μοντέλα.
- Τα δεδομένα κίνησης δικτύου πρέπει να μετασχηματίζονται σε κατάλληλα μετα-δεδομένα που περιλαμβάνουν και το payload, για την αντίστοιχη προαιρετική μείωση ανάγκης αποθηκευτικών χώρων.
- Η πλατφόρμα πρέπει να ενσωματώνει λειτουργικότητα NTA Detections, συμπεριλαμβάνοντας Application Usage Anomalies, Long App Session Anomalies, και Unapproved Asset Activity
- Το σύστημα θα πρέπει να εντοπίζει ανωμαλίες στη συμπεριφορά των Firewalls, denial anomalies ή rule usage anomalies

User Behavior Analytics (UBA)

Σε συνδυασμό με την ανάλυση πακέτων, το σύστημα θα πρέπει να μπορεί να συνδεθεί με πηγές δεδομένων χρηστών, το MS Active Directory

- Το σύστημα πρέπει να πραγματοποιεί ανάλυση και εντοπισμό ανωμαλιών στη συμπεριφορά του χρήστη (user behavior)
- Το σύστημα πρέπει να ενσωματώνει μοντέλα εντοπισμού ανωμαλιών αδύνατου ταξιδιού (Impossible Travel Anomaly) ή ώρες αυθεντικοποίησης (Log In Time Anomaly)
- Εντοπισμούς NTA, έτσι κι εδώ όλα τα detections και τα σχετικά events στα logs και σε πηγές πρέπει να συσχετίζονται αυτόματα.

Endpoint Behavior Analytics (EBA)

Με τα αναλυτικά δεδομένα δικτύου και χρηστών, το σύστημα πρέπει να μπορεί να συλλέγει δεδομένα από assets/endpoints στο περιβάλλον, να εκτελεί analytics και να εντοπίζει συμπεριφορικές ανωμαλίες.

- Το σύστημα θα πρέπει να μπορεί να εισάγει δεδομένα από τρίτα συστήματα εντοπισμού ευπαθειών (vulnerability scanners) Nessus, Tenable, Rapid7 και να συσχετίζει τα ευρήματα με σχετικά γεγονότα ασφαλείας.
- Το σύστημα θα πρέπει να μπορεί να ανακαλύψει όλα τα assets σε ένα περιβάλλον και να τα κατηγοριοποιεί με βάση τη διεύθυνση MAC και IP.
- Η λίστα των ανακαλυφθέντων/εντοπισθέντων assets θα πρέπει να μπορεί να επαυξάνεται και να παραμετροποιείται με τη χρήση αρχείων csv με λίστες assets και περιγραφές.
- Το σύστημα πρέπει να μπορεί να καταγράφει όλους συσχετισμούς με ένα asset με IP διευθύνσεις, ιστορικά στοιχεία για τη χρήση εφαρμογών κτλ.

Ορατότητα Δικτύου και Υπηρεσιών (Network & Service Visibility)

Το σύστημα θα πρέπει να περιλαμβάνει δυνατά εργαλεία απεικόνισης δικτύων και υπηρεσιών, μαζί με analytics, με στόχο να προσφέρει ορατότητα επιδόσεις δικτύου (network performance), application usage κτλ.

Κυνήγι Απειλών και Διερεύνηση (Threat Hunting & Investigation)

Με πηγές δεδομένων στο unified data lake, τα κανονικοποιημένα και συσχετισμένα δεδομένα πρέπει να είναι διαθέσιμα για διερεύνηση και threat hunting οποιαδήποτε στιγμή.

- Το σύστημα πρέπει να έχει ενσωματωμένα σχετικά εργαλεία, προκαθορισμένες αναζητήσεις και ερωτήματα, και οπτικοποιήσεις (visualizations).
- Τα visualizations πρέπει να είναι παραμετροποιήσιμα
- Το σύστημα πρέπει να προσφέρει εξελιγμένες δυνατότητες συσχετισμένες αναζητήσεις, που επιτρέπουν αναλυτές να συνδέσουν πολλαπλά ανεξάρτητα ερωτήματα με κοινά κριτήρια προκειμένου να δομήσουν πληροφορίες από attack sequences ή να απομονώσουν κοινές πληροφορίες.
- Όλα τα ερωτήματα θα πρέπει να μπορούν να αποθηκευθούν, επεξεργαστούν, κλωνοποιηθούν κτλ από χρήστες.
- Τα visualizations πρέπει να μπορούν να αποθηκευθούν σαν custom dashboards.
- Τα ερωτήματα θα πρέπει να μπορούν να συνδυαστούν με ενέργειες/αποκρίσεις για PlayBooks

Playbooks / Integrated Orchestration & Response (SOAR)

- Το σύστημα πρέπει να συμπεριλαμβάνει μια βιβλιοθήκη με έτοιμα ενσωματωμένα playbooks, που είναι αυτό-εκτελέσιμα ερωτήματα με ενσωματωμένες ενέργειες.
- Οι ενσωματωμένες ενέργειες/αποκρίσεις θα πρέπει να συμπεριλαμβάνουν
 - Alerts – Αποστολή e-mail/slack message κτλ
 - Actions – Άνοιγμα case, εκτέλεση ημερολογίου API, δημιουργία security event κτλ
 - Responses – Μπλοκάρισμα μιας IP στο Firewall, απενεργοποίηση χρήστη στο AD, εκτέλεση δέσμης ενεργειών κτλ
- Παράλληλα με αυτοματοποιημένες ενέργειες, εξωτερικές ενέργειες το μπλοκάρισμα μια IP ή χρήστη θα πρέπει να είναι διαθέσιμες στο χρήστη μέσω του UI ώστε να μπορούν παράλληλα να υλοποιηθούν ως μέρος διερεύνησης/αντιμετώπισης ή ανάλυσης.
- Δυνατότητα ενσωμάτωσης με ήδη έτοιμα εμπορικά εργαλεία SOAR

Επιπλέον Δυνατότητες

Ειδοποιήσεις (Alarming)

- Το σύστημα θα πρέπει να προσφέρει έναν έξυπνο, μοντέρνο και παραμετροποιήσιμο μηχανισμό ειδοποιήσεων που να δύναται να οριστεί με βάση παραλήπτες και άλλα κριτήρια (score severity, killchain category, etc.)
- Οι ειδοποιήσεις πρέπει να μπορούν να αποσταλούν με email ή slack μηνύματα και τα μηνύματα πρέπει να είναι παραμετροποιήσιμα ως το περιεχόμενο και τα σχετικά δεδομένα.

Αναφορές (Reporting)

- Το σύστημα πρέπει να περιέχει ένα σύγχρονο εξελιγμένο μηχανισμό αναφορών που θα επιτρέπει παράλληλα εύκολη δημιουργία νέων αναφορών με drag and drop και αποθήκευσή για χρήση σε οποιοδήποτε σημείο.
- Οι αναφορές θα πρέπει να παράγονται με χρονοπρογραμματισμό και να αποστέλλονται σε διαφορετικούς χρήστες.
- Οι αναφορές πρέπει να είναι δυνατόν να αποστέλλονται με email σαν pdf ή csv ή να γράφονται σε αρχείο.
- Το σύστημα θα πρέπει να περιλαμβάνει πληθώρα έτοιμων αναφορών και templates.

Portal

- Πρόσβαση των χρηστών βάση ρόλου (User RBAC access) στο Portal με συνολική ή περιορισμένη πρόσβαση πληροφορίες.
- Custom Dashboards ανάρολοχρήστη.
- Χρονοπρογραμματισμένες αναφορές για κάθε tenant, tenant group και RBAC users.
- Η πρόσβαση των χρηστών πρέπει να μπορεί να περιορίζεται σε Read-Only, limited view, μέχρι full visibility and access.

7.1.4.6.13 Λύση Προστασίας Βάσεων Δεδομένων

Οι βάσεις δεδομένων είναι από τα βασικά δομικά συστατικά της υποδομής πληροφοριακών συστημάτων και επομένως η προστασία τους και η παρακολούθησή τους είναι υψίστης σημασίας.

Για την αποτελεσματική προστασία των Βάσεων Δεδομένων απαιτείται η προμήθεια και υλοποίηση μιας ολοκληρωμένης λύσης Database Security η οποία θα ενσωματώνει κατ' ελάχιστον τις ακόλουθες λειτουργίες:

- User Accountability - πλήρης καταγραφή και παρακολούθηση των προσβάσεων και ενεργειών στη Βάση Δεδομένων σε επίπεδο χρήστη
- Detailed DB Auditing (query level) – έλεγχος όλης της δικτυακής κίνησης και των προσβάσεων προς τη Βάση Δεδομένων σε επίπεδο SQL query
- Database Application protection – προστασία σε επίπεδο εφαρμογής Βάσης Δεδομένων

Η προσφερόμενη λύση προστασίας Βάσεων Δεδομένων θα πρέπει να πραγματοποιεί πλήρη καταγραφή και παρακολούθηση σε πραγματικό χρόνο των προσβάσεων σε επίπεδο ερωτημάτων προς την Βάση Δεδομένων (query-level auditing), καθώς και να εφαρμόζει πολιτική ελέγχου πρόσβασης στη Βάση Δεδομένων και στα δεδομένα αυτής, ακόμα και για τους διαχειριστές της Βάσης Δεδομένων. Κάθε αίτηση προς μια προστατευόμενη Βάση Δεδομένων θα πρέπει να αναλύεται εις βάθος προκειμένου να διαπιστωθεί το κατά πόσο είναι ασφαλής και δεν αποτελεί απειλή για την ασφάλεια των εταιρικών δεδομένων.

Ταυτόχρονα θα πρέπει να καταγράφει και να εξετάζει σε πραγματικό χρόνο τις κινήσεις στις Βάσεις Δεδομένων δημιουργώντας έτσι ένα δυναμικό προφίλ βασισμένο στην δομή και τα δυναμικά χαρακτηριστικά της κάθε Βάσης. Το προφίλ που θα δημιουργείται έπειτα από επιβεβαίωση του διαχειριστή θα πρέπει να μπορεί χρησιμοποιείται ως βάση και μέτρο σύγκρισης από τον μηχανισμό ως προς την ανίχνευση και καταστολή επιθέσεων και κάθε είδους μη εξουσιοδοτημένων ενεργειών οι οποίες εκτελούνται στην Βάση Δεδομένων.

Συνοπτικά το σύστημα θα πρέπει να παρέχει τις ακόλουθες λειτουργίες ασφάλειας:

- Λειτουργία ως Database Firewall-Auditing, με στόχο την παρακολούθηση και προστασία συστημάτων βάσεων δεδομένων πολλαπλών κατασκευαστών (όπως MS SQL, Oracle, κτλ.) από επιθέσεις τόσο από εξωτερικούς επιτιθεμένους, όσο και από εσωτερικούς κακόβουλους χρήστες.
- Δυνατότητα παραμετροποίησης και ορισμού πολιτικών ασφαλείας βάσει user names, IP addresses, tables, operations, queries, query patterns, privileged commands και stored procedures.
 - Δυνατότητα δημιουργίας αναφορών (reporting)
 - Παραμετροποίηση αναφορών
 - Κεντρική διαχείριση
- Προώθηση των συμβάντων ασφαλείας σε λύση SIEM

7.1.4.6.14 Λογισμικό κυβερνοασφάλειας ΑΙ

Η λύση αφορά Λογισμικό κυβερνοασφάλειας ΑΙ σύμφωνα με τις προδιαγραφές του πίνακα συμμόρφωσης 7.2.2.22

7.1.5 Φυσικό αντικείμενο Τμήματος 3 «Εξειδικευμένες λύσεις και υπηρεσίες ασφάλειας για το Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο»»

7.1.5.1 Διαστασιολόγηση λογισμικού, εξοπλισμού και υπηρεσιών

Κατηγορία	Μονάδα διαστασιολόγησης	Ελάχιστο μέγεθος
Διαμόρφωση πολιτικών ασφάλειας κρίσιμων οντοτήτων με στόχο την ανάδειξη τεχνικών και οργανωτικών μέτρων για την προστασία τους από Κυβερνοαπειλές	A/M	14
διαμόρφωση πολιτικών ορθής χρήσης Πληροφοριακών συστημάτων και εφαρμογών	A/M	14
διενέργεια δράσεων ενημέρωσης για τη μεταφορά τεχνογνωσίας και την διαμόρφωση κουλτούρας ενεργούς ευαισθητοποίησης για τους κινδύνους κυβερνοασφάλειας	A/M	14
διαμόρφωση πλάνου ανάκαμψης από καταστροφές για κρίσιμες οντότητες	A/M	14
Εκπόνηση Μελέτης εξωτερικού και εσωτερικού περιβάλλοντος και την ανάδειξη βέλτιστων πρακτικών	A/M	14
διαμόρφωση πολιτικής αντιγράφων ασφαλείας, που θα περιγράφει σκοπό, πεδίο εφαρμογής, ρόλους και ευθύνες	A/M	14
Διαμόρφωση Συστήματος Διαχείρισης της Ασφάλειας των Πληροφοριών (ΣΔΑΠ) με βάση το πρότυπο ISO 27001 & Εκπόνηση Μελέτης Ανάλυσης και Αξιολόγησης Κινδύνων	A/M	14
Διενέργεια ελέγχων διεύθυνσης εξωτερικών δικτύων, εφαρμογών Ιστού, φυσικής ασφάλειας και διαρροής δεδομένων για τον εντοπισμό των ευπαθειών σε υποδομές, συσκευές και διακομιστές που είναι προσβάσιμοι από το διαδίκτυο	A/M	16
Αξιοποίηση τεχνολογικής καινοτομίας και ερευνητικής πρωτοπορίας	A/M	46
Παροχή υπηρεσίας SOC	Μήνες	30
Λύση DDOS	Μήνες	30

Κατηγορία	Μονάδα διαστασιολόγησης	Ελάχιστο μέγεθος
Παροχή υπηρεσιών ανάκαμψης από καταστροφή & λήψης αντιγράφων ασφαλείας (disaster recovery as a service & data backup as a service)	CREDITS €	500.000,00
Υπηρεσίες εγκατάστασης/παραμετροποίησης υπηρεσιών ανάκαμψης από καταστροφή & λήψης αντιγράφων ασφαλείας (disaster recovery as a service & data backup as a service)	A/M	40
Λύση Προστασίας Βάσεων Δεδομένων	Βάσεις δεδομένων	20
Πλατφόρμα Κυβερνοασφάλειας – Εκτεταμένης Ανίχνευσης & Απόκρισης (CyberSecurity)	Assets GB log files/ημέρα	3.000 100
MailSecurity (αφορά 3.000 σταθμούς εργασίας)	Σταθμοί εργασίας	3.000
Endpoint Security User level (αφορά 3.000 σταθμούς εργασίας)	Σταθμοί εργασίας	3.000
Managed services security endpoint & mail (αφορά 3.000 σταθμούς εργασίας)	Σταθμοί εργασίας	3.000
Λύση Διαβάθμισης και Σήμανσης Εγγράφων	Σταθμοί εργασίας	1.000
Λύση Προστασίας Δεδομένων από Διαρροή	Σταθμοί εργασίας	1.000
Λύση Διαχείρισης Δικαιωμάτων Εγγράφων	Χρήστες	1.000
Λύση Διαχείρισης Λογαριασμών και Δικαιωμάτων Πρόσβασης Χρηστών	Λογαριασμοί	1.000
Λύση Διαχείρισης Προνομιούχων Λογαριασμών Πρόσβασης	Λογαριασμοί διαχειριστών Λογαριασμοί συνεργατών (named users)	100 50

7.1.5.2 Πολιτικές – Διαδικασίες και Μέτρα Αντιμετώπισης και Πρόληψης

7.1.5.2.1 Διαμόρφωση πολιτικών ορθής χρήσης Πληροφοριακών συστημάτων και εφαρμογών

Ο Ανάδοχος θα εκπονήσει μελέτη πολιτικής ορθής χρήσης πληροφοριακών συστημάτων και εφαρμογών, προκειμένου να καθοριστούν οι υποχρεώσεις όλων των χρηστών, καθώς και οι αρχές, οι κανόνες και οι συνέπειες για το σύνολο των προσώπων στα οποία εκχωρείται το δικαίωμα πρόσβασης στα πληροφοριακά συστήματα και τις εφαρμογές. Η πολιτική ορθής χρήσης αποβλέπει στην αποτροπή καταχρηστικής άσκησης των δικαιωμάτων των χρηστών και της τέλεσης πράξεων που συνιστούν κίνδυνο παραβίασης του απορρήτου των δεδομένων / πληροφοριών, ή διακύβευσης της ασφάλειας των πληροφοριακών συστημάτων και εφαρμογών ή της ακεραιότητας και διαθεσιμότητας των υποδομών.

Στο πλαίσιο της εργασίας αυτής, ο Ανάδοχος κατ' ελάχιστον:

- Θα διενεργήσει κατάλληλη κατηγοριοποίηση του συνόλου των υφιστάμενων και δυνητικών χρηστών, προκειμένου να προτείνει στη συνέχεια μια διαφοροποιημένη πολιτική ορθής χρήσης προσαρμοσμένη σε κάθε κατηγορία.
- Θα διενεργήσει μια κατηγοριοποίηση των πληροφοριακών συστημάτων και εφαρμογών, προκειμένου να προσδιορίσει στη συνέχεια τα συστήματα εκείνα που είναι ευάλωτα σε ένα περιστατικό ανάρμοστης χρήσης.
- Θα αναλύσει τα ιδιαίτερα χαρακτηριστικά κάθε κατηγορίας χρηστών, που θα προκύψουν από τη σχετική έρευνα και κατηγοριοποίηση που θα έχει ήδη κάνει και στη συνέχεια θα προσδιορίσει τις ανάγκες και υποχρεώσεις χρήσης κάθε κατηγορίας
- Θα προσδιορίσει τις διαδικασίες που πρέπει να εφαρμόζονται, τις ενέργειες που συνιστώνται και τα μέτρα που πρέπει να παίρνονται, προκειμένου να διασφαλιστεί η ορθή χρήση του δικτύου
- Θα προσδιορίσει τις ενέργειες που απαγορεύονται ή πρέπει να αποφεύγονται και οι οποίες συνιστούν μια ανάρμοστη χρήση πληροφοριακών συστημάτων και εφαρμογών.
- Θα προτείνει τις διαδικασίες και τα διορθωτικά και/ή αποτρεπτικά μέτρα που πρέπει να εφαρμόζονται σε περίπτωση που διαπιστωθεί κάποιο περιστατικό ανάρμοστης χρήσης πληροφοριακών συστημάτων και εφαρμογών
- Θα συντάξει σχέδια συμφωνητικών ορθής χρήσης, τα οποία θα υπογράφονται από τους δυνητικούς χρήστες πληροφοριακών συστημάτων και εφαρμογών, κατόπιν επιθυμίας του Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο». Το ελάχιστο περιεχόμενο των συμφωνητικών αυτών περιλαμβάνει μια σύνοψη των δικαιωμάτων και υποχρεώσεων κάθε κατηγορίας χρήστη
- Θα μεριμνήσει για την κατάλληλη ενημέρωση όλων των χρηστών (φτάνοντας μέχρι το επίπεδο τελικού χρήστη) επί της πολιτικής ορθής χρήσης που θα εφαρμοσθεί, αφού εγκριθεί από το Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο»
- Θα προσδιορίσει τις διαδικασίες που πρέπει να εφαρμοστούν και τις ενέργειες που πρέπει να πραγματοποιηθούν, προκειμένου να καταστεί δυνατός ο τακτικός έλεγχος και παρακολούθηση της εφαρμογής ή όχι της πολιτικής ορθής χρήσης.

7.1.5.2.2 Διενέργεια δράσεων ενημέρωσης για τη μεταφορά τεχνογνωσίας και τη διαμόρφωση κουλτούρας ενεργούς ευαισθητοποίησης για τους κινδύνους κυβερνοασφάλειας

Ο Ανάδοχος καλείται να παράσχει υπηρεσίες σχεδιασμού και υλοποίησης δράσεων ενημέρωσης προς τις αρμόδιες υπηρεσίες του Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο» κατά την υλοποίηση του έργου, στις ακόλουθες θεματικές ενότητες:

- Εισαγωγή στην Ασφάλεια Πληροφοριών
- Οι κυβερνοπειλές (Cyber Threats)
- Υλική Ασφάλεια Αρχείων και Μηχανημάτων
- Ασφάλεια Επιφάνειας Εργασίας
- Αποθήκευση αρχείων και δεδομένων
- Αποστολή και διαμοιρασμός αρχείων

- Ασφάλεια κωδικών πρόσβασης
- Ασύρματα δίκτυα και κινητή επικοινωνία
- Διαδικτυακή Ασφάλεια
- Συστήματα Κοινωνικής Μηχανικής (Social Engineering)
- Ασφάλεια ηλεκτρονικού ταχυδρομείου
- Κακόβουλο λογισμικό (Ιοί, Worms, Trojans, Spyware, Adware)
- Ηλεκτρονικό «ψάρεμα» (Phishing)
- Μέσα Κοινωνικής Δικτύωσης

Οι συμμετέχοντες μόλις ολοκληρώσουν την εκπαίδευση θα έχουν κατανοήσει τα θέματα των νέων τεχνολογιών και διαδικτύου, ασφάλειας υπολογιστικών συστημάτων και υποδομών, ασφαλούς χρήσης του διαδικτύου αλλά και χειρισμού διαδικτυακών προγραμμάτων και προγραμμάτων ηλεκτρονικού υπολογιστή. Επιπλέον, θα μπορούν να αναγνωρίσουν τα διάφορα είδη κυβερνοαπειλών και θα έχουν μάθει βασικούς κανόνες ασφαλείας για την αποτροπή τους.

Πιο ειδικά ο Ανάδοχος καλείται να παρέχει τις παρακάτω υπηρεσίες:

Ι. Μεθοδολογία εκπαίδευσης, εκπαιδευτικό υλικό και εισαγωγή των δεδομένων στην εκπαιδευτική πλατφόρμα

Ο Ανάδοχος θα πρέπει να τεκμηριώσει και να παραδώσει τη μεθοδολογία εκπαίδευσης που θα ακολουθήσει πριν την έναρξη του προγράμματος. Η μεθοδολογία θα πρέπει να επιδιώκει την επίτευξη των παρακάτω εκπαιδευτικών στόχων για τους εκπαιδευόμενους:

- Ανάκληση γνώσεων
- Κατανόηση εκπαιδευτικού υλικού
- Εφαρμογή γνώσεων στην πράξη και σε περιβάλλον προσομοίωσης ή/και σε μελέτες περίπτωσης
- Ανάλυση και σύνθεση γνώσεων
- Η θεωρία και οι ασκήσεις αξιολόγησης/εξέτασης να αποδίδονται μέσω σύγχρονων authoring tools (όπως Articulate, Captivate κ.α.), εξειδικευμένων στην εκπαίδευση ενηλίκων.
- Ενσωμάτωση μηχανισμών παιχνιδιού στην εκπαιδευτική διαδικασία, με δυνατότητες επιβράβευσης (π.χ. πόντοι, σήματα, εικονικά νομίσματα κ.ά.)

Ο Ανάδοχος θα αναλάβει τον σχεδιασμό των εκπαιδευτικών προγραμμάτων λαμβάνοντας υπόψη συγκεκριμένες παραμέτρους. Οι παράμετροι αυτοί αφορούν τη διαφοροποιημένη προσέγγιση ανάλογα με την ομάδα-στόχο, τον τρόπο εκπαίδευσης και τα μέσα που θα χρησιμοποιηθούν.

Ο Ανάδοχος καλείται να μελετήσει τα μοντέλα που έχουν ακολουθήσει άλλες ευρωπαϊκές χώρες για σχετικά προγράμματα εκπαίδευσης, ενημέρωσης και ευαισθητοποίησης εταιρειών και οργανισμών. Ο στόχος της μελέτης είναι να μπορεί ο Ανάδοχος να παρέχει τις κατάλληλες κατευθύνσεις και να αντλήσει καλές πρακτικές στο πεδίο της κατάρτισης και ευαισθητοποίησης εργαζόμενων σε θέματα Κυβερνοασφάλειας.

Ο Ανάδοχος, καλείται να παραδώσει για κάθε εκπαιδευτική ενότητα του προγράμματος, τους εκπαιδευτικούς στόχους, τα εκπαιδευτικά αποτελέσματα, τη διάρκεια αλλά και πιθανές

ασκήσεις/ερωτήσεις προς πρακτική εξάσκηση των γνώσεων. Ο σχεδιασμός του εκπαιδευτικού προγράμματος πρέπει να υποστηρίζεται από μια πολυμεσική υλοποίηση, η οποία θα περιλαμβάνει διάφορα οπτικοακουστικά μέσα (π.χ. ήχος, εικόνες, βίντεο, mini games, gamification, quizzes, learning modalities, slideshow κ.α).

Για την ασύγχρονη εκπαίδευση απαιτείται ένα σύγχρονο και πλήρως φιλικό προς το χρήστη σύστημα Learning Management (Learning Management System, LMS), το οποίο να βασίζεται σε εφαρμογή PWA (Progressive Web Application) έτσι ώστε να μην απαιτείται εγκατάσταση της μέσω Google/Apple Store καθώς και όλες οι απαραίτητες ενημερώσεις (updates) να γίνονται κεντρικά και να ενημερώνονται αυτόματα όλοι οι χρήστες, χωρίς να χρειάζεται να προβούν σε καμία ενέργεια αναβάθμισης. Επιπλέον, το LMS θα πρέπει να είναι μία απόλυτα εξατομικευμένη λύση που θα παραμετροποιηθεί, προσαρμοστεί και ενσωματωθεί πλήρως τόσο στα μηχανογραφικά συστήματα όσο και στους μηχανισμούς ασφαλείας του Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο». Θα πρέπει να καλύπτει τις ανάγκες στο σύνολο των εκπαιδευόμενων (ιδιωτικός και δημόσιος τομέας), να παρέχει στενή διασύνδεση (integration) με όλα τα εργαλεία του MS Office και να αποτελεί συμβατή πλατφόρμα με διεθνή πρότυπα ηλεκτρονικής μάθησης όπως SCORM με τα οποία εξασφαλίζεται η επαναχρησιμοποίηση, η προσβασιμότητα και η ανθεκτικότητα του εκπαιδευτικού υλικού στις τεχνολογικές μεταβολές, καθώς και η διαλειτουργικότητα μεταξύ συστημάτων ηλεκτρονικής μάθησης. Η αρχιτεκτονική της πλατφόρμας (πλατφορμών) θα δίνει τη δυνατότητα στον χρήστη να αλληλεπιδρά δυναμικά με όλο το εκπαιδευτικό υλικό. Επιπλέον, ο Ανάδοχος θα πρέπει να παρακολουθεί με αναφορές το πλήθος των χρηστών που θα παρακολουθούν ή/και ολοκληρώνουν το εκπαιδευτικό ασύγχρονο πρόγραμμα κατάρτισης καθώς και να καταγράφονται αναλυτικά όλα τα ερωτηματολόγια με τις απαντήσεις στα τελικά διαδικτυακά (ψηφιακά) τεστ όλων των χρηστών σε αναλυτική καρτέλα προφίλ.

Για τον σχεδιασμό του εκπαιδευτικού υλικού πρέπει να ακολουθούνται με ακρίβεια τα πρότυπα σχεδιασμού εκπαιδευτικού υλικού, όπως περιγράφονται:

- Ο εκπαιδευτικός σχεδιασμός ψηφιακού υλικού ("instructional design") θα πρέπει να βασίζεται στη σαφή και αιτιολογημένη κατάτμηση του υλικού ενοτήτων σε υποενότητες μάθησης, με ορισμένη μέγιστη διάρκεια. Παράλληλα για την πλήρη κατανόηση της κατάτμησης των ενοτήτων σε υποενότητες μάθησης ο Ανάδοχος οφείλει να συνδέσει κάθε ενότητα/υποένότητα με διακριτούς εκπαιδευτικούς στόχους.
- Ο χρήστης θα πρέπει να ακολουθεί σαφή εκπαιδευτικά μονοπάτια (Θεωρία, Αυτοαξιολόγηση, Εξέταση, Πιστοποίηση), για τα οποία να δύνανται να έχουν υποχρεωτική σειριακή ακολουθία παρακολούθησης, ανάλογα με τους σκοπούς της εκπαίδευσης.
- Η διάδραση με το περιεχόμενο και η ενεργητική μάθηση των καταρτιζόμενων πρέπει με σαφή τρόπο να επιτυγχάνεται μέσω σύνθετων εργαλείων, εξειδικευμένων στην εκπαίδευση ενηλίκων, όπως business case studies, role playing, psychometric analysis κ.ά.
- Ο πρακτικός προσανατολισμός: μέθοδος «μαθαίνω κάνοντας» (learning by doing) θα επιτυγχάνεται με προσομοίωση πραγματικών συνθηκών (μελέτες περίπτωσης, επίλυση προβλήματος) και άλλες τεχνικές που ο ανάδοχος μπορεί να επιλέξει ώστε να ενθαρρύνει τη μάθηση μέσα από την επαφή των καταρτιζόμενων με πραγματικές συνθήκες λήψης απόφασης, συμπεριφορικές δραστηριότητες και ανάλυση επιλογών.
- Η πολυμεσική μάθηση είναι ο βασικός στόχος αυτού του έργου. Προκειμένου ο Ανάδοχος να διασφαλίσει ένα πολυμεσικό περιβάλλον μάθησης, οι παρουσιάσεις, τα βίντεο και η δόμηση του υλικού σε διαφορετικά εκπαιδευτικά μέσα και εκπαιδευτικά εργαλεία θα πρέπει να τηρεί προδιαγραφές της πολυμεσικής μάθησης και να διευκολύνει την επεξεργασία, κατανόηση και

αφομοίωση των πληροφοριών και της παρεχόμενης γνώσης και την εύκολη και διαδραστική πλοήγηση.

- Οι προδιαγραφές αξιολόγησης της κατανόησης και αφομοίωσης της γνώσης από τους καταρτιζόμενους θα πρέπει να γίνεται με τη μέθοδο αξιολόγησης βάσει μετρήσιμων μαθησιακών αποτελεσμάτων – ταξινομία ADDIE και να απεικονίζεται σε ανάλογες αναφορές.
- Κάθε ενότητα ή/ και υποενότητα μάθησης θα ακολουθείται από αξιολόγηση με quiz πολλαπλής ή μοναδικής επιλογής, ερωτήσεις σωστό λάθος. Προτεινόμενο μοντέλο είναι η αξιολόγηση να αποτελείται από ένα quiz αυτοαξιολόγησης και ένα βαθμολογούμενο, ανά υποενότητα μάθησης, ενώ οι ερωτήσεις θα πρέπει να αναφέρονται κυρίως σε συμπεριφορικά στοιχεία, επιλογές και αποκρίσεις σε πιθανά σενάρια σχετικά με το περιεχόμενο του εκπαιδευτικού προγράμματος και τους εκπαιδευτικούς στόχους.

Ο Ανάδοχος θα αναλάβει τον σχεδιασμό της μεθοδολογίας αξιολόγησης των αποτελεσμάτων γνώσεων, ο οποίος θα προκύπτει από σχετικά κριτήρια αξιολόγησης όπου θα συμμετέχουν οι εκπαιδευόμενοι με το πέρας της εκπαίδευσης. Πιο συγκεκριμένα, οι συμμετέχοντες θα πρέπει να συμμετάσχουν στην παραπάνω διαδικασία, η οποία θα τους αξιολογεί αυτόματα και άμεσα. Τα αποτελέσματα αυτά θα πρέπει να είναι άμεσα συγκρίσιμα και να παράγουν αναφορές με συνέπεια και συνεκτικότητα. Οι αναφορές θα απεικονίζονται και με ιεραρχικό επίπεδο της θέσης εργασίας που κατέχει κάθε υπάλληλος και ανά τμήμα όπου θα προκύπτουν συγκεντρωτικά ή ατομικά γνωστικά αποτελέσματα.

Το εκπαιδευτικό υλικό, για το οποίο ο Ανάδοχος θα έχει την επιμέλεια και επίβλεψη, σύμφωνα με τις ανάγκες και τον σχεδιασμό, θα είναι διαθέσιμο στην εκπαιδευτική πλατφόρμα και θα πρέπει να κατατεθεί ως ένα από τα παραδοτέα του έργου αυτού.

II. Σχεδιασμός και ανάπτυξη της ψηφιακής πλατφόρμας για την ασύγχρονη εξ' αποστάσεως εκπαίδευση

Το σύστημα τηλεεκπαίδευσης (E-Learning platform) θα είναι εύκολα προσβάσιμο και θα εξυπηρετεί τις ανάγκες του έργου. Το σύστημα ηλεκτρονικής εκπαίδευσης θα αποτελείται από μία πλατφόρμα ασύγχρονης τηλε-εκπαίδευσης (Learning Management System) για διαχείριση και παράδοση ασύγχρονων προγραμμάτων ηλεκτρονικής (ψηφιακής) μάθησης (e-learning). Ο Ανάδοχος θα πρέπει να διασφαλίσει ότι θα παρεμετροποιήσει και θα διαμορφώσει την αρχιτεκτονική της πλατφόρμας ώστε να μπορεί να φιλοξενήσει την εκπαιδευτική διαδικασία καθώς και τη φόρτωση και διαχείριση κάθε είδους εκπαιδευτικού υλικού, την ανταλλαγή και διάχυση πληροφορίας και την υποστήριξη κάθε είδους διεργασίας ανταλλαγής πληροφοριών. Το σύστημα θα πρέπει να μπορεί να χρησιμοποιηθεί προκειμένου να διαχειρίζονται και χρονοπρογραμματίζονται τα εκπαιδευτικά προγράμματα ασύγχρονης μορφής, οι μαθησιακές διαδικασίες καθώς η δυνατότητα διενέργειας δοκιμασιών (test) αξιολόγησης της επίτευξης των εκπαιδευτικών στόχων και αξιολόγησης του εκπαιδευτικού προγράμματος από τους συμμετέχοντες.

Ο Ανάδοχος πριν από τον σχεδιασμό της αρχιτεκτονικής και την ανάπτυξη της εκπαιδευτικής πλατφόρμας (ή πλατφορμών), καλείται να παρουσιάσει μια ενδελεχή ανάλυση των στοιχείων που θα παρακολουθούνται δυναμικά εντός της πλατφόρμας και να ορίσει ένα σαφές, ρεαλιστικό και περιγραφικό σύστημα δεικτών για την καταγραφή του εκπαιδευτικού και επιμορφωτικού κέρδους.

Η πρόσβαση στο σύστημα τηλεεκπαίδευσης θα πρέπει να μπορεί να πραγματοποιείται μέσα από δημοφιλείς φυλλομετρητές διαδικτύου που πληρούν τα διεθνή standards, όπως οι: Google Chrome, Mozilla Firefox, Microsoft Edge, από οποιοδήποτε σημείο του κόσμου, οποιαδήποτε στιγμή της ημέρας και από οποιαδήποτε συσκευή (desktop, laptop, tablet, smartphone). Δεν θα πρέπει να απαιτείται κανένα άλλο, πρόσθετο λογισμικό στη συσκευή που θα επιλέξει ο χρήστης καθώς και καμία εγκατάσταση. Όλες οι λειτουργίες και τα υποσυστήματα της εφαρμογής μπορούν να συνδυαστούν

ελεύθερα. Ο σχεδιασμός και η ανάπτυξη της ψηφιακής πλατφόρμας θα πρέπει να διασφαλίζει ότι το σύστημα θα είναι άμεσα προσιτό και εύκολο στην πλοήγηση και χρήση από τους συμμετέχοντες, όπου αυτός επιθυμεί, και να υποστηρίζει τη διαχείριση μεγάλου αριθμού ενεργών χρηστών. Το σύστημα το οποίο θα διαμορφώσει ο Ανάδοχος θα πρέπει να επιτρέπει τη δημιουργία προσωπικού λογαριασμού για κάθε εκπαιδευόμενο, στον οποίο θα καταγράφεται όλη του η δραστηριότητα όπως επίσης και τα αποτελέσματα της εξέτασης/ αξιολόγησης.

Γενικές κατευθύνσεις που πρέπει να ακολουθούνται για το σύστημα τηλεεκπαίδευσης:

- Το λογισμικό ασύγχρονης εκπαίδευσης θα πρέπει να παρέχει χρήσιμα εργαλεία, όπως:
 - Βαθμολόγιο
 - Ημερολόγιο
 - Helpdesk
 - Ερωτηματολόγια (Review) για τη συλλογή δεδομένων από τους καταρτιζόμενους
 - Ηλεκτρονικά τεστ (online quiz)
 - Άμεσα μηνύματα (Forum/chat) με βαθμολόγηση απαντήσεων
 - Βιβλιοθήκη περιεχομένου
 - Μικροεκπαιδεύσεις – Microlearnings
 - Αιτήματα εγγραφής εκπαιδευόμενων σε νέες εκπαιδεύσεις
 - Ενσωματωμένο σύστημα ερωτηματολογίων (survey) ανά ομάδες χρηστών
- Πολύγλωσσο περιβάλλον και περιεχόμενο.
- Δημιουργία οργανογράμματος για οργάνωση των χρηστών ανά τομέα / διεύθυνση / γεωγραφική τοποθεσία κ.ά. σε γραφικό περιβάλλον
- Δημιουργία απεριόριστων χρηστών και ομάδων χρηστών.
- Δημιουργία απεριόριστων εκπαιδεύσεων με τελική πιστοποίηση.
- Δημιουργία εκπαιδευτικών μονοπατιών.
- Υποστήριξη διαφορετικών επιπέδων διαχείρισης, χρήσης, ρόλων και ομάδων χρηστών υποστηρίζοντας τα Azure, Microsoft Active Directory ,LDAP και Google Business.
- Υποστήριξη κατάλληλων μέτρων για την προστασία των προσωπικών δεδομένων τόσο των χρηστών της εφαρμογής, όσο και ευαίσθητων πληροφοριών στο υλικό παρουσίασης, σύμφωνα με τον κανονισμό GDPR. Πιο συγκεκριμένα:
 - Αποδοχή/Συναίνεση συλλογής δεδομένων: Το σύστημα υποστηρίζει λειτουργικότητες καταχώρησης και καταγραφής της συναίνεσης του χρήστη αναφορικά με τη συλλογή και διαχείριση των δεδομένων που έχουν ήδη καταχωρηθεί στο σύστημα ή των δεδομένων που θα συλλεχθούν κατά τη διάρκεια των διαδικασιών κατάρτισης κρυπτογραφημένα.
 - Ενημέρωση περί συλλεγόμενων δεδομένων. Ο χρήστης μπορεί να ενημερωθεί αναλυτικά και με σαφή τρόπο για το ποια δεδομένα συλλέγονται, τους λόγους για τους οποίους γίνεται η συλλογή τους, τον τρόπο χρήσης τους, καθώς επίσης και για τη διάρκεια διατήρησης αυτών των δεδομένων στα συστήματα. Επίσης, μπορεί να ενημερωθεί αναλυτικά για τους όρους χρήσης του συστήματος και τις εκπαιδευτικές διαδικασίες στις οποίες θα συμμετάσχει.

- Λειτουργία αυτόματης δημιουργίας και εισαγωγής εκπαιδευτικού περιεχομένου με εφαρμογές MS Office για την θεωρία και τα ερωτηματολόγια με online editor.
- Πλήρης συμμόρφωση με την τρέχουσα έκδοση του διεθνούς προτύπου SCORM.
- Λειτουργία μέσω Web Browser και είναι συμβατό με τα διεθνή πρότυπα του W3C.
- Λειτουργία σε περιβάλλον HTTPS. Όλες οι επιμέρους λειτουργίες να παρέχονται εντός πρωτοκόλλου HTTPS και πάνω από secure channel SSL/TLS.
- Πολιτική ασφάλειας κωδικών πρόσβασης. Το σύστημα να υποστηρίζει:
 - ο Πολιτική πολυπλοκότητας κωδικών (ελάχιστο πλήθος χαρακτήρων, συμπερίληψη special characters, συμπερίληψη χαρακτήρων με κεφαλαία, συμπερίληψη αριθμητικών χαρακτήρων, αποτροπή χρήσης ακολουθίας π.χ. 1234, αποτροπή χρήσης κοινών κωδικών π.χ. qwerty).
 - ο Παραγωγή κωδικών με τυχαίο τρόπο και σύμφωνα με την πολιτική πολυπλοκότητας χωρίς την επέμβαση φυσικού προσώπου (διαχειριστή) > Διαδικασίες επαναφοράς κωδικού χωρίς ενημέρωση και χωρίς την επέμβαση φυσικού προσώπου (διαχειριστή) > Διαδικασίες υποχρεωτικής αλλαγής κωδικού (π.χ. κατά την 1η είσοδο στο σύστημα).
 - ο Διατήρηση ιστορικού κωδικών πρόσβασης και αποτροπή επαναχρησιμοποίησης παλιού κωδικού.
- Υποστήριξη αρθρωτής (modular) και ανοικτής αρχιτεκτονικής, ώστε να επιτρέπονται επεκτάσεις/αναβαθμίσεις.
- Δυνατότητα δημιουργίας πολλαπλών Portals με βάση τον ρόλο του Χρήστη (Δημόσιος τομέας, Ιδιωτικός Τομέας, Ομάδες Διεύθυνσης, Εκπαιδευτές, Εκπαιδευόμενοι, κ.ά.)
- Δυνατότητα καταγραφής της πορείας και των ενεργειών του καταρτιζόμενου (tracking-timeline) καθ' όλη τη διάρκεια εκάστου εκπαιδευτικού προγράμματος.
- Μηχανισμό χρονοπρογραμματισμού και αποστολής αυτοματοποιημένων ειδοποιήσεων μέσω e-Mail ή/και SMS, in app notifications, έτσι ώστε να παρέχονται όλες οι κατάλληλες πληροφορίες για την επιλογή της βέλτιστης διαδικασίας αποστολής σε όλες τις λειτουργίες της πλατφόρμας δυνατότητα:
 - ο Αποστολή σε όλους: Θα γίνει αποστολή σε όσους έχουν ενεργές τις ειδοποιήσεις, και έχουν αποδεχθεί τους όρους.
 - ο Εξαίρεση: Ο διαχειριστής μπορεί να επιλέξει ποιοι θα εξαιρεθούν της αποστολής
 - ο Ατομική Αποστολή: Ο διαχειριστής μπορεί να επιλέξει συγκεκριμένα άτομα που θα γίνει η αποστολή
 - ο Δεν έχουν λάβει ειδοποίηση: Ο διαχειριστής μπορεί να επιλέξει τους όσους δεν έχουν λάβει τη συγκεκριμένη ειδοποίηση από προηγούμενη αποστολή.

Το σύστημα επιπλέον θα πρέπει να διαθέτει σύστημα αναφορών έτσι ώστε να μπορούν να παράγονται αναφορές για τις ενέργειες που υποστηρίζονται από το σύστημα. Ενδεικτικά:

- Αναφορές για το σύνολο των χρηστών / ομάδα / χρήστη
- Αναφορές ανά θεματικό πεδίο / μάθημα / εξέταση / πιστοποίηση.

Που θα περιλαμβάνουν τουλάχιστον τα παρακάτω δεδομένα:

- Ποσοστό συμμετοχής (δλδ πόσοι έχουν ξεκινήσει ή ολοκληρώσει)

- Χρόνους κατανάλωσης περιεχομένου (μέσο όρο, σύνολο)
- Μέσο χρόνο ολοκλήρωσης ανά εκπαιδευτικό πρόγραμμα
- Αποτελέσματα εξετάσεων / μάθημα, αξιολόγηση, πιστοποίηση και Top 10 /100
- Ποιες ερωτήσεις εμφανίζουν συχνά λάθη ανά θεματικό πεδίο, μάθημα
- Προσωποποιημένες αναφορές επίδοσης με στατιστικά ανά γνωστικό αντικείμενο
- Αναλυτικά αποτελέσματα ερευνών
- Big data analytics για ανάλυση δεξιοτήτων που αναπτύχθηκαν με συγκεκριμένους δείκτες (KPI's)

Το σύστημα τηλεκπαίδευσης θα πρέπει να υποστηρίζει τουλάχιστον τις εξής κατηγορίες χρηστών και σχετικά δικαιώματα:

- Εκπαιδευόμενους
- Εκπαιδευτές
- Διαχειριστές της πλατφόρμας εξ αποστάσεως εκπαίδευσης

Οι δυνατότητες του συστήματος σε σχέση με τον χρήστη/εκπαιδευόμενο αναφέρονται συνοπτικά παρακάτω:

- Εγγραφή στο εκπαιδευτικό πρόγραμμα
- Προβολή και παρακολούθηση εκπαιδευτικού υλικού
- Συμμετοχή σε τυποποιημένες έρευνες (αξιολόγηση εκπαιδευτικού προγράμματος) με σκοπό την έκφραση των απόψεων του εκπαιδευμένου σχετικά με το εκπαιδευτικό υλικό ή τη διαδικασία εκπαίδευσης
- Συμμετοχή σε μη υποχρεωτικά μαθήματα μικρής διάρκειας, μεγάλης ποικιλίας με συνδυασμό πολλαπλών μορφών περιεχομένου και δυνατότητα αναζήτησης με λέξεις κλειδιά.
- Συμμετοχή σε εξέταση (test αξιολόγησης) που μπορεί να έχει διάφορες μορφές ερωτήσεων όπως πολλαπλής επιλογής, σωστό-λάθος και ερωτήσεις με σύντομες απαντήσεις κ.λ.π.
- Προβολή και εκτύπωση βεβαίωσης της ολοκλήρωσης της συμμετοχής στο εκπαιδευτικό πρόγραμμα μετά την επιτυχή ολοκλήρωση του τεστ αξιολόγησης

Οι δυνατότητες του συστήματος σε σχέση με τον χρήστη Διαχειριστή αναφέρονται συνοπτικά παρακάτω.

Ως Διαχειριστής ορίζεται το στέλεχος το οποίο θα παρακολουθεί την υλοποίηση του έργου και θα είναι υπεύθυνος για τα παρακάτω (ενδεικτική και όχι εξαντλητική λίστα):

- Προσθήκη έτοιμου εκπαιδευτικού υλικού ή δημιουργίας μέσω Online editor σε ιδιαίτερα φιλικό περιβάλλον πλοήγησης και με λίγες οθόνες (wizards).
- Δημιουργία ερωτηματολογίων (Test Bank) με αυτόματη εισαγωγή από συγκεκριμένα πρότυπα MS Office.
- Δημιουργία και χρονοπρογραμματισμό του εκπαιδευτικού προγράμματος με τις απαραίτητες αυτόματες ειδοποιήσεις (SMS,email,In-app notification)
- Διαχείριση δραστηριοτήτων (quiz, αξιολογήσεις, τεστ κ.ο.κ.)

- Δημιουργία επεξεργασία και διαγραφή χρηστών οποιασδήποτε μορφής στο σύστημα και απόδοση ρόλων
- Προβολή λίστας συνδεδεμένων χρηστών στην LMS
- Διαχείριση αιτήσεων που υποβάλλονται για συμμετοχή στην εκπαίδευση
- Επικοινωνία με όλους τους χρήστες του συστήματος
- Δυνατότητα επαναφοράς της εκπαίδευσης σε μια προηγούμενη κατάσταση
- Εξαγωγή των αποτελεσμάτων όλων των εκπαιδευομένων σε αρχεία Excel ή PDF με βάση αν ολοκλήρωσαν ή όχι το πρόγραμμα κατάρτισης και αν πέρασαν την τελική αξιολόγηση/εξέταση

Δυνατότητες του συστήματος σε σχέση με τη δημιουργία αναφορών:

Το σύστημα πρέπει να υποστηρίζει την αποτύπωση live αναφορών με κατ' ελάχιστον τις ακόλουθες κατηγορίες:

- Αναφορές αποδοχής όρων χρήσης
- Αναφορές επισκέψεων (ημερήσιες, μηνιαίες, ετήσιες)
- Αναφορές πρόσβασης κάθε κατηγορίας χρηστών με επιλογή της επιθυμητής χρονικής περιόδου
- Αποτελέσματα αξιολογήσεων, εξετάσεων, τελικών Πιστοποιήσεων.
- Καρτέλα εκπαιδευόμενου με όλα τα στοιχεία που σχετίζονται με τον συγκεκριμένο εκπαιδευόμενο και τη συμμετοχή του στο εκπαιδευτικό πρόγραμμα
- Αξιολόγηση/ εξέταση εκπαιδευόμενου, αποτελέσματα και βεβαίωση συμμετοχής του εκπαιδευόμενου

«Επικοινωνιακή Διαχείριση Κρίσεων στον Κυβερνοχώρο»

Η υιοθέτηση νέων τεχνολογιών, η συλλογή, επεξεργασία και αποθήκευση τεράστιου όγκου δεδομένων, έχουν δημιουργήσει νέους κινδύνους που απαιτούν ειδικό σχεδιασμό, προετοιμασία και αντιμετώπιση. Ακόμα και μικρής έκτασης κυβερνοεπιθέσεις, μπορούν να προκαλέσουν σοβαρά προβλήματα στην φήμη, την παραγωγικότητα και την ομαλή λειτουργία ενός οργανισμού.

Το αντικείμενο του παρόντος αφορά στον σχεδιασμό και υλοποίηση ενός εκπαιδευτικού προγράμματος με στόχο την έγκαιρη προετοιμασία και την αποτελεσματική αντίδραση της Ομάδας Διαχείρισης Κρίσεων σε περίπτωση κρίσεων στον κυβερνοχώρο.

Στόχος του προγράμματος είναι:

- α) η δημιουργία ισχυρής εταιρικής συναντίληψης σχετικά με τους κινδύνους τόσο στο «παραδοσιακό» περιβάλλον όσο και στον κυβερνοχώρο
- β) η συγκρότηση & εκπαίδευση της Ομάδας Διαχείρισης Κρίσεων στον Κυβερνοχώρο ώστε να λειτουργεί αποτελεσματικά κατά την αντιμετώπιση τέτοιων κρίσεων
- γ) η επεξεργασία των εσωτερικών διαδικασιών που πρέπει να ακολουθούνται σε περίπτωση κρίσεων στον κυβερνοχώρο και
- δ) η ανάπτυξη ειδικών δεξιοτήτων για την ορθή επικοινωνιακή διαχείριση των κρίσεων

Στο εκπαιδευτικό πρόγραμμα θα παρουσιαστούν και θα αναλυθούν στα μέλη της Ομάδας Διαχείρισης Κρίσεων τα ακόλουθα:

A. Εκτίμηση της υφιστάμενης κατάστασης/ Communication Cyber Crisis Preparedness Assessment

- Αξιολόγηση του υφιστάμενου σχεδίου επικοινωνιακής διαχείρισης κρίσεων στον κυβερνοχώρο και του βαθμού ετοιμότητας του οργανισμού
- Αξιολόγηση του επιπέδου awareness υπαλλήλων και στελεχών σχετικά με ζητήματα ασφάλειας στον κυβερνοχώρο

B. Συγκρότηση της Ομάδας Διαχείρισης Κρίσεων στον Κυβερνοχώρο

Συγκρότηση ή αναδιάρθρωση της υφιστάμενης Ομάδας Διαχείρισης Κρίσεων με την προσθήκη νέων μελών, ανακατανομή αρμοδιοτήτων, καθορισμός ρόλων και διαδικασιών επικοινωνίας και συνεργασίας των μελών της κατά την διάρκεια μιας κρίσης στον κυβερνοχώρο.

Γ. Crisis Management Basics & Cyber Security Basics

- Οριοθέτηση cyber incident και cyber crisis
- Cyber threats landscape

Δ. Case studies

- Παρουσίαση και ανάλυση σημαντικών και περίπλοκων case studies. Αξιολόγηση της ετοιμότητας των εταιρειών που έπεσαν θύματα κυβερνοεπίθεσης, παρουσίαση και

αξιολόγηση της δημόσιας αντίδρασής τους, της επικοινωνίας τους με stakeholders και κοινό κατά την διάρκεια της κρίσης.

Ε. Σχεδιασμός Σεναρίων & Ανάπτυξη της Αντίδρασης της Ομάδας Διαχείρισης Κρίσεων στον Κυβερνοχώρο (Tabletop exercise)

- Σχεδιασμός και συνδιαμόρφωση των πιθανότερων, για τον οργανισμό, σεναρίων κρίσεων στον κυβερνοχώρο
- Παρουσίαση και εξάσκηση στις τεχνικές πρόληψης και διαχείρισης κρίσεων στον κυβερνοχώρο με βάση τα προεπιλεγμένα σενάρια. Προσομοίωση σε round table περιβάλλον

ΣΤ. Διαπραγματεύσεις

Workshop στις τεχνικές διαπραγμάτευσης που πρέπει να ακολουθηθούν σε περίπτωση κρίσης στον κυβερνοχώρο με hackers, media ή άλλους stakeholders.

Ζ. Media Training

- α) Εκπαίδευση των στελεχών της Ομάδας Διαχείρισης Κρίσεων στον Κυβερνοχώρο στις τεχνικές πρόληψης και διαχείρισης επικοινωνιακών κρίσεων στον κυβερνοχώρο,
- β) Οδηγίες για σύνταξη δελτίων τύπου, δηλώσεων, non papers,
- γ) Επιλογή των κατάλληλων καναλιών επικοινωνίας και τεχνικές παρέμβασης.

Η. Παραδοτέο

Δημιουργία εξειδικευμένου οδηγού Επικοινωνιακής Διαχείρισης Κρίσεων στον Κυβερνοχώρο.

7.1.5.2.3 Διαμόρφωση πλάνου ανάκαμψης από καταστροφές για κρίσιμες οντότητες

Ο κύριος στόχος του παρόντος είναι η εκπόνηση Πλάνου Ανάκαμψης από Καταστροφές (DRP) για τις κρίσιμες υποδομές. Επιμέρους στόχοι του Σχεδίου Ανάκαμψης από Καταστροφή αφορούν τα εξής:

- καθορισμός των υποδομών και των συστημάτων με προτεραιοποίησή τους, όσον αφορά στην ετοιμότητα ανάκαμψης από καταστροφή,
- καθορισμός των παραμέτρων και των εξαρτήσεων των υποδομών και των συστημάτων, σε σχέση και με την υποδομή εφεδρείας ανάκαμψης από καταστροφή
- καθορισμός των αποδεκτών διαστημάτων απώλειας πληροφοριών από τον προηγούμενο

συγχρονισμό δεδομένων (RecoveryPointObjective "RPO") και των αναγκών και αποδεκτών χρόνων ενεργοποίησης εκάστου υποσυστήματος (RecoveryTimeObjective "RTO")

- καθορισμός των αναγκών σε υποδομές εξυπηρετητών φιλοξενίας με όλα τα τεχνικά χαρακτηριστικά λειτουργίας τους και των απαραίτητων δικτυακών υποδομών
- καθορισμός του τρόπου – μεθόδου λειτουργίας των νέων συστημάτων ανάκαμψης από καταστροφή και της τεχνολογίας που θα επιλεγεί για τη συχνότητα συγχρονισμού – ενημέρωσης
- καθορισμός των αναγκών τροποποιήσεων ή αναβαθμίσεων που θα πρέπει να υλοποιηθούν στο υφιστάμενο DataCenter, για τη συνεργασία και συγχρονισμό με το DisasterRecoverySite
- καθορισμός τυχόν αναγκών για επέκταση συμβολαίων υποστήριξης των Αναδόχων των υφιστάμενων συστημάτων και υποδομών ή για υπογραφή νέων SLAs.

Για την επίτευξη των ανωτέρω στόχων, ο Ανάδοχος θα βασιστεί στις κατευθύνσεις και καλές πρακτικές του διεθνούς προτύπου ISO 22301:2012, το οποίο αποτελεί ένα πρότυπο που θεσπίζει καλές πρακτικές, ώστε:

- να συνταχθεί Πλάνο Ανάκαμψης από Καταστροφή (DRP) για τις εφαρμογές και τα συστήματα
- να αναπτυχθούν οι απαραίτητες διοικητικές και υποστηρικτικές διαδικασίες για τη συντήρηση και επικαιροποίηση τουDRP.

Επίσης θα ληφθούν υπόψη καλές πρακτικές που προκύπτουν από τα πρότυπα ISOPAS 22399:2007 και ISO/ IEC 27001:2013.

7.1.5.2.4 Εκπόνηση Μελέτης εξωτερικού και εσωτερικού περιβάλλοντος και την ανάδειξη βέλτιστων πρακτικών

Απαραίτητο συστατικό για τον αποτελεσματικό έλεγχο ασφάλειας των υποδομών και συστημάτων είναι η αντίληψη και η αξιολόγηση του ευρύτερου περιβάλλοντος στους τομείς της ασφάλειας των δικτύων / πληροφοριακών συστημάτων και της διασφάλισης του απορρήτου των επικοινωνιών. Επομένως, θα πρέπει να διενεργηθεί μια μελέτη της κατάστασης που επικρατεί και των πρακτικών που εφαρμόζονται στον τομέα ασφάλειας σε παρεμφερή συστήματα τόσο εντός της χώρας όσο και σε διεθνές επίπεδο. Σκοπός της μελέτης αυτής είναι να δημιουργηθεί μια ολοκληρωμένη βάση γνώσης για το πλήρες ιστορικό που αφορά την ασφάλεια και στη συνέχεια να εξαχθούν χρήσιμα συμπεράσματα, τα οποία θα αξιοποιηθούν από τον Ανάδοχο για να φέρει εις πέρας τις υπόλοιπες εργασίες που απαιτούνται.

Στο πλαίσιο της εργασίας αυτής, θα συλλεχθούν και στη συνέχεια επεξεργασθούν και αναλυθούν πληροφορίες και δεδομένα που αφορούν στην ασφάλεια παρόμοιων υποδομών και συστημάτων τόσο εντός της χώρας όσο και σε άλλες χώρες. Τα δεδομένα θα εστιάσουν κατ' ελάχιστον:

- Στα υιοθετημένα Συστήματα Διαχείρισης της Ασφάλειας των Πληροφοριών (ΣΔΑΠ) και τις υποκείμενες σε αυτά διαδικασίες, πολιτικές και πρακτικές
- Στους κινδύνους ασφάλειας, στις ευπάθειες ανάλογων συστημάτων και στις μεθόδους αποτίμησης της επικινδυνότητας που συνήθως εμφανίζονται ή εφαρμόζονται αντίστοιχα
- Στις αποτελεσματικές μεθόδους παρακολούθησης της ασφάλειας ανάλογων υποδομών και συστημάτων

- Στα καταξιωμένα εργαλεία και μηχανισμούς ΤΠΕ που χρησιμοποιούνται για τον επιτυχή έλεγχο ασφάλειας ανάλογων υποδομών και συστημάτων
- Στο ιστορικό περιστατικών ασφάλειας και στις μεθόδους αντιμετώπισης αυτών, από τα οποία να μπορεί να εξαχθεί χρήσιμη γνώση για την καλύτερη διασφάλιση της ασφάλειας

Τα συστήματα που θα αποτελέσουν αντικείμενο της παρούσας μελέτης, θα μπορούν να είναι είτε δημόσια είτε ιδιωτικά, αλλά θα πρέπει να παρουσιάζουν ανάλογα επιχειρησιακά χαρακτηριστικά με αυτά του Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο», ώστε να μπορούν στη συνέχεια να πραγματοποιηθούν οι ενέργειες παραλληλισμού μεταξύ τους και εξαγωγής χρήσιμων συμπερασμάτων. Για τη συλλογή των δεδομένων και τη δημιουργία μιας πλήρους και αντιπροσωπευτικής βάσης γνώσης ασφάλειας συστημάτων, απαιτείται όπως μελετηθούν τουλάχιστον τρεις (3) περιπτώσεις (businesscases) ανάλογων δικτύων, εκ των οποίων τουλάχιστον οι δύο (2) θα είναι οπωσδήποτε στο εξωτερικό, η καθεμία σε διαφορετική χώρα, τεχνολογικά προηγμένη όπως συγκεκριμένα είναι τα πλέον ανεπτυγμένα κράτη μέλη της Ευρωπαϊκής Ένωσης, οι ΗΠΑ, το Ισραήλ, η Ιαπωνία, η Νότια Κορέα, κλπ.

Παράλληλα με τη διερεύνηση της ασφάλειας των προαναφερθέντων έτερων συστημάτων, η παρούσα εργασία θα λάβει υπόψη και τις πλέον επιστημονικά καταξιωμένες μεθόδους και πρακτικές που εφαρμόζονται στην πρόληψη, αντιμετώπιση, και εν γένει διαχείριση της ασφάλειας παρόμοιων συστημάτων. Η πληροφορία αυτή θα αποτελέσει επίσης τμήμα της ολοκληρωμένης βάσης

7.1.5.2.5 Διαμόρφωση πολιτικής αντιγράφων ασφαλείας

Η πολιτική αντιγράφων ασφαλείας αποτελεί κρίσιμο παράγοντα για την επιχειρησιακή συνέχεια και τη δυνατότητα ανάκαμψης από καταστροφή.

Ο Ανάδοχος καλείται να διαμορφώσει πολιτική αντιγράφων ασφαλείας για τις υποδομές και τα πληροφοριακά συστήματα του Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο», η οποία θα περιλαμβάνει κατ' ελάχιστο τα εξής:

- Συχνότητα λήψης αντιγράφων ασφαλείας
- Τύπος δεδομένων / αρχείων τα οποία θα αφορά
- Τοποθεσία και μέσο λήψης αντιγράφων
- Χρόνος διατήρησης αντιγράφων
- Αρμοδιότητες προσωπικού και προμηθευτών σχετικά με τη λήψη αντιγράφων ασφαλείας
- Διαδικασίες και κανόνες ελέγχου της ακεραιότητας των αντιγράφων
- Διαδικασία ανάκτησης δεδομένων από τα αντίγραφα ασφαλείας

7.1.5.2.6 Διαμόρφωση Συστήματος Διαχείρισης της Ασφάλειας των Πληροφοριών (ΣΔΑΠ) με βάση το πρότυπο ISO 27001 & Εκπόνηση Μελέτης Ανάλυσης και Αξιολόγησης Κινδύνων

Για τη διαμόρφωση ενός ολοκληρωμένου ΣΔΑΠ για το Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο», ο Ανάδοχος θα πραγματοποιήσει τις ενέργειες που αναφέρονται στο πρότυπο ISO 27001 συμπεριλαμβανομένου του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR) και αφορούν στη Φάση "Plan" που αναφέρεται στο πρότυπο, όπως κατ' ελάχιστον αναφέρονται οι ακόλουθες:

- Θα ορίσει το Πεδίο Εφαρμογής του ΣΔΑΠ (scope and boundaries of the ISMS), όσον αφορά τα επιχειρησιακά χαρακτηριστικά του Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο» και τα αγαθά που πρέπει να προστατευθούν. Παράλληλα, θα καταγράψει τις συνιστώσες εκείνες του περιβάλλοντος που δεν θα περιλαμβάνονται στο πεδίο εφαρμογής, συνοδευμένες από κατάλληλη τεκμηρίωση για την εξαίρεση τους

- Θα ορίσει την πολιτική του ΣΔΑΠ, όσον αφορά το ευρύτερο περιβάλλον λειτουργίας
- Θα ορίσει τη μεθοδολογία αποτίμησης της επικινδυνότητας που θα εφαρμοστεί
- Θα προσδιορίσει τους κινδύνους που ενέχονται στη λειτουργία του Δικτύου
- Θα αναλύσει και θα εκτιμήσει τους κινδύνους αυτούς
- Θα προσδιορίσει και υπολογίσει μεθόδους για την αντιμετώπιση των κινδύνων
- Θα επιλέξει κατάλληλα σημεία ελέγχου (controls) αντιμετώπισης των κινδύνων
- Θα μεριμνήσει για να λάβει την έγκριση της Διοίκησης του Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο» όσον αφορά τους προτεινόμενους υπολειμματικούς κινδύνους
- Θα μεριμνήσει για να λάβει την έγκριση της Διοίκησης του Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο» για να υλοποιήσει και να λειτουργήσει το υιοθετημένο ΣΔΑΠ
- Θα προετοιμάσει μια Δήλωση Εφαρμοσιμότητας (Statement of Applicability), η οποία θα περιλαμβάνει τα προβλεπόμενα στο πρότυπο ISO 27001.

Στο πλαίσιο των ενεργειών διαμόρφωσης του ΣΔΑΠ, θα πραγματοποιήσει κατ' ελάχιστον τις παρακάτω εργασίες, τα αποτελέσματα των οποίων θα συμπεριληφθούν κατά περίπτωση στις πολιτικές, διαδικασίες σχέδια και λοιπά έγγραφα του ΣΔΑΠ.

Ανάλυση επιχειρησιακών επιπτώσεων

Ο Ανάδοχος θα εκπονήσει ανάλυση επιχειρησιακών επιπτώσεων, με την οποία θα εντοπίσει και καταγράψει τις επιχειρησιακές λειτουργίες και τους πόρους που υποστηρίζουν τις λειτουργίες αυτές και σχετίζονται ή μπορεί να επηρεάσουν την ακεραιότητα των υποδομών του Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο» και τη διαθεσιμότητα των παρεχόμενων από αυτήν υπηρεσιών.

Ανάλυση κινδύνου και αποτίμηση επικινδυνότητας

Ο Ανάδοχος θα πραγματοποιήσει μελέτη ανάλυσης κινδύνου και αποτίμησης επικινδυνότητας, προκειμένου να αναγνωρίσει και αναλύσει τις ενδεχόμενες απειλές στην ακεραιότητα των υποδομών.

Στο πλαίσιο της εργασίας αυτής, ο Ανάδοχος κατ' ελάχιστον:

- Θα μελετήσει και καταγράψει όλες τις απειλές και κινδύνους που πιθανά αντιμετωπίζει ή αναμένεται να αντιμετωπίσουν οι υποδομές.
- Θα κατηγοριοποιήσει και εξετάσει τις απειλές που θα αναγνωρίσει σε (α) ενδογενείς, οι οποίες προέρχονται από το εσωτερικό του συστήματος και εξαρτώνται από το επίπεδο της εσωτερικής αξιοπιστίας, ασφάλειας και ανθεκτικότητας, σε (β) εξωγενείς, οι οποίες προέρχονται από το εξωτερικό περιβάλλον, όπως καιρικές συνθήκες, φυσικές καταστροφές κλπ και (γ) σε απειλές που προέρχονται από άλλα διασυνδεδεμένα συστήματα ή δίκτυα. Παράλληλα, θα διενεργηθεί εκτίμηση της σοβαρότητας κάθε απειλής.
- Θα διενεργήσει μια συσχέτιση μεταξύ των διαθέσιμων πόρων (πληροφοριακά συστήματα, δίκτυα, εγκαταστάσεις, ανθρώπινο δυναμικό) και των εκτιμώμενων απειλών που δύναται να τους επηρεάσουν εφόσον εκδηλωθούν.
- Θα καταγράψει τα ευάλωτα σημεία και τις αδυναμίες των πόρων που απαιτούνται για τη συνέχιση κάθε επιχειρησιακής λειτουργίας. Στη συνέχεια θα αξιολογήσει την πιθανότητα εκδήλωσης των απειλών που έχει ήδη αναγνωρίσει και θα εκτιμήσει την επίδραση τους στη λειτουργία συστημάτων και υποδομών και τη διάθεση των παρεχόμενων υπηρεσιών.

- Θα αναλύσει τις ανάγκες και απαιτήσεις προστασίας.
- Θα προσδιορίσει και προτείνει τη διαδικασία που θα ακολουθήσει καθώς και τα μέτρα που θα λάβει, προκειμένου να αντιμετωπίσει κάθε ενδεχόμενη απειλή
- Θα προτείνει διαδικασίες αξιολόγησης της αποτελεσματικότητας των μέτρων που προτείνει να εφαρμοσθούν κατά περίπτωση απειλής.

Διαμόρφωση πολιτικών ασφάλειας κρίσιμων οντοτήτων με στόχο την ανάδειξη τεχνικών και οργανωτικών μέτρων για την προστασία τους από Κυβερνοαπειλές

Η διαμόρφωση πολιτικών θα πρέπει να είναι κατάλληλα δομημένη, ώστε να καλύπτει όλες τις παραμέτρους / συνιστώσες λειτουργίας των κρίσιμων υποδομών του Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο». Ειδικότερα, θα γίνει σαφής αναφορά και ανάλυση στα ακόλουθα:

- Εύρος των πολιτικών. Αρχικά θα προσδιοριστεί το σύνολο των αγαθών των κρίσιμων υποδομών του Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο», για τα οποία θα διαμορφωθούν οι πολιτικές και στη συνέχεια θα προσδιοριστούν και αναλυθούν οι απειλές που αντιμετωπίζουν τα αγαθά αυτά
- Ασφάλεια των υποδομών, των πληροφοριακών συστημάτων και των υποκείμενων δεδομένων
 - ο Φυσική ασφάλεια (μέθοδοι υλοποίησης, κανόνες προστασίας, κλπ)
 - ο Ασφάλεια δικτύου (VPNs, ασφάλεια συνδέσεων, συνδέσεις εξωτερικών συνεργατών, κανόνες πρόσβασης στο δικτυακό εξοπλισμό, κανόνες χρησιμοποίησης δικτύου, κλπ)
 - ο Ασφάλεια εξυπηρετητών (Διαχείριση, πρόσβαση, λογισμικό, δικτυακές υπηρεσίες, αναβάθμιση, προσθήκη νέου συστήματος, κλπ)
 - ο Συστήματα χρηστών (κανόνες ασφάλειας, διαχείριση χρηστών, λογισμικό χρηστών, πολιτικών κωδικών πρόσβασης (passwords))
 - ο Κακόβουλο λογισμικό
- Προστασία πληροφοριών (έλεγχος διασποράς στοιχείων, κρυπτογράφηση δεδομένων, διαχείριση στοιχείων που δίνονται σε τρίτους, κλπ)

Υλοποίηση και λειτουργία του ΣΔΑΠ

Για την υλοποίηση και λειτουργία του υιοθετημένου ΣΔΑΠ, ο Ανάδοχος θα πραγματοποιήσει τις ενέργειες που αναφέρονται στο πρότυπο ISO 27001 συμπεριλαμβανομένου του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR) και αφορούν στη Φάση "Do" που αναφέρεται στο πρότυπο, όπως κατ' ελάχιστον αναφέρονται οι ακόλουθες:

- Θα αναπτύξει ένα σχέδιο αντιμετώπισης των κινδύνων (risk treatment plan), το οποίο προσδιορίζει τις κατάλληλες ενέργειες που πρέπει να γίνουν για την ορθή διαχείριση των κινδύνων ασφάλειας
- Θα υλοποιήσει το σχέδιο αντιμετώπισης κινδύνων, ώστε να επιτύχει τους αντίστοιχους στόχους που έχουν τεθεί
- Θα υλοποιήσει τα σημεία ελέγχου (controls) για την αντιμετώπιση των κινδύνων, που έχουν επιλεγεί κατά τη φάση διαμόρφωσης του ΣΔΑΠ, ώστε να επιτευχθούν οι αντίστοιχοι στόχοι
- Θα ορίσει τους δείκτες με τους οποίους θα μετριέται η αποτελεσματικότητα των επιλεγθέντων μέτρων αντιμετώπισης και στη συνέχεια θα προσδιορίσει την αποτελεσματικότητα των δεικτών αυτών στην παραγωγή συγκρίσιμων και αναπαραγωγίμων αποτελεσμάτων
- Θα υλοποιήσει προγράμματα εκπαίδευσης και ευαισθητοποίησης

- Θα διαχειριστεί τη λειτουργία του ΣΔΑΠ
- Θα διαχειριστεί τους απαιτούμενους πόρους για τη λειτουργία του ΣΔΑΠ
- Θα υλοποιήσει διαδικασίες και όποια άλλα μέτρα κρίνει, ώστε να καταστεί δυνατή η έγκαιρη ανίχνευση περιστατικών ασφάλειας και η αποτελεσματική ανταπόκριση σε αυτά
- Θα προσδιορίσει και στη συνέχεια μεριμνήσει να διαθέσει τους πόρους που απαιτούνται:
 - ο για την ορθή διαμόρφωση, υλοποίηση, παρακολούθηση, ανασκόπηση, συντήρηση και βελτίωση του ΣΔΑΠ
 - ο ώστε να διασφαλιστεί ότι οι υιοθετημένες διαδικασίες ασφάλειας των πληροφοριών υποστηρίζουν τις επιχειρησιακές απαιτήσεις
 - ο για να προσδιοριστούν και αντιμετωπιστούν οι απαιτήσεις που προέρχονται από το υφιστάμενο νομικό ή ρυθμιστικό πλαίσιο καθώς και οι ενδεχόμενες συμβατικές υποχρεώσεις
 - ο Διατηρήσει ένα επαρκές επίπεδο ασφάλειας, εφαρμόζοντας κατάλληλα τα επιλεγμένα μέτρα ελέγχου για την αντιμετώπιση των κινδύνων
 - ο Εκπονεί ανασκοπήσεις του ΣΔΑΠ, όποτε κριθεί απαραίτητο και στη συνέχεια να ανταποκρίνεται κατάλληλα, ανάλογα με τα πορίσματα των ανασκοπήσεων αυτών
 - ο Να βελτιώνει την αποτελεσματικότητα του ΣΔΑΠ, όπου κριθεί απαραίτητο
- Θα εκπονήσει προγράμματα εκπαίδευσης και ευαισθητοποίησης σε όλα τα στελέχη της Αναθέτουσας Αρχής και του Φορέα Λειτουργίας, στα οποία τους έχουν ανατεθεί αρμοδιότητες που ορίζονται στο υιοθετημένο ΣΔΑΠ, ώστε αυτά να καταστούν ικανά να προβούν στην επιτυχή άσκηση των καθηκόντων τους.

Παρακολούθηση και ανασκόπηση του ΣΔΑΠ

Για την παρακολούθηση και ανασκόπηση του υιοθετημένου ΣΔΑΠ, ο Ανάδοχος θα πραγματοποιήσει τις ενέργειες που αναφέρονται στο πρότυπο ISO 27001 συμπεριλαμβανομένου του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR) και αφορούν στη Φάση "Check" που αναφέρεται στο πρότυπο, όπως κατ' ελάχιστον αναφέρονται οι ακόλουθες:

- Θα πραγματοποιήσει κατάλληλες διαδικασίες και ενέργειες παρακολούθησης και ανασκόπησης του ΣΔΑΠ
- Θα πραγματοποιεί τακτικές ανασκοπήσεις της αποτελεσματικότητας του ΣΔΑΠ, λαμβάνοντας υπόψη τα ευρήματα των εσωτερικών ελέγχων που θα πραγματοποιεί, τα συμπεράσματα που θα προκύπτουν από τα περιστατικά ασφάλειας που έχουν συμβεί, καθώς και τις προτάσεις άλλων εμπλεκόμενων φορέων
- Θα μετρήσει την αποτελεσματικότητα των μέτρων αντιμετώπισης των κινδύνων, ώστε να επιβεβαιώσει ότι ικανοποιούνται οι απαιτήσεις ασφάλειας
- Θα προβεί σε ανασκόπηση της αποτίμησης επικινδυνότητας σε τακτά χρονικά διαστήματα και των υπολειμματικών κινδύνων (residual risks) καθώς και τα επίπεδα κινδύνου που θεωρήθηκαν αποδεκτά, λαμβάνοντα υπόψη τα πλέον πρόσφατα δεδομένα
- Θα διενεργεί εσωτερικούς ελέγχους ασφάλειας σε τακτά χρονικά διαστήματα (που θα οριστούν επακριβώς κατά την Φάση ανάλυσης απαιτήσεων του έργου)
- Θα μεριμνήσει για την ανασκόπηση του υιοθετημένου ΣΔΑΠ από το αρμόδιο όργανο σε τακτά χρονικά διαστήματα
- Θα επικαιροποιεί τα σχέδια ασφάλειας, λαμβάνοντας υπόψη τα ευρήματα από τις ενέργειες παρακολούθησης και ανασκόπησης του ΣΔΑΠ
- Θα καταγράφει τις ενέργειες και τα γεγονότα, που θα μπορούσαν να έχουν επίπτωση στην αποτελεσματικότητα ή στην απόδοση του υιοθετημένου ΣΔΑΠ.

Συντήρηση και βελτίωση του ΣΔΑΠ

Για τη συντήρηση και βελτίωση του υιοθετημένου ΣΔΑΠ, ο Ανάδοχος θα πραγματοποιήσει τις ενέργειες που αναφέρονται στο πρότυπο ISO 27001 συμπεριλαμβανομένου του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR) και αφορούν στη Φάση "Act" που αναφέρεται στο πρότυπο, όπως κατ' ελάχιστον αναφέρονται οι ακόλουθες:

- Θα πραγματοποιήσει τις βελτιώσεις στο ΣΔΑΠ, που έχουν προσδιοριστεί
- Θα προβεί σε κατάλληλες διορθωτικές και προληπτικές ενέργειες, εφαρμόζοντας τα ευρήματα της αποτύπωσης κατάστασης και ειδικότερα τις βέλτιστες πρακτικές της Παρ. 1.3.1 και των υποπαραγράφων αυτής.
- Θα επικοινωνήσει τις ενέργειες βελτίωσης σε όλα τα εμπλεκόμενα μέρη, με όλα τα απαραίτητα στοιχεία και λεπτομέρειες
- Θα διασφαλίσει ότι οι πραγματοποιημένες βελτιώσεις επιτυγχάνουν το σχετικό στόχο τους.

7.1.5.2.7 Διενέργεια ελέγχων διείσδυσης εξωτερικών δικτύων, εφαρμογών Ιστού, φυσικής ασφάλειας και διαρροής δεδομένων

Έλεγχοι διείσδυσης εξωτερικών δικτύων

Στο σύγχρονο περιβάλλον κυβερνοαπειλών κάθε ευπάθεια μπορεί να αποτελέσει αντικείμενο εκμετάλλευσης με καταστροφικές συνέπειες. Οι έλεγχοι διείσδυσης εξωτερικών δικτύων (external network penetration test) εντοπίζουν ευπάθειες σε υποδομές, συσκευές και διακομιστές που είναι προσβάσιμες από το διαδίκτυο.

Οι έλεγχοι προσομοιάζουν τις επιθέσεις κακόβουλων εισβολέων, οι οποίοι έχουν ως στόχο τη ναπόκτηση πρόσβαση σε συστήματα και τις εφαρμογές της περιμέτρου. Η μέθοδος εκτέλεσης των ελέγχων θα πρέπει να εξασφαλίζουν ότι δεν θα προκληθούν φθορές ή οποιουδήποτε τύπου προβλήματα στη λειτουργία υποδομών και συστημάτων.

Έλεγχοι διείσδυσης εφαρμογών Ιστού

Οι δοκιμές διείσδυσης διαδικτυακών εφαρμογών στοχεύουν στον εντοπισμό τρωτών σημείων ασφαλείας που προκύπτουν από ανασφαλείς πρακτικές ανάπτυξης στη δημιουργία τη σχεδίαση και τη διαχείριση του λογισμικού ή ιστότοπου. Οι διαδικτυακές εφαρμογές χρησιμοποιούνται όλο και περισσότερο και αποτελούν κατεξοχήν στόχο κακόβουλων επιθέσεων. Στα πλαίσια των ελέγχων θα πρέπει να πραγματοποιηθεί μια σειρά προσομοιωμένων επιθέσεων, οι οποίες προσομοιάζουν κακόβουλες επιθέσεις, με σκοπό την αποτύπωση κάθε ευπάθειας και τη συνολική αποτίμηση του βαθμού ασφάλειας μιας εφαρμογής.

Έλεγχοι Φυσικής Ασφάλειας

Ο έλεγχος φυσικής ασφάλειας αξιολογεί τα μέτρα ασφαλείας που προστατεύουν τα περιουσιακά στοιχεία του οργανισμού από απειλές και στοχεύει σε προτάσεις για τυχόν βελτιώσεις. Οι έλεγχοι πρέπει να σχεδιάζονται με στόχο την παραβίαση της φυσικής ασφάλειας μίας ή περισσότερων τοποθεσιών. Τα σενάρια θα πρέπει να καθοριστούν βάσει ανάλυσης των υποδομών, με στόχο τη μη εξουσιοδοτημένη πρόσβαση σε φυσικές τοποθεσίες και πρόσβαση στο εσωτερικό δίκτυο με τη χρήση ειδικών συσκευών.

Ο υποψήφιος ανάδοχος καλείται να περιγράψει στην τεχνική του προσφορά τη μεθοδολογία εκτέλεσης των ελέγχων.

Έλεγχοι Διαρροής Δεδομένων

Οι έλεγχοι διαρροής δεδομένων αφορούνστη συγκέντρωση, ανάλυση και αξιολόγηση της βαρύτητας και του βαθμού ευαισθησίας πληροφοριών του οργανισμού από διάφορες πηγές (συμπεριλαμβανομένου του σκοτεινού διαδικτύου).

Ο έλεγχος θα πρέπει να αφορά πληθώρα δεδομένων, όπως ενδεικτικά ονόματα χρήστη και κωδικοί χρηστών, μηνύματα ηλεκτρονικού ταχυδρομείου κλπ. Στη συνέχεια θα πρέπει να προτείνονται μέτρα για την αντιμετώπιση ή το μετριασμό των συνεπειών της διαρροής και την αποφυγή της επανάληψής της.

Ο υποψήφιος ανάδοχος καλείται να περιγράψει στην τεχνική του προσφορά τη μεθοδολογία εκτέλεσης του συνόλου των παραπάνω ελέγχων.

7.1.5.2.8 Αξιοποίηση τεχνολογικής καινοτομίας και ερευνητικής πρωτοπορίας

Η διασφάλιση επαρκούς Επιχειρησιακής Συνέχειας, ειδικά απέναντι στο ενδεχόμενο κυβερνοεπιθέσεων, προϋποθέτει συνδυαστικές δράσεις πολλαπλής στόχευσης. Από τη μια πλευρά πρέπει να υπάρχει συστηματική μέριμνα για την αντιμετώπιση ήδη γνωστών τύπων κυβερνοαπειλών, με χρήση βέλτιστων πρακτικών και διαθέσιμων αποτελεσματικών τεχνολογιών. Από την άλλη, πρέπει να υπάρχει επίσης μέριμνα για την αντιμετώπιση καινοφανών κυβερνοεπιθέσεων, με αξιοποίηση προηγμένων μεθοδολογιών και τεχνολογικών λύσεων, όπως αυτές προκύπτουν, προδιαγράφονται και αξιολογούνται σε εξειδικευμένα ακαδημαϊκά ερευνητικά περιβάλλοντα.

Δεδομένων των ρηξικέλευθων εξελίξεων σε θέματα Κυβερνοασφάλειας, ο συνδυασμός βέλτιστων πρακτικών, δοκιμασμένων λύσεων και προηγμένων (state-of-the-art) μεθοδολογιών και τεχνολογιών αποτελεί το επαρκέστερο μέσο διασφάλισης της Επιχειρησιακής Συνέχειας. Συνεπώς, τα ζητούμενα πληροφοριακά συστήματα, τεχνολογικά προϊόντα και εξειδικευμένες υπηρεσίες θα πρέπει να παρέχονται με τρόπο που εγγυάται ότι όχι μόνο τα καταλληλότερα διαθέσιμα συστήματα της Αγοράς, αλλά και οι πρωτότυπες μεθοδολογίες και τεχνολογίες που παρέχει ο σχετικά εξειδικευμένος ακαδημαϊκός τομέας θα αξιοποιούνται συνδυαστικά.

Επιπρόσθετα, οι δόκιμες μεθοδολογίες και τεχνολογίες διασφάλισης της Επιχειρησιακής Συνέχειας προϋποθέτουν τακτικούς και συστηματικούς ελέγχους (penetration tests), αξιολογήσεις (audits), πιστοποιήσεις (certifications), μελέτες ανάλυσης και διαχείρισης επικινδυνότητας (risk analysis and management) κλπ., οι οποίες πρέπει να εκπονούνται σύμφωνα με διεθνή πρότυπα και αντίστοιχες καλές πρακτικές. Οι αδιαμφισβήτητες αυτές αναγκαιότητες, με τη σειρά τους, προϋποθέτουν συνθήκες λειτουργικής ανεξαρτησίας και αβίαστων επιστημονικών αποτιμήσεων, κάτι που μπορεί να εξυπηρετηθεί αποτελεσματικά με τη συνδρομή του εξειδικευμένου ακαδημαϊκού τομέα.

7.1.5.3 Εξειδικευμένες Λύσεις Ασφάλειας Πληροφοριών, Εγγράφων και εφαρμογών

7.1.5.3.1 Λύση Διαβάθμισης και Σήμανσης Εγγράφων

Η λύση Διαβάθμισης εγγράφων (Documents Classification) θα πρέπει να δίνει τη δυνατότητα στον χρήστη να επιλέξει και να αποδώσει με απλές κινήσεις, το κατάλληλο επίπεδο διαβάθμισης σε ένα έγγραφο, με βάση την Πολιτική Ασφάλειας του Φορέα. Το επιλεγμένο επίπεδο διαβάθμισης θα πρέπει να συνοδεύει το έγγραφο μέσω κατάλληλης σήμανσης στα μεταδεδομένα (metadata), αλλά και στην εμφάνιση του εγγράφου, ώστε να καθίσταται ορατό στους χρήστες, να εντείνεται η εγρήγορση του χρήστη (awareness) και να αποφεύγεται η κακή χρήση του εγγράφου λόγω αμέλειας. Η λύση

Διαβάθμισης εγγράφων θα πρέπει να συμπληρώνει και να αναδεικνύει της δυνατότητες του συστήματος DLP.

7.1.5.3.2 Λύση Προστασίας Δεδομένων από Διαρροή

Η επέκταση της ψηφιακής διαχείρισης εγγράφων σε συνδυασμό με τη διαθεσιμότητα πληθώρας διαφορετικών μεθόδων για την αποστολή και γενικά τη διακίνηση εγγράφων, έχει δημιουργήσει επιπλέον κινδύνους για τη διαρροή κρίσιμων εγγράφων εκτός του οργανισμού. Η λύση αποτροπής διαρροής πληροφοριών θα πρέπει να ανιχνεύει και να προλαμβάνει τη διακίνηση ευαίσθητων και εμπιστευτικών εγγράφων μέσω κάθε δυνατής οδού πχ μέσω αποσπώμενων αποθηκευτικών μέσων (usb), μέσω αλληλογραφίας (email), μέσω δικτυακής μεταφοράς αρχείων (ftp), μέσω internetupload, κλπ.

Η λύση θα πρέπει να εκμεταλλεύεται τη σήμανση των εγγράφων από λύσεις διαβάθμισης εγγράφων, για τον εντοπισμό ευαίσθητων και εμπιστευτικών εγγράφων.

7.1.5.3.3 Λύση Διαχείρισης Δικαιωμάτων Εγγράφων

Για την αποτελεσματική προστασία των εγγράφων του οργανισμού τα οποία πρέπει να υποστούν επεξεργασία από απομακρυσμένους χρήστες ή να διατηρηθούν σε υποδομές εκτός της περιμέτρου του οργανισμού, απαιτείται μία λύση διαχείρισης των δικαιωμάτων χρήσης των εγγράφων αυτών η οποία να επιτρέπει τον καθορισμό των δικαιωμάτων πρόσβασης στα έγγραφα αυτά και τον απομακρυσμένο έλεγχο τους (IRM - InformationRightsManagement). Η λύση πρέπει να προστατεύει τον οργανισμό από επιχειρηματικούς και κανονιστικούς κινδύνους που σχετίζονται με την μη αποδεκτή χρήση των εγγράφων του οργανισμού από εξωτερικούς συνεργάτες ή την χρήση τους για σκοπούς μη συμβατούς με τους σκοπούς επεξεργασίας που θέτει ο οργανισμός.

Η λύση πρέπει να είναι εύχρηστη ώστε οι κανόνες και οι πολιτικές προστασίας των εγγράφων να καθορίζονται από τους ίδιους τους χρήστες χωρίς να απαιτείται πάντα η εμπλοκή του τμήματος Πληροφορικής (IT). Οι κανόνες και οι πολιτικές προστασίας εγγράφων πρέπει να εφαρμόζονται είτε σε μεμονωμένους χρήστες είτε σε ομάδες χρηστών και να δίνουν την δυνατότητα στους ιδιοκτήτες των εγγράφων όχι μόνο να καθορίζουν τους χρήστες που έχουν δικαίωμα πρόσβασης στα έγγραφα,

αλλά και να εποπτεύουν την χρήση των εγγράφων ή να ανακαλούν τα δικαιώματα πρόσβασης. Η λύση

πρέπει να δίνει την δυνατότητα εφαρμογής πολιτικών και κανόνων προστασίας είτε σε μεμονωμένα έγγραφα είτε σε ομάδες εγγράφων που διατηρούνται σε φακέλους, fileservers, κλπ.

Αναλυτικότερα η λύση πρέπει να έχει τα χαρακτηριστικά που περιγράφονται στις επόμενες παραγράφους.

Καθορισμός δικαιωμάτων χρήσης και απομακρυσμένος έλεγχος επί των εγγράφων

- Η λύση πρέπει να επιτρέπει τον καθορισμό του είδους των δικαιωμάτων που έχει κάθε χρήστης επί του εγγράφου (πχ μόνο ανάγνωση, επεξεργασία, ορισμός δικαιούχων, κλπ)
- Η λύση πρέπει να δίνει την δυνατότητα εξ αποστάσεως αναίρεσης των δικαιωμάτων που έχουν παραχωρηθεί σε χρήστες ή διαγραφής ενός εγγράφου
- Η λύση πρέπει να δίνει την δυνατότητα ορισμού ημερομηνιών λήξης της ισχύος των δικαιωμάτων πρόσβασης.
- Η λύση πρέπει να δίνει την δυνατότητα σε διαχειριστές να καθορίζουν πολιτικές πρόσβασης και σε χρήστες να εφαρμόζουν αυτές τις πολιτικές πρόσβασης σε έγγραφα.

Απόδοση δικαιωμάτων σε χρήστες

- Η λύση πρέπει να έχει την δυνατότητα να αποδίδει συγκεκριμένα δικαιώματα πρόσβασης είτε σε μεμονωμένους χρήστες είτε σε ομάδες χρηστών.
- Η λύση πρέπει να δίνει την δυνατότητα καθορισμού των διαδικτυακών διευθύνσεων από τις οποίες επιτρέπεται η πρόσβαση στα έγγραφα.
- Η λύση πρέπει να αναγνωρίζει και να αυθεντικοποιεί τους χρήστες του οργανισμού μέσω πλήρους λειτουργικής διασύνδεσης με το AD του οργανισμού.
- Η λύση πρέπει να έχει την δυνατότητα απόδοσης συγκεκριμένων δικαιωμάτων πρόσβασης σε χρήστες που ανήκουν σε συγκεκριμένες ομάδες του οργανισμού (ActiveDirectorygroups).
- Η λύση πρέπει να δίνει την δυνατότητα να καθορίζονται ονομαστικά οι χρήστες (εσωτερικοί ή εξωτερικοί) στους οποίους επιτρέπεται η πρόσβαση στα έγγραφα του οργανισμού καθώς και το είδος της πρόσβασης που παρέχεται.
- Η λύση πρέπει να έχει την δυνατότητα αποστολής ειδοποιήσεων/προσκήσεων (invitations) σε εξωτερικούς χρήστες στους οποίους παραχωρείται πρόσβαση σε ένα έγγραφο.
- Οι χρήστες στους οποίους αποδίδεται δικαίωμα πρόσβασης πρέπει να μπορούν να διαχειρίζονται το έγγραφο χωρίς την χρήση ειδικών προγραμμάτων (transparency).

Είδη εγγράφων φακέλοι και μέσα αποθήκευσης

- Η λύση πρέπει να δίνει την δυνατότητα καθορισμού δικαιωμάτων πρόσβασης είτε σε διακριτά έγγραφα είτε σε όλα τα έγγραφα που διατηρούνται σε συγκεκριμένα διακριτά σημεία διατήρησης (φακέλους ή μέσα αποθήκευσης).
- Η λύση πρέπει να δίνει δυνατότητα καθορισμού δικαιωμάτων πρόσβασης σε αρχεία που διατηρούνται είτε σε τοπικούς servers είτε σε εφαρμογές νέφους (Office365, Dropbox, Sharepoint, κλπ).

- Ο τρόπος διαχείρισης των δικαιωμάτων πρόσβασης θα πρέπει να είναι ίδιος ανεξάρτητα από το μέσο διατήρησης των αρχείων (πχ. τοπικοί servers, ή εφαρμογές cloud).

Συμβατότητα και αλληλεπίδραση με εφαρμογές τρίτων κατασκευαστών

- Η λύση πρέπει να έχει πλήρη συμβατότητα με τις εφαρμογές του MicrosoftOffice και να δίνει δυνατότητα στους χρήστες των εφαρμογών να καθορίζουν τα δικαιώματα επί των εγγράφων μέσα από το περιβάλλον των ίδιων των εφαρμογών.
- Η λύση πρέπει να έχει πλήρη συμβατότητα με τις εφαρμογές Outlook και Exchange.
- Η λύση πρέπει να έχει δυνατότητα καθορισμού δικαιωμάτων και σε αρχεία pdf.
- Η λύση πρέπει να έχει την δυνατότητα λειτουργικής διασύνδεσης με λύση DLP (DataLossPrevention).
- Η λύση να έχει πλήρη συμβατότητα με την εφαρμογή SIEM

7.1.5.3.4 Λύση Διαχείρισης Λογαριασμών και Δικαιωμάτων Πρόσβασης Χρηστών

Η λύση Διαχείρισης Λογαριασμών και Δικαιωμάτων πρόσβασης χρηστών (Identity & Access Rights Management - IAM) θα πρέπει να διασυνδέεται και να επικοινωνεί με τα Πληροφοριακά Συστήματα του Οργανισμού (πιο συγκεκριμένα να διατεθούν adapters με τον ActiveDirectory και με μία βάση (Oracle ή MSSQL) του Φορέα), ώστε να ενημερώνεται σε πραγματικό χρόνο για τα accounts και τα δικαιώματα που διατηρούνται σε κάθε πληροφοριακό σύστημα. Επιπρόσθετα, η λύση IAM θα πρέπει να διασυνδέεται με το πληροφοριακό σύστημα στο οποίο διατηρείται το μητρώο των εργαζομένων και συνεργατών του Οργανισμού, ώστε να ενημερώνεται σε πραγματικό χρόνο για τα φυσικά πρόσωπα που εργάζονται για τον Οργανισμό, την θέση και τον ρόλο τους, καθώς και για οποιαδήποτε σχετική αλλαγή.

Βασική λειτουργικότητα της λύσης IAM θα πρέπει να είναι η αντιστοίχιση κάθε λογαριασμού (Account) σε φυσικό πρόσωπο, ώστε να μην υπάρχουν λογαριασμοί με άγνωστο ιδιοκτήτη, αλλά και ο εντοπισμός οποιουδήποτε λογαριασμού δημιουργείται από ανώνυμο εισβολέα. Με τον τρόπο αυτό, θα πρέπει να εξασφαλίζεται ότι για κάθε λογαριασμό υπάρχει κάποιο φυσικό πρόσωπο που φέρει την ευθύνη του, και ότι για κάθε εξουσιοδοτημένο χρήστη υπάρχει πλήρης εικόνα για τα δικαιώματα πρόσβασης που του έχουν αποδοθεί. Η λύση IAM θα πρέπει να έχει τη δυνατότητα να αυτοματοποιεί τις ροές εργασιών μέσω από τις οποίες δημιουργούνται ή αναιρούνται λογαριασμοί και δικαιώματα πρόσβασης, να αποφεύγονται ανθρώπινα λάθη και παραλείψεις κατά την απόδοση ή αναίρεση λογαριασμών και δικαιωμάτων πρόσβασης.

7.1.5.3.5 Λύση Διαχείρισης Προνομιούχων Λογαριασμών Πρόσβασης

Ορισμένοι χρήστες έχουν πρόσθετα δικαιώματα, λόγω της φύσης του ρόλου που επιτελούν εντός του οργανισμού. Για τον λόγο αυτό, απαιτείται η ύπαρξη επιπλέον μηχανισμών που θα προστατεύουν από μη εξουσιοδοτημένη χρήση των λογαριασμών των εν λόγω χρηστών. Η λύση θα πρέπει να περιλαμβάνει κατ' ελάχιστο:

- Ασφαλή διαχείριση των κωδικών πρόσβασης των διαχειριστών συστημάτων και εφαρμογών, συμπεριλαμβανομένου ασφαλούς αποθετηρίου των κωδικών πρόσβασης.
- Μηχανισμούς επιβολής κανόνων συνθετότητας και αποφυγής ανακύκλωσης των κωδικών πρόσβασης και προσωποποίησης των κοινόχρηστων (Shared) accounts
- Μηχανισμούς λογοδοσίας για τη χρήση των λογαριασμών

- Καταγραφή των ενεργειών των διαχειριστών σε κρίσιμα συστήματα και εφαρμογές

7.1.5.4 Υπηρεσίες νεφοϋπολογιστικών υποδομών και υπηρεσιών

7.1.5.4.1 Υπηρεσίες ανάκαμψης από καταστροφή και λήψης αντιγράφων ασφαλείας

Μεσκοπό την ενίσχυση της επιχειρησιακής συνέχειας, απαιτείται η παροχή υπηρεσιών λήψης Αντιγράφων ασφαλείας (Backup) και ανάκαμψης από καταστροφή (Επαναφοράς (Recovery)). Απαιτείται να λαμβάνονται αντιγράφα ασφαλείας σε υπολογιστικούς πόρους που βρίσκονται εγκατεστημένοι είτε τοπικά (On-premises) είτε στον πάροχο του Νέφους (Cloud). Ως προστατευόμενοι υπολογιστικοί πόροι δύναται να θεωρηθούν στοιχεία όπως [VMs, DBs, Folders/Files]. Επίσης, θα υπάρχει η δυνατότητα επιλογής επαναφοράς των προστατευμένων υποδομών είτε τοπικά (On-premises) είτε στον πάροχο του Νέφους (Cloud). Θα υπάρχουν επιλογές της υπηρεσίας αυτής με βάση τον όγκο των προστατευόμενων πόρων/δεδομένων ώστε να καλύπτονται διαφορετικού τύπου ανάγκες.

Ο ανάδοχος είναι υπεύθυνος και για την Εγκατάσταση / παραμετροποίηση υπηρεσιών ανάκαμψης από καταστροφή και λήψης αντιγράφων ασφαλείας ανάλογα με τις ανάγκες.

7.1.5.5 Υπηρεσίες SOC & Ddos

Οι υπηρεσίες αφορούν αδιάλειπτης και σε πραγματικό χρόνο (24x7) επιτήρησης των συστημάτων του Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο» από εξειδικευμένο και σε διεθνώς αναγνωρισμένο πάροχο για την πρόληψη και αντιμετώπιση κυβερνοαπειλών, καθώς επίσης και ανίχνευσης επιθέσεων DDoS σε πραγματικό χρόνο.

Η πρωτοβουλία στοχεύει στην ενδυνάμωση του επιπέδου ασφαλείας για τις υποδομές του Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο» και η πλήρης συμμόρφωση της με τις κανονιστικές απαιτήσεις (όπως ο νόμος ν. 4577/2018 «Ενσωμάτωση στην ελληνική νομοθεσία της Οδηγίας 2016/1148/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφαλείας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση και άλλες διατάξεις», ο Γενικός Κανονισμός Προσωπικών Δεδομένων, κλπ.).

Το έργο θα αντιμετωπίσει τις προκλήσεις που σχετίζονται με α) την πολυπλοκότητα του περιβάλλοντος των υποδομών του Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο» και των διαδικασιών παρακολούθησής τους καθώς και β) την έλλειψη εξειδικευμένων σχετικών εργαλείων και τεχνογνωσίας με αποτέλεσμα την περιορισμένη δυνατότητα εντοπισμού και αποτροπής κυβερνοεπιθέσεων οι οποίες αποτελούν μια από τις μεγαλύτερες σύγχρονες απειλές.

Ειδικότερα, μέσω της υπηρεσίας επιτήρησης των συστημάτων του Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο» σε πραγματικό χρόνο (24x7) θα διασφαλίζεται ο συνεχής έλεγχος της ασφαλείας των συστημάτων, ο έγκαιρος εντοπισμός επιβεβαιωμένων περιστατικών ασφαλείας καθώς και η λήψη των κατάλληλων ενεργειών πρόληψης και αντιμετώπισης των εν λόγω περιστατικών, από τον ανάδοχο, σε 24ωρη βάση. Ο Ανάδοχος θα έχει τη τεχνική δυνατότητα να εκτελέσει συγκεκριμένες ενέργειες για την αντιμετώπιση/ περιορισμό (containment) περιστατικών. Άλλες ενέργειες (όπως για παράδειγμα μία αλλαγή σε ένα firewall κλπ.) θα πρέπει να γίνεται από μηχανικό του Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο» με δικαιώματα διαχείρισης (admin rights) πάνω στα συστήματα.

Απώτερος σκοπός του προτεινόμενου έργου είναι η δυνατότητα έγκαιρης προειδοποίησης και απόκρισης έναντι κυβερνοαπειλών, με την αξιοποίηση κατάλληλων τεχνικών μέτρων, ώστε να

διασφαλιστούν οι επιχειρησιακές λειτουργίες του Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο» και να παραμένουν ασφαλείς μέσω της προληπτικής παρακολούθησης και αντιμετώπισης έναντι των κυβερνοαπειλών.

Οι τεχνικές προδιαγραφές της υπηρεσίας SoCaaS & DDoS παρουσιάζονται αναλυτικά στους πίνακες συμμόρφωσης 7.2.3.1 και 7.2.3.2.

Οι υπηρεσίες που θα παρασχεθούν στο πλαίσιο του παρόντος έργου παρουσιάζονται παρακάτω, κατανεμημένες ανά φάση.

7.1.5.5.1 Προπαρασκευαστική Φάση

Στην προπαρασκευαστική φάση του έργου περιλαμβάνονται οι κάτωθι δραστηριότητες:

- Καταγραφή της αρχιτεκτονικής της υποδομής και των πληροφοριακών εργαλείων του Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο».
- Εκτίμηση και αξιολόγηση των αναγκών του Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο».
- Εκτίμηση αναγκών για παρακολούθηση της Υποδομής του Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο», όσο και των Servers και virtual servers.
- Προτεραιοποίηση των συστημάτων του Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο» προς ένταξη στο πεδίο εφαρμογής του Κέντρου Επιχειρήσεων Ασφαλείας (Security Operations Center – SOC).

7.1.5.5.2 Υλοποίηση Έργου

Κατά τη φάση υλοποίησης του έργου θα πραγματοποιηθούν οι εξής δραστηριότητες:

- Ανάπτυξη Τεκμηρίωσης σχετικά με το SOCaaS: Καταγραφή, σχεδιασμός και τεκμηρίωση, όλων των απαραίτητων πολιτικών, διαδικασιών (συμπεριλαμβανομένων των σχετικών διαδικασιών του Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο»), τεχνικών προτύπων κι οδηγιών, για την αξιοποίηση των τεχνικών λύσεων και υπηρεσιών παρακολούθησης ασφάλειας, αναφορικά με τον καθορισμό πλαισίου διαχείρισης και απόκρισης σε συμβάντα κυβερνοεπιθέσεων. Η ενδεικτική τεκμηρίωση περιλαμβάνει: Εγχειρίδια χρήσης των Web Consoles (Web Consoles Manuals), Διαδικασία Κλιμάκωσης Περιστατικών (Incident Escalation Process), Διαδικασία Διαχείρισης Αλλαγών (Change Management Process), Διαδικασία Διαχείρισης Προβλημάτων (Problem Management Process).
- Παραμετροποίηση Υποδομής του Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο» για την Ενσωμάτωση συσκευών στο SOCaaS, μέσα από αναλυτικές οδηγίες παραμετροποίησης που θα κατατεθούν από τον Ανάδοχο.
- Οδηγίες Παραμετροποίησης Συστημάτων - Παροχή γραπτών αναλυτικών οδηγιών στο Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο» για την ενεργοποίηση/ παραμετροποίηση των μηχανισμών συλλογής logs από τα συστήματά της, καθώς και υποστήριξη της κατά τη διάρκεια της διαδικασίας αυτής.
- Εγκατάσταση μηχανισμών και λογισμικού για τη συλλογή logs από τα συστήματα του Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο» εφόσον απαιτείται.
- Ενεργοποίηση της Πλατφόρμας SOCaaS.
- Εγκατάσταση μηχανισμών και λογισμικού για τη διαχείριση των logs από τις συσκευές του Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο».

- Ενεργοποίηση προσβάσεων για το Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο» στις διεπαφές της Πλατφόρμας SOCaaS.
- Καταγραφή των κανόνων διαχείρισης συμβάντων μεταξύ παρόχου και του Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο».
- Καταγραφή των επικοινωνιών, των πληροφοριών και των διαδικασιών διαχείρισης (management), αναφορικά με περιστατικά που προκύπτουν.
- Ενεργοποίηση προϋπάρχοντος περιεχομένου και ανάπτυξη περιεχομένου όπως κανόνες συσχέτισης, αλγόριθμοι και αναφορές, προσαρμοσμένες στα ειδικά χαρακτηριστικά των υποδομών του Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο».
- Χρήση υφιστάμενης τεχνογνωσίας όπως κανόνες συσχέτισης, αλγόριθμοι ανάλυσης δεδομένων και εντοπισμού περιστατικών ασφάλειας και αναφορές, προσαρμοσμένες στα ειδικά χαρακτηριστικά των υποδομών του Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο» καθώς και ανάπτυξη νέων καθ' όλη τη διάρκεια της συμβάσης.
- Προσαρμογή των οργανωτικών δομών του Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο» (ανάθεση ρόλων, δημιουργία ομάδων εργασίας, δημιουργία νέας δομής, κλπ) για την υποστήριξη των περιγραφόμενων υπηρεσιών.
- Εκπαίδευση του αρμόδιου προσωπικού του Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο» πριν την έναρξη της υπηρεσίας παρακολούθησης.
- Ειδικά για το σύστημα ανίχνευσης δικτυακών ανωμαλιών και αντιμετώπισης επιθέσεων άρνησης υπηρεσίας (DDoS - Distributed Denial-of-Service), η προσφερόμενη λύση θα πρέπει να βασίζεται σε εξειδικευμένη συσκευή προστασίας από επιθέσεις τύπου DoS/DDoS η οποία έχει σχεδιαστεί ειδικά για να παρέχει on-premise προστασία της διαθεσιμότητας των δικτυακών πόρων από μια συνεχώς επεκτεινόμενη γκάμα απειλών σε επίπεδο εφαρμογής (application-level), διασφαλίζοντας έτσι την αξιόπιστη πρόσβαση σε δικτυακές υπηρεσίες ζωτικής σημασίας και την επιχειρησιακή συνέχεια της Αναθέτουσας Αρχής. Η συσκευή αυτή θα πρέπει να διαθέτει την κατάλληλη stateless τεχνολογία ανίχνευσης και φιλτραρίσματος, η οποία θα της επιτρέψει να παραμείνει σε λειτουργία κατά την διάρκεια εκδήλωσης επιθέσεων μικρού όγκου (low volume attacks), οι οποίες έχουν σχεδιαστεί με στόχο να θέτουν εκτός λειτουργίας μηχανισμούς όπως τα firewalls και τα IPS.

Η προσφερόμενη λύση θα πρέπει κατ' ελάχιστο να περιλαμβάνει τις παρακάτω λειτουργίες:

- Προστασία από γνωστές και άγνωστες επιθέσεις – Η προσφερόμενη λύση θα πρέπει να ανιχνεύει επιθέσεις τύπου DoS/ DDoS βάση υπογραφών και συμπεριφοράς
- Προστασία από επιθέσεις βασιζόμενες στον δικτυακό όγκο - Η προσφερόμενη λύση θα πρέπει να διαχειρίζεται επιθέσεις τύπου DoS/ DDoS μεγάλου όγκου δικτυακής κίνησης.
- Προστασία από επιθέσεις σε επίπεδο εφαρμογών – Η προσφερόμενη λύση θα πρέπει να προστατεύει εφαρμογές όπως IIS, Apache, κ.λπ. από επιθέσεις τύπου DoS/ DDoS.
- Προστατεύει από επιθέσεις σε επίπεδο πρωτοκόλλου - Η προσφερόμενη λύση θα πρέπει να διαχειρίζεται επιθέσεις τύπου DoS/ DDoS σε πρωτόκολλα όπως HTTP, SMTP κ.λπ.

7.1.5.5.3 Παρακολούθηση (Monitoring)

Η έναρξη παρακολούθησης μέσω του Κέντρου Επιχειρήσεων Ασφαλείας (Security Operations Center – SOC) / SOCaaS οριοθετείται από τη στιγμή της ενσωμάτωσης των πρώτων συστημάτων / υποδομών του Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο».

Στη φάση αυτή περιλαμβάνονται οι κάτωθι δραστηριότητες:

- Παρακολούθηση 24/7 των υποδομών του Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο»
 - ο Το SOCaaS λειτουργεί σε πραγματικό χρόνο, σε συνεχή βάση 24x7 και επιτηρεί (monitor) προληπτικά συστήματα και εφαρμογές προς αναζήτηση ύποπτης δραστηριότητας.
 - ο Αποτέλεσμα της παρακολούθησης είναι η επισήμανση περιστατικών προς περαιτέρω ανάλυση, έρευνα ή ανθρώπινη και πλήρως εξειδικευμένη δράση.
 - ο Το SOCaaS εντοπίζει τη συνάφεια οποιουδήποτε δοθέντος συμβάντος τοποθετώντας το στο πλαίσιο του ποιος, τι, που, πότε και γιατί συνέβη το συμβάν, προκειμένου να αποκομίσει τον αντίκτυπο του σε όρους επιχειρηματικού κινδύνου. Τα αρχεία καταγραφών (logs) των υποδομών του Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο» που συλλέγονται από πολλαπλές πηγές, όπως συστήματα ασφάλειας, συσκευές δικτύου, διακομιστές, εφαρμογές και βάσεις δεδομένων κλπ. αλληλοσυσχετίζονται, καθώς και αναλύονται έναντι δεδομένων threat intelligence, προκειμένου να εντοπιστούν πραγματικά περιστατικά ασφάλειας σε πραγματικό χρόνο.
- Άμεση σε πραγματικό χρόνο απόκριση σε περιστατικά ασφάλειας (incident response). Ανταπόκριση από ομάδα ανταπόκρισης συμβάντων ασφαλείας, συμπεριλαμβανομένης της ανάλυσης και επικύρωσης των ειδοποιήσεων, της ερμηνείας τους σε σημαντικές και εφαρμόσιμες πληροφορίες, κλιμάκωση βάσει αμοιβαία συμφωνημένων κανόνων διαχείρισης συμβάντων και καθοδήγηση καθ' όλη τη διάρκεια του κύκλου ζωής των περιστατικών ασφαλείας μέχρι τον μετριασμό και την αποκατάστασή τους.
- Πραγματοποίηση άμεσης επικοινωνίας με τα εξουσιοδοτημένα φυσικά πρόσωπα 'Single Points of Contact' (SPOC) που θα έχουν οριστεί από το Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο» για την ενημέρωση και την αντιμετώπιση κρίσιμων συμβάντων ασφαλείας,
- Ενεργοποίηση και διαρκής ανάπτυξη, ανάπτυξη περιπτώσεων χρήσης 'use cases' και περιεχομένου όπως κανόνες συσχέτισης, αλγόριθμοι και αναφορές, προσαρμοσμένες στα ειδικά χαρακτηριστικά των υποδομών του Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο».
- Αξιοποίηση περιεχομένου όπως κανόνες συσχετισμού, δηλαδή εκτέλεση της βασικής επεξεργασίας συμβάντων με βάση τους πραγματικούς κανόνες και τη συμπεριφορική ανάλυση των δεδομένων που τροφοδοτούν τα σενάρια.
- Συσχέτιση των πληροφοριών ασφάλειας των logs των συστημάτων του Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο» τόσο μεταξύ τους όσο και σε σχέση με το εξωτερικό περιβάλλον.
- Δυνατότητα επεκτασιμότητας της παρεχόμενης υπηρεσίας για τη σε βάθος ανάλυση μεγάλων όγκων αρχείων καταγραφής (logs).
- Παραγωγή Αναφορών (Reporting)
- Πλήρης διαφάνεια προς το Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο» της λειτουργικότητας της Πλατφόρμας παροχής της SOCaaS υπηρεσίας, μέσω της οποίας παρουσιάζονται στον χρήστη:
 - ο Τα δεδομένα που συλλέγονται, αναλύονται και δρομολογούνται με τη χρήση του αντίστοιχου διαύλου, στην αρχική τους μορφή,
 - ο Οι συσχετισμοί που παράγονται από την παροχή της υπηρεσίας για τον εντοπισμό συμβάντων και ύποπτων δραστηριοτήτων,

- Οι ειδοποιήσεις που δημιουργούνται από την παροχή της υπηρεσίας σε περιπτώσεις πιθανών κακόβουλων δραστηριοτήτων και οι οποίες κατευθύνονται και αναλύονται από το Κέντρο Επιχειρήσεων Ασφαλείας (SOC),
- Τα περιστατικά ασφάλειας/ συμβάντα, τα οποία διαχειρίζονται και αναλύονται από το Κέντρο Επιχειρήσεων Ασφαλείας (SOC),
- Όλα τα περιστατικά που κοινοποιήθηκαν στο Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο» διότι κρίθηκε αναγκαία η συμμετοχή του προσωπικού της και αφορούν τα περιστατικά και τους κινδύνους που αξιολογήθηκαν ως σημαντικοί.
- Ενοποιημένη εικόνα όλων των δεδομένων που καταγράφηκαν και αναλύθηκαν από το προσωπικό του Κέντρου Επιχειρήσεων Ασφαλείας (SOC).
- πίνακες (dashboards) με την απεικόνιση δεδομένων σχετικών με το SOCaaS,
- ειδοποιήσεις (alerts) και τις σχετικές με τις ειδοποιήσεις πληροφορίες που λαμβάνουν οι αναλυτές σε μία ενοποιημένη εικόνα,
- καταγραφή των περιστατικών (incidents) και στατιστικά στοιχεία που σχετίζονται με αυτά,
- αυτοματοποιημένες μετρήσεις διαθεσιμότητας και αντίστοιχοι δείκτες που σχετίζονται με τα επίπεδα παροχής της υπηρεσίας (KPIs),
- δυνατότητα παρουσίασης όλων των συσκευών και των τεχνολογικών στοιχείων που συμμετέχουν στην υπηρεσία, κ.α.
- Συστήματος διαχείρισης περιστατικών ασφάλειας για την παρακολούθηση περιστατικών ενώ χρησιμοποιούνται χαρακτηριστικά κλιμάκωσης περιστατικών.
- Εντοπισμός ευπαθειών στις υποδομές του Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο»
 - Εκτέλεση τακτικών ελέγχων ευπαθειών (Vulnerability Scan) στις υποδομές που έχουν ενσωματωθεί στην υπηρεσία .
 - Παροχή πλατφόρμας διαχείρισης ευπαθειών μέσω της οποίας εκτελείται η διαχείριση των ευπαθειών με δυνατότητα πρόσβασης από το προσωπικό του Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο» για την ανάθεση ευπαθειών σε προσωπικό του Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο» προς διόρθωση, την παροχή πληροφοριών για τις τρέχουσες εκτελούμενες δραστηριότητες διόρθωσης ευπαθειών την παρακολούθηση του κύκλου ζωής των ευπαθειών, καθώς και την παρουσίαση της τρέχουσας κατάστασης του Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο».
- Συνεχής βελτιστοποίηση της υπηρεσίας SOCaaS
 - Ανάλυση και βελτιστοποίηση των αρχείων καταγραφής (logs) κατά τη διάρκεια της ημερήσιας λειτουργίας, σύμφωνα με τα περιστατικά που προκύπτουν.
 - Διαχείριση Πληροφοριών Ασφαλείας και Γεγονότων και ενημέρωση του προσωπικού του Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο» που είναι αρμόδιο να τα χειριστεί.
 - Βελτιστοποίηση των κανόνων εφαρμογής και λειτουργίας.
 - Αναφορές λειτουργίας κατά την προοδευτική ενσωμάτωση των νέων πληροφοριακών συστημάτων του Δημόσιου Τομέα.

7.1.5.6 Εξειδικευμένες λύσεις ασφάλειας

7.1.5.6.1 Πλατφόρμα Κυβερνοασφάλειας – Εκτεταμένης Ανίχνευσης & Απόκρισης (Cyber Security)

Η πλατφόρμα πρέπει να αποτελεί μια ολοκληρωμένη λύση open XDR (Extended Detection & Response) με χαρακτηριστικά και λειτουργίες Next Gen SOC (Security Operation Center), η οποία να εξασφαλίζει την κεντρική παρακολούθηση και διαχείριση, αποφεύγοντας παλαιού τύπου τεχνικές με την εγκατάσταση διαφορετικών ξεχωριστών απλών εργαλείων SIEM (Security Information & Events Management) και άλλων που εγκαθίσταται και διαχειρίζονται ξεχωριστά ή απαιτείται χειροκίνητη ξεχωριστή διαδικασία ενσωμάτωσής του.

Η πλατφόρμα πρέπει να έχει τη δυνατότητα συλλογής και επεξεργασίας από πολλαπλών τύπων πηγές δεδομένων και όχι μόνο αρχείων καταγραφής, κινούμενη στη φιλοσοφία του big data security analytics. Συνδυάζοντας πληροφορίες από δικτυακή κίνηση (network traffic), user data, cloud data, file data στόχος είναι η εξάλειψη πιθανών τυφλών σημείων και ο συσχετισμός όλων των δεδομένων για την παραγωγή καλύτερων αποτελεσμάτων. Μέσα από αυτοματοποιημένες διαδικασίες εμπλουτισμού και συσχετισμών, τα δεδομένα θα βελτιστοποιούνται για αξιοποίηση από μηχανισμούς έρευνας και εντοπισμού. Ειδικότερα με την εκμετάλλευση αυτοματοποιημένης επεξεργασίας και μηχανικής μάθησης, το σύστημα θα πρέπει να μπορεί να λειτουργεί αποτελεσματικά ως ένα ολοκληρωμένο κέντρο αναφοράς και αυτόματης πρότασης και λήψης αντιμέτρων. Το σύστημα θα πρέπει κατ' ελάχιστον να συνοδεύεται από τεχνολογίες SIEM, NTA και Threat Intelligence και να μην απαιτείται η ξεχωριστή προμήθεια λογισμικού.

Το προσφερόμενο σύστημα θα πρέπει να έχει τη δυνατότητα να υποστηρίζει και το μοντέλο MDR (Managed Detection & Response) και στο σύνολό του θα πρέπει να υποστηρίζει όλο τον κύκλο ζωής αναγνώρισης και αντιμετώπισης απειλών, που αναλύεται στα στάδια:

- Συλλογή (Collect)
- Εντοπισμός (Detect)
- Έρευνα (Investigate)
- Απόκριση (Respond)

Το υπο προμήθεια σύστημα θα πρέπει να περιλαμβάνει την προμήθεια, εγκατάσταση και παραμετροποίηση αισθητήρων ασφαλείας (φυσικών ή εικονικών), οι οποίοι θα εφαρμόζουν λειτουργίες ML-IDS, antivirus, sandboxing και NTA.

Χαρακτηριστικά Next Gen Soc

- Μοντέρνο περιβάλλον χρήσης (GUI) που ενσωματώνει απαραίτητες λειτουργίες παρακολούθησης και διαχείρισης.
- Πρόσβαση με χρήση ρόλων χρηστών (RBAC – Role Based Access) για την διαχείριση δικαιωμάτων (user privilege management)
- Υποστήριξη πολλαπλών ενοίκων (multi-tenant) για την ξεχωριστή διαχείριση οντοτήτων, φυσικών δικτύων κτλ
- Εφαρμογή ξεχωριστού μοντέλου μηχανικής μάθησης ανά tenant για τη βελτίωση ακρίβειας των αποτελεσμάτων και τη μείωση των εσφαλμένων θετικών συμβάντων (false positives), εφαρμόζοντας ξεχωριστά συμπεριφορικά μοντέλα.
- Εξελιγμένες δυνατότητες μηχανικής μάθησης Δυνατότητες ενσωμάτωσης με εργαλεία και τεχνολογίες ασφαλείας Firewalls, WAF, EDR, SOAR κτλ
- Υποστήριξη API για ενσωμάτωση με τεχνολογίες HoneyPots, εργαλεία OSINT κτλ.
- Μία ενοποιημένη, υψηλής απόδοσης, αποθήκη δεδομένων ("Big Data" High Speed Lake)
- Δυνατότητα εγκατάστασης τόσο σε φυσικό εξοπλισμό, όσο και σε εικονικό ή περιβάλλον cloud
- Κατανεμημένη και επεκτάσιμη αρχιτεκτονική που να υποστηρίζει ωστόσο και "All In One" σενάρια.

- Υψηλή διαθεσιμότητα με τη χρήση clusters και ευέλικτη τήρηση και αποθήκευση δεδομένων.
- Μηχανισμοί Συλλογής που να μπορούν να εγκατασταθούν τόσο σε φυσικό όσο και σε εικονικό περιβάλλον
- Το σύστημα θα πρέπει να ακολουθεί ανοιχτή αρχιτεκτονική που να επιτρέπει την εισαγωγή δεδομένων από οποιαδήποτε συσκευή με τη χρήση Integration APIS.
- Κεντροποιημένη διαχείριση
- Απλό ενοποιημένο μοντέλο αδειών χωρίς επιπλέον κόστη

Next-Generation SIEM

Η πλατφόρμα θα πρέπει να βασίζεται σε μια ενοποιημένη αποθήκη δεδομένων βασισμένη στην αρχιτεκτονική του big data lake. Τα δεδομένα θα πρέπει κατ' ελάχιστον να μπορούν να εισαχθούν μέσω syslog. Όπου είναι εφικτό θα πρέπει να παρέχεται η δυνατότητα χρήσης parsers για κυριότερες και δημοφιλέστερες λύσεις δικτύων και ασφαλείας ώστε οι πληροφορίες να κανονικοποιούνται και να συσχετίζονται με αυτοματοποιημένο τρόπο. Θα πρέπει να παρέχονται οι παρακάτω ελάχιστες λειτουργικότητες:

- Απλός όσο και εξεζητημένος μηχανισμός αναζήτησης που να βασίζεται σε λογικούς τελεστές (Boolean modifiers)
- Οι αναζητήσεις να μπορούν να εφαρμοστούν ως μόνιμα φίλτρα σε όλο το περιβάλλον για ταχύτερη διερεύνηση και ανάλυση περιστατικών.
- Υψηλής απόδοσης και άμεσες ανταποκρίσεις στην αναζήτηση και το φιλτράρισμα στο big data
- Πρόσβαση σε πηγές δεδομένων και όχι μόνο σε syslog δεδομένα
- Συλλογή δεδομένων από δικτυακή κίνηση (μέσω TAP ή Mirror Traffic). Τα πακέτα θα πρέπει να γίνονται reduce, να κανονικοποιούνται και να μετατρέπονται σε αξιοποιήσιμα μετα-δεδομένα για την ενσωμάτωση στο big data lake.
- Συλλογή δεδομένων από user sources όπως το Microsoft AD μέσω API Connector
- Συλλογή δεδομένων από πηγές νέφους (cloud) Office365 μέσω Connectors
- Τα δεδομένα από πηγές πρέπει να κανονικοποιούνται, να εμπλουτίζονται και να συσχετίζονται αυτόματα από το σύστημα
- Πηγές εμπλουτισμού πρέπει να περιλαμβάνονται γεωγραφικού προσδιορισμού (Geo-Awareness), IP Reputation, Threat Intelligence και DPI Application awareness.
- Μοντέρνο περιβάλλον χρήστη με λειτουργίες SIEM που περιλαμβάνουν ερωτήματα και δημιουργίες κανόνων.
- Πρόσθετο για παραδοσιακή απεικόνιση SIEM (π.χ. Kibana)

Εντοπισμός KillChain (KillChain Detections)

(συμπεριλαμβάνοντας IDS/Exploit, Malware και APT Sandboxing, Anti-Phishing κτλ.)

- Το σύστημα πρέπει να έχει ενσωματωμένους μηχανισμούς εντοπισμών σε κάθε φάση του CyberSecurity KillChain, συμπεριλαμβάνοντας Reconnaissance, Delivery, Exploitation, Installation, Command & Control, and Actions & Exfiltrations
- Το σύστημα πρέπει να περιλαμβάνει ενσωματωμένη βάση υπογραφών IDS, ενισχυμένη από ανάλυση μηχανικής μάθησης (ML-IDS)
- Η πλατφόρμα πρέπει να υποστηρίζει πολλαπλά Threat Intelligence Feeds, συμπεριλαμβάνοντας εμπορικές πηγές, open-source, anti-phishing κ.α.

- Η πλατφόρμα πρέπει να επιτρέπει ενσωμάτωση με 3rd party feeds μέσω STIX/TAXII και/η MISP
- Η πλατφόρμα πρέπει να έχει ενσωματωμένες δυνατότητες APT Sandboxing για να αναγνωρίζει και να περιορίζει άγνωστα αρχεία, και για εντοπισμό ransomware, spyware.

Ανάλυση Δικτύου (Network Traffic Analysis)

Με την επιθεώρηση δικτυακής κίνησης σε πραγματικό χρόνο, η πλατφόρμα πρέπει να μπορεί να μοντελοποιήσει την κίνηση για αναγνώριση παράτυπων συμπεριφορών και ειδοποιήσεων.

- Η πλατφόρμα πρέπει να ενσωματώνει λειτουργικότητα Deep Packet Inspection (DPI) για την αναγνώριση τουλάχιστον 4000 εφαρμογών και να δομεί σχετικά συμπεριφορικά μοντέλα.
- Τα δεδομένα κίνησης δικτύου πρέπει να μετασχηματίζονται σε κατάλληλα μετα-δεδομένα που περιλαμβάνουν και το payload, για την αντίστοιχη προαιρετική μείωση ανάγκης αποθηκευτικών χώρων.
- Η πλατφόρμα πρέπει να ενσωματώνει λειτουργικότητα NTA Detections, συμπεριλαμβάνοντας Application Usage Anomalies, Long App Session Anomalies, και Unapproved Asset Activity
- Το σύστημα θα πρέπει να εντοπίζει ανωμαλίες στη συμπεριφορά των Firewalls, denial anomalies ή rule usage anomalies

User Behavior Analytics (UBA)

Σε συνδυασμό με την ανάλυση πακέτων, το σύστημα θα πρέπει να μπορεί να συνδεθεί με πηγές δεδομένων χρηστών, το MS Active Directory

- Το σύστημα πρέπει να πραγματοποιεί ανάλυση και εντοπισμό ανωμαλιών στη συμπεριφορά του χρήστη (user behavior)
- Το σύστημα πρέπει να ενσωματώνει μοντέλα εντοπισμού ανωμαλιών αδύνατου ταξιδιού (Impossible Travel Anomaly) ή ώρες αυθεντικοποίησης (Log In Time Anomaly)
- Εντοπισμούς NTA, έτσι κι εδώ όλα τα detections και τα σχετικά events στα logs και σε πηγές πρέπει να συσχετίζονται αυτόματα.

Endpoint Behavior Analytics (EBA)

Με τα αναλυτικά δεδομένα δικτύου και χρηστών, το σύστημα πρέπει να μπορεί να συλλέγει δεδομένα από assets/endpoints στο περιβάλλον, να εκτελεί analytics και να εντοπίζει συμπεριφορικές ανωμαλίες.

- Το σύστημα θα πρέπει να μπορεί να εισάγει δεδομένα από τρίτα συστήματα εντοπισμού ευπαθειών (vulnerability scanners) Nessus, Tenable, Rapid7 και να συσχετίζει τα ευρήματα με σχετικά γεγονότα ασφαλείας.
- Το σύστημα θα πρέπει να μπορεί να ανακαλύψει όλα τα assets σε ένα περιβάλλον και να τα κατηγοριοποιεί με βάση τη διεύθυνση MAC και IP.
- Η λίστα των ανακαλυφθέντων/εντοπισθέντων assets θα πρέπει να μπορεί να επαυξάνεται και να παραμετροποιείται με τη χρήση αρχείων csv με λίστες assets και περιγραφές.
- Το σύστημα πρέπει να μπορεί να καταγράφει όλους συσχετισμούς με ένα asset με IP διευθύνσεις, ιστορικά στοιχεία για τη χρήση εφαρμογών κτλ.

Ορατότητα Δικτύου και Υπηρεσιών (Network & Service Visibility)

Το σύστημα θα πρέπει να περιλαμβάνει δυνατά εργαλεία απεικόνισης δικτύων και υπηρεσιών, μαζί με analytics, με στόχο να προσφέρει ορατότητα επιδόσεις δικτύου (network performance), application usage κτλ.

Κυνήγι Απειλών και Διερεύνηση (Threat Hunting & Investigation)

Με πηγές δεδομένων στο unified data lake, τα κανονικοποιημένα και συσχετισμένα δεδομένα πρέπει να είναι διαθέσιμα για διερεύνηση και threat hunting οποιαδήποτε στιγμή.

- Το σύστημα πρέπει να έχει ενσωματωμένα σχετικά εργαλεία, προκαθορισμένες αναζητήσεις και ερωτήματα, και οπτικοποιήσεις (visualizations).
- Τα visualizations πρέπει να είναι παραμετροποιήσιμα
- Το σύστημα πρέπει να προσφέρει εξελιγμένες δυνατότητες συσχετισμένες αναζητήσεις, που επιτρέπουν αναλυτές να συνδέσουν πολλαπλά ανεξάρτητα ερωτήματα με κοινά κριτήρια προκειμένου να δομήσουν πληροφορίες από attack sequences ή να απομονώσουν κοινές πληροφορίες.
- Όλα τα ερωτήματα θα πρέπει να μπορούν να αποθηκευθούν, επεξεργαστούν, κλωνοποιηθούν κτλ από χρήστες.
- Τα visualizations πρέπει να μπορούν να αποθηκευθούν σαν custom dashboards.
- Τα ερωτήματα θα πρέπει να μπορούν να συνδυαστούν με ενέργειες/αποκρίσεις για PlayBooks

Playbooks / Integrated Orchestration & Response (SOAR)

- Το σύστημα πρέπει να συμπεριλαμβάνει μια βιβλιοθήκη με έτοιμα ενσωματωμένα playbooks, που είναι αυτό-εκτελέσιμα ερωτήματα με ενσωματωμένες ενέργειες.
- Οι ενσωματωμένες ενέργειες/αποκρίσεις θα πρέπει να συμπεριλαμβάνουν
 - Alerts – Αποστολή e-mail/slack message κτλ
 - Actions – Άνοιγμα case, εκτέλεση αιεαντολής API, δημιουργία security event κτλ
 - Responses – Μπλοκάρισμα μιας IP στο Firewall, απενεργοποίηση χρήστη στο AD, εκτέλεση δέσμης ενεργειών κτλ
- Παράλληλα με αυτοματοποιημένες ενέργειες, εξωτερικές ενέργειες το μπλοκάρισμα μια IP ή χρήστη θα πρέπει να είναι διαθέσιμες στο χρήστη μέσω του UI ώστε να μπορούν παράλληλα να υλοποιηθούν ως μέρος διερεύνησης/αντιμετώπισης ή ανάλυσης.
- Δυνατότητα ενσωμάτωσης με ήδη έτοιμα εμπορικά εργαλεία SOAR

Επιπλέον Δυνατότητες

Ειδοποιήσεις (Alarming)

- Το σύστημα θα πρέπει να προσφέρει έναν έξυπνο, μοντέρνο και παραμετροποιήσιμο μηχανισμό ειδοποιήσεων που να δύναται να οριστεί με βάση παραλήπτες και άλλα κριτήρια (score severity, killchain category, etc.)
- Οι ειδοποιήσεις πρέπει να μπορούν να αποσταλούν με email ή slack μηνύματα και τα μηνύματα πρέπει να είναι παραμετροποιήσιμα ως το περιεχόμενο και τα σχετικά δεδομένα.

Αναφορές (Reporting)

- Το σύστημα πρέπει να περιέχει ένα σύγχρονο εξελιγμένο μηχανισμό αναφορών που θα επιτρέπει παράλληλα εύκολη δημιουργία νέων αναφορών με drag and drop και αποθήκευσή για χρήση σε οποιοδήποτε σημείο.

- Οι αναφορές θα πρέπει να παράγονται με χρονοπρογραμματισμό και να αποστέλλονται σε διαφορετικούς χρήστες.
- Οι αναφορές πρέπει να είναι δυνατόν να αποστέλλονται με email σαν pdf ή csv ή να γράφονται σε αρχείο.
- Το σύστημα θα πρέπει να περιλαμβάνει πληθώρα έτοιμων αναφορών και templates.

Portal

- Πρόσβαση των χρηστών βάση ρόλου (User RBAC access) στο Portal με συνολική ή περιορισμένη πρόσβαση πληροφορίες.
- Custom Dashboards ανάρόλοχρήστη.
- Χρονοπρογραμματισμένες αναφορές για κάθε tenant, tenant group και RBAC users.
- Η πρόσβαση των χρηστών πρέπει να μπορεί να περιορίζεται σε Read-Only, limited view, μέχρι full visibility and access.

7.1.5.6.2 Λύση Προστασίας Βάσεων Δεδομένων

Οι βάσεις δεδομένων είναι από τα βασικά δομικά συστατικά της υποδομής πληροφοριακών συστημάτων και επομένως η προστασία τους και η παρακολούθησή τους είναι υψίστης σημασίας.

Για την αποτελεσματική προστασία των Βάσεων Δεδομένων απαιτείται η προμήθεια και υλοποίηση μιας ολοκληρωμένης λύσης Database Security η οποία θα ενσωματώνει κατ' ελάχιστον τις ακόλουθες λειτουργίες:

- User Accountability - πλήρης καταγραφή και παρακολούθηση των προσβάσεων και ενεργειών στη Βάση Δεδομένων σε επίπεδο χρήστη
- Detailed DB Auditing (query level) – έλεγχος όλης της δικτυακής κίνησης και των προσβάσεων προς τη Βάση Δεδομένων σε επίπεδο SQL query
- Database Application protection – προστασία σε επίπεδο εφαρμογής Βάσης Δεδομένων

Η προσφερόμενη λύση προστασίας Βάσεων Δεδομένων θα πρέπει να πραγματοποιεί πλήρη καταγραφή και παρακολούθηση σε πραγματικό χρόνο των προσβάσεων σε επίπεδο ερωτημάτων προς την Βάση Δεδομένων (query-level auditing), καθώς και να εφαρμόζει πολιτική ελέγχου πρόσβασης στη Βάση Δεδομένων και στα δεδομένα αυτής, ακόμα και για τους διαχειριστές της Βάσης Δεδομένων. Κάθε αίτηση προς μια προστατευόμενη Βάση Δεδομένων θα πρέπει να αναλύεται εις βάθος προκειμένου να διαπιστωθεί το κατά πόσο είναι ασφαλής και δεν αποτελεί απειλή για την ασφάλεια των εταιρικών δεδομένων.

Ταυτόχρονα θα πρέπει να καταγράφει και να εξετάζει σε πραγματικό χρόνο τις κινήσεις στις Βάσεις Δεδομένων δημιουργώντας έτσι ένα δυναμικό προφίλ βασισμένο στην δομή και τα δυναμικά χαρακτηριστικά της κάθε Βάσης. Το προφίλ που θα δημιουργείται έπειτα από επιβεβαίωση του διαχειριστή θα πρέπει να μπορεί χρησιμοποιείται ως βάση και μέτρο σύγκρισης από τον μηχανισμό ως προς την ανίχνευση και καταστολή επιθέσεων και κάθε είδους μη εξουσιοδοτημένων ενεργειών οι οποίες εκτελούνται στην Βάση Δεδομένων.

Συνοπτικά το σύστημα θα πρέπει να παρέχει τις ακόλουθες λειτουργίες ασφάλειας:

- Λειτουργία ως Database Firewall-Auditing, με στόχο την παρακολούθηση και προστασία συστημάτων βάσεων δεδομένων πολλαπλών κατασκευαστών (όπως MS SQL, Oracle, κτλ.) από επιθέσεις τόσο από εξωτερικούς επιτιθεμένους, όσο και από εσωτερικούς κακόβουλους χρήστες.

- Δυνατότητα παραμετροποίησης και ορισμού πολιτικών ασφαλείας βάσει user names, IP addresses, tables, operations, queries, query patterns, privileged commands και stored procedures.
 - ο Δυνατότητα δημιουργίας αναφορών (reporting)
 - ο Παραμετροποίηση αναφορών
 - ο Κεντρική διαχείριση
- Προώθηση των συμβάντων ασφαλείας σε λύση SIEM

7.1.5.6.3 Λύση προστασίας ηλεκτρονικού ταχυδρομείου MailSecurity - 3.000 σταθμούς εργασίας

Η λύση προστασίας ηλεκτρονικού ταχυδρομείου αποτελεί μια ακόμα γραμμή άμυνας για το ηλεκτρονικό ταχυδρομείο των χρηστών. Ο στόχος της λύσης είναι να προστατεύει τα εισερχόμενα, εξερχόμενα και εσωτερικά email από επιθέσεις phishing. Η λύση θα επιθεωρεί τα μεταδεδομένα, τα συνημμένα (attachments), τους συνδέσμους και τη γλώσσα επικοινωνίας, καθώς και όλες τις ιστορικές επικοινωνίες, για να προσδιορίσει τις σχέσεις μεταξύ του αποστολέα και του παραλήπτη, αυξάνοντας την πιθανότητα αναγνώρισης πλαστοπροσωπίας χρήστη ή δόλιων μηνυμάτων. Επίσης επιθεωρεί εσωτερική επικοινωνία σε πραγματικό χρόνο προκειμένου να αποφευχθούν πλευρικές επιθέσεις και εσωτερικές απειλές.

7.1.5.6.4 Λύση Endpoint Detection and Response - 3.000 σταθμούς εργασίας

Η λύση EDR είναι απαραίτητη για την προστασία των συστημάτων από κακόβουλα λογισμικά. Η λύση EDR πρέπει να είναι ικανή να ανιχνεύει απειλές χρησιμοποιώντας δυναμική ανάλυση συμπεριφοράς για τον εντοπισμό γνωστών και άγνωστων απειλών. Ο οργανισμός μπορεί να αποκτήσει πλήρη ορατότητα στα τελικά σημεία, να εντοπίζει και να ανταποκρίνεται σε απειλές αυτόνομα, χωρίς να απαιτείται πρόσθετο προσωπικό υψηλής εξειδίκευσης. Η λύση πρέπει να διαθέτει εγγενείς δυνατότητες χρήσης τεχνητής νοημοσύνης στην ανίχνευση απειλών στα τερματικά.

Οι βασικές δυνατότητες της πλατφόρμας πρέπει να περιλαμβάνουν:

- Λεπτομερείς πληροφορίες σχετικά με διαδικασίες και εφαρμογές που εκτελούνται σε τελικά σημεία
- Πλήρη ορατότητα στα τελικά σημεία, χαρτογράφηση απειλών με βάση το MITRE ATT&CK και οπτικοποίηση των απειλών.
- Ανίχνευση απειλών βασισμένων σε υπογραφές (signature based) αλλά και σε νέες απειλές που εντοπίζονται με ανάλυση της συμπεριφοράς του τελικού σημείου (behavioral based).
- Ταχεία αυτόνομη απόκριση σε συμβάντα.
- Δυνατότητα υλοποίησης και λειτουργίας χωρίς internet (air-gapped).
- agent να έχει χαμηλές απαιτήσεις σε resources (<1% CPU) και να μην επηρεάζει την ομαλή λειτουργία των τελικών σημείων.
- Ο agent να υποστηρίζει τη δυνατότητα παρακολούθησης του λειτουργικού συστήματος από το επίπεδο του hypervisor (όπου υποστηρίζεται).
- Δυνατότητες Threat Hunting που επιτρέπει στους αναλυτές να αναζητούν την παρουσία συγκεκριμένων δεικτών κινδύνου – indicators of compromise

7.1.5.6.5 Managed services security endpoint & mail (αφορά 3.000 σταθμούς εργασίας)

Η υπηρεσία θα πρέπει να παρέχει παρακολούθηση και έλεγχο των endpoints του πελάτη με άμεση ενημέρωση για περιστατικά ασφάλειας, δυνατότητα ανίχνευσης απειλών και γρήγορης απόκρισης 24 ώρες το 24ωρο, 7 ημέρες την εβδομάδα. Η υπηρεσία θα πρέπει να παρέχει 24ωρη παρακολούθηση των endpoints (Managed Detection and Response) με στόχο τον εντοπισμό περιστατικών ασφάλειας και ενημέρωση του πελάτη μέσω τηλεφώνου/e-mail για περιστατικά ασφάλειας βάση SLA. Επίσης θα πρέπει να περιλαμβάνει παροχή συμβουλών για τη διερεύνηση και την αντιμετώπιση του περιστατικού.

7.1.6 Φυσικό αντικείμενο Τμήματος 4 «Εξειδικευμένες λύσεις και υπηρεσίες ασφάλειας για την Ε.Δ.Υ.Τ.Ε. Α.Ε.»

7.1.6.1 Διαστασιολόγηση λογισμικού, εξοπλισμού και υπηρεσιών

Κατηγορία	Μονάδα διαστασιολόγησης	Ελάχιστο μέγεθος
Διαμόρφωση πολιτικών ασφάλειας κρίσιμων οντοτήτων με στόχο την ανάδειξη τεχνικών και οργανωτικών μέτρων για την προστασία τους από Κυβερνοαπειλές	A/M	14
Διαμόρφωση πολιτικών ορθής χρήσης Πληροφοριακών συστημάτων και εφαρμογών	A/M	14
Διενέργεια δράσεων ενημέρωσης για τη μεταφορά τεχνογνωσίας και την διαμόρφωση κουλτούρας ενεργούς ευαισθητοποίησης για τους κινδύνους κυβερνοασφάλειας	A/M	14
Διαμόρφωση πλάνου ανάκαμψης από καταστροφές για κρίσιμες οντότητες	A/M	14
Εκπόνηση Μελέτης εξωτερικού και εσωτερικού περιβάλλοντος και την ανάδειξη βέλτιστων πρακτικών	A/M	14
Διαμόρφωση πολιτικής αντιγράφων ασφαλείας, που θα περιγράφει σκοπό, πεδίο εφαρμογής, ρόλους και ευθύνες	A/M	14
Διαμόρφωση Συστήματος Διαχείρισης της Ασφάλειας των Πληροφοριών (ΣΔΑΠ) με βάση το πρότυπο ISO 27001 & Εκπόνηση Μελέτης Ανάλυσης και Αξιολόγησης Κινδύνων	A/M	14
Διενέργεια ελέγχων διεξόδου εξωτερικών δικτύων, εφαρμογών Ιστού, φυσικής ασφάλειας και διαρροής δεδομένων για τον εντοπισμό των ευπαθειών σε υποδομές, συσκευές και διακομιστές που είναι προσβάσιμοι από το διαδίκτυο	A/M	16

Κατηγορία	Μονάδα διαστασιολόγησης	Ελάχιστο μέγεθος
Αξιοποίηση τεχνολογικής καινοτομίας και ερευνητικής πρωτοπορίας	A/M	46
Παροχή υπηρεσίας SOC	Μήνες	30
Λύση DDOS	Μήνες	30
Παροχή υπηρεσιών ανάκαμψης από καταστροφή & λήψης αντιγράφων ασφαλείας (disaster recovery as a service & data backup as a service)	CREDITS €	500.000,00
Υπηρεσίες εγκατάστασης/παραμετροποίησης υπηρεσιών ανάκαμψης από καταστροφή & λήψης αντιγράφων ασφαλείας (disaster recovery as a service & data backup as a service)	A/M	40
Λύση Προστασίας Βάσεων Δεδομένων	Βάσεις δεδομένων	20
Πλατφόρμα Κυβερνοασφάλειας – Εκτεταμένης Ανίχνευσης & Απόκρισης (CyberSecurity)	Assets GB log files/ημέρα	3.000 100
Λύση Διαβάθμισης και Σήμανσης Εγγράφων	Σταθμοί εργασίας	400
Λύση Προστασίας Δεδομένων από Διαρροή	Σταθμοί εργασίας	400
Λύση Διαχείρισης Δικαιωμάτων Εγγράφων	Χρήστες	400
Λύση Διαχείρισης Λογαριασμών και Δικαιωμάτων Πρόσβασης Χρηστών	Λογαριασμοί	400
Λύση Διαχείρισης Προνομιούχων Λογαριασμών Πρόσβασης	Λογαριασμοί διαχειριστών Λογαριασμοί συνεργατών (named users)	40 15

7.1.6.2 Πολιτικές – Διαδικασίες και Μέτρα Αντιμετώπισης και Πρόληψης

7.1.6.2.1 Διαμόρφωση πολιτικών ορθής χρήσης Πληροφοριακών συστημάτων και εφαρμογών

Ο Ανάδοχος θα εκπονήσει μελέτη πολιτικής ορθής χρήσης πληροφοριακών συστημάτων και εφαρμογών, προκειμένου να καθοριστούν οι υποχρεώσεις όλων των χρηστών, καθώς και οι αρχές, οι κανόνες και οι συνέπειες για το σύνολο των προσώπων στα οποία εκχωρείται το δικαίωμα πρόσβασης στα πληροφοριακά συστήματα και τις εφαρμογές. Η πολιτική ορθής χρήσης αποβλέπει στην αποτροπή καταχρηστικής άσκησης των δικαιωμάτων των χρηστών και της τέλεσης πράξεων που συνιστούν κίνδυνο παραβίασης του απορρήτου των δεδομένων / πληροφοριών, ή διακύβευσης της ασφάλειας των πληροφοριακών συστημάτων και εφαρμογών ή της ακεραιότητας και διαθεσιμότητας των υποδομών.

Στο πλαίσιο της εργασίας αυτής, ο Ανάδοχος κατ' ελάχιστον:

- Θα διενεργήσει κατάλληλη κατηγοριοποίηση του συνόλου των υφιστάμενων και δυνητικών χρηστών, προκειμένου να προτείνει στη συνέχεια μια διαφοροποιημένη πολιτική ορθής χρήσης προσαρμοσμένη σε κάθε κατηγορία.
- Θα διενεργήσει μια κατηγοριοποίηση των πληροφοριακών συστημάτων και εφαρμογών, προκειμένου να προσδιορίσει στη συνέχεια τα συστήματα εκείνα που είναι ευάλωτα σε ένα περιστατικό ανάρμοστης χρήσης.
- Θα αναλύσει τα ιδιαίτερα χαρακτηριστικά κάθε κατηγορίας χρηστών, που θα προκύψουν από τη σχετική έρευνα και κατηγοριοποίηση που θα έχει ήδη κάνει και στη συνέχεια θα προσδιορίσει τις ανάγκες και υποχρεώσεις χρήσης κάθε κατηγορίας
- Θα προσδιορίσει τις διαδικασίες που πρέπει να εφαρμόζονται, τις ενέργειες που συνιστώνται και τα μέτρα που πρέπει να παίρνονται, προκειμένου να διασφαλιστεί η ορθή χρήση του δικτύου
- Θα προσδιορίσει τις ενέργειες που απαγορεύονται ή πρέπει να αποφεύγονται και οι οποίες συνιστούν μια ανάρμοστη χρήση πληροφοριακών συστημάτων και εφαρμογών.
- Θα προτείνει τις διαδικασίες και τα διορθωτικά και/ή αποτρεπτικά μέτρα που πρέπει να εφαρμόζονται σε περίπτωση που διαπιστωθεί κάποιο περιστατικό ανάρμοστης χρήσης πληροφοριακών συστημάτων και εφαρμογών
- Θα συντάξει σχέδια συμφωνητικών ορθής χρήσης, τα οποία θα υπογράφονται από τους δυνητικούς χρήστες πληροφοριακών συστημάτων και εφαρμογών, κατόπιν επιθυμίας της Ε.Δ.Υ.Τ.Ε.. Το ελάχιστο περιεχόμενο των συμφωνητικών αυτών περιλαμβάνει μια σύνοψη των δικαιωμάτων και υποχρεώσεων κάθε κατηγορίας χρήστη
- Θα μεριμνήσει για την κατάλληλη ενημέρωση όλων των χρηστών (φτάνοντας μέχρι το επίπεδο τελικού χρήστη) επί της πολιτικής ορθής χρήσης που θα εφαρμοσθεί, αφού εγκριθεί από την Ε.Δ.Υ.Τ.Ε.
- Θα προσδιορίσει τις διαδικασίες που πρέπει να εφαρμοστούν και τις ενέργειες που πρέπει να πραγματοποιηθούν, προκειμένου να καταστεί δυνατός ο τακτικός έλεγχος και παρακολούθηση της εφαρμογής ή όχι της πολιτικής ορθής χρήσης.

7.1.6.2.2 Διενέργεια δράσεων ενημέρωσης για τη μεταφορά τεχνογνωσίας και την διαμόρφωση κουλτούρας ενεργούς ευαισθητοποίησης για τους κινδύνους κυβερνοασφάλειας

Ο Ανάδοχος καλείται να παράσχει υπηρεσίες σχεδιασμού και υλοποίησης δράσεων ενημέρωσης προς τις αρμόδιες υπηρεσίες της Ε.Δ.Υ.Τ.Ε. κατά την υλοποίηση του έργου, στις ακόλουθες θεματικές ενότητες:

- Εισαγωγή στην Ασφάλεια Πληροφοριών
- Οι κυβερνοπειλές (Cyber Threats)
- Υλική Ασφάλεια Αρχείων και Μηχανημάτων
- Ασφάλεια Επιφάνειας Εργασίας
- Αποθήκευση αρχείων και δεδομένων
- Αποστολή και διαμοιρασμός αρχείων

- Ασφάλεια κωδικών πρόσβασης
- Ασύρματα δίκτυα και κινητή επικοινωνία
- Διαδικτυακή Ασφάλεια
- Συστήματα Κοινωνικής Μηχανικής (Social Engineering)
- Ασφάλεια ηλεκτρονικού ταχυδρομείου
- Κακόβουλο λογισμικό (Ιοί, Worms, Trojans, Spyware, Adware)
- Ηλεκτρονικό «ψάρεμα» (Phishing)
- Μέσα Κοινωνικής Δικτύωσης

Οι συμμετέχοντες μόλις ολοκληρώσουν την εκπαίδευση θα έχουν κατανοήσει τα θέματα των νέων τεχνολογιών και διαδικτύου, ασφάλειας υπολογιστικών συστημάτων και υποδομών, ασφαλούς χρήσης του διαδικτύου αλλά και χειρισμού διαδικτυακών προγραμμάτων και προγραμμάτων ηλεκτρονικού υπολογιστή. Επιπλέον, θα μπορούν να αναγνωρίσουν τα διάφορα είδη κυβερνοαπειλών και θα έχουν μάθει βασικούς κανόνες ασφαλείας για την αποτροπή τους.

Πιο ειδικά ο Ανάδοχος καλείται να παρέχει τις παρακάτω υπηρεσίες:

Ι. Μεθοδολογία εκπαίδευσης, εκπαιδευτικό υλικό και εισαγωγή των δεδομένων στην εκπαιδευτική πλατφόρμα

Ο Ανάδοχος θα πρέπει να τεκμηριώσει και να παραδώσει τη μεθοδολογία εκπαίδευσης που θα ακολουθήσει πριν την έναρξη του προγράμματος. Η μεθοδολογία θα πρέπει να επιδιώκει την επίτευξη των παρακάτω εκπαιδευτικών στόχων για τους εκπαιδευόμενους:

- Ανάκληση γνώσεων
- Κατανόηση εκπαιδευτικού υλικού
- Εφαρμογή γνώσεων στην πράξη και σε περιβάλλον προσομοίωσης ή/και σε μελέτες περίπτωσης
- Ανάλυση και σύνθεση γνώσεων
- Η θεωρία και οι ασκήσεις αξιολόγησης/εξέτασης να αποδίδονται μέσω σύγχρονων authoring tools (όπως Articulate, Captivate κ.α.), εξειδικευμένων στην εκπαίδευση ενηλίκων.
- Ενσωμάτωση μηχανισμών παιχνιδιού στην εκπαιδευτική διαδικασία, με δυνατότητες επιβράβευσης (π.χ. πόντοι, σήματα, εικονικά νομίσματα κ.ά.)

Ο Ανάδοχος θα αναλάβει τον σχεδιασμό των εκπαιδευτικών προγραμμάτων λαμβάνοντας υπόψη συγκεκριμένες παραμέτρους. Οι παράμετροι αυτοί αφορούν τη διαφοροποιημένη προσέγγιση ανάλογα με την ομάδα-στόχο, τον τρόπο εκπαίδευσης και τα μέσα που θα χρησιμοποιηθούν.

Ο Ανάδοχος καλείται να μελετήσει τα μοντέλα που έχουν ακολουθήσει άλλες ευρωπαϊκές χώρες για σχετικά προγράμματα εκπαίδευσης, ενημέρωσης και ευαισθητοποίησης εταιρειών και οργανισμών. Ο στόχος της μελέτης είναι να μπορεί ο Ανάδοχος να παρέχει τις κατάλληλες κατευθύνσεις και να αντλήσει καλές πρακτικές στο πεδίο της κατάρτισης και ευαισθητοποίησης εργαζόμενων σε θέματα Κυβερνοασφάλειας.

Ο Ανάδοχος, καλείται να παραδώσει για κάθε εκπαιδευτική ενότητα του προγράμματος, τους εκπαιδευτικούς στόχους, τα εκπαιδευτικά αποτελέσματα, τη διάρκεια αλλά και πιθανές

ασκήσεις/ερωτήσεις προς πρακτική εξάσκηση των γνώσεων. Ο σχεδιασμός του εκπαιδευτικού προγράμματος πρέπει να υποστηρίζεται από μια πολυμεσική υλοποίηση, η οποία θα περιλαμβάνει διάφορα οπτικοακουστικά μέσα (π.χ. ήχος, εικόνες, βίντεο, mini games, gamification, quizzes, learning modalities, slideshow κ.α).

Για την ασύγχρονη εκπαίδευση απαιτείται ένα σύγχρονο και πλήρως φιλικό προς το χρήστη σύστημα Learning Management (Learning Management System, LMS), το οποίο να βασίζεται σε εφαρμογή PWA (Progressive Web Application) έτσι ώστε να μην απαιτείται εγκατάσταση της μέσω Google/Apple Store καθώς και όλες οι απαραίτητες ενημερώσεις (updates) να γίνονται κεντρικά και να ενημερώνονται αυτόματα όλοι οι χρήστες, χωρίς να χρειάζεται να προβούν σε καμία ενέργεια αναβάθμισης. Επιπλέον, το LMS θα πρέπει να είναι μία απόλυτα εξατομικευμένη λύση που θα παραμετροποιηθεί, προσαρμοστεί και ενσωματωθεί πλήρως τόσο στα μηχανογραφικά συστήματα όσο και στους μηχανισμούς ασφαλείας της Ε.Δ.Υ.Τ.Ε.. Θα πρέπει να καλύπτει τις ανάγκες στο σύνολο των εκπαιδευόμενων (ιδιωτικός και δημόσιος τομέας), να παρέχει στενή διασύνδεση (integration) με όλα τα εργαλεία του MS Office και να αποτελεί συμβατή πλατφόρμα με διεθνή πρότυπα ηλεκτρονικής μάθησης όπως SCORM με τα οποία εξασφαλίζεται η επαναχρησιμοποίηση, η προσβασιμότητα και η ανθεκτικότητα του εκπαιδευτικού υλικού στις τεχνολογικές μεταβολές, καθώς και η διαλειτουργικότητα μεταξύ συστημάτων ηλεκτρονικής μάθησης. Η αρχιτεκτονική της πλατφόρμας (πλατφορμών) θα δίνει τη δυνατότητα στον χρήστη να αλληλεπιδρά δυναμικά με όλο το εκπαιδευτικό υλικό. Επιπλέον, ο Ανάδοχος θα πρέπει να παρακολουθεί με αναφορές το πλήθος των χρηστών που θα παρακολουθούν ή/και ολοκληρώνουν το εκπαιδευτικό ασύγχρονο πρόγραμμα κατάρτισης καθώς και να καταγράφονται αναλυτικά όλα τα ερωτηματολόγια με τις απαντήσεις στα τελικά διαδικτυακά (ψηφιακά) τεστ όλων των χρηστών σε αναλυτική καρτέλα προφίλ.

Για τον σχεδιασμό του εκπαιδευτικού υλικού πρέπει να ακολουθούνται με ακρίβεια τα πρότυπα σχεδιασμού εκπαιδευτικού υλικού, όπως περιγράφονται:

- Ο εκπαιδευτικός σχεδιασμός ψηφιακού υλικού ("instructional design") θα πρέπει να βασίζεται στη σαφή και αιτιολογημένη κατάτμηση του υλικού ενοτήτων σε υποενότητες μάθησης, με ορισμένη μέγιστη διάρκεια. Παράλληλα για την πλήρη κατανόηση της κατάτμησης των ενοτήτων σε υποενότητες μάθησης ο Ανάδοχος οφείλει να συνδέσει κάθε ενότητα/υποένότητα με διακριτούς εκπαιδευτικούς στόχους.
- Ο χρήστης θα πρέπει να ακολουθεί σαφή εκπαιδευτικά μονοπάτια (Θεωρία, Αυτοαξιολόγηση, Εξέταση, Πιστοποίηση), για τα οποία να δύνανται να έχουν υποχρεωτική σειριακή ακολουθία παρακολούθηση, ανάλογα με τους σκοπούς της εκπαίδευσης.
- Η διάδραση με το περιεχόμενο και η ενεργητική μάθηση των καταρτιζόμενων πρέπει με σαφή τρόπο να επιτυγχάνεται μέσω σύνθετων εργαλείων, εξειδικευμένων στην εκπαίδευση ενηλίκων, όπως business case studies, role playing, psychometric analysis κ.ά.
- Ο πρακτικός προσανατολισμός: μέθοδος «μαθαίνω κάνοντας» (learning by doing) θα επιτυγχάνεται με προσομοίωση πραγματικών συνθηκών (μελέτες περίπτωσης, επίλυση προβλήματος) και άλλες τεχνικές που ο ανάδοχος μπορεί να επιλέξει ώστε να ενθαρρύνει τη μάθηση μέσα από την επαφή των καταρτιζόμενων με πραγματικές συνθήκες λήψης απόφασης, συμπεριφορικές δραστηριότητες και ανάλυση επιλογών.
- Η πολυμεσική μάθηση είναι ο βασικός στόχος αυτού του έργου. Προκειμένου ο Ανάδοχος να διασφαλίσει ένα πολυμεσικό περιβάλλον μάθησης, οι παρουσιάσεις, τα βίντεο και η δόμηση του υλικού σε διαφορετικά εκπαιδευτικά μέσα και εκπαιδευτικά εργαλεία θα πρέπει να τηρεί προδιαγραφές της πολυμεσικής μάθησης και να διευκολύνει την επεξεργασία, κατανόηση και αφομοίωση των πληροφοριών και της παρεχόμενης γνώσης και την εύκολη και διαδραστική πλοήγηση.

- Οι προδιαγραφές αξιολόγησης της κατανόησης και αφομοίωσης της γνώσης από τους καταρτιζόμενους θα πρέπει να γίνεται με τη μέθοδο αξιολόγησης βάσει μετρήσιμων μαθησιακών αποτελεσμάτων – ταξινόμια ADDIE και να απεικονίζεται σε ανάλογες αναφορές.
- Κάθε ενότητα ή/ και υποενότητα μάθησης θα ακολουθείται από αξιολόγηση με quiz πολλαπλής ή μοναδικής επιλογής, ερωτήσεις σωστό λάθος. Προτεινόμενο μοντέλο είναι η αξιολόγηση να αποτελείται από ένα quiz αυτοαξιολόγησης και ένα βαθμολογούμενο, ανά υποενότητα μάθησης, ενώ οι ερωτήσεις θα πρέπει να αναφέρονται κυρίως σε συμπεριφορικά στοιχεία, επιλογές και αποκρίσεις σε πιθανά σενάρια σχετικά με το περιεχόμενο του εκπαιδευτικού προγράμματος και τους εκπαιδευτικούς στόχους.

Ο Ανάδοχος θα αναλάβει τον σχεδιασμό της μεθοδολογίας αξιολόγησης των αποτελεσμάτων γνώσεων, ο οποίος θα προκύπτει από σχετικά κριτήρια αξιολόγησης όπου θα συμμετέχουν οι εκπαιδευόμενοι με το πέρας της εκπαίδευσης. Πιο συγκεκριμένα, οι συμμετέχοντες θα πρέπει να συμμετάσχουν στην παραπάνω διαδικασία, η οποία θα τους αξιολογεί αυτόματα και άμεσα. Τα αποτελέσματα αυτά θα πρέπει να είναι άμεσα συγκρίσιμα και να παράγουν αναφορές με συνέπεια και συνεκτικότητα. Οι αναφορές θα απεικονίζονται και με ιεραρχικό επίπεδο της θέσης εργασίας που κατέχει κάθε υπάλληλος και ανά τμήμα όπου θα προκύπτουν συγκεντρωτικά ή ατομικά γνωστικά αποτελέσματα.

Το εκπαιδευτικό υλικό, για το οποίο ο Ανάδοχος θα έχει την επιμέλεια και επίβλεψη, σύμφωνα με τις ανάγκες και τον σχεδιασμό, θα είναι διαθέσιμο στην εκπαιδευτική πλατφόρμα και θα πρέπει να κατατεθεί ως ένα από τα παραδοτέα του έργου αυτού.

II. Σχεδιασμός και ανάπτυξη της ψηφιακής πλατφόρμας για την ασύγχρονη εξ' αποστάσεως εκπαίδευση

Το σύστημα τηλεεκπαίδευσης (E-Learning platform) θα είναι εύκολα προσβάσιμο και θα εξυπηρετεί τις ανάγκες του έργου. Το σύστημα ηλεκτρονικής εκπαίδευσης θα αποτελείται από μία πλατφόρμα ασύγχρονης τηλε-εκπαίδευσης (Learning Management System) για διαχείριση και παράδοση ασύγχρονων προγραμμάτων ηλεκτρονικής (ψηφιακής) μάθησης (e-learning). Ο Ανάδοχος θα πρέπει να διασφαλίσει ότι θα παρεμετροποιήσει και θα διαμορφώσει την αρχιτεκτονική της πλατφόρμας ώστε να μπορεί να φιλοξενήσει την εκπαιδευτική διαδικασία καθώς και τη φόρτωση και διαχείριση κάθε είδους εκπαιδευτικού υλικού, την ανταλλαγή και διάχυση πληροφορίας και την υποστήριξη κάθε είδους διεργασίας ανταλλαγής πληροφοριών. Το σύστημα θα πρέπει να μπορεί να χρησιμοποιηθεί προκειμένου να διαχειρίζονται και χρονοπρογραμματίζονται τα εκπαιδευτικά προγράμματα ασύγχρονης μορφής, οι μαθησιακές διαδικασίες καθώς η δυνατότητα διενέργειας δοκιμασιών (test) αξιολόγησης της επίτευξης των εκπαιδευτικών στόχων και αξιολόγησης του εκπαιδευτικού προγράμματος από τους συμμετέχοντες.

Ο Ανάδοχος πριν από τον σχεδιασμό της αρχιτεκτονικής και την ανάπτυξη της εκπαιδευτικής πλατφόρμας (ή πλατφορμών), καλείται να παρουσιάσει μια ενδελεχή ανάλυση των στοιχείων που θα παρακολουθούνται δυναμικά εντός της πλατφόρμας και να ορίσει ένα σαφές, ρεαλιστικό και περιγραφικό σύστημα δεικτών για την καταγραφή του εκπαιδευτικού και επιμορφωτικού κέρδους.

Η πρόσβαση στο σύστημα τηλεεκπαίδευσης θα πρέπει να μπορεί να πραγματοποιείται μέσα από δημοφιλείς φυλλομετρητές διαδικτύου που πληρούν τα διεθνή standards, όπως οι: Google Chrome, Mozilla Firefox, Microsoft Edge, από οποιοδήποτε σημείο του κόσμου, οποιαδήποτε στιγμή της ημέρας και από οποιαδήποτε συσκευή (desktop, laptop, tablet, smartphone). Δεν θα πρέπει να απαιτείται κανένα άλλο, πρόσθετο λογισμικό στη συσκευή που θα επιλέξει ο χρήστης καθώς και καμία εγκατάσταση. Όλες οι λειτουργίες και τα υποσυστήματα της εφαρμογής μπορούν να συνδυαστούν ελεύθερα. Ο σχεδιασμός και η ανάπτυξη της ψηφιακής πλατφόρμας θα πρέπει να διασφαλίζει ότι το σύστημα θα είναι άμεσα προσιτό και εύκολο στην πλοήγηση και χρήση από τους συμμετέχοντες,

όπου αυτός επιθυμεί, και να υποστηρίζει τη διαχείριση μεγάλου αριθμού ενεργών χρηστών. Το σύστημα το οποίο θα διαμορφώσει ο Ανάδοχος θα πρέπει να επιτρέπει τη δημιουργία προσωπικού λογαριασμού για κάθε εκπαιδευόμενο, στον οποίο θα καταγράφεται όλη του η δραστηριότητα όπως επίσης και τα αποτελέσματα της εξέτασης/ αξιολόγησης.

Γενικές κατευθύνσεις που πρέπει να ακολουθούνται για το σύστημα τηλεκπαίδευσης:

- Το λογισμικό ασύγχρονης εκπαίδευσης θα πρέπει να παρέχει χρήσιμα εργαλεία, όπως:
 - Βαθμολόγιο
 - Ημερολόγιο
 - Helpdesk
 - Ερωτηματολόγια (Review) για τη συλλογή δεδομένων από τους καταρτιζόμενους
 - Ηλεκτρονικά τεστ (online quiz)
 - Άμεσα μηνύματα (Forum/chat) με βαθμολόγηση απαντήσεων
 - Βιβλιοθήκη περιεχομένου
 - Μικροεκπαιδεύσεις – Microlearnings
 - Αιτήματα εγγραφής εκπαιδευόμενων σε νέες εκπαιδεύσεις
 - Ενσωματωμένο σύστημα ερωτηματολογίων (survey) ανά ομάδες χρηστών
- Πολύγλωσσο περιβάλλον και περιεχόμενο.
- Δημιουργία οργανογράμματος για οργάνωση των χρηστών ανά τομέα / διεύθυνση / γεωγραφική τοποθεσία κ.ά. σε γραφικό περιβάλλον
- Δημιουργία απεριόριστων χρηστών και ομάδων χρηστών.
- Δημιουργία απεριόριστων εκπαιδεύσεων με τελική πιστοποίηση.
- Δημιουργία εκπαιδευτικών μονοπατιών.
- Υποστήριξη διαφορετικών επιπέδων διαχείρισης, χρήσης, ρόλων και ομάδων χρηστών υποστηρίζοντας τα Azure, Microsoft Active Directory ,LDAP και Google Business.
- Υποστήριξη κατάλληλων μέτρων για την προστασία των προσωπικών δεδομένων τόσο των χειριστών της εφαρμογής, όσο και ευαίσθητων πληροφοριών στο υλικό παρουσίασης, σύμφωνα με τον κανονισμό GDPR. Πιο συγκεκριμένα:
 - Αποδοχή/Συναίνεση συλλογής δεδομένων: Το σύστημα υποστηρίζει λειτουργικότητες καταχώρησης και καταγραφής της συναίνεσης του χρήστη αναφορικά με τη συλλογή και διαχείριση των δεδομένων που έχουν ήδη καταχωρηθεί στο σύστημα ή των δεδομένων που θα συλλεχθούν κατά τη διάρκεια των διαδικασιών κατάρτισης κρυπτογραφημένα.
 - Ενημέρωση περί συλλεγόμενων δεδομένων. Ο χρήστης μπορεί να ενημερωθεί αναλυτικά και με σαφή τρόπο για το ποια δεδομένα συλλέγονται, τους λόγους για τους οποίους γίνεται η συλλογή τους, τον τρόπο χρήσης τους, καθώς επίσης και για τη διάρκεια διατήρησης αυτών των δεδομένων στα συστήματα. Επίσης, μπορεί να ενημερωθεί αναλυτικά για τους όρους χρήσης του συστήματος και τις εκπαιδευτικές διαδικασίες στις οποίες θα συμμετάσχει.

- Λειτουργία αυτόματης δημιουργίας και εισαγωγής εκπαιδευτικού περιεχομένου με εφαρμογές MS Office για την θεωρία και τα ερωτηματολόγια με online editor.
- Πλήρης συμμόρφωση με την τρέχουσα έκδοση του διεθνούς προτύπου SCORM.
- Λειτουργία μέσω Web Browser και είναι συμβατό με τα διεθνή πρότυπα του W3C.
- Λειτουργία σε περιβάλλον HTTPS. Όλες οι επιμέρους λειτουργίες να παρέχονται εντός πρωτοκόλλου HTTPS και πάνω από secure channel SSL/TLS.
- Πολιτική ασφάλειας κωδικών πρόσβασης. Το σύστημα να υποστηρίζει:
 - ο Πολιτική πολυπλοκότητας κωδικών (ελάχιστο πλήθος χαρακτήρων, συμπερίληψη special characters, συμπερίληψη χαρακτήρων με κεφαλαία, συμπερίληψη αριθμητικών χαρακτήρων, αποτροπή χρήσης ακολουθίας π.χ. 1234, αποτροπή χρήσης κοινών κωδικών π.χ. qwerty).
 - ο Παραγωγή κωδικών με τυχαίο τρόπο και σύμφωνα με την πολιτική πολυπλοκότητας χωρίς την επέμβαση φυσικού προσώπου (διαχειριστή) > Διαδικασίες επαναφοράς κωδικού χωρίς ενημέρωση και χωρίς την επέμβαση φυσικού προσώπου (διαχειριστή) > Διαδικασίες υποχρεωτικής αλλαγής κωδικού (π.χ. κατά την 1η είσοδο στο σύστημα).
 - ο Διατήρηση ιστορικού κωδικών πρόσβασης και αποτροπή επαναχρησιμοποίησης παλιού κωδικού.
- Υποστήριξη αρθρωτής (modular) και ανοικτής αρχιτεκτονικής, ώστε να επιτρέπονται επεκτάσεις/αναβαθμίσεις.
- Δυνατότητα δημιουργίας πολλαπλών Portals με βάση τον ρόλο του Χρήστη (Δημόσιος τομέας, Ιδιωτικός Τομέας, Ομάδες Διεύθυνσης, Εκπαιδευτές, Εκπαιδευόμενοι, κ.ά.)
- Δυνατότητα καταγραφής της πορείας και των ενεργειών του καταρτιζόμενου (tracking-timeline) καθ' όλη τη διάρκεια εκάστου εκπαιδευτικού προγράμματος.
- Μηχανισμό χρονοπρογραμματισμού και αποστολής αυτοματοποιημένων ειδοποιήσεων μέσω e-Mail ή/και SMS, in app notifications, έτσι ώστε να παρέχονται όλες οι κατάλληλες πληροφορίες για την επιλογή της βέλτιστης διαδικασίας αποστολής σε όλες τις λειτουργίες της πλατφόρμας δυνατότητα:
 - ο Αποστολή σε όλους: Θα γίνει αποστολή σε όσους έχουν ενεργές τις ειδοποιήσεις, και έχουν αποδεχθεί τους όρους.
 - ο Εξαίρεση: Ο διαχειριστής μπορεί να επιλέξει ποιοι θα εξαιρεθούν της αποστολής
 - ο Ατομική Αποστολή: Ο διαχειριστής μπορεί να επιλέξει συγκεκριμένα άτομα που θα γίνει η αποστολή
 - ο Δεν έχουν λάβει ειδοποίηση: Ο διαχειριστής μπορεί να επιλέξει τους όσους δεν έχουν λάβει τη συγκεκριμένη ειδοποίηση από προηγούμενη αποστολή.

Το σύστημα επιπλέον θα πρέπει να διαθέτει σύστημα αναφορών έτσι ώστε να μπορούν να παράγονται αναφορές για τις ενέργειες που υποστηρίζονται από το σύστημα. Ενδεικτικά:

- Αναφορές για το σύνολο των χρηστών / ομάδα / χρήστη
- Αναφορές ανά θεματικό πεδίο / μάθημα / εξέταση / πιστοποίηση.

Που θα περιλαμβάνουν τουλάχιστον τα παρακάτω δεδομένα:

- Ποσοστό συμμετοχής (δλδ πόσοι έχουν ξεκινήσει ή ολοκληρώσει)

- Χρόνους κατανάλωσης περιεχομένου (μέσο όρο, σύνολο)
- Μέσο χρόνο ολοκλήρωσης ανά εκπαιδευτικό πρόγραμμα
- Αποτελέσματα εξετάσεων / μάθημα, αξιολόγηση, πιστοποίηση και Top 10 /100
- Ποιες ερωτήσεις εμφανίζουν συχνά λάθη ανά θεματικό πεδίο, μάθημα
- Προσωποποιημένες αναφορές επίδοσης με στατιστικά ανά γνωστικό αντικείμενο
- Αναλυτικά αποτελέσματα ερευνών
- Big data analytics για ανάλυση δεξιοτήτων που αναπτύχθηκαν με συγκεκριμένους δείκτες (KPI's)

Το σύστημα τηλεκπαίδευσης θα πρέπει να υποστηρίζει τουλάχιστον τις εξής κατηγορίες χρηστών και σχετικά δικαιώματα:

- Εκπαιδευόμενους
- Εκπαιδευτές
- Διαχειριστές της πλατφόρμας εξ αποστάσεως εκπαίδευσης

Οι δυνατότητες του συστήματος σε σχέση με τον χρήστη/εκπαιδευόμενο αναφέρονται συνοπτικά παρακάτω:

- Εγγραφή στο εκπαιδευτικό πρόγραμμα
- Προβολή και παρακολούθηση εκπαιδευτικού υλικού
- Συμμετοχή σε τυποποιημένες έρευνες (αξιολόγηση εκπαιδευτικού προγράμματος) με σκοπό την έκφραση των απόψεων του εκπαιδευμένου σχετικά με το εκπαιδευτικό υλικό ή τη διαδικασία εκπαίδευσης
- Συμμετοχή σε μη υποχρεωτικά μαθήματα μικρής διάρκειας, μεγάλης ποικιλίας με συνδυασμό πολλαπλών μορφών περιεχομένου και δυνατότητα αναζήτησης με λέξεις κλειδιά.
- Συμμετοχή σε εξέταση (test αξιολόγησης) που μπορεί να έχει διάφορες μορφές ερωτήσεων όπως πολλαπλής επιλογής, σωστό-λάθος και ερωτήσεις με σύντομες απαντήσεις κ.λ.π.
- Προβολή και εκτύπωση βεβαίωσης της ολοκλήρωσης της συμμετοχής στο εκπαιδευτικό πρόγραμμα μετά την επιτυχή ολοκλήρωση του τεστ αξιολόγησης

Οι δυνατότητες του συστήματος σε σχέση με τον χρήστη Διαχειριστή αναφέρονται συνοπτικά παρακάτω.

Ως Διαχειριστής ορίζεται το στέλεχος το οποίο θα παρακολουθεί την υλοποίηση του έργου και θα είναι υπεύθυνος για τα παρακάτω (ενδεικτική και όχι εξαντλητική λίστα):

- Προσθήκη έτοιμου εκπαιδευτικού υλικού ή δημιουργίας μέσω Online editor σε ιδιαίτερα φιλικό περιβάλλον πλοήγησης και με λίγες οθόνες (wizards).
- Δημιουργία ερωτηματολογίων (Test Bank) με αυτόματη εισαγωγή από συγκεκριμένα πρότυπα MS Office.
- Δημιουργία και χρονοπρογραμματισμό του εκπαιδευτικού προγράμματος με τις απαραίτητες αυτόματες ειδοποιήσεις (SMS,email,In-app notification)
- Διαχείριση δραστηριοτήτων (quiz, αξιολογήσεις, τεστ κ.ο.κ.)

- Δημιουργία επεξεργασία και διαγραφή χρηστών οποιασδήποτε μορφής στο σύστημα και απόδοση ρόλων
- Προβολή λίστας συνδεδεμένων χρηστών στην LMS
- Διαχείριση αιτήσεων που υποβάλλονται για συμμετοχή στην εκπαίδευση
- Επικοινωνία με όλους τους χρήστες του συστήματος
- Δυνατότητα επαναφοράς της εκπαίδευσης σε μια προηγούμενη κατάσταση
- Εξαγωγή των αποτελεσμάτων όλων των εκπαιδευομένων σε αρχεία Excel ή PDF με βάση αν ολοκλήρωσαν ή όχι το πρόγραμμα κατάρτισης και αν πέρασαν την τελική αξιολόγηση/εξέταση

Δυνατότητες του συστήματος σε σχέση με τη δημιουργία αναφορών:

Το σύστημα πρέπει να υποστηρίζει την αποτύπωση live αναφορών με κατ' ελάχιστον τις ακόλουθες κατηγορίες:

- Αναφορές αποδοχής όρων χρήσης
- Αναφορές επισκέψεων (ημερήσιες, μηνιαίες, ετήσιες)
- Αναφορές πρόσβασης κάθε κατηγορίας χρηστών με επιλογή της επιθυμητής χρονικής περιόδου
- Αποτελέσματα αξιολογήσεων, εξετάσεων, τελικών Πιστοποιήσεων.
- Καρτέλα εκπαιδευόμενου με όλα τα στοιχεία που σχετίζονται με τον συγκεκριμένο εκπαιδευόμενο και τη συμμετοχή του στο εκπαιδευτικό πρόγραμμα
- Αξιολόγηση/ εξέταση εκπαιδευόμενου, αποτελέσματα και βεβαίωση συμμετοχής του εκπαιδευόμενου

«Επικοινωνιακή Διαχείριση Κρίσεων στον Κυβερνοχώρο»

Η υιοθέτηση νέων τεχνολογιών, η συλλογή, επεξεργασία και αποθήκευση τεράστιου όγκου δεδομένων, έχουν δημιουργήσει νέους κινδύνους που απαιτούν ειδικό σχεδιασμό, προετοιμασία και αντιμετώπιση. Ακόμα και μικρής έκτασης κυβερνοεπιθέσεις, μπορούν να προκαλέσουν σοβαρά προβλήματα στην φήμη, την παραγωγικότητα και την ομαλή λειτουργία ενός οργανισμού.

Το αντικείμενο του παρόντος αφορά στον σχεδιασμό και υλοποίηση ενός εκπαιδευτικού προγράμματος με στόχο την έγκαιρη προετοιμασία και την αποτελεσματική αντίδραση της Ομάδας Διαχείρισης Κρίσεων σε περίπτωση κρίσεων στον κυβερνοχώρο.

Στόχος του προγράμματος είναι:

- α) η δημιουργία ισχυρής εταιρικής συναντίληψης σχετικά με τους κινδύνους τόσο στο «παραδοσιακό» περιβάλλον όσο και στον κυβερνοχώρο
- β) η συγκρότηση & εκπαίδευση της Ομάδας Διαχείρισης Κρίσεων στον Κυβερνοχώρο ώστε να λειτουργεί αποτελεσματικά κατά την αντιμετώπιση τέτοιων κρίσεων
- γ) η επεξεργασία των εσωτερικών διαδικασιών που πρέπει να ακολουθούνται σε περίπτωση κρίσεων στον κυβερνοχώρο και
- δ) η ανάπτυξη ειδικών δεξιοτήτων για την ορθή επικοινωνιακή διαχείριση των κρίσεων

Στο εκπαιδευτικό πρόγραμμα θα παρουσιαστούν και θα αναλυθούν στα μέλη της Ομάδας Διαχείρισης Κρίσεων τα ακόλουθα:

A. Εκτίμηση της υφιστάμενης κατάστασης/ Communication Cyber Crisis Preparedness Assessment

- Αξιολόγηση του υφιστάμενου σχεδίου επικοινωνιακής διαχείρισης κρίσεων στον κυβερνοχώρο και του βαθμού ετοιμότητας του οργανισμού
- Αξιολόγηση του επιπέδου awareness υπαλλήλων και στελεχών σχετικά με ζητήματα ασφάλειας στον κυβερνοχώρο

B. Συγκρότηση της Ομάδας Διαχείρισης Κρίσεων στον Κυβερνοχώρο

Συγκρότηση ή αναδιάρθρωση της υφιστάμενης Ομάδας Διαχείρισης Κρίσεων με την προσθήκη νέων μελών, ανακατανομή αρμοδιοτήτων, καθορισμός ρόλων και διαδικασιών επικοινωνίας και συνεργασίας των μελών της κατά την διάρκεια μιας κρίσης στον κυβερνοχώρο.

Γ. Crisis Management Basics & Cyber Security Basics

- Οριοθέτηση cyber incident και cyber crisis
- Cyber threats landscape

Δ. Case studies

- Παρουσίαση και ανάλυση σημαντικών και περίπλοκων case studies. Αξιολόγηση της ετοιμότητας των εταιρειών που έπεσαν θύματα κυβερνοεπίθεσης, παρουσίαση και

αξιολόγηση της δημόσιας αντίδρασής τους, της επικοινωνίας τους με stakeholders και κοινό κατά την διάρκεια της κρίσης.

Ε. Σχεδιασμός Σεναρίων & Ανάπτυξη της Αντίδρασης της Ομάδας Διαχείρισης Κρίσεων στον Κυβερνοχώρο (Tabletop exercise)

- Σχεδιασμός και συνδιαμόρφωση των πιθανότερων, για τον οργανισμό, σεναρίων κρίσεων στον κυβερνοχώρο
- Παρουσίαση και εξάσκηση στις τεχνικές πρόληψης και διαχείρισης κρίσεων στον κυβερνοχώρο με βάση τα προεπιλεγμένα σενάρια. Προσομοίωση σε round table περιβάλλον

ΣΤ. Διαπραγματεύσεις

Workshop στις τεχνικές διαπραγμάτευσης που πρέπει να ακολουθηθούν σε περίπτωση κρίσης στον κυβερνοχώρο με hackers, media ή άλλους stakeholders.

Ζ. Media Training

- α) Εκπαίδευση των στελεχών της Ομάδας Διαχείρισης Κρίσεων στον Κυβερνοχώρο στις τεχνικές πρόληψης και διαχείρισης επικοινωνιακών κρίσεων στον κυβερνοχώρο,
- β) Οδηγίες για σύνταξη δελτίων τύπου, δηλώσεων, non papers,
- γ) Επιλογή των κατάλληλων καναλιών επικοινωνίας και τεχνικές παρέμβασης.

Η. Παραδοτέο

Δημιουργία εξειδικευμένου οδηγού Επικοινωνιακής Διαχείρισης Κρίσεων στον Κυβερνοχώρο.

7.1.6.2.3 Διαμόρφωση πλάνου ανάκαμψης από καταστροφές για κρίσιμες οντότητες

Ο κύριος στόχος του παρόντος είναι η εκπόνηση Πλάνου Ανάκαμψης από Καταστροφές (DRP) για τις κρίσιμες υποδομές. Επιμέρους στόχοι του Σχεδίου Ανάκαμψης από Καταστροφή αφορούν τα εξής:

- καθορισμός των υποδομών και των συστημάτων με προτεραιοποίησή τους, όσον αφορά στην ετοιμότητα ανάκαμψης από καταστροφή,
- καθορισμός των παραμέτρων και των εξαρτήσεων των υποδομών και των συστημάτων, σε σχέση και με την υποδομή εφεδρείας ανάκαμψης από καταστροφή
- καθορισμός των αποδεκτών διαστημάτων απώλειας πληροφοριών από τον προηγούμενο

συγχρονισμό δεδομένων (RecoveryPointObjective "RPO") και των αναγκών και αποδεκτών χρόνων ενεργοποίησης εκάστου υποσυστήματος (RecoveryTimeObjective "RTO")

- καθορισμός των αναγκών σε υποδομές εξυπηρετητών φιλοξενίας με όλα τα τεχνικά χαρακτηριστικά λειτουργίας τους και των απαραίτητων δικτυακών υποδομών
- καθορισμός του τρόπου – μεθόδου λειτουργίας των νέων συστημάτων ανάκαμψης από καταστροφή και της τεχνολογίας που θα επιλεγεί για τη συχνότητα συγχρονισμού – ενημέρωσης
- καθορισμός των αναγκών τροποποιήσεων ή αναβαθμίσεων που θα πρέπει να υλοποιηθούν στο υφιστάμενο DataCenter, για τη συνεργασία και συγχρονισμό με το DisasterRecoverySite
- καθορισμός τυχόν αναγκών για επέκταση συμβολαίων υποστήριξης των Αναδόχων των υφιστάμενων συστημάτων και υποδομών ή για υπογραφή νέων SLAs.

Για την επίτευξη των ανωτέρω στόχων, ο Ανάδοχος θα βασιστεί στις κατευθύνσεις και καλές πρακτικές του διεθνούς προτύπου ISO 22301:2012, το οποίο αποτελεί ένα πρότυπο που θεσπίζει καλές πρακτικές, ώστε:

- να συνταχθεί Πλάνο Ανάκαμψης από Καταστροφή (DRP) για τις εφαρμογές και τα συστήματα
- να αναπτυχθούν οι απαραίτητες διοικητικές και υποστηρικτικές διαδικασίες για τη συντήρηση και επικαιροποίηση τουDRP.

Επίσης θα ληφθούν υπόψη καλές πρακτικές που προκύπτουν από τα πρότυπα ISOPAS 22399:2007 και ISO/ IEC 27001:2013.

7.1.6.2.4 Εκπόνηση Μελέτης εξωτερικού και εσωτερικού περιβάλλοντος και την ανάδειξη βέλτιστων πρακτικών

Απαραίτητο συστατικό για τον αποτελεσματικό έλεγχο ασφάλειας των υποδομών και συστημάτων είναι η αντίληψη και η αξιολόγηση του ευρύτερου περιβάλλοντος στους τομείς της ασφάλειας των δικτύων / πληροφοριακών συστημάτων και της διασφάλισης του απορρήτου των επικοινωνιών. Επομένως, θα πρέπει να διενεργηθεί μια μελέτη της κατάστασης που επικρατεί και των πρακτικών που εφαρμόζονται στον τομέα ασφάλειας σε παρεμφερή συστήματα τόσο εντός της χώρας όσο και σε διεθνές επίπεδο. Σκοπός της μελέτης αυτής είναι να δημιουργηθεί μια ολοκληρωμένη βάση γνώσης για το πλήρες ιστορικό που αφορά την ασφάλεια και στη συνέχεια να εξαχθούν χρήσιμα συμπεράσματα, τα οποία θα αξιοποιηθούν από τον Ανάδοχο για να φέρει εις πέρας τις υπόλοιπες εργασίες που απαιτούνται.

Στο πλαίσιο της εργασίας αυτής, θα συλλεχθούν και στη συνέχεια επεξεργασθούν και αναλυθούν πληροφορίες και δεδομένα που αφορούν στην ασφάλεια παρόμοιων υποδομών και συστημάτων τόσο εντός της χώρας όσο και σε άλλες χώρες. Τα δεδομένα θα εστιάσουν κατ' ελάχιστον:

- Στα υιοθετημένα Συστήματα Διαχείρισης της Ασφάλειας των Πληροφοριών (ΣΔΑΠ) και τις υποκείμενες σε αυτά διαδικασίες, πολιτικές και πρακτικές
- Στους κινδύνους ασφάλειας, στις ευπάθειες ανάλογων συστημάτων και στις μεθόδους αποτίμησης της επικινδυνότητας που συνήθως εμφανίζονται ή εφαρμόζονται αντίστοιχα
- Στις αποτελεσματικές μεθόδους παρακολούθησης της ασφάλειας ανάλογων υποδομών και συστημάτων

- Στα καταξιωμένα εργαλεία και μηχανισμούς ΤΠΕ που χρησιμοποιούνται για τον επιτυχή έλεγχο ασφάλειας ανάλογων υποδομών και συστημάτων
- Στο ιστορικό περιστατικών ασφάλειας και στις μεθόδους αντιμετώπισης αυτών, από τα οποία να μπορεί να εξαχθεί χρήσιμη γνώση για την καλύτερη διασφάλιση της ασφάλειας

Τα συστήματα που θα αποτελέσουν αντικείμενο της παρούσας μελέτης, θα μπορούν να είναι είτε δημόσια είτε ιδιωτικά, αλλά θα πρέπει να παρουσιάζουν ανάλογα επιχειρησιακά χαρακτηριστικά με αυτά της Ε.Δ.Υ.Τ.Ε., ώστε να μπορούν στη συνέχεια να πραγματοποιηθούν οι ενέργειες παραλληλισμού μεταξύ τους και εξαγωγής χρήσιμων συμπερασμάτων. Για τη συλλογή των δεδομένων και τη δημιουργία μιας πλήρους και αντιπροσωπευτικής βάσης γνώσης ασφάλειας συστημάτων, απαιτείται όπως μελετηθούν τουλάχιστον τρεις (3) περιπτώσεις (businesscases) ανάλογων δικτύων, εκ των οποίων τουλάχιστον οι δύο (2) θα είναι οπωσδήποτε στο εξωτερικό, η καθεμία σε διαφορετική χώρα, τεχνολογικά προηγμένη όπως συγκεκριμένα είναι τα πλέον ανεπτυγμένα κράτη μέλη της Ευρωπαϊκής Ένωσης, οι ΗΠΑ, το Ισραήλ, η Ιαπωνία, η Νότια Κορέα, κλπ.

Παράλληλα με τη διερεύνηση της ασφάλειας των προαναφερθέντων έτερων συστημάτων, η παρούσα εργασία θα λάβει υπόψη και τις πλέον επιστημονικά καταξιωμένες μεθόδους και πρακτικές που εφαρμόζονται στην πρόληψη, αντιμετώπιση, και εν γένει διαχείριση της ασφάλειας παρόμοιων συστημάτων. Η πληροφορία αυτή θα αποτελέσει επίσης τμήμα της ολοκληρωμένης βάσης

7.1.6.2.5 Διαμόρφωση πολιτικής αντιγράφων ασφαλείας

Η πολιτική αντιγράφων ασφαλείας αποτελεί κρίσιμο παράγοντα για την επιχειρησιακή συνέχεια και τη δυνατότητα ανάκαμψης από καταστροφή.

Ο Ανάδοχος καλείται να διαμορφώσει πολιτική αντιγράφων ασφαλείας για τις υποδομές και τα πληροφοριακά συστήματα της Ε.Δ.Υ.Τ.Ε., η οποία θα περιλαμβάνει κατ' ελάχιστο τα εξής:

- Συχνότητα λήψης αντιγράφων ασφαλείας
- Τύπος δεδομένων / αρχείων τα οποία θα αφορά
- Τοποθεσία και μέσο λήψης αντιγράφων
- Χρόνος διατήρησης αντιγράφων
- Αρμοδιότητες προσωπικού και προμηθευτών σχετικά με τη λήψη αντιγράφων ασφαλείας
- Διαδικασίες και κανόνες ελέγχου της ακεραιότητας των αντιγράφων
- Διαδικασία ανάκτησης δεδομένων από τα αντίγραφα ασφαλείας

7.1.6.2.6 Διαμόρφωση Συστήματος Διαχείρισης της Ασφάλειας των Πληροφοριών (ΣΔΑΠ) με βάση το πρότυπο ISO 27001 & Εκπόνηση Μελέτης Ανάλυσης και Αξιολόγησης Κινδύνων

Για τη διαμόρφωση ενός ολοκληρωμένου ΣΔΑΠ για την Ε.Δ.Υ.Τ.Ε., ο Ανάδοχος θα πραγματοποιήσει τις ενέργειες που αναφέρονται στο πρότυπο ISO 27001 συμπεριλαμβανομένου του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR) και αφορούν στη Φάση "Plan" που αναφέρεται στο πρότυπο, όπως κατ' ελάχιστον αναφέρονται οι ακόλουθες:

- Θα ορίσει το Πεδίο Εφαρμογής του ΣΔΑΠ (scope and boundaries of the ISMS), όσον αφορά τα επιχειρησιακά χαρακτηριστικά της Ε.Δ.Υ.Τ.Ε. και τα αγαθά που πρέπει να προστατευθούν. Παράλληλα, θα καταγράψει τις συνιστώσες εκείνες του περιβάλλοντος που δεν θα περιλαμβάνονται στο πεδίο εφαρμογής, συνοδευμένες από κατάλληλη τεκμηρίωση για την εξαίρεση τους
- Θα ορίσει την πολιτική του ΣΔΑΠ, όσον αφορά το ευρύτερο περιβάλλον λειτουργίας

- Θα ορίσει τη μεθοδολογία αποτίμησης της επικινδυνότητας που θα εφαρμοστεί
- Θα προσδιορίσει τους κινδύνους που ενέχονται στη λειτουργία του Δικτύου
- Θα αναλύσει και θα εκτιμήσει τους κινδύνους αυτούς
- Θα προσδιορίσει και υπολογίσει μεθόδους για την αντιμετώπιση των κινδύνων
- Θα επιλέξει κατάλληλα σημεία ελέγχου (controls) αντιμετώπισης των κινδύνων
- Θα μεριμνήσει για να λάβει την έγκριση της Διοίκησης της Ε.Δ.Υ.Τ.Ε. όσον αφορά τους προτεινόμενους υπολειμματικούς κινδύνους
- Θα μεριμνήσει για να λάβει την έγκριση της Διοίκησης της Ε.Δ.Υ.Τ.Ε. για να υλοποιήσει και να λειτουργήσει το υιοθετημένο ΣΔΑΠ
- Θα προετοιμάσει μια Δήλωση Εφαρμοσιμότητας (Statement of Applicability), η οποία θα περιλαμβάνει τα προβλεπόμενα στο πρότυπο ISO 27001.

Στο πλαίσιο των ενεργειών διαμόρφωσης του ΣΔΑΠ, θα πραγματοποιήσει κατ' ελάχιστον τις παρακάτω εργασίες, τα αποτελέσματα των οποίων θα συμπεριληφθούν κατά περίπτωση στις πολιτικές, διαδικασίες σχέδια και λοιπά έγγραφα του ΣΔΑΠ.

Ανάλυση επιχειρησιακών επιπτώσεων

Ο Ανάδοχος θα εκπονήσει ανάλυση επιχειρησιακών επιπτώσεων, με την οποία θα εντοπίσει και καταγράψει τις επιχειρησιακές λειτουργίες και τους πόρους που υποστηρίζουν τις λειτουργίες αυτές και σχετίζονται ή μπορεί να επηρεάσουν την ακεραιότητα των υποδομών της Ε.Δ.Υ.Τ.Ε. και τη διαθεσιμότητα των παρεχόμενων από αυτήν υπηρεσιών.

Ανάλυση κινδύνου και αποτίμηση επικινδυνότητας

Ο Ανάδοχος θα πραγματοποιήσει μελέτη ανάλυσης κινδύνου και αποτίμησης επικινδυνότητας, προκειμένου να αναγνωρίσει και αναλύσει τις ενδεχόμενες απειλές στην ακεραιότητα των υποδομών.

Στο πλαίσιο της εργασίας αυτής, ο Ανάδοχος κατ' ελάχιστον:

- Θα μελετήσει και καταγράψει όλες τις απειλές και κινδύνους που πιθανά αντιμετωπίζει ή αναμένεται να αντιμετωπίσουν οι υποδομές.
- Θα κατηγοριοποιήσει και εξετάσει τις απειλές που θα αναγνωρίσει σε (α) ενδογενείς, οι οποίες προέρχονται από το εσωτερικό του συστήματος και εξαρτώνται από το επίπεδο της εσωτερικής αξιοπιστίας, ασφάλειας και ανθεκτικότητας, σε (β) εξωγενείς, οι οποίες προέρχονται από το εξωτερικό περιβάλλον, όπως καιρικές συνθήκες, φυσικές καταστροφές κλπ και (γ) σε απειλές που προέρχονται από άλλα διασυνδεδεμένα συστήματα ή δίκτυα. Παράλληλα, θα διενεργηθεί εκτίμηση της σοβαρότητας κάθε απειλής.
- Θα διενεργήσει μια συσχέτιση μεταξύ των διαθέσιμων πόρων (πληροφοριακά συστήματα, δίκτυα, εγκαταστάσεις, ανθρώπινο δυναμικό) και των εκτιμώμενων απειλών που δύναται να τους επηρεάσουν εφόσον εκδηλωθούν.
- Θα καταγράψει τα ευάλωτα σημεία και τις αδυναμίες των πόρων που απαιτούνται για τη συνέχιση κάθε επιχειρησιακής λειτουργίας. Στη συνέχεια θα αξιολογήσει την πιθανότητα εκδήλωσης των απειλών που έχει ήδη αναγνωρίσει και θα εκτιμήσει την επίδραση τους στη λειτουργία συστημάτων και υποδομών και τη διάθεση των παρεχόμενων υπηρεσιών.
- Θα αναλύσει τις ανάγκες και απαιτήσεις προστασίας.

- Θα προσδιορίσει και προτείνει τη διαδικασία που θα ακολουθήσει καθώς και τα μέτρα που θα λάβει, προκειμένου να αντιμετωπίσει κάθε ενδεχόμενη απειλή
- Θα προτείνει διαδικασίες αξιολόγησης της αποτελεσματικότητας των μέτρων που προτείνει να εφαρμοσθούν κατά περίπτωση απειλής.

Διαμόρφωση πολιτικών ασφάλειας κρίσιμων οντοτήτων με στόχο την ανάδειξη τεχνικών και οργανωτικών μέτρων για την προστασία τους από Κυβερνοαπειλές

Η διαμόρφωση πολιτικών θα πρέπει να είναι κατάλληλα δομημένη, ώστε να καλύπτει όλες τις παραμέτρους / συνιστώσες λειτουργίας των κρίσιμων υποδομών της Ε.Δ.Υ.Τ.Ε. Ειδικότερα, θα γίνει σαφής αναφορά και ανάλυση στα ακόλουθα:

- Εύρος των πολιτικών. Αρχικά θα προσδιοριστεί το σύνολο των αγαθών των κρίσιμων υποδομών της Ε.Δ.Υ.Τ.Ε., για τα οποία θα διαμορφωθούν οι πολιτικές και στη συνέχεια θα προσδιοριστούν και αναλυθούν οι απειλές που αντιμετωπίζουν τα αγαθά αυτά
- Ασφάλεια των υποδομών, των πληροφοριακών συστημάτων και των υποκείμενων δεδομένων
 - ο Φυσική ασφάλεια (μέθοδοι υλοποίησης, κανόνες προστασίας, κλπ)
 - ο Ασφάλεια δικτύου (VPNs, ασφάλεια συνδέσεων, συνδέσεις εξωτερικών συνεργατών, κανόνες πρόσβασης στο δικτυακό εξοπλισμό, κανόνες χρησιμοποίησης δικτύου, κλπ)
 - ο Ασφάλεια εξυπηρετητών (Διαχείριση, πρόσβαση, λογισμικό, δικτυακές υπηρεσίες, αναβάθμιση, προσθήκη νέου συστήματος, κλπ)
 - ο Συστήματα χρηστών (κανόνες ασφάλειας, διαχείριση χρηστών, λογισμικό χρηστών, πολιτικών κωδικών πρόσβασης (passwords))
 - ο Κακόβουλο λογισμικό
- Προστασία πληροφοριών (έλεγχος διασποράς στοιχείων, κρυπτογράφηση δεδομένων, διαχείριση στοιχείων που δίνονται σε τρίτους, κλπ)

Υλοποίηση και λειτουργία του ΣΔΑΠ

Για την υλοποίηση και λειτουργία του υιοθετημένου ΣΔΑΠ, ο Ανάδοχος θα πραγματοποιήσει τις ενέργειες που αναφέρονται στο πρότυπο ISO 27001 συμπεριλαμβανομένου του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR) και αφορούν στη Φάση "Do" που αναφέρεται στο πρότυπο, όπως κατ' ελάχιστον αναφέρονται οι ακόλουθες:

- Θα αναπτύξει ένα σχέδιο αντιμετώπισης των κινδύνων (risk treatment plan), το οποίο προσδιορίζει τις κατάλληλες ενέργειες που πρέπει να γίνουν για την ορθή διαχείριση των κινδύνων ασφάλειας
- Θα υλοποιήσει το σχέδιο αντιμετώπισης κινδύνων, ώστε να επιτύχει τους αντίστοιχους στόχους που έχουν τεθεί
- Θα υλοποιήσει τα σημεία ελέγχου (controls) για την αντιμετώπιση των κινδύνων, που έχουν επιλεγεί κατά τη φάση διαμόρφωσης του ΣΔΑΠ, ώστε να επιτευχθούν οι αντίστοιχοι στόχοι
- Θα ορίσει τους δείκτες με τους οποίους θα μετριέται η αποτελεσματικότητα των επιλεγθέντων μέτρων αντιμετώπισης και στη συνέχεια θα προσδιορίσει την αποτελεσματικότητα των δεικτών αυτών στην παραγωγή συγκρίσιμων και αναπαραγώγιμων αποτελεσμάτων
- Θα υλοποιήσει προγράμματα εκπαίδευσης και ευαισθητοποίησης
- Θα διαχειριστεί τη λειτουργία του ΣΔΑΠ
- Θα διαχειριστεί τους απαιτούμενους πόρους για τη λειτουργία του ΣΔΑΠ

- Θα υλοποιήσει διαδικασίες και όποια άλλα μέτρα κρίνει, ώστε να καταστεί δυνατή η έγκαιρη ανίχνευση περιστατικών ασφάλειας και η αποτελεσματική ανταπόκριση σε αυτά
- Θα προσδιορίσει και στη συνέχεια μεριμνήσει να διαθέσει τους πόρους που απαιτούνται:
 - ο για την ορθή διαμόρφωση, υλοποίηση, παρακολούθηση, ανασκόπηση, συντήρηση και βελτίωση του ΣΔΑΠ
 - ο ώστε να διασφαλιστεί ότι οι υιοθετημένες διαδικασίες ασφάλειας των πληροφοριών υποστηρίζουν τις επιχειρησιακές απαιτήσεις
 - ο για να προσδιοριστούν και αντιμετωπιστούν οι απαιτήσεις που προέρχονται από το υφιστάμενο νομικό ή ρυθμιστικό πλαίσιο καθώς και οι ενδεχόμενες συμβατικές υποχρεώσεις
 - ο Διατηρήσει ένα επαρκές επίπεδο ασφάλειας, εφαρμόζοντας κατάλληλα τα επιλεγμένα μέτρα ελέγχου για την αντιμετώπιση των κινδύνων
 - ο Εκπονεί ανασκοπήσεις του ΣΔΑΠ, όποτε κριθεί απαραίτητο και στη συνέχεια να ανταποκρίνεται κατάλληλα, ανάλογα με τα πορίσματα των ανασκοπήσεων αυτών
 - ο Να βελτιώνει την αποτελεσματικότητα του ΣΔΑΠ, όπου κριθεί απαραίτητο
- Θα εκπονήσει προγράμματα εκπαίδευσης και ευαισθητοποίησης σε όλα τα στελέχη της Αναθέτουσας Αρχής και του Φορέα Λειτουργίας, στα οποία τους έχουν ανατεθεί αρμοδιότητες που ορίζονται στο υιοθετημένο ΣΔΑΠ, ώστε αυτά να καταστούν ικανά να προβούν στην επιτυχή άσκηση των καθηκόντων τους.

Παρακολούθηση και ανασκόπηση του ΣΔΑΠ

Για την παρακολούθηση και ανασκόπηση του υιοθετημένου ΣΔΑΠ, ο Ανάδοχος θα πραγματοποιήσει τις ενέργειες που αναφέρονται στο πρότυπο ISO 27001 συμπεριλαμβανομένου του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR) και αφορούν στη Φάση "Check" που αναφέρεται στο πρότυπο, όπως κατ' ελάχιστον αναφέρονται οι ακόλουθες:

- Θα πραγματοποιήσει κατάλληλες διαδικασίες και ενέργειες παρακολούθησης και ανασκόπησης του ΣΔΑΠ
- Θα πραγματοποιεί τακτικές ανασκοπήσεις της αποτελεσματικότητας του ΣΔΑΠ, λαμβάνοντας υπόψη τα ευρήματα των εσωτερικών ελέγχων που θα πραγματοποιεί, τα συμπεράσματα που θα προκύπτουν από τα περιστατικά ασφάλειας που έχουν συμβεί, καθώς και τις προτάσεις άλλων εμπλεκόμενων φορέων
- Θα μετρήσει την αποτελεσματικότητα των μέτρων αντιμετώπισης των κινδύνων, ώστε να επιβεβαιώσει ότι ικανοποιούνται οι απαιτήσεις ασφάλειας
- Θα προβεί σε ανασκόπηση της αποτίμησης επικινδυνότητας σε τακτά χρονικά διαστήματα και των υπολειμματικών κινδύνων (residual risks) καθώς και τα επίπεδα κινδύνου που θεωρήθηκαν αποδεκτά, λαμβάνοντα υπόψη τα πλέον πρόσφατα δεδομένα
- Θα διενεργεί εσωτερικούς ελέγχους ασφάλειας σε τακτά χρονικά διαστήματα (που θα οριστούν επακριβώς κατά την Φάση ανάλυσης απαιτήσεων του έργου)
- Θα μεριμνήσει για την ανασκόπηση του υιοθετημένου ΣΔΑΠ από το αρμόδιο όργανο σε τακτά χρονικά διαστήματα
- Θα επικαιροποιεί τα σχέδια ασφάλειας, λαμβάνοντας υπόψη τα ευρήματα από τις ενέργειες παρακολούθησης και ανασκόπησης του ΣΔΑΠ
- Θα καταγράφει τις ενέργειες και τα γεγονότα, που θα μπορούσαν να έχουν επίπτωση στην αποτελεσματικότητα ή στην απόδοση του υιοθετημένου ΣΔΑΠ.

Συντήρηση και βελτίωση του ΣΔΑΠ

Για τη συντήρηση και βελτίωση του υιοθετημένου ΣΔΑΠ, ο Ανάδοχος θα πραγματοποιήσει τις ενέργειες που αναφέρονται στο πρότυπο ISO 27001 συμπεριλαμβανομένου του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR) και αφορούν στη Φάση "Act" που αναφέρεται στο πρότυπο, όπως κατ' ελάχιστον αναφέρονται οι ακόλουθες:

- Θα πραγματοποιήσει τις βελτιώσεις στο ΣΔΑΠ, που έχουν προσδιοριστεί
- Θα προβεί σε κατάλληλες διορθωτικές και προληπτικές ενέργειες, εφαρμόζοντας τα ευρήματα της αποτύπωσης κατάστασης και ειδικότερα τις βέλτιστες πρακτικές της Παρ. 1.3.1 και των υποπαραγράφων αυτής.
- Θα επικοινωνήσει τις ενέργειες βελτίωσης σε όλα τα εμπλεκόμενα μέρη, με όλα τα απαραίτητα στοιχεία και λεπτομέρειες
- Θα διασφαλίσει ότι οι πραγματοποιημένες βελτιώσεις επιτυγχάνουν το σχετικό στόχο τους.

7.1.6.2.7 Διενέργεια ελέγχων διείσδυσης εξωτερικών δικτύων, εφαρμογών Ιστού, φυσικής ασφάλειας και διαρροής δεδομένων

Έλεγχοι διείσδυσης εξωτερικών δικτύων

Στο σύγχρονο περιβάλλον κυβερνοαπειλών κάθε ευπάθεια μπορεί να αποτελέσει αντικείμενο εκμετάλλευσης με καταστροφικές συνέπειες. Οι έλεγχοι διείσδυσης εξωτερικών δικτύων (external network penetration test) εντοπίζουν ευπάθειες σε υποδομές, συσκευές και διακομιστές που είναι προσβάσιμες από το διαδίκτυο.

Οι έλεγχοι προσομοιάζουν τις επιθέσεις κακόβουλων εισβολέων, οι οποίοι έχουν ως στόχο τη ναπόκτηση πρόσβαση σε συστήματα και τις εφαρμογές της περιμέτρου. Η μέθοδος εκτέλεσης των ελέγχων θα πρέπει να εξασφαλίζουν ότι δεν θα προκληθούν φθορές ή οποιουδήποτε τύπου προβλήματα στη λειτουργία υποδομών και συστημάτων.

Έλεγχοι διείσδυσης εφαρμογών Ιστού

Οι δοκιμές διείσδυσης διαδικτυακών εφαρμογών στοχεύουν στον εντοπισμό τρωτών σημείων ασφαλείας που προκύπτουν από ανασφαλείς πρακτικές ανάπτυξης στη δημιουργία τη σχεδίαση και τη διαχείριση του λογισμικού ή ιστότοπου. Οι διαδικτυακές εφαρμογές χρησιμοποιούνται όλο και περισσότερο και αποτελούν κατεξοχήν στόχο κακόβουλων επιθέσεων. Στα πλαίσια των ελέγχων θα πρέπει να πραγματοποιηθεί μια σειρά προσομοιωμένων επιθέσεων, οι οποίες προσομοιάζουν κακόβουλες επιθέσεις, με σκοπό την αποτύπωση κάθε ευπάθειας και τη συνολική αποτίμηση του βαθμού ασφάλειας μιας εφαρμογής.

Έλεγχοι Φυσικής Ασφάλειας

Ο έλεγχος φυσικής ασφάλειας αξιολογεί τα μέτρα ασφαλείας που προστατεύουν τα περιουσιακά στοιχεία του οργανισμού από απειλές και στοχεύει σε προτάσεις για τυχόν βελτιώσεις. Οι έλεγχοι πρέπει να σχεδιάζονται με στόχο την παραβίαση της φυσικής ασφάλειας μίας ή περισσότερων τοποθεσιών. Τα σενάρια θα πρέπει να καθοριστούν βάσει ανάλυσης των υποδομών, με στόχο τη μη εξουσιοδοτημένη πρόσβαση σε φυσικές τοποθεσίες και πρόσβαση στο εσωτερικό δίκτυο με τη χρήση ειδικών συσκευών.

Ο υποψήφιος ανάδοχος καλείται να περιγράψει στην τεχνική του προσφορά τη μεθοδολογία εκτέλεσης των ελέγχων.

Έλεγχοι Διαρροής Δεδομένων

Οι έλεγχοι διαρροής δεδομένων αφορούν στη συγκέντρωση, ανάλυση και αξιολόγηση της βαρύτητας και του βαθμού ευαισθησίας πληροφοριών του οργανισμού από διάφορες πηγές (συμπεριλαμβανομένου του σκοτεινού διαδικτύου).

Ο έλεγχος θα πρέπει να αφορά πληθώρα δεδομένων, όπως ενδεικτικά ονόματα χρήστη και κωδικοί χρηστών, μηνύματα ηλεκτρονικού ταχυδρομείου κλπ. Στη συνέχεια θα πρέπει να προτείνονται μέτρα για την αντιμετώπιση ή το μετριασμό των συνεπειών της διαρροής και την αποφυγή της επανάληψής της.

Ο υποψήφιος ανάδοχος καλείται να περιγράψει στην τεχνική του προσφορά τη μεθοδολογία εκτέλεσης των ελέγχων.

Ο υποψήφιος ανάδοχος καλείται να περιγράψει στην τεχνική του προσφορά τη μεθοδολογία εκτέλεσης του συνόλου των παραπάνω ελέγχων.

7.1.6.2.8 Αξιοποίηση τεχνολογικής καινοτομίας και ερευνητικής πρωτοπορίας

Η διασφάλιση επαρκούς Επιχειρησιακής Συνέχειας, ειδικά απέναντι στο ενδεχόμενο κυβερνοεπιθέσεων, προϋποθέτει συνδυαστικές δράσεις πολλαπλής στόχευσης. Από τη μια πλευρά πρέπει να υπάρχει συστηματική μέριμνα για την αντιμετώπιση ήδη γνωστών τύπων κυβερνοαπειλών, με χρήση βέλτιστων πρακτικών και διαθέσιμων αποτελεσματικών τεχνολογιών. Από την άλλη, πρέπει να υπάρχει επίσης μέριμνα για την αντιμετώπιση καινοφανών κυβερνοεπιθέσεων, με αξιοποίηση προηγμένων μεθοδολογιών και τεχνολογικών λύσεων, όπως αυτές προκύπτουν, προδιαγράφονται και αξιολογούνται σε εξειδικευμένα ακαδημαϊκά ερευνητικά περιβάλλοντα.

Δεδομένων των ρηξικέλευθων εξελίξεων σε θέματα Κυβερνοασφάλειας, ο συνδυασμός βέλτιστων πρακτικών, δοκιμασμένων λύσεων και προηγμένων (state-of-the-art) μεθοδολογιών και τεχνολογιών αποτελεί το επαρκέστερο μέσο διασφάλισης της Επιχειρησιακής Συνέχειας. Συνεπώς, τα ζητούμενα πληροφοριακά συστήματα, τεχνολογικά προϊόντα και εξειδικευμένες υπηρεσίες θα πρέπει να παρέχονται με τρόπο που εγγυάται ότι όχι μόνο τα καταλληλότερα διαθέσιμα συστήματα της Αγοράς, αλλά και οι πρωτότυπες μεθοδολογίες και τεχνολογίες που παρέχει ο σχετικά εξειδικευμένος ακαδημαϊκός τομέας θα αξιοποιούνται συνδυαστικά.

Επιπρόσθετα, οι δόκιμες μεθοδολογίες και τεχνολογίες διασφάλισης της Επιχειρησιακής Συνέχειας προϋποθέτουν τακτικούς και συστηματικούς ελέγχους (penetration tests), αξιολογήσεις (audits), πιστοποιήσεις (certifications), μελέτες ανάλυσης και διαχείρισης επικινδυνότητας (risk analysis and management) κλπ., οι οποίες πρέπει να εκπονούνται σύμφωνα με διεθνή πρότυπα και αντίστοιχες καλές πρακτικές. Οι αδιαμφισβήτητες αυτές αναγκαιότητες, με τη σειρά τους, προϋποθέτουν συνθήκες λειτουργικής ανεξαρτησίας και αβίαστων επιστημονικών αποτιμήσεων, κάτι που μπορεί να εξυπηρετηθεί αποτελεσματικά με τη συνδρομή του εξειδικευμένου ακαδημαϊκού τομέα.

7.1.6.3 Εξειδικευμένες Λύσεις Ασφάλειας Πληροφοριών, Εγγράφων και εφαρμογών

7.1.6.3.1 Λύση Διαβάθμισης και Σήμανσης Εγγράφων

Η λύση Διαβάθμισης εγγράφων (Documents Classification) θα πρέπει να δίνει τη δυνατότητα στον χρήστη να επιλέξει και να αποδώσει με απλές κινήσεις, το κατάλληλο επίπεδο διαβάθμισης σε ένα έγγραφο, με βάση την Πολιτική Ασφάλειας του Φορέα. Το επιλεγμένο επίπεδο διαβάθμισης θα πρέπει να συνοδεύει το έγγραφο μέσω κατάλληλης σήμανσης στα μεταδεδομένα (metadata), αλλά και στην εμφάνιση του εγγράφου, ώστε να καθίσταται ορατό στους χρήστες, να εντείνεται η εγρήγορση του χρήστη (awareness) και να αποφεύγεται η κακή χρήση του εγγράφου λόγω αμέλειας. Η λύση Διαβάθμισης εγγράφων θα πρέπει να συμπληρώνει και να αναδεικνύει της δυνατότητες του συστήματος DLP.

7.1.6.3.2 Λύση Προστασίας Δεδομένων από Διαρροή

Η επέκταση της ψηφιακής διαχείρισης εγγράφων σε συνδυασμό με τη διαθεσιμότητα πληθώρας διαφορετικών μεθόδων για την αποστολή και γενικά τη διακίνηση εγγράφων, έχει δημιουργήσει επιπλέον κινδύνους για τη διαρροή κρίσιμων εγγράφων εκτός του οργανισμού. Η λύση αποτροπής διαρροής πληροφοριών θα πρέπει να ανιχνεύει και να προλαμβάνει τη διακίνηση ευαίσθητων και εμπιστευτικών εγγράφων μέσω κάθε δυνατής οδού πχ μέσω αποσπώμενων αποθηκευτικών μέσων (usb), μέσω αλληλογραφίας (email), μέσω δικτυακής μεταφοράς αρχείων (ftp), μέσω internetupload, κλπ.

Η λύση θα πρέπει να εκμεταλλεύεται τη σήμανση των εγγράφων από λύσεις διαβάθμισης εγγράφων, για τον εντοπισμό ευαίσθητων και εμπιστευτικών εγγράφων.

7.1.6.3.3 Λύση Διαχείρισης Δικαιωμάτων Εγγράφων

Για την αποτελεσματική προστασία των εγγράφων του οργανισμού τα οποία πρέπει να υποστούν επεξεργασία από απομακρυσμένους χρήστες ή να διατηρηθούν σε υποδομές εκτός της περιμέτρου του οργανισμού, απαιτείται μία λύση διαχείρισης των δικαιωμάτων χρήσης των εγγράφων αυτών η οποία να επιτρέπει τον καθορισμό των δικαιωμάτων πρόσβασης στα έγγραφα αυτά και τον απομακρυσμένο έλεγχο τους (IRM - InformationRightsManagement). Η λύση πρέπει να προστατεύει τον οργανισμό από επιχειρηματικούς και κανονιστικούς κινδύνους που σχετίζονται με την μη αποδεκτή χρήση των εγγράφων του οργανισμού από εξωτερικούς συνεργάτες ή την χρήση τους για σκοπούς μη συμβατούς με τους σκοπούς επεξεργασίας που θέτει ο οργανισμός.

Η λύση πρέπει να είναι εύχρηστη ώστε οι κανόνες και οι πολιτικές προστασίας των εγγράφων να καθορίζονται από τους ίδιους τους χρήστες χωρίς να απαιτείται πάντα η εμπλοκή του τμήματος Πληροφορικής (IT). Οι κανόνες και οι πολιτικές προστασίας εγγράφων πρέπει να εφαρμόζονται είτε σε μεμονωμένους χρήστες είτε σε ομάδες χρηστών και να δίνουν την δυνατότητα στους ιδιοκτήτες των εγγράφων όχι μόνο να καθορίζουν τους χρήστες που έχουν δικαίωμα πρόσβασης στα έγγραφα,

αλλά και να εποπτεύουν την χρήση των εγγράφων ή να ανακαλούν τα δικαιώματα πρόσβασης. Η λύση

πρέπει να δίνει την δυνατότητα εφαρμογής πολιτικών και κανόνων προστασίας είτε σε μεμονωμένα έγγραφα είτε σε ομάδες εγγράφων που διατηρούνται σε φακέλους, fileservers, κλπ.

Αναλυτικότερα η λύση πρέπει να έχει τα χαρακτηριστικά που περιγράφονται στις επόμενες παραγράφους.

Καθορισμός δικαιωμάτων χρήσης και απομακρυσμένος έλεγχος επί των εγγράφων

- Η λύση πρέπει να επιτρέπει τον καθορισμό του είδους των δικαιωμάτων που έχει κάθε χρήστης επί του εγγράφου (πχ μόνο ανάγνωση, επεξεργασία, ορισμός δικαιούχων, κλπ)
- Η λύση πρέπει να δίνει την δυνατότητα εξ αποστάσεως αναίρεσης των δικαιωμάτων που έχουν παραχωρηθεί σε χρήστες ή διαγραφής ενός εγγράφου
- Η λύση πρέπει να δίνει την δυνατότητα ορισμού ημερομηνιών λήξης της ισχύος των δικαιωμάτων πρόσβασης.
- Η λύση πρέπει να δίνει την δυνατότητα σε διαχειριστές να καθορίζουν πολιτικές πρόσβασης και σε χρήστες να εφαρμόζουν αυτές τις πολιτικές πρόσβασης σε έγγραφα.

Απόδοση δικαιωμάτων σε χρήστες

- Η λύση πρέπει να έχει την δυνατότητα να αποδίδει συγκεκριμένα δικαιώματα πρόσβασης είτε σε μεμονωμένους χρήστες είτε σε ομάδες χρηστών.
- Η λύση πρέπει να δίνει την δυνατότητα καθορισμού των διαδικτυακών διευθύνσεων από τις οποίες επιτρέπεται η πρόσβαση στα έγγραφα.
- Η λύση πρέπει να αναγνωρίζει και να αυθεντικοποιεί τους χρήστες του οργανισμού μέσω πλήρους λειτουργικής διασύνδεσης με το AD του οργανισμού.
- Η λύση πρέπει να έχει την δυνατότητα απόδοσης συγκεκριμένων δικαιωμάτων πρόσβασης σε χρήστες που ανήκουν σε συγκεκριμένες ομάδες του οργανισμού (ActiveDirectorygroups).
- Η λύση πρέπει να δίνει την δυνατότητα να καθορίζονται ονομαστικά οι χρήστες (εσωτερικοί ή εξωτερικοί) στους οποίους επιτρέπεται η πρόσβαση στα έγγραφα του οργανισμού καθώς και το είδος της πρόσβασης που παρέχεται.
- Η λύση πρέπει να έχει την δυνατότητα αποστολής ειδοποιήσεων/προσκήσεων (invitations) σε εξωτερικούς χρήστες στους οποίους παραχωρείται πρόσβαση σε ένα έγγραφο.
- Οι χρήστες στους οποίους αποδίδεται δικαίωμα πρόσβασης πρέπει να μπορούν να διαχειρίζονται το έγγραφο χωρίς την χρήση ειδικών προγραμμάτων (transparency).

Είδη εγγράφων φακέλοι και μέσα αποθήκευσης

- Η λύση πρέπει να δίνει την δυνατότητα καθορισμού δικαιωμάτων πρόσβασης είτε σε διακριτά έγγραφα είτε σε όλα τα έγγραφα που διατηρούνται σε συγκεκριμένα διακριτά σημεία διατήρησης (φακέλους ή μέσα αποθήκευσης).
- Η λύση πρέπει να δίνει δυνατότητα καθορισμού δικαιωμάτων πρόσβασης σε αρχεία που διατηρούνται είτε σε τοπικούς servers είτε σε εφαρμογές νέφους (Office365, Dropbox, Sharepoint, κλπ).

- Ο τρόπος διαχείρισης των δικαιωμάτων πρόσβασης θα πρέπει να είναι ίδιος ανεξάρτητα από το μέσο διατήρησης των αρχείων (πχ. τοπικοί servers, ή εφαρμογές cloud).

Συμβατότητα και αλληλεπίδραση με εφαρμογές τρίτων κατασκευαστών

- Η λύση πρέπει να έχει πλήρη συμβατότητα με τις εφαρμογές του MicrosoftOffice και να δίνει δυνατότητα στους χρήστες των εφαρμογών να καθορίζουν τα δικαιώματα επί των εγγράφων μέσα από το περιβάλλον των ίδιων των εφαρμογών.
- Η λύση πρέπει να έχει πλήρη συμβατότητα με τις εφαρμογές Outlook και Exchange.
- Η λύση πρέπει να έχει δυνατότητα καθορισμού δικαιωμάτων και σε αρχεία pdf.
- Η λύση πρέπει να έχει την δυνατότητα λειτουργικής διασύνδεσης με λύση DLP (DataLossPrevention).
- Η λύση να έχει πλήρη συμβατότητα με την εφαρμογή SIEM

7.1.6.3.4 Λύση Διαχείρισης Λογαριασμών και Δικαιωμάτων Πρόσβασης Χρηστών

Η λύση Διαχείρισης Λογαριασμών και Δικαιωμάτων πρόσβασης χρηστών (Identity & Access Rights Management - IAM) θα πρέπει να διασυνδέεται και να επικοινωνεί με τα Πληροφοριακά Συστήματα του Οργανισμού(πιο συγκεκριμένα να διατεθούν adapters με τον ActiveDirectory και με μία βάση (Oracle ή MSSQL) του Φορέα),, ώστε να ενημερώνεται σε πραγματικό χρόνο για τα accounts και τα δικαιώματα που διατηρούνται σε κάθε πληροφοριακό σύστημα. Επιπρόσθετα, η λύση IAM θα πρέπει να διασυνδέεται με το πληροφοριακό σύστημα στο οποίο διατηρείται το μητρώο των εργαζομένων και συνεργατών του Οργανισμού, ώστε να ενημερώνεται σε πραγματικό χρόνο για τα φυσικά πρόσωπα που εργάζονται για τον Οργανισμό, την θέση και τον ρόλο τους, καθώς και για οποιαδήποτε σχετική αλλαγή.

Βασική λειτουργικότητα της λύσης IAM θα πρέπει να είναι η αντιστοίχιση κάθε λογαριασμού (Account) σε φυσικό πρόσωπο, ώστε να μην υπάρχουν λογαριασμοί με άγνωστο ιδιοκτήτη, αλλά και ο εντοπισμός οποιουδήποτε λογαριασμού δημιουργείται από ανώνυμο εισβολέα. Με τον τρόπο αυτό, θα πρέπει να εξασφαλίζεται ότι για κάθε λογαριασμό υπάρχει κάποιο φυσικό πρόσωπο που φέρει την ευθύνη του, και ότι για κάθε εξουσιοδοτημένο χρήστη υπάρχει πλήρης εικόνα για τα δικαιώματα πρόσβασης που του έχουν αποδοθεί. Η λύση IAM θα πρέπει να έχει τη δυνατότητα να αυτοματοποιεί τις ροές εργασιών μέσω από τις οποίες δημιουργούνται ή αναιρούνται λογαριασμοί και δικαιώματα πρόσβασης, να αποφεύγονται ανθρώπινα λάθη και παραλείψεις κατά την απόδοση ή αναίρεση λογαριασμών και δικαιωμάτων πρόσβασης.

7.1.6.3.5 Λύση Διαχείρισης Προνομιούχων Λογαριασμών Πρόσβασης

Ορισμένοι χρήστες έχουν πρόσθετα δικαιώματα, λόγω της φύσης του ρόλου που επιτελούν εντός του οργανισμού. Για τον λόγο αυτό, απαιτείται η ύπαρξη επιπλέον μηχανισμών που θα προστατεύουν από μη εξουσιοδοτημένη χρήση των λογαριασμών των εν λόγω χρηστών. Η λύση θα πρέπει να περιλαμβάνει κατ' ελάχιστο:

- Ασφαλή διαχείριση των κωδικών πρόσβασης των διαχειριστών συστημάτων και εφαρμογών, συμπεριλαμβανομένου ασφαλούς αποθετηρίου των κωδικών πρόσβασης.
- Μηχανισμούς επιβολής κανόνων συνθετότητας και αποφυγής ανακύκλωσης των κωδικών πρόσβασης και προσωποποίησης των κοινόχρηστων (Shared) accounts
- Μηχανισμούς λογοδοσίας για τη χρήση των λογαριασμών

- Καταγραφή των ενεργειών των διαχειριστών σε κρίσιμα συστήματα και εφαρμογές

7.1.6.4 Υπηρεσίες νεφοϋπολογιστικών υποδομών και υπηρεσιών

7.1.6.4.1 Υπηρεσίες ανάκαμψης από καταστροφή και λήψης αντιγράφων ασφαλείας

Μεσκοπό την ενίσχυση της επιχειρησιακής συνέχειας, απαιτείται η παροχή υπηρεσιών λήψης Αντιγράφων ασφαλείας (Backup) και ανάκαμψης από καταστροφή (Επαναφοράς (Recovery)). Απαιτείται να λαμβάνονται αντίγραφα ασφαλείας σε υπολογιστικούς πόρους που βρίσκονται εγκατεστημένοι είτε τοπικά (On-premises) είτε στον πάροχο του Νέφους (Cloud). Ως προστατευόμενοι υπολογιστικοί πόροι δύνανται να θεωρηθούν στοιχεία όπως [VMs, DBs, Folders/Files]. Επίσης, θα υπάρχει η δυνατότητα επιλογής επαναφοράς των προστατευμένων υποδομών είτε τοπικά (On-premises) είτε στον πάροχο του Νέφους (Cloud). Θα υπάρχουν επιλογές της υπηρεσίας αυτής με βάση τον όγκο των προστατευόμενων πόρων/δεδομένων ώστε να καλύπτονται διαφορετικού τύπου ανάγκες.

Ο ανάδοχος είναι υπεύθυνος και για την Εγκατάσταση / παραμετροποίηση υπηρεσιών ανάκαμψης από καταστροφή και λήψης αντιγράφων ασφαλείας ανάλογα με τις ανάγκες.

7.1.6.5 Υπηρεσίες SOC & Ddos

Οι υπηρεσίες αφορούν αδιάλειπτης και σε πραγματικό χρόνο (24x7) επιτήρησης των συστημάτων της ΕΔΥΤΕ ΑΕ από εξειδικευμένο και σε διεθνώς αναγνωρισμένο πάροχο για την πρόληψη και αντιμετώπιση κυβερνοαπειλών, καθώς επίσης και ανίχνευσης επιθέσεων DDoS σε πραγματικό χρόνο.

Η πρωτοβουλία στοχεύει στην ενδυνάμωση του επιπέδου ασφάλειας για τις υποδομές της ΕΔΥΤΕ ΑΕ και η πλήρης συμμόρφωση της με τις κανονιστικές απαιτήσεις (όπως ο νόμος ν. 4577/2018 «Ενσωμάτωση στην ελληνική νομοθεσία της Οδηγίας 2016/1148/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση και άλλες διατάξεις», ο Γενικός Κανονισμός Προσωπικών Δεδομένων, κλπ.).

Το έργο θα αντιμετωπίσει τις προκλήσεις που σχετίζονται με α) την πολυπλοκότητα του περιβάλλοντος των υποδομών της ΕΔΥΤΕ ΑΕ και των διαδικασιών παρακολούθησής τους καθώς και β) την έλλειψη εξειδικευμένων σχετικών εργαλείων και τεχνογνωσίας με αποτέλεσμα την περιορισμένη δυνατότητα εντοπισμού και αποτροπής κυβερνοεπιθέσεων οι οποίες αποτελούν μια από τις μεγαλύτερες σύγχρονες απειλές.

Ειδικότερα, μέσω της υπηρεσίας επιτήρησης των συστημάτων της ΕΔΥΤΕ ΑΕ σε πραγματικό χρόνο (24x7) θα διασφαλίζεται ο συνεχής έλεγχος της ασφαλείας των συστημάτων, ο έγκαιρος εντοπισμός επιβεβαιωμένων περιστατικών ασφαλείας καθώς και η λήψη των κατάλληλων ενεργειών πρόληψης και αντιμετώπισης των εν λόγω περιστατικών, από τον ανάδοχο, σε 24ωρη βάση. Ο Ανάδοχος θα έχει τη τεχνική δυνατότητα να εκτελέσει συγκεκριμένες ενέργειες για την αντιμετώπιση/ περιορισμό (containment) περιστατικών Άλλες ενέργειες (όπως για παράδειγμα μία αλλαγή σε ένα firewall κλπ.) θα πρέπει να γίνεται από μηχανικό της ΕΔΥΤΕ ΑΕ με δικαιώματα διαχείρισης (admin rights) πάνω στα συστήματα.

Απώτερος σκοπός του προτεινόμενου έργου είναι η δυνατότητα έγκαιρης προειδοποίησης και απόκρισης έναντι κυβερνοαπειλών, με την αξιοποίηση κατάλληλων τεχνικών μέτρων, ώστε να διασφαλιστούν οι επιχειρησιακές λειτουργίες της ΕΔΥΤΕ ΑΕ και να παραμένουν ασφαλείς μέσω της προληπτικής παρακολούθησης και αντιμετώπισης έναντι των κυβερνοαπειλών.

Οι τεχνικές προδιαγραφές της υπηρεσίας SoCaaS & DDoS παρουσιάζονται αναλυτικά στους πίνακες συμμόρφωσης **Error! Reference source not found.&Error! Reference source not found.** του Παραρτήματος ΙΙ.

Οι υπηρεσίες που θα παρασχεθούν στο πλαίσιο του παρόντος έργου παρουσιάζονται παρακάτω, κατανεμημένες ανά φάση.

7.1.6.5.1 Προπαρασκευαστική Φάση

Στην προπαρασκευαστική φάση του έργου περιλαμβάνονται οι κάτωθι δραστηριότητες:

- Καταγραφή της αρχιτεκτονικής της υποδομής και των πληροφοριακών εργαλείων της ΕΔΥΤΕ ΑΕ .
- Εκτίμηση και αξιολόγηση των αναγκών της ΕΔΥΤΕ ΑΕ .
- Εκτίμηση αναγκών για παρακολούθηση της Υποδομής της ΕΔΥΤΕ ΑΕ , όσο και των Servers και virtual servers
- Προτεραιοποίηση των συστημάτων της ΕΔΥΤΕ ΑΕ προς ένταξη στο πεδίο εφαρμογής του Κέντρου Επιχειρήσεων Ασφαλείας (Security Operations Center – SOC).

7.1.6.5.2 Υλοποίηση Έργου

Κατά τη φάση υλοποίησης του έργου θα πραγματοποιηθούν οι εξής δραστηριότητες:

- Ανάπτυξη Τεκμηρίωσης σχετικά με το SOCaaS: Καταγραφή, σχεδιασμός και τεκμηρίωση, όλων των απαραίτητων πολιτικών, διαδικασιών (συμπεριλαμβανομένων των σχετικών διαδικασιών της ΕΔΥΤΕ ΑΕ), τεχνικών προτύπων κι οδηγιών, για την αξιοποίηση των τεχνικών λύσεων και υπηρεσιών παρακολούθησης ασφάλειας, αναφορικά με τον καθορισμό πλαισίου διαχείρισης και απόκρισης σε συμβάντα κυβερνοεπιθέσεων. Η ενδεικτική τεκμηρίωση περιλαμβάνει: Εγχειρίδια χρήσης των Web Consoles (Web Consoles Manuals), Διαδικασία Κλιμάκωσης Περιστατικών (Incident Escalation Process), Διαδικασία Διαχείρισης Αλλαγών (Change Management Process), Διαδικασία Διαχείρισης Προβλημάτων (Problem Management Process).
- Παραμετροποίηση Υποδομής της ΕΔΥΤΕ ΑΕ για την Ενσωμάτωση συσκευών στο SOCaaS, μέσα από αναλυτικές οδηγίες παραμετροποίησης που θα κατατεθούν από τον Ανάδοχο.
- Οδηγίες Παραμετροποίησης Συστημάτων - Παροχή γραπτών αναλυτικών οδηγιών στην ΕΔΥΤΕ ΑΕ για την ενεργοποίηση/ παραμετροποίηση των μηχανισμών συλλογής logs από τα συστήματά της, καθώς και υποστήριξη της κατά τη διάρκεια της διαδικασίας αυτής.
- Εγκατάσταση μηχανισμών και λογισμικού για τη συλλογή logs από τα συστήματα της ΕΔΥΤΕ ΑΕ εφόσον απαιτείται.
- Ενεργοποίηση της Πλατφόρμας SOCaaS.
- Εγκατάσταση μηχανισμών και λογισμικού για τη διαχείριση των logs από τις συσκευές της ΕΔΥΤΕ ΑΕ .
- Ενεργοποίηση προσβάσεων για το Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο» στις διεπαφές της Πλατφόρμας SOCaaS.
- Καταγραφή των κανόνων διαχείρισης συμβάντων μεταξύ παρόχου και της ΕΔΥΤΕ ΑΕ .

- Καταγραφή των επικοινωνιών, των πληροφοριών και των διαδικασιών διαχείρισης (management), αναφορικά με περιστατικά που προκύπτουν.
- Ενεργοποίηση προϋπάρχοντος περιεχομένου και ανάπτυξη περιεχομένου όπως κανόνες συσχέτισης, αλγόριθμοι και αναφορές, προσαρμοσμένες στα ειδικά χαρακτηριστικά των υποδομών της ΕΔΥΤΕ ΑΕ .
- Χρήση υφιστάμενης τεχνογνωσίας όπως κανόνες συσχέτισης, αλγόριθμοι ανάλυσης δεδομένων και εντοπισμού περιστατικών ασφάλειας και αναφορές, προσαρμοσμένες στα ειδικά χαρακτηριστικά των υποδομών της ΕΔΥΤΕ ΑΕ καθώς και ανάπτυξη νέων καθ' όλη τη διάρκεια της συμβάσης.
- Προσαρμογή των οργανωτικών δομών της ΕΔΥΤΕ ΑΕ (ανάθεση ρόλων, δημιουργία ομάδων εργασίας, δημιουργία νέας δομής, κλπ) για την υποστήριξη των περιγραφόμενων υπηρεσιών.
- Εκπαίδευση του αρμόδιου προσωπικού της ΕΔΥΤΕ ΑΕ πριν την έναρξη της υπηρεσίας παρακολούθησης.
- Ειδικά για το σύστημα ανίχνευσης δικτυακών ανωμαλιών και αντιμετώπισης επιθέσεων άρνησης υπηρεσίας (DDoS - Distributed Denial-of-Service), η προσφερόμενη λύση θα πρέπει να βασίζεται σε εξειδικευμένη συσκευή προστασίας από επιθέσεις τύπου DoS/DDoS η οποία έχει σχεδιαστεί ειδικά για να παρέχει on-premise προστασία της διαθεσιμότητας των δικτυακών πόρων από μια συνεχώς επεκτεινόμενη γκάμα απειλών σε επίπεδο εφαρμογής (application-level), διασφαλίζοντας έτσι την αξιόπιστη πρόσβαση σε δικτυακές υπηρεσίες ζωτικής σημασίας και την επιχειρησιακή συνέχεια της Αναθέτουσας Αρχής. Η συσκευή αυτή θα πρέπει να διαθέτει την κατάλληλη stateless τεχνολογία ανίχνευσης και φιλτραρίσματος, η οποία θα της επιτρέψει να παραμείνει σε λειτουργία κατά την διάρκεια εκδήλωσης επιθέσεων μικρού όγκου (low volume attacks), οι οποίες έχουν σχεδιαστεί με στόχο να θέτουν εκτός λειτουργίας μηχανισμούς όπως τα firewalls και τα IPS.

Η προσφερόμενη λύση θα πρέπει κατ' ελάχιστο να περιλαμβάνει τις παρακάτω λειτουργίες:

- Προστασία από γνωστές και άγνωστες επιθέσεις – Η προσφερόμενη λύση θα πρέπει να ανιχνεύει επιθέσεις τύπου DoS/ DDoS βάση υπογραφών και συμπεριφοράς
- Προστασία από επιθέσεις βασιζόμενες στον δικτυακό όγκο - Η προσφερόμενη λύση θα πρέπει να διαχειρίζεται επιθέσεις τύπου DoS/ DDoS μεγάλου όγκου δικτυακής κίνησης.
- Προστασία από επιθέσεις σε επίπεδο εφαρμογών – Η προσφερόμενη λύση θα πρέπει να προστατεύει εφαρμογές όπως IIS, Apache, κ.λπ. από επιθέσεις τύπου DoS/ DDoS.
- Προστατεύει από επιθέσεις σε επίπεδο πρωτοκόλλου - Η προσφερόμενη λύση θα πρέπει να διαχειρίζεται επιθέσεις τύπου DoS/ DDoS σε πρωτόκολλα όπως HTTP, SMTP κ.λπ.

7.1.6.5.3 Παρακολούθηση (Monitoring)

Η έναρξη παρακολούθησης μέσω του Κέντρου Επιχειρήσεων Ασφαλείας (Security Operations Center – SOC) / SOCaaS οριοθετείται από τη στιγμή της ενσωμάτωσης των πρώτων συστημάτων / υποδομών της ΕΔΥΤΕ ΑΕ ..

Στη φάση αυτή περιλαμβάνονται οι κάτωθι δραστηριότητες:

- Παρακολούθηση 24/7 των υποδομών της ΕΔΥΤΕ ΑΕ
 - ο Το SOCaaS λειτουργεί σε πραγματικό χρόνο, σε συνεχή βάση 24x7 και επιτηρεί (monitor) προληπτικά συστήματα και εφαρμογές προς αναζήτηση ύποπτης δραστηριότητας.



- ο Αποτέλεσμα της παρακολούθησης είναι η επισήμανση περιστατικών προς περαιτέρω ανάλυση, έρευνα ή ανθρώπινη και πλήρως εξειδικευμένη δράση.
- ο Το SOCaaS εντοπίζει τη συνάφεια οποιουδήποτε δοθέντος συμβάντος τοποθετώντας το στο πλαίσιο του ποιος, τι, που, πότε και γιατί συνέβη το συμβάν, προκειμένου να αποκομίσει τον αντίκτυπο του σε όρους επιχειρηματικού κινδύνου. Τα αρχεία καταγραφών (logs) των υποδομών της ΕΔΥΤΕ ΑΕ που συλλέγονται από πολλαπλές πηγές, όπως συστήματα ασφάλειας, συσκευές δικτύου, διακομιστές, εφαρμογές και βάσεις δεδομένων κλπ. αλληλοσυσχετίζονται, καθώς και αναλύονται έναντι δεδομένων threat intelligence, προκειμένου να εντοπιστούν πραγματικά περιστατικά ασφάλειας σε πραγματικό χρόνο.
- Άμεση σε πραγματικό χρόνο απόκριση σε περιστατικά ασφάλειας (incident response). Ανταπόκριση από ομάδα ανταπόκρισης συμβάντων ασφαλείας, συμπεριλαμβανομένης της ανάλυσης και επικύρωσης των ειδοποιήσεων, της ερμηνείας τους σε σημαντικές και εφαρμόσιμες πληροφορίες, κλιμάκωση βάσει αμοιβαία συμφωνημένων κανόνων διαχείρισης συμβάντων και καθοδήγηση καθ' όλη τη διάρκεια του κύκλου ζωής των περιστατικών ασφαλείας μέχρι τον μετριασμό και την αποκατάστασή τους.
- Πραγματοποίηση άμεσης επικοινωνίας με τα εξουσιοδοτημένα φυσικά πρόσωπα 'Single Points of Contact' (SPOC) που θα έχουν οριστεί από την ΕΔΥΤΕ ΑΕ για την ενημέρωση και την αντιμετώπιση κρίσιμων συμβάντων ασφαλείας,
- Ενεργοποίηση και διαρκής ανάπτυξη, ανάπτυξη περιπτώσεων χρήσης 'use cases' και περιεχομένου όπως κανόνες συσχέτισης, αλγόριθμοι και αναφορές, προσαρμοσμένες στα ειδικά χαρακτηριστικά των υποδομών της ΕΔΥΤΕ ΑΕ.
- Αξιοποίηση περιεχομένου όπως κανόνες συσχετισμού, δηλαδή εκτέλεση της βασικής επεξεργασίας συμβάντων με βάση τους πραγματικούς κανόνες και τη συμπεριφορική ανάλυση των δεδομένων που τροφοδοτούν τα σενάρια.
- Συσχέτιση των πληροφοριών ασφαλείας των logs των συστημάτων της ΕΔΥΤΕ ΑΕ τόσο μεταξύ τους όσο και σε σχέση με το εξωτερικό περιβάλλον.
- Δυνατότητα επεκτασιμότητας της παρεχόμενης υπηρεσίας για τη σε βάθος ανάλυση μεγάλων όγκων αρχείων καταγραφής (logs).
- Παραγωγή Αναφορών (Reporting)
- Πλήρης διαφάνεια προς την ΕΔΥΤΕ ΑΕ της λειτουργικότητας της Πλατφόρμας παροχής της SOCaaS υπηρεσίας, μέσω της οποίας παρουσιάζονται στον χρήστη:
 - ο Τα δεδομένα που συλλέγονται, αναλύονται και δρομολογούνται με τη χρήση του αντίστοιχου διαύλου, στην αρχική τους μορφή,
 - ο Οι συσχετισμοί που παράγονται από την παροχή της υπηρεσίας για τον εντοπισμό συμβάντων και ύποπτων δραστηριοτήτων,
 - ο Οι ειδοποιήσεις που δημιουργούνται από την παροχή της υπηρεσίας σε περιπτώσεις πιθανών κακόβουλων δραστηριοτήτων και οι οποίες κατευθύνονται και αναλύονται από το Κέντρο Επιχειρήσεων Ασφαλείας (SOC),
 - ο Τα περιστατικά ασφαλείας/ συμβάντα, τα οποία διαχειρίζονται και αναλύονται από το Κέντρο Επιχειρήσεων Ασφαλείας (SOC),
 - ο Όλα τα περιστατικά που κοινοποιήθηκαν στην ΕΔΥΤΕ ΑΕ διότι κρίθηκε αναγκαία η συμμετοχή του προσωπικού της και αφορούν τα περιστατικά και τους κινδύνους που αξιολογήθηκαν ως σημαντικοί.
 - ο Ενοποιημένη εικόνα όλων των δεδομένων που καταγράφηκαν και αναλύθηκαν από το προσωπικό του Κέντρου Επιχειρήσεων Ασφαλείας (SOC).



- ο πίνακες (dashboards) με την απεικόνιση δεδομένων σχετικών με το SOCaaS,
- ο ειδοποιήσεις (alerts) και τις σχετικές με τις ειδοποιήσεις πληροφορίες που λαμβάνουν οι αναλυτές σε μία ενοποιημένη εικόνα,
- ο καταγραφή των περιστατικών (incidents) και στατιστικά στοιχεία που σχετίζονται με αυτά,
- ο αυτοματοποιημένες μετρήσεις διαθεσιμότητας και αντίστοιχοι δείκτες που σχετίζονται με τα επίπεδα παροχής της υπηρεσίας (KPIs),
- ο δυνατότητα παροχής όλων των συσκευών και των τεχνολογικών στοιχείων που συμμετέχουν στην υπηρεσία, κ.α.
- ο Συστήματος διαχείρισης περιστατικών ασφάλειας για την παρακολούθηση περιστατικών ενώ χρησιμοποιούνται χαρακτηριστικά κλιμάκωσης περιστατικών.
- Εντοπισμός ευπαθειών στις υποδομές της ΕΔΥΤΕ ΑΕ
 - ο Εκτέλεση τακτικών ελέγχων ευπαθειών (Vulnerability Scan) στις υποδομές που έχουν ενσωματωθεί στην υπηρεσία .
 - ο Παροχή πλατφόρμας διαχείρισης ευπαθειών μέσω της οποίας εκτελείται η διαχείριση των ευπαθειών με δυνατότητα πρόσβασης από το προσωπικό της ΕΔΥΤΕ ΑΕ για την ανάθεση ευπαθειών σε προσωπικό της ΕΔΥΤΕ ΑΕ προς διόρθωση, την παροχή πληροφοριών για τις τρέχουσες εκτελούμενες δραστηριότητες διόρθωσης ευπαθειών την παρακολούθηση του κύκλου ζωής των ευπαθειών, καθώς και την παρουσίαση της τρέχουσας κατάστασης της ΕΔΥΤΕ ΑΕ.
- Συνεχής βελτιστοποίηση της υπηρεσίας SOCaaS
 - ο Ανάλυση και βελτιστοποίηση των αρχείων καταγραφής (logs) κατά τη διάρκεια της ημερήσιας λειτουργίας, σύμφωνα με τα περιστατικά που προκύπτουν.
 - ο Διαχείριση Πληροφοριών Ασφαλείας και Γεγονότων και ενημέρωση του προσωπικού της ΕΔΥΤΕ ΑΕ που είναι αρμόδιο να τα χειριστεί.
 - ο Βελτιστοποίηση των κανόνων εφαρμογής και λειτουργίας.
 - ο Αναφορές λειτουργίας κατά την προοδευτική ενσωμάτωση των νέων πληροφοριακών συστημάτων του Δημόσιου Τομέα.
 - ο Καταγραφή των διαδικασιών για την ενημέρωση της εφαρμογής των SOC όταν φιλοξενούνται νέα συστήματα στοRE-Cloud.
- Την παροχή υπηρεσιών ανίχνευσης δικτυακών ανωμαλιών και αντιμετώπισης επιθέσεων άρνησης υπηρεσίας (DDoS - Distributed Denial-of-Service), με βάση δεδομένα ροών (flow-records) από τους υφιστάμενους δρομολογητές IP του δικτύου του Φορέα, με τα ακόλουθα χαρακτηριστικά:
 - ο Δυνατότητα για ανίχνευση επιθέσεων μέσω της ανίχνευσης συγκεκριμένων patterns κίνησης που υποκρύπτουν κακόβουλη ενέργεια (όπως port-scans),
 - ο Δυνατότητα για ανίχνευση επιθέσεων χρησιμοποιώντας "υπογραφές" (fingerprints) οι οποίες θα παρέχονται από τον κατασκευαστή ή από τρίτους,
 - ο Δυνατότητα για ανίχνευση επιθέσεων ανιχνεύοντας ανωμαλίες, δηλαδή τυχόν αποκλίσεις από το σύνηθες προφίλ, στην τρέχουσα κίνηση του δικτύου που μπορεί να υποκρύπτουν επιθέσεις.

7.1.6.6 Εξειδικευμένες λύσεις ασφάλειας

7.1.6.6.1 Λύση Προστασίας Βάσεων Δεδομένων

Οι βάσεις δεδομένων είναι από τα βασικά δομικά συστατικά της υποδομής πληροφοριακών συστημάτων και επομένως η προστασία τους και η παρακολούθησή τους είναι υψίστης σημασίας.

Για την αποτελεσματική προστασία των Βάσεων Δεδομένων απαιτείται η προμήθεια και υλοποίηση μιας ολοκληρωμένης λύσης Database Security η οποία θα ενσωματώνει κατ' ελάχιστον τις ακόλουθες λειτουργίες:

- User Accountability - πλήρης καταγραφή και παρακολούθηση των προσβάσεων και ενεργειών στη Βάση Δεδομένων σε επίπεδο χρήστη
- Detailed DB Auditing (query level) – έλεγχος όλης της δικτυακής κίνησης και των προσβάσεων προς τη Βάση Δεδομένων σε επίπεδο SQL query
- Database Application protection – προστασία σε επίπεδο εφαρμογής Βάσης Δεδομένων

Η προσφερόμενη λύση προστασίας Βάσεων Δεδομένων θα πρέπει να πραγματοποιεί πλήρη καταγραφή και παρακολούθηση σε πραγματικό χρόνο των προσβάσεων σε επίπεδο ερωτημάτων προς την Βάση Δεδομένων (query-level auditing), καθώς και να εφαρμόζει πολιτική ελέγχου πρόσβασης στη Βάση Δεδομένων και στα δεδομένα αυτής, ακόμα και για τους διαχειριστές της Βάσης Δεδομένων. Κάθε αίτηση προς μια προστατευόμενη Βάση Δεδομένων θα πρέπει να αναλύεται εις βάθος προκειμένου να διαπιστωθεί το κατά πόσο είναι ασφαλής και δεν αποτελεί απειλή για την ασφάλεια των εταιρικών δεδομένων.

Ταυτόχρονα θα πρέπει να καταγράφει και να εξετάζει σε πραγματικό χρόνο τις κινήσεις στις Βάσεις Δεδομένων δημιουργώντας έτσι ένα δυναμικό προφίλ βασισμένο στην δομή και τα δυναμικά χαρακτηριστικά της κάθε Βάσης. Το προφίλ που θα δημιουργείται έπειτα από επιβεβαίωση του διαχειριστή θα πρέπει να μπορεί χρησιμοποιείται ως βάση και μέτρο σύγκρισης από τον μηχανισμό ως προς την ανίχνευση και καταστολή επιθέσεων και κάθε είδους μη εξουσιοδοτημένων ενεργειών οι οποίες εκτελούνται στην Βάση Δεδομένων.

Συνοπτικά το σύστημα θα πρέπει να παρέχει τις ακόλουθες λειτουργίες ασφάλειας:

- Λειτουργία ως Database Firewall-Auditing, με στόχο την παρακολούθηση και προστασία συστημάτων βάσεων δεδομένων πολλαπλών κατασκευαστών (όπως MS SQL, Oracle, κτλ.) από επιθέσεις τόσο από εξωτερικούς επιτιθεμένους, όσο και από εσωτερικούς κακόβουλους χρήστες.
- Δυνατότητα παραμετροποίησης και ορισμού πολιτικών ασφαλείας βάσει user names, IP addresses, tables, operations, queries, query patterns, privileged commands και stored procedures.
 - Δυνατότητα δημιουργίας αναφορών (reporting)
 - Παραμετροποίηση αναφορών
 - Κεντρική διαχείριση
- Προώθηση των συμβάντων ασφαλείας σε λύση SIEM

7.1.6.6.2 Πλατφόρμα Κυβερνοασφάλειας – Εκτεταμένης Ανίχνευσης & Απόκρισης (Cyber Security)

Η πλατφόρμα πρέπει να αποτελεί μια ολοκληρωμένη λύση open XDR (Extended Detection & Response) με χαρακτηριστικά και λειτουργίες Next Gen SOC (Security Operation Center), η οποία να εξασφαλίζει την κεντρική παρακολούθηση και διαχείριση, αποφεύγοντας παλαιού τύπου τεχνικές με την εγκατάσταση διαφορετικών ξεχωριστών απλών εργαλείων SIEM (Security Information & Events Management) και άλλων που εγκαθίσταται και διαχειρίζονται ξεχωριστά ή απαιτείται χειροκίνητη ξεχωριστή διαδικασία ενσωμάτωσής του.

Η πλατφόρμα πρέπει να έχει τη δυνατότητα συλλογής και επεξεργασίας από πολλαπλών τύπων πηγές δεδομένων και όχι μόνο αρχείων καταγραφής, κινούμενη στη φιλοσοφία του big data security analytics. Συνδυάζοντας πληροφορίες από δικτυακή κίνηση (network traffic), user data, cloud data, file data στόχος είναι η εξάλειψη πιθανών τυφλών σημείων και ο συσχετισμός όλων των δεδομένων για την παραγωγή καλύτερων αποτελεσμάτων. Μέσα από αυτοματοποιημένες διαδικασίες εμπλουτισμού και συσχετισμών, τα δεδομένα θα βελτιστοποιούνται για αξιοποίηση από μηχανισμούς έρευνας και εντοπισμού. Ειδικότερα με την εκμετάλλευση αυτοματοποιημένης επεξεργασίας και μηχανικής μάθησης, το σύστημα θα πρέπει να μπορεί να λειτουργεί αποτελεσματικά ως ένα ολοκληρωμένο κέντρο αναφοράς και αυτόματης πρότασης και λήψης αντιμέτρων. Το σύστημα θα πρέπει κατ' ελάχιστον να συνοδεύεται από τεχνολογίες SIEM, Sandbox, NTA, Threat Intelligence και IDS και να μην απαιτείται η ξεχωριστή προμήθεια λογισμικού.

Το προσφερόμενο σύστημα θα πρέπει να έχει τη δυνατότητα να υποστηρίζει και το μοντέλο MDR (Managed Detection & Response) και στο σύνολό του θα πρέπει να υποστηρίζει όλο τον κύκλο ζωής αναγνώρισης και αντιμετώπισης απειλών, που αναλύεται στα στάδια:

- Συλλογή (Collect)
- Εντοπισμός (Detect)
- Έρευνα (Investigate)
- Απόκριση (Respond)

Το υπο προμήθεια σύστημα θα πρέπει να περιλαμβάνει την προμήθεια, εγκατάσταση και παραμετροποίηση αισθητήρων ασφαλείας (φυσικών ή εικονικών), οι οποίοι θα εφαρμόζουν λειτουργίες ML-IDS, antivirus, sandboxing και NTA.

Χαρακτηριστικά Next Gen Soc

- Μοντέρνο περιβάλλον χρήσης (GUI) που ενσωματώνει απαραίτητες λειτουργίες παρακολούθησης και διαχείρισης.
- Πρόσβαση με χρήση ρόλων χρηστών (RBAC – Role Based Access) για την διαχείριση δικαιωμάτων (user privilege management)
- Υποστήριξη πολλαπλών ενοίκων (multi-tenant) για την ξεχωριστή διαχείριση οντοτήτων, φυσικών δικτύων κτλ
- Εφαρμογή ξεχωριστού μοντέλου μηχανικής μάθησης ανά tenant για τη βελτίωση ακρίβειας των αποτελεσμάτων και τη μείωση των εσφαλμένων θετικών συμβάντων (false positives), εφαρμόζοντας ξεχωριστά συμπεριφορικά μοντέλα.
- Εξελεξιμένες δυνατότητες μηχανικής μάθησης που να συμπεριλαμβάνουν τόσο supervised όσο και unsupervised διαδικασίες, τεχνολογίες graph ML και να συνδυάζονται μεταξύ τους για την παραγωγή βέλτιστων αποτελεσμάτων
- Δυνατότητες ενσωμάτωσης με εργαλεία και τεχνολογίες ασφαλείας Firewalls, WAF, SWG, EDR, SOAR κτλ
- Υποστήριξη API για ενσωμάτωση με τεχνολογίες HoneyPots, εργαλεία OSINT κτλ.
- Μία ενοποιημένη, υψηλής απόδοσης, αποθήκη δεδομένων ("Big Data" High Speed Lake)
- Δυνατότητα εγκατάστασης τόσο σε φυσικό εξοπλισμό, όσο και σε εικονικό ή περιβάλλον cloud
- Κατανεμημένη και επεκτάσιμη αρχιτεκτονική που να υποστηρίζει ωστόσο και "All In One" σενάρια.
- Υψηλή διαθεσιμότητας με τη χρήση clusters και ευέλικτη τήρηση και αποθήκευση δεδομένων.
- Μηχανισμοί Συλλογής που να μπορούν να εγκατασταθούν τόσο σε φυσικό όσο και σε εικονικό περιβάλλον

- Το σύστημα θα πρέπει να ακολουθεί ανοιχτή αρχιτεκτονική που να επιτρέπει την εισαγωγή δεδομένων από οποιαδήποτε συσκευή με τη χρήση Integration APIS.
- Κεντροποιημένη διαχείριση
- Απλό ενοποιημένο μοντέλο αδειών χωρίς επιπλέον κόστη

Next-Generation SIEM

Η πλατφόρμα θα πρέπει να βασίζεται σε μια ενοποιημένη αποθήκη δεδομένων βασισμένη στην αρχιτεκτονική του big data lake. Τα δεδομένα θα πρέπει κατ' ελάχιστον να μπορούν να εισαχθούν μέσω syslog. Όπου είναι εφικτό θα πρέπει να παρέχεται η δυνατότητα χρήσης parsers για κυριότερες και δημοφιλέστερες λύσεις δικτύων και ασφαλείας ώστε οι πληροφορίες να κανονικοποιούνται και να συσχετίζονται με αυτοματοποιημένο τρόπο. Θα πρέπει να παρέχονται οι παρακάτω ελάχιστες λειτουργικότητες:

- Απλός όσο και εξεζητημένος μηχανισμός αναζήτησης που να βασίζεται σε λογικούς τελεστές (Boolean modifiers)
- Οι αναζητήσεις να μπορούν να εφαρμοστούν ως μόνιμα φίλτρα σε όλο το περιβάλλον για ταχύτερη διερεύνηση και ανάλυση περιστατικών.
- Υψηλής απόδοσης και άμεσες ανταποκρίσεις στην αναζήτηση και το φιλτράρισμα στο big data
- Πρόσβαση σε πηγές δεδομένων και όχι μόνο σε syslog δεδομένα
- Συλλογή δεδομένων από δικτυακή κίνηση (μέσω TAP ή Mirror Traffic). Τα πακέτα θα πρέπει να γίνονται reduce, να κανονικοποιούνται και να μετατρέπονται σε αξιοποιήσιμα μετα-δεδομένα για την ενσωμάτωση στο big data lake.
- Συλλογή δεδομένων από user sources όπως το Microsoft AD μέσω API Connector
- Συλλογή δεδομένων από πηγές νέφους (cloud) Office365 μέσω Connectors
- Τα δεδομένα από πηγές πρέπει να κανονικοποιούνται, να εμπλουτίζονται και να συσχετίζονται αυτόματα από το σύστημα
- Πηγές εμπλουτισμού πρέπει να περιλαμβάνονται γεωγραφικού προσδιορισμού (Geo-Awareness), IP Reputation, Threat Intelligence και DPI Application awareness.
- Μοντέρνο περιβάλλον χρήστη με λειτουργίες SIEM που περιλαμβάνουν ερωτήματα και δημιουργίες κανόνων.
- Πρόσθετο για παραδοσιακή απεικόνιση SIEM (π.χ. Kibana)

Εντοπισμός KillChain (KillChain Detections)

(συμπεριλαμβάνοντας IDS/Exploit, Malware και APT Sandboxing, Anti-Phishing κτλ.)

- Το σύστημα πρέπει να έχει ενσωματωμένους μηχανισμούς εντοπισμών σε κάθε φάση του CyberSecurity KillChain, συμπεριλαμβάνοντας Reconnaissance, Delivery, Exploitation, Installation, Command & Control, and Actions & Exfiltrations
- Το σύστημα πρέπει να περιλαμβάνει ενσωματωμένη βάση υπογραφών IDS, ενισχυμένη από ανάλυση μηχανικής μάθησης (ML-IDS)
- Η πλατφόρμα πρέπει να υποστηρίζει πολλαπλά Threat Intelligence Feeds, συμπεριλαμβάνοντας εμπορικές πηγές, open-source, anti-phishing κ.α.
- Η πλατφόρμα πρέπει να επιτρέπει ενσωμάτωση με 3rd party feeds μέσω STIX/TAXII και/η MISP

- Η πλατφόρμα πρέπει να έχει ενσωματωμένες δυνατότητες APT Sandboxing για να αναγνωρίζει και να περιορίζει άγνωστα αρχεία, και για εντοπισμό ransomware, spyware.

Ανάλυση Δικτύου (Network Traffic Analysis)

Με την επιθεώρηση δικτυακής κίνησης σε πραγματικό χρόνο, η πλατφόρμα πρέπει να μπορεί να μοντελοποιήσει την κίνηση για αναγνώριση παράτυπων συμπεριφορών και ειδοποιήσεων.

- Η πλατφόρμα πρέπει να ενσωματώνει λειτουργικότητα Deep Packet Inspection (DPI) για την αναγνώριση τουλάχιστον 4000 εφαρμογών και να δομεί σχετικά συμπεριφορικά μοντέλα.
- Τα δεδομένα κίνησης δικτύου πρέπει να μετασχηματίζονται σε κατάλληλα μετα-δεδομένα που περιλαμβάνουν και το payload, για την αντίστοιχη προαιρετική μείωση ανάγκης αποθηκευτικών χώρων.
- Η πλατφόρμα πρέπει να ενσωματώνει λειτουργικότητα NTA Detections, συμπεριλαμβάνοντας Application Usage Anomalies, Long App Session Anomalies, και Unapproved Asset Activity
- Το σύστημα θα πρέπει να εντοπίζει ανωμαλίες στη συμπεριφορά των Firewalls, denial anomalies ή rule usage anomalies

User Behavior Analytics (UBA)

Σε συνδυασμό με την ανάλυση πακέτων, το σύστημα θα πρέπει να μπορεί να συνδεθεί με πηγές δεδομένων χρηστών, το MS Active Directory

- Το σύστημα πρέπει να πραγματοποιεί ανάλυση και εντοπισμό ανωμαλιών στη συμπεριφορά του χρήστη (user behavior)
- Το σύστημα πρέπει να ενσωματώνει μοντέλα εντοπισμού ανωμαλιών αδύνατου ταξιδιού (Impossible Travel Anomaly) ή ώρες αυθεντικοποίησης (Log In Time Anomaly)
- Εντοπισμούς NTA, έτσι κι εδώ όλα τα detections και τα σχετικά events στα logs και σε πηγές πρέπει να συσχετίζονται αυτόματα.

Endpoint Behavior Analytics (EBA)

Με τα αναλυτικά δεδομένα δικτύου και χρηστών, το σύστημα πρέπει να μπορεί να συλλέγει δεδομένα από assets/endpoints στο περιβάλλον, να εκτελεί analytics και να εντοπίζει συμπεριφορικές ανωμαλίες.

- Το σύστημα θα πρέπει να μπορεί να εισάγει δεδομένα από τρίτα συστήματα εντοπισμού ευπαθειών (vulnerability scanners) Nessus, Tenable, Rapid7 και να συσχετίζει τα ευρήματα με σχετικά γεγονότα ασφαλείας.
- Το σύστημα θα πρέπει να μπορεί να ανακαλύψει όλα τα assets σε ένα περιβάλλον και να τα κατηγοριοποιεί με βάση τη διεύθυνση MAC και IP.
- Η λίστα των ανακαλυφθέντων/εντοπισθέντων assets θα πρέπει να μπορεί να επαυξάνεται και να παραμετροποιείται με τη χρήση αρχείων csv με λίστες assets και περιγραφές.
- Το σύστημα πρέπει να μπορεί να καταγράφει όλους συσχετισμούς με ένα asset με IP διευθύνσεις, ιστορικά στοιχεία για τη χρήση εφαρμογών κτλ.

Ορατότητα Δικτύου και Υπηρεσιών (Network & Service Visibility)

Το σύστημα θα πρέπει να περιλαμβάνει δυνατά εργαλεία απεικόνισης δικτύων και υπηρεσιών, μαζί με analytics, με στόχο να προσφέρει ορατότητα επιδόσεις δικτύου (network performance), application usage κτλ.

Κυνήγι Απειλών και Διερεύνηση (Threat Hunting & Investigation)

Με πηγές δεδομένων στο unified data lake, τα κανονικοποιημένα και συσχετισμένα δεδομένα πρέπει να είναι διαθέσιμα για διερεύνηση και threat hunting οποιαδήποτε στιγμή.

- Το σύστημα πρέπει να έχει ενσωματωμένα σχετικά εργαλεία, προκαθορισμένες αναζητήσεις και ερωτήματα, και οπτικοποιήσεις (visualizations).
- Τα visualizations πρέπει να είναι παραμετροποιήσιμα
- Το σύστημα πρέπει να προσφέρει εξελιγμένες δυνατότητες συσχετισμένες αναζητήσεις, που επιτρέπουν αναλυτές να συνδέσουν πολλαπλά ανεξάρτητα ερωτήματα με κοινά κριτήρια προκειμένου να δομήσουν πληροφορίες από attack sequences ή να απομονώσουν κοινές πληροφορίες.
- Όλα τα ερωτήματα θα πρέπει να μπορούν να αποθηκευθούν, επεξεργαστούν, κλωνοποιηθούν κτλ από χρήστες.
- Τα visualizations πρέπει να μπορούν να αποθηκευθούν σαν custom dashboards.
- Τα ερωτήματα θα πρέπει να μπορούν να συνδυαστούν με ενέργειες/αποκρίσεις για PlayBooks

Playbooks / Integrated Orchestration & Response (SOAR)

- Το σύστημα πρέπει να συμπεριλαμβάνει μια βιβλιοθήκη με έτοιμα ενσωματωμένα playbooks, που είναι αυτό-εκτελέσιμα ερωτήματα με ενσωματωμένες ενέργειες.
- Οι ενσωματωμένες ενέργειες/αποκρίσεις θα πρέπει να συμπεριλαμβάνουν
 - ο Alerts – Αποστολή e-mail/slack message κτλ
 - ο Actions – Άνοιγμα case, εκτέλεση μισαντολής API, δημιουργία security event κτλ
 - ο Responses – Μπλοκάρισμα μιας IP στο Firewall, απενεργοποίηση χρήστη στο AD, εκτέλεση δέσμης ενεργειών κτλ
- Παράλληλα με αυτοματοποιημένες ενέργειες, εξωτερικές ενέργειες το μπλοκάρισμα μια IP ή χρήστη θα πρέπει να είναι διαθέσιμες στο χρήστη μέσω του UI ώστε να μπορούν παράλληλα να υλοποιηθούν ως μέρος διερεύνησης/αντιμετώπισης ή ανάλυσης.
- Δυνατότητα ενσωμάτωσης με ήδη έτοιμα εμπορικά εργαλεία SOAR

Επιπλέον Δυνατότητες

Ειδοποιήσεις (Alarming)

- Το σύστημα θα πρέπει να προσφέρει έναν έξυπνο, μοντέρνο και παραμετροποιήσιμο μηχανισμό ειδοποιήσεων που να δύναται να οριστεί με βάση παραλήπτες και άλλα κριτήρια (score severity, killchain category, etc.)
- Οι ειδοποιήσεις πρέπει να μπορούν να αποσταλούν με email ή slack μηνύματα και τα μηνύματα πρέπει να είναι παραμετροποιήσιμα ως το περιεχόμενο και τα σχετικά δεδομένα.

Αναφορές (Reporting)

- Το σύστημα πρέπει να περιέχει ένα σύγχρονο εξελιγμένο μηχανισμό αναφορών που θα επιτρέπει παράλληλα εύκολη δημιουργία νέων αναφορών με drag and drop και αποθήκευσή για χρήση σε οποιοδήποτε σημείο.
- Οι αναφορές θα πρέπει να παράγονται με χρονοπρογραμματισμό και να αποστέλλονται σε διαφορετικούς χρήστες.
- Οι αναφορές πρέπει να είναι δυνατόν να αποστέλλονται με email σαν pdf ή csv ή να γράφονται σε αρχείο.
- Το σύστημα θα πρέπει να περιλαμβάνει πληθώρα έτοιμων αναφορών και templates.

Portal

- Πρόσβαση των χρηστών βάση ρόλου (User RBAC access) στο Portal με συνολική ή περιορισμένη πρόσβαση πληροφορίες.
- Custom Dashboards ανάρολοχρήστη.
- Χρονοπρογραμματισμένες αναφορές για κάθε tenant, tenant group και RBAC users.
- Η πρόσβαση των χρηστών πρέπει να μπορεί να περιορίζεται σε Read-Only, limited view, μέχρι full visibility and access.

7.1.7 Φάσεις - παραδοτέα

7.1.7.1 Χρονοδιάγραμμαυλοποίησης εκτελεστικών συμβάσεων

Σε κάθε εκτελεστική σύμβαση θα πρέπει να υπάρχουν αναλυτικές προβλέψεις για το χρονοδιάγραμμα υλοποίησής τους, οι οποίες θα περιλαμβάνουν:

- Τον συνολικό χρόνο υλοποίησης κάθε εκτελεστικής σύμβασης
- Τις επιμέρους φάσεις και τη διάρκειά τους
- Ελληλεξαρτήσεις μεταξύ των φάσεων

Ο συνολικός χρόνος υλοποίησης καθώς και οι επιμέρους φάσεις θα εξαρτηθούν από το είδος και τη διαστασιολόγηση εξοπλισμού, λογισμικού και υπηρεσιών που θα περιληφθούν σε κάθε εκτελεστική σύμβαση, τις εκάστοτε ανάγκες του φορέα που θα αφορούν οι λύσεις, καθώς και τους περιορισμούς του κεφαλαίου 1.3.3 της διακήρυξης.

Επιπλέον, ο Ανάδοχος θα υποβάλει το αργότερο έναν (1) μήνα μετά την υπογραφή κάθε εκτελεστικής σύμβασης κάθε τμήματος της συμφωνίας-πλαίσιο,

7.1.7.2 Παραδοτέα ανά λύση

7.1.7.2.1 Τμήμα 1

Στον παρακάτω πίνακα παρουσιάζονται τα παραδοτέα για κάθε λύση που περιλαμβάνεται στο τμήμα 1. Σημειώνεται ότι ανάλογα με το περιεχόμενο κάθε εκτελεστικής σύμβασης τα παραδοτέα είναι δυνατό, με τη σύμφωνη γνώμη της Αναθέτουσας Αρχής και του εκάστοτε φορέα, να συγχωνεύονται (για παράδειγμα εκπόνηση μίας μελέτης εφαρμογής για περισσότερες της μίας λύσεις λογισμικού).

Κατηγορία	Παραδοτέα	Περιεχόμενο παραδοτέων
Ransomware Assessment Readiness	Π1.1.1 Μεθοδολογία αξιολόγησης ετοιμότητας	Αναλυτική μεθοδολογία αξιολόγησης, συμπεριλαμβανομένων των κριτηρίων.
	Π1.1.2 Αρχική αξιολόγηση ετοιμότητας	Αποτελέσματα αρχικής αξιολόγησης ετοιμότητας, πριν την υλοποίηση παρεμβάσεων.
	Π1.1.3 Τελική αξιολόγηση ετοιμότητας	Αποτελέσματα τελικής αξιολόγησης ετοιμότητας, μετά την υλοποίηση παρεμβάσεων.

Κατηγορία	Παραδοτέα	Περιεχόμενο παραδοτέων
Εκπόνηση Μελέτης Ανάλυσης και Αξιολόγησης Κινδύνων	Π1.2.1 Μελέτη Ανάλυσης και Αξιολόγησης Κινδύνων	Σύμφωνα με το κεφάλαιο 7.1.3.2.2 του Παραρτήματος Ι
Διενέργεια δράσεων ενημέρωσης για τη μεταφορά τεχνογνωσίας και την διαμόρφωση κουλτούρας ενεργούς ευαισθητοποίησης για τους κινδύνους κυβερνοασφάλειας	Π1.3.1 Μεθοδολογία εκπαίδευσης	Σύμφωνα με το σημείο Ι του κεφαλαίου 7.1.3.2.3 του Παραρτήματος Ι
	Π1.3.2 Εκπαιδευτικό υλικό	Σύμφωνα με το σημείο Ι του κεφαλαίου 7.1.3.2.3 του Παραρτήματος Ι
	Π1.3.3 Ψηφιακή πλατφόρμα ασύγχρονης εκπαίδευσης	Σύμφωνα με το σημείο ΙΙ του κεφαλαίου 7.1.3.2.3 του Παραρτήματος Ι
	Π1.3.4 Δημιουργία εξειδικευμένου οδηγού Επικοινωνιακής Διαχείρισης Κρίσεων στον Κυβερνοχώρο	Σύμφωνα με κεφάλαιο 7.1.3.2.3 του Παραρτήματος Ι
Διαμόρφωση πλάνου ανάκαμψης από καταστροφές για κρίσιμες οντότητες	Π1.4.1 Πλάνο ανάκαμψης από καταστροφή	Σύμφωνα με το κεφάλαιο 7.1.3.2.4 του Παραρτήματος Ι
Εκπόνηση Μελέτης εξωτερικού και εσωτερικού περιβάλλοντος και την ανάδειξη βέλτιστων πρακτικών	Π1.5.1 Μελέτη εξωτερικού και εσωτερικού περιβάλλοντος και την ανάδειξη βέλτιστων πρακτικών	Σύμφωνα με το κεφάλαιο 7.1.3.2.5 του Παραρτήματος Ι
Διενέργεια ελέγχων διείσδυσης εξωτερικών δικτύων, εφαρμογών Ιστού, φυσικής ασφάλειας και διαρροής δεδομένων για τον εντοπισμό των ευπαθειών σε υποδομές, συσκευές και διακομιστές που είναι προσβάσιμοι από το διαδίκτυο	Π1.6.1 Αναφορά ελέγχων διείσδυσης εξωτερικών δικτύων	Αναλυτική περιγραφή της μεθοδολογίας διεξαγωγής και των ευρημάτων των ελέγχων, καθώς και συστάσεις για την αντιμετώπιση ενδεχόμενων ευπαθειών.
	Π1.6.2 Αναφορά ελέγχων διείσδυσης εφαρμογών Ιστού	Αναλυτική περιγραφή της μεθοδολογίας διεξαγωγής και των ευρημάτων των ελέγχων, καθώς και συστάσεις για την αντιμετώπιση ενδεχόμενων ευπαθειών.
	Π1.6.3 Αναφορά ελέγχων φυσικής ασφάλειας	Αναλυτική περιγραφή της μεθοδολογίας διεξαγωγής και των ευρημάτων των ελέγχων, καθώς και συστάσεις για την

Κατηγορία	Παραδοτέα	Περιεχόμενο παραδοτέων
		αντιμετώπιση ενδεχόμενων ευπαθειών.
	Π1.6.4 Αναφορά ελέγχων διαρροής δεδομένων	Αναλυτική περιγραφή της μεθοδολογίας διεξαγωγής και των ευρημάτων των ελέγχων, καθώς και συστάσεις για την αντιμετώπιση ενδεχόμενων ευπαθειών.
Αξιοποίηση τεχνολογικής καινοτομίας και ερευνητικής πρωτοπορίας	Π1.7.1 Εξαμηνιαίες αναφορές τεχνολογικής καινοτομίας και ερευνητικής πρωτοπορίας	Παρουσίαση των καινοτομιών και ερευνητικών ευρημάτων στον τομέα της κυβερνοασφάλειας και προτάσεις για την αξιοποίησή τους.
Παροχή υπηρεσιών ανάκαμψης από καταστροφή & λήψης αντιγράφων ασφαλείας (disaster recovery as a service & data backup as a service)	Π1.8.1 Αναφορά υπηρεσιών ανάκαμψης από καταστροφή & λήψης αντιγράφων ασφαλείας	Αναλυτική αναφορά της παροχής υπηρεσιών συμπεριλαμβανομένου του πλήθους αντιγράφων ασφαλείας, του χρόνου που ελήφθησαν, καθώς και των τεχνικών τους χαρακτηριστικών.
Υπηρεσίες εγκατάστασης/παραμετροποίησης υπηρεσιών ανάκαμψης από καταστροφή & λήψης αντιγράφων ασφαλείας (disaster recovery as a service & data backup as a service)	Π1.9.1 Αναφορά εγκατάστασης / παραμετροποίησης υπηρεσιών ανάκαμψης από καταστροφή & λήψης αντιγράφων ασφαλείας	Αναλυτική αναφορά εγκατάστασης και παραμετροποίησης με τεκμηρίωση των παραμέτρων που ορίστηκαν και των σχετικών τιμών και ρυθμίσεων.
Backup σε tape 1.960PB χωρητικότητα	Π1.10.1 Εξοπλισμός και λογισμικό διαχείρισης	Σύμφωνα με το κεφάλαιο 7.1.3.5.1 του Παραρτήματος Ι και τον πίνακα συμμόρφωσης 7.2.1.4
	Π1.10.2 Τεκμηρίωση εξοπλισμού και λογισμικού διαχείρισης	Εγχειρίδια χρήσης και διαχείρισης εξοπλισμού και λογισμικού διαχείρισης
Backup σε disk για το 50% της χωρητικότητας (800 TB ωφέλιμης χωρητικότητας)	Π1.10.1 Εξοπλισμός και λογισμικό διαχείρισης	Σύμφωνα με το κεφάλαιο 7.1.3.5.2 του Παραρτήματος Ι και τον πίνακα συμμόρφωσης 7.2.1.5
	Π1.10.2 Τεκμηρίωση εξοπλισμού και λογισμικού διαχείρισης	Εγχειρίδια χρήσης και διαχείρισης εξοπλισμού και λογισμικού διαχείρισης
MailSecurity (αφορά 20000 σταθμούς εργασίας)	Π1.11.1 Μελέτη εφαρμογής	Μελέτη υλοποίησης του λογισμικού, η οποία θα περιλαμβάνει κατ' ελάχιστο αρχιτεκτονική, ανάλυση ενδεχόμενων μηχανισμών

Κατηγορία	Παραδοτέα	Περιεχόμενο παραδοτέων
		διαλειτουργικότητας και προβλέψεις για την ασφάλεια και την προστασία προσωπικών δεδομένων.
	Π1.11.2 Τεχνική και λειτουργική τεκμηρίωση	Εγχειρίδια χρήσης και διαχείρισης λογισμικού
Endpoint Security User level (αφορά 20000 σταθμούς εργασίας)	Π1.12.1 Μελέτη εφαρμογής	Μελέτη υλοποίησης του λογισμικού, η οποία θα περιλαμβάνει κατ' ελάχιστο αρχιτεκτονική, ανάλυση ενδεχόμενων μηχανισμών διαλειτουργικότητας και προβλέψεις για την ασφάλεια και την προστασία προσωπικών δεδομένων.
	Π1.12.2 Τεχνική και λειτουργική τεκμηρίωση	Εγχειρίδια χρήσης και διαχείρισης λογισμικού
Managed services security endpoint & mail (αφορά 20000 σταθμούς εργασίας)	Π1.13.1 Μηνιαίες αναφορές υπηρεσιών	Αναφορά παρακολούθησης με περαιτέρω ανάλυση για τα περιστατικά που εντοπίστηκαν και τις συμβουλές για τη διερεύνηση και αντιμετώπισή τους.
Λύση που αφορά τον έλεγχο της πρόσβασης των εσωτερικών χρηστών στο Διαδίκτυο	Π1.14.1α Μελέτη εφαρμογής (εάν προσφερθεί λογισμικό)	Μελέτη υλοποίησης του λογισμικού, η οποία θα περιλαμβάνει κατ' ελάχιστο αρχιτεκτονική, ανάλυση ενδεχόμενων μηχανισμών διαλειτουργικότητας και προβλέψεις για την ασφάλεια και την προστασία προσωπικών δεδομένων.
	Π1.14.2α Τεχνική και λειτουργική τεκμηρίωση (εάν προσφερθεί λογισμικό)	Εγχειρίδια χρήσης και διαχείρισης λογισμικού
	Π1.14.1β Εξοπλισμός και λογισμικό διαχείρισης (εάν προσφερθεί εξοπλισμός)	Σύμφωνα με τον πίνακα συμμόρφωσης 7.2.1.8

Κατηγορία	Παραδοτέα	Περιεχόμενο παραδοτέων
	Π1.14.2β Τεκμηρίωση και εξοπλισμού λογισμικού διαχείρισης (εάν προσφερθεί εξοπλισμός)	Εγχειρίδια χρήσης και διαχείρισης εξοπλισμού και λογισμικού διαχείρισης
Λύση Ασφαλείας και προστασίας των χρηστών από απειλές του διαδικτύου (WebSecurityGateway)	Π1.15.1 Μελέτη εφαρμογής	Μελέτη υλοποίησης του λογισμικού, η οποία θα περιλαμβάνει κατ' ελάχιστο αρχιτεκτονική, ανάλυση ενδεχόμενων μηχανισμών διαλειτουργικότητας και προβλέψεις για την ασφάλεια και την προστασία προσωπικών δεδομένων.
	Π1.15.2 Τεχνική και λειτουργική τεκμηρίωση	Εγχειρίδια χρήσης και διαχείρισης λογισμικού
	Π1.15.3 Εξοπλισμός και λογισμικό διαχείρισης	Σύμφωνα με τον πίνακα συμμόρφωσης 7.2.1.9
	Π1.15.4 Τεκμηρίωση και εξοπλισμού λογισμικού διαχείρισης	Εγχειρίδια χρήσης και διαχείρισης εξοπλισμού και λογισμικού διαχείρισης
Μηχανισμός ελέγχου πρόσβασης χρηστών πολλαπλών παραγόντων (Multi Factor Authentication MFA)	Π1.16.1 Μελέτη εφαρμογής	Μελέτη υλοποίησης του λογισμικού, η οποία θα περιλαμβάνει κατ' ελάχιστο αρχιτεκτονική, ανάλυση ενδεχόμενων μηχανισμών διαλειτουργικότητας και προβλέψεις για την ασφάλεια και την προστασία προσωπικών δεδομένων.
	Π1.16.2 Τεχνική και λειτουργική τεκμηρίωση	Εγχειρίδια χρήσης και διαχείρισης λογισμικού

7.1.7.2.1 Τμήμα 2

Στον παρακάτω πίνακα παρουσιάζονται τα παραδοτέα για κάθε λύση που περιλαμβάνεται στο τμήμα 2. Σημειώνεται ότι ανάλογα με το περιεχόμενο κάθε εκτελεστικής σύμβασης τα παραδοτέα είναι δυνατό, με τη σύμφωνη γνώμη της Αναθέτουσας Αρχής και του εκάστοτε φορέα, να συγχωνεύονται (για παράδειγμα εκπόνηση μίας μελέτης εφαρμογής για περισσότερες της μίας λύσεις λογισμικού).

Κατηγορία	Παραδοτέα	Περιεχόμενο παραδοτέων
Διαμόρφωση πολιτικών ασφάλειας κρίσιμων οντοτήτων με στόχο την ανάδειξη τεχνικών και οργανωτικών μέτρων για την προστασία τους από Κυβερνοαπειλές	Π2.1.1 Πολιτικές ασφάλειας κρίσιμων οντοτήτων	Σύμφωνα με το κεφάλαιο 7.1.4.2.6 του Παραρτήματος Ι
Διαμόρφωση πολιτικών ορθής χρήσης Πληροφοριακών συστημάτων και εφαρμογών	Π2.2.1 Πολιτικές ορθής χρήσης Πληροφοριακών συστημάτων και εφαρμογών	Σύμφωνα με το κεφάλαιο 7.1.4.2.1 του Παραρτήματος Ι
Διενέργεια δράσεων ενημέρωσης για τη μεταφορά τεχνογνωσίας και την διαμόρφωση κουλτούρας ενεργούς ευαισθητοποίησης για τους κινδύνους κυβερνοασφάλειας	Π2.3.1 Μεθοδολογία εκπαίδευσης	Σύμφωνα με τοσημείοΙ του κεφαλαίου 7.1.4.2.2 του Παραρτήματος Ι
	Π2.3.2 Εκπαιδευτικό υλικό	Σύμφωνα με τοσημείοΙ του κεφαλαίου 7.1.4.2.2 του Παραρτήματος Ι
	Π2.3.3 Ψηφιακή πλατφόρμα ασύγχρονης εκπαίδευσης	Σύμφωνα με τοσημείοII του κεφαλαίου 7.1.4.2.2 του Παραρτήματος Ι
	Π1.3.4 Δημιουργία εξειδικευμένου οδηγού Επικοινωνιακής Διαχείρισης Κρίσεων στον Κυβερνοχώρο	Σύμφωνα με κεφάλαιο 7.1.3.2.3 του Παραρτήματος Ι
Διαμόρφωση πλάνου ανάκαμψης από καταστροφές για κρίσιμες οντότητες	Π2.4.1 Πλάνο ανάκαμψης παό καταστροφή	Σύμφωνα με το κεφάλαιο 7.1.4.2.3 του Παραρτήματος Ι
Εκπόνηση Μελέτης εξωτερικού και εσωτερικού περιβάλλοντος και την ανάδειξη βέλτιστων πρακτικών	Π2.5.1 Μελέτη εξωτερικού και εσωτερικού περιβάλλοντος και την ανάδειξη βέλτιστων πρακτικών	Σύμφωνα με το κεφάλαιο 7.1.4.2.4 του Παραρτήματος Ι
Διαμόρφωση πολιτικής αντιγράφων ασφαλείας, που θα περιγράφει σκοπό, πεδίο εφαρμογής, ρόλους και ευθύνες	Π2.6.1 Πολιτικές αντιγράφων ασφαλείας	Σύμφωνα με το κεφάλαιο 7.1.4.2.5 του Παραρτήματος Ι
Διαμόρφωση Συστήματος Διαχείρισης της Ασφάλειας των Πληροφοριών (ΣΔΑΠ) με βάση το πρότυπο ISO 27001 &	Π2.7.1 Σύστημα Διαχείρισης της Ασφάλειας των Πληροφοριών (ΣΔΑΠ)	Σύμφωνα με το κεφάλαιο 7.1.4.2.6 του Παραρτήματος Ι

Κατηγορία	Παραδοτέα	Περιεχόμενο παραδοτέων
Εκπόνηση Μελέτης Ανάλυσης και Αξιολόγησης Κινδύνων	Π2.7.2 Μελέτη Ανάλυσης και Αξιολόγησης Κινδύνων	Σύμφωνα με το κεφάλαιο 7.1.4.2.6 του Παραρτήματος Ι
Διενέργεια ελέγχων δεισδυσσης εξωτερικών δικτύων, εφαρμογών Ιστού, φυσικής ασφάλειας και διαρροής δεδομένων για τον εντοπισμό των ευπαθειών σε υποδομές, συσκευές και διακομιστές που είναι προσβάσιμοι από το διαδίκτυο	Π2.8.1 Αναφορά ελέγχων δεισδυσσης εξωτερικών δικτύων	Αναλυτική περιγραφή της μεθοδολογίας διεξαγωγής και των ευρημάτων των ελέγχων, καθώς και συστάσεις για την αντιμετώπιση ενδεχόμενων ευπαθειών.
	Π2.8.2 Αναφορά ελέγχων δεισδυσσης εφαρμογών ιστού	Αναλυτική περιγραφή της μεθοδολογίας διεξαγωγής και των ευρημάτων των ελέγχων, καθώς και συστάσεις για την αντιμετώπιση ενδεχόμενων ευπαθειών.
	Π2.8.3 Αναφορά ελέγχων φυσικής ασφάλειας	Αναλυτική περιγραφή της μεθοδολογίας διεξαγωγής και των ευρημάτων των ελέγχων, καθώς και συστάσεις για την αντιμετώπιση ενδεχόμενων ευπαθειών.
	Π2.8.4 Αναφορά ελέγχων διαρροής δεδομένων	Αναλυτική περιγραφή της μεθοδολογίας διεξαγωγής και των ευρημάτων των ελέγχων, καθώς και συστάσεις για την αντιμετώπιση ενδεχόμενων ευπαθειών.
Αξιοποίηση τεχνολογικής καινοτομίας και ερευνητικής πρωτοπορίας	Π2.9.1 Εξαμηνιαίες αναφορές τεχνολογικής καινοτομίας και ερευνητικής πρωτοπορίας	Παρουσίαση των καινοτομιών και ερευνητικών ευρημάτων στον τομέα της κυβερνοασφάλειας και προτάσεις για την αξιοποίησή τους.
Λύση Ddos	Π2.10.1 Εξοπλισμός και λογισμικό διαχείρισης	Σύμφωνα με τον πίνακα συμμόρφωσης 7.2.2.8
	Π2.10.2 Τεκμηρίωση εξοπλισμού και λογισμικού διαχείρισης	Εγχειρίδια χρήσης και διαχείρισης εξοπλισμού και λογισμικού διαχείρισης
Παροχή υπηρεσιών ανάκαμψης από καταστροφή & λήψης αντιγράφων ασφαλείας (disaster recovery as a service & data backup as as service)	Π2.11.1 Αναφορά υπηρεσιών ανάκαμψης από καταστροφή & λήψης αντιγράφων ασφαλείας	Αναλυτική αναφορά της παροχής υπηρεσιών συμπεριλαμβανομένου του πλήθους αντιγράφων ασφαλείας, του χρόνου που ελήφθησαν, καθώς και των τεχνικών τους χαρακτηριστικών.

Κατηγορία	Παραδοτέα	Περιεχόμενο παραδοτέων
Υπηρεσίες εγκατάστασης/παραμετροποίησης υπηρεσιών ανάκαμψης από καταστροφή & λήψης αντιγράφων ασφαλείας (disasterrecoveryasaservice&databackupasasservice)	Π2.12.1 Αναφορά εγκατάστασης / παραμετροποίησης υπηρεσιών ανάκαμψης από καταστροφή & λήψης αντιγράφων ασφαλείας	Αναλυτική αναφορά εγκατάστασης και παραμετροποίησης με τεκμηρίωση των παραμέτρων που ορίστηκαν και των σχετικών τιμών και ρυθμίσεων.
NGFW για το DataCenter, για την πρόσβαση των εσωτερικών χρηστών στο Διαδίκτυο και την ανάλυση των επικοινωνιών τους και για την απομακρυσμένη πρόσβαση. Άδειες για προστασία IPS, antimalware, ApplicationControl. Διαχειριστικό εργαλείο για τα firewall	Π2.13.1 Εξοπλισμός και λογισμικό διαχείρισης	Σύμφωνα με τον πίνακα συμμόρφωσης 7.2.2.9
	Π2.13.2 Τεκμηρίωση εξοπλισμού και λογισμικού διαχείρισης	Εγχειρίδια χρήσης και διαχείρισης εξοπλισμού και λογισμικού διαχείρισης
Switches για τη διασύνδεση των firewalls	Π2.14.1 Εξοπλισμός και λογισμικό διαχείρισης	Σύμφωνα με τον πίνακα συμμόρφωσης 7.2.2.10
	Π2.14.2 Τεκμηρίωση εξοπλισμού και λογισμικού διαχείρισης	Εγχειρίδια χρήσης και διαχείρισης εξοπλισμού και λογισμικού διαχείρισης
Virtual firewall Για 10 tenants με High availability και άδειες IPS και antimalware	Π2.15.1 Μελέτη εφαρμογής	Μελέτη υλοποίησης του λογισμικού, η οποία θα περιλαμβάνει κατ' ελάχιστο αρχιτεκτονική, ανάλυση ενδεχόμενων μηχανισμών διαλειτουργικότητας και προβλέψεις για την ασφάλεια και την προστασία προσωπικών δεδομένων.
	Π2.15.2 Τεχνική και λειτουργική τεκμηρίωση	Εγχειρίδια χρήσης και διαχείρισης λογισμικού
Λύση Microsegmentation	Π2.16.1 Μελέτη εφαρμογής	Μελέτη υλοποίησης του λογισμικού, η οποία θα περιλαμβάνει κατ' ελάχιστο αρχιτεκτονική, ανάλυση ενδεχόμενων μηχανισμών διαλειτουργικότητας και προβλέψεις για την ασφάλεια και την προστασία προσωπικών δεδομένων.
	Π2.16.2 Τεχνική και λειτουργική τεκμηρίωση	Εγχειρίδια χρήσης και διαχείρισης λογισμικού



Κατηγορία	Παραδοτέα	Περιεχόμενο παραδοτέων
Λύση Ασφαλείας και προστασίας των χρηστών από απειλές του διαδικτύου (WebSecurityGateway) - 250 χρήστες και Συσκευές υλικού (HWappliances)	Π2.17.1 Εξοπλισμός και λογισμικό διαχείρισης	Σύμφωνα με τον πίνακα συμμόρφωσης 7.2.2.13
	Π2.17.2 Τεκμηρίωση εξοπλισμού και λογισμικού διαχείρισης	Εγχειρίδια χρήσης και διαχείρισης εξοπλισμού και λογισμικού διαχείρισης
Λύση Αυστηρής πιστοποίησης για την απομακρυσμένη πρόσβαση (MFA, ZeroTrust)	Π2.18.1 Μελέτη εφαρμογής	Μελέτη υλοποίησης του λογισμικού, η οποία θα περιλαμβάνει κατ' ελάχιστο αρχιτεκτονική, ανάλυση ενδεχόμενων μηχανισμών διαλειτουργικότητας και προβλέψεις για την ασφάλεια και την προστασία προσωπικών δεδομένων.
	Π2.18.2 Τεχνική και λειτουργική τεκμηρίωση	Εγχειρίδια χρήσης και διαχείρισης λογισμικού
Λύση CloudProxy προστασίας απομακρυσμένων χρηστών	Π2.19.1 Μελέτη εφαρμογής	Μελέτη υλοποίησης του λογισμικού, η οποία θα περιλαμβάνει κατ' ελάχιστο αρχιτεκτονική, ανάλυση ενδεχόμενων μηχανισμών διαλειτουργικότητας και προβλέψεις για την ασφάλεια και την προστασία προσωπικών δεδομένων.
	Π2.19.2 Τεχνική και λειτουργική τεκμηρίωση	Εγχειρίδια χρήσης και διαχείρισης λογισμικού
ΛύσηAntimalwareαπομακρυσμένων χρηστών (AV,EDR, XDR)	Π2.20.1 Μελέτη εφαρμογής	Μελέτη υλοποίησης του λογισμικού, η οποία θα περιλαμβάνει κατ' ελάχιστο αρχιτεκτονική, ανάλυση ενδεχόμενων μηχανισμών διαλειτουργικότητας και προβλέψεις για την ασφάλεια και την προστασία προσωπικών δεδομένων.
	Π2.20.2 Τεχνική και λειτουργική τεκμηρίωση	Εγχειρίδια χρήσης και διαχείρισης λογισμικού
Λύση εκπαίδευσης για 250 χρήστες σε phishingcampaigns και cyberattacks	Π2.21.1 Μελέτη εφαρμογής	Μελέτη υλοποίησης του λογισμικού, η οποία θα περιλαμβάνει κατ' ελάχιστο αρχιτεκτονική, ανάλυση ενδεχόμενων μηχανισμών

Κατηγορία	Παραδοτέα	Περιεχόμενο παραδοτέων
		διαλειτουργικότητας και προβλέψεις για την ασφάλεια και την προστασία προσωπικών δεδομένων.
	Π2.21.2 Τεχνική και λειτουργική τεκμηρίωση	Εγχειρίδια χρήσης και διαχείρισης λογισμικού
Λύση Ασφαλούς Προσβασης χρηστών στο εταιρικό δίκτυο	Π2.22.1 Μελέτη εφαρμογής	Μελέτη υλοποίησης του λογισμικού, η οποία θα περιλαμβάνει κατ' ελάχιστο αρχιτεκτονική, ανάλυση ενδεχόμενων μηχανισμών διαλειτουργικότητας και προβλέψεις για την ασφάλεια και την προστασία προσωπικών δεδομένων.
	Π2.22.2 Τεχνική και λειτουργική τεκμηρίωση	Εγχειρίδια χρήσης και διαχείρισης λογισμικού
Λύση Πλατφόρμας Ενορχήστρωσης Ασφαλείας, Αυτοματοποίησης	Π2.23.1 Μελέτη εφαρμογής	Μελέτη υλοποίησης του λογισμικού, η οποία θα περιλαμβάνει κατ' ελάχιστο αρχιτεκτονική, ανάλυση ενδεχόμενων μηχανισμών διαλειτουργικότητας και προβλέψεις για την ασφάλεια και την προστασία προσωπικών δεδομένων.
	Π2.23.2 Τεχνική και λειτουργική τεκμηρίωση	Εγχειρίδια χρήσης και διαχείρισης λογισμικού
Πλατφόρμα Κυβερνοασφάλειας – Εκτεταμένης Ανίχνευσης & Απόκρισης (CyberSecurity)	Π2.24.1 Μελέτη εφαρμογής	Μελέτη υλοποίησης του λογισμικού, η οποία θα περιλαμβάνει κατ' ελάχιστο αρχιτεκτονική, ανάλυση ενδεχόμενων μηχανισμών διαλειτουργικότητας και προβλέψεις για την ασφάλεια και την προστασία προσωπικών δεδομένων.
	Π2.24.2 Τεχνική και λειτουργική τεκμηρίωση	Εγχειρίδια χρήσης και διαχείρισης λογισμικού
Λύση Προστασίας Βάσεων Δεδομένων	Π2.25.1 Μελέτη εφαρμογής	Μελέτη υλοποίησης του λογισμικού, η οποία θα περιλαμβάνει κατ' ελάχιστο αρχιτεκτονική, ανάλυση ενδεχόμενων μηχανισμών

Κατηγορία	Παραδοτέα	Περιεχόμενο παραδοτέων
		διαλειτουργικότητας και προβλέψεις για την ασφάλεια και την προστασία προσωπικών δεδομένων.
	Π2.25.2 Τεχνική και λειτουργική τεκμηρίωση	Εγχειρίδια χρήσης και διαχείρισης λογισμικού
Λογισμικό κυβερνοασφάλειας ΑΙ, συμπεριλαμβανομένης εγκατάστασης, εκπαίδευσης και υποστήριξης 24/7. 1000 Άδειες	Π2.26.1 Μελέτη εφαρμογής	Μελέτη υλοποίησης του λογισμικού, η οποία θα περιλαμβάνει κατ' ελάχιστο αρχιτεκτονική, ανάλυση ενδεχόμενων μηχανισμών διαλειτουργικότητας και προβλέψεις για την ασφάλεια και την προστασία προσωπικών δεδομένων.
	Π2.26.2 Τεχνική και λειτουργική τεκμηρίωση	Εγχειρίδια χρήσης και διαχείρισης λογισμικού
	Π2.26.3 Εκπαιδευτικό υλικό	Υλικό για την εκπαίδευση των χρηστών.
Λύση Διαβάθμισης και Σήμανσης Εγγράφων	Π2.27.1 Μελέτη εφαρμογής	Μελέτη υλοποίησης του λογισμικού, η οποία θα περιλαμβάνει κατ' ελάχιστο αρχιτεκτονική, ανάλυση ενδεχόμενων μηχανισμών διαλειτουργικότητας και προβλέψεις για την ασφάλεια και την προστασία προσωπικών δεδομένων.
	Π2.27.2 Τεχνική και λειτουργική τεκμηρίωση	Εγχειρίδια χρήσης και διαχείρισης λογισμικού
Λύση Προστασίας Δεδομένων από Διάρροή	Π2.28.1 Μελέτη εφαρμογής	Μελέτη υλοποίησης του λογισμικού, η οποία θα περιλαμβάνει κατ' ελάχιστο αρχιτεκτονική, ανάλυση ενδεχόμενων μηχανισμών διαλειτουργικότητας και προβλέψεις για την ασφάλεια και την προστασία προσωπικών δεδομένων.
	Π2.28.2 Τεχνική και λειτουργική τεκμηρίωση	Εγχειρίδια χρήσης και διαχείρισης λογισμικού
Λύση Διαχείρισης Δικαιωμάτων Εγγράφων	Π2.29.1 Μελέτη εφαρμογής	Μελέτη υλοποίησης του λογισμικού, η οποία θα

Κατηγορία	Παραδοτέα	Περιεχόμενο παραδοτέων
		περιλαμβάνει κατ' ελάχιστο αρχιτεκτονική, ανάλυση ενδεχόμενων μηχανισμών διαλειτουργικότητας και προβλέψεις για την ασφάλεια και την προστασία προσωπικών δεδομένων.
	Π2.29.2 Τεχνική και λειτουργική τεκμηρίωση	Εγχειρίδια χρήσης και διαχείρισης λογισμικού
Λύση Διαχείρισης Λογαριασμών και Δικαιωμάτων Πρόσβασης Χρηστών	Π2.30.1 Μελέτη εφαρμογής	Μελέτη υλοποίησης του λογισμικού, η οποία θα περιλαμβάνει κατ' ελάχιστο αρχιτεκτονική, ανάλυση ενδεχόμενων μηχανισμών διαλειτουργικότητας και προβλέψεις για την ασφάλεια και την προστασία προσωπικών δεδομένων.
	Π2.30.2 Τεχνική και λειτουργική τεκμηρίωση	Εγχειρίδια χρήσης και διαχείρισης λογισμικού
Λύση Διαχείρισης Προνομιούχων Λογαριασμών Πρόσβασης	Π2.31.1 Μελέτη εφαρμογής	Μελέτη υλοποίησης του λογισμικού, η οποία θα περιλαμβάνει κατ' ελάχιστο αρχιτεκτονική, ανάλυση ενδεχόμενων μηχανισμών διαλειτουργικότητας και προβλέψεις για την ασφάλεια και την προστασία προσωπικών δεδομένων.
	Π2.31.2 Τεχνική και λειτουργική τεκμηρίωση	Εγχειρίδια χρήσης και διαχείρισης λογισμικού
Λύση μηχανισμών ισχυρής ταυτοποίησης	Π2.32.1 Μελέτη εφαρμογής	Μελέτη υλοποίησης του λογισμικού, η οποία θα περιλαμβάνει κατ' ελάχιστο αρχιτεκτονική, ανάλυση ενδεχόμενων μηχανισμών διαλειτουργικότητας και προβλέψεις για την ασφάλεια και την προστασία προσωπικών δεδομένων.
	Π2.32.2 Τεχνική και λειτουργική τεκμηρίωση	Εγχειρίδια χρήσης και διαχείρισης λογισμικού

7.1.7.2.1 Τμήμα 3

Στον παρακάτω πίνακα παρουσιάζονται τα παραδοτέα για κάθε λύση που περιλαμβάνεται στο τμήμα 3. Σημειώνεται ότι ανάλογα με το περιεχόμενο κάθε εκτελεστικής σύμβασης τα παραδοτέα είναι δυνατό, με τη σύμφωνη γνώμη της Αναθέτουσας Αρχής και του εκάστοτε φορέα, να συγχωνεύονται (για παράδειγμα εκπόνηση μίας μελέτης εφαρμογής για περισσότερες της μίας λύσεις λογισμικού).

Κατηγορία	Παραδοτέα	Περιεχόμενο παραδοτέων
Διαμόρφωση πολιτικών ασφαλείας κρίσιμων οντοτήτων με στόχο την ανάδειξη τεχνικών και οργανωτικών μέτρων για την προστασία τους από Κυβερνοαπειλές	Π3.1.1 Πολιτικές ασφαλείας κρίσιμων οντοτήτων	Σύμφωνα με το κεφάλαιο 7.1.5.2.6 του Παραρτήματος Ι
Διαμόρφωση πολιτικών ορθής χρήσης Πληροφοριακών συστημάτων και εφαρμογών	Π3.2.1 Πολιτικές ορθής χρήσης Πληροφοριακών συστημάτων και εφαρμογών	Σύμφωνα με το κεφάλαιο 7.1.5.2.1 του Παραρτήματος Ι
Διενέργεια δράσεων ενημέρωσης για τη μεταφορά τεχνογνωσίας και την διαμόρφωση κουλτούρας ενεργούς ευαισθητοποίησης για τους κινδύνους κυβερνοασφάλειας	Π3.3.1 Μεθοδολογία εκπαίδευσης	Σύμφωνα με τοσημείοI του κεφαλαίου 7.1.5.2.2 του Παραρτήματος Ι
	Π3.3.2 Εκπαιδευτικό υλικό	Σύμφωνα με τοσημείοI του κεφαλαίου 7.1.5.2.2 του Παραρτήματος Ι
	Π3.3.3 Ψηφιακή πλατφόρμα ασύγχρονης εκπαίδευσης	Σύμφωνα με τοσημείοII του κεφαλαίου 7.1.5.2.2 του Παραρτήματος Ι
	Π1.3.4 Δημιουργία εξειδικευμένου οδηγού Επικοινωνιακής Διαχείρισης Κρίσεων στον Κυβερνοχώρο	Σύμφωνα με κεφάλαιο 7.1.3.2.3 του Παραρτήματος Ι
Διαμόρφωση πλάνου ανάκαμψης από καταστροφές για κρίσιμες οντότητες	Π3.4.1 Πλάνο ανάκαμψης παό καταστροφή	Σύμφωνα με το κεφάλαιο 7.1.5.2.3 του Παραρτήματος Ι
Εκπόνηση Μελέτης εξωτερικού και εσωτερικού περιβάλλοντος και την ανάδειξη βέλτιστων πρακτικών	Π3.5.1 Μελέτη εξωτερικού και εσωτερικού περιβάλλοντος και την ανάδειξη βέλτιστων πρακτικών	Σύμφωνα με το κεφάλαιο 7.1.5.2.4 του Παραρτήματος Ι
Διαμόρφωση πολιτικής αντιγράφων ασφαλείας, που θα περιγράφει σκοπό, πεδίο εφαρμογής, ρόλους και ευθύνες	Π3.6.1 Πολιτικές αντιγράφων ασφαλείας	Σύμφωνα με το κεφάλαιο 7.1.5.2.5 του Παραρτήματος Ι

Κατηγορία	Παραδοτέα	Περιεχόμενο παραδοτέων
Διαμόρφωση Συστήματος Διαχείρισης της Ασφάλειας των Πληροφοριών (ΣΔΑΠ) με βάση το πρότυπο ISO 27001 & Εκπόνηση Μελέτης Ανάλυσης και Αξιολόγησης Κινδύνων	Π3.7.1 Σύστημα Διαχείρισης της Ασφάλειας των Πληροφοριών (ΣΔΑΠ)	Σύμφωνα με το κεφάλαιο 7.1.5.2.6 του Παραρτήματος Ι
	Π3.7.2 Μελέτη Ανάλυσης και Αξιολόγησης Κινδύνων	Σύμφωνα με το κεφάλαιο 7.1.5.2.6 του Παραρτήματος Ι
Διενέργεια ελέγχων διείσδυσης εξωτερικών δικτύων, εφαρμογών Ιστού, φυσικής ασφάλειας και διαρροής δεδομένων για τον εντοπισμό των ευπαθειών σε υποδομές, συσκευές και διακομιστές που είναι προσβάσιμοι από το διαδίκτυο	Π3.8.1 Αναφορά ελέγχων διείσδυσης εξωτερικών δικτύων	Αναλυτική περιγραφή της μεθοδολογίας διεξαγωγής και των ευρημάτων των ελέγχων, καθώς και συστάσεις για την αντιμετώπιση ενδεχόμενων ευπαθειών.
	Π3.8.2 Αναφορά ελέγχων διείσδυσης εφαρμογών ιστού	Αναλυτική περιγραφή της μεθοδολογίας διεξαγωγής και των ευρημάτων των ελέγχων, καθώς και συστάσεις για την αντιμετώπιση ενδεχόμενων ευπαθειών.
	Π3.8.3 Αναφορά ελέγχων φυσικής ασφάλειας	Αναλυτική περιγραφή της μεθοδολογίας διεξαγωγής και των ευρημάτων των ελέγχων, καθώς και συστάσεις για την αντιμετώπιση ενδεχόμενων ευπαθειών.
	Π3.8.4 Αναφορά ελέγχων διαρροής δεδομένων	Αναλυτική περιγραφή της μεθοδολογίας διεξαγωγής και των ευρημάτων των ελέγχων, καθώς και συστάσεις για την αντιμετώπιση ενδεχόμενων ευπαθειών.
Αξιοποίηση τεχνολογικής καινοτομίας και ερευνητικής πρωτοπορίας	Π3.9.1 Εξαμηνιαίες αναφορές τεχνολογικής καινοτομίας και ερευνητικής πρωτοπορίας	Παρουσίαση των καινοτομιών και ερευνητικών ευρημάτων στον τομέα της κυβερνοασφάλειας και προτάσεις για την αξιοποίησή τους.
Υπηρεσίες SOC	Π3.10.1 Μελέτη εφαρμογής υπηρεσιών SOC	Σύμφωνα με το κεφάλαιο 7.1.5.5.1 του Παραρτήματος Ι
	Π3.10.2 Τεκμηρίωση SOCaaS	Σύμφωνα με το κεφάλαιο 7.1.5.5.2 του Παραρτήματος Ι
	Π3.10.3 Αναφορές SOCaaS	Σύμφωνα με το κεφάλαιο 7.1.5.5.3 του Παραρτήματος Ι

Κατηγορία	Παραδοτέα	Περιεχόμενο παραδοτέων
Λύση Ddos	Π3.10.1 Εξοπλισμός και λογισμικό διαχείρισης	Σύμφωνα με τον πίνακα συμμόρφωσης 7.2.3.2
	Π3.10.2 Τεκμηρίωση εξοπλισμού και λογισμικού διαχείρισης	Εγχειρίδια χρήσης και διαχείρισης εξοπλισμού και λογισμικού διαχείρισης
Παροχή υπηρεσιών ανάκαμψης από καταστροφή & λήψης αντιγράφων ασφαλείας (disaster recovery as a service & data backup as a service)	Π3.11.1 Αναφορά υπηρεσιών ανάκαμψης από καταστροφή & λήψης αντιγράφων ασφαλείας	Αναλυτική αναφορά της παροχής υπηρεσιών συμπεριλαμβανομένου του πλήθους αντιγράφων ασφαλείας, του χρόνου που ελήφθησαν, καθώς και των τεχνικών τους χαρακτηριστικών.
Υπηρεσίες εγκατάστασης/παραμετροποίησης υπηρεσιών ανάκαμψης από καταστροφή & λήψης αντιγράφων ασφαλείας (disaster recovery as a service & data backup as a service)	Π3.12.1 Αναφορά εγκατάστασης / παραμετροποίησης υπηρεσιών ανάκαμψης από καταστροφή & λήψης αντιγράφων ασφαλείας	Αναλυτική αναφορά εγκατάστασης και παραμετροποίησης με τεκμηρίωση των παραμέτρων που ορίστηκαν και των σχετικών τιμών και ρυθμίσεων.
Λύση Προστασίας Βάσεων Δεδομένων	Π3.13.1 Μελέτη εφαρμογής	Μελέτη υλοποίησης του λογισμικού, η οποία θα περιλαμβάνει κατ' ελάχιστο αρχιτεκτονική, ανάλυση ενδεχόμενων μηχανισμών διαλειτουργικότητας και προβλέψεις για την ασφάλεια και την προστασία προσωπικών δεδομένων.
	Π3.13.2 Τεχνική και λειτουργική τεκμηρίωση	Εγχειρίδια χρήσης και διαχείρισης λογισμικού
Πλατφόρμα Κυβερνοασφάλειας – Εκτεταμένης Ανίχνευσης & Απόκρισης (CyberSecurity)	Π3.14.1 Μελέτη εφαρμογής	Μελέτη υλοποίησης του λογισμικού, η οποία θα περιλαμβάνει κατ' ελάχιστο αρχιτεκτονική, ανάλυση ενδεχόμενων μηχανισμών διαλειτουργικότητας και προβλέψεις για την ασφάλεια και την προστασία προσωπικών δεδομένων.
	Π3.14.2 Τεχνική και λειτουργική τεκμηρίωση	Εγχειρίδια χρήσης και διαχείρισης λογισμικού
MailSecurity (αφορά 3.000 σταθμούς εργασίας)	Π3.15.1 Μελέτη εφαρμογής	Μελέτη υλοποίησης του λογισμικού, η οποία θα περιλαμβάνει κατ' ελάχιστο

Κατηγορία	Παραδοτέα	Περιεχόμενο παραδοτέων
		αρχιτεκτονική, ανάλυση ενδεχόμενων μηχανισμών διαλειτουργικότητας και προβλέψεις για την ασφάλεια και την προστασία προσωπικών δεδομένων.
	Π3.15.2 Τεχνική και λειτουργική τεκμηρίωση	Εγχειρίδια χρήσης και διαχείρισης λογισμικού
Endpoint Security User level (αφορά 3.000 σταθμούς εργασίας)	Π3.16.1 Μελέτη εφαρμογής	Μελέτη υλοποίησης του λογισμικού, η οποία θα περιλαμβάνει κατ' ελάχιστο αρχιτεκτονική, ανάλυση ενδεχόμενων μηχανισμών διαλειτουργικότητας και προβλέψεις για την ασφάλεια και την προστασία προσωπικών δεδομένων.
	Π3.16.2 Τεχνική και λειτουργική τεκμηρίωση	Εγχειρίδια χρήσης και διαχείρισης λογισμικού
Managed services security endpoint & mail (αφορά 3.000 σταθμούς εργασίας)	Π3.17.1 Μηνιαίες αναφορές υπηρεσιών	Αναφορά παρακολούθησης με περαιτέρω ανάλυση για τα περιστατικά που εντοπίστηκαν και τις συμβουλές για τη διερεύνηση και αντιμετώπισή τους.
Λύση Διαβάθμισης και Σήμανσης Εγγράφων	Π3.18.1 Μελέτη εφαρμογής	Μελέτη υλοποίησης του λογισμικού, η οποία θα περιλαμβάνει κατ' ελάχιστο αρχιτεκτονική, ανάλυση ενδεχόμενων μηχανισμών διαλειτουργικότητας και προβλέψεις για την ασφάλεια και την προστασία προσωπικών δεδομένων.
	Π3.18.2 Τεχνική και λειτουργική τεκμηρίωση	Εγχειρίδια χρήσης και διαχείρισης λογισμικού
Λύση Προστασίας Δεδομένων από Διαρροή	Π3.20.1 Μελέτη εφαρμογής	Μελέτη υλοποίησης του λογισμικού, η οποία θα περιλαμβάνει κατ' ελάχιστο

Κατηγορία	Παραδοτέα	Περιεχόμενο παραδοτέων
		αρχιτεκτονική, ανάλυση ενδεχόμενων μηχανισμών διαλειτουργικότητας και προβλέψεις για την ασφάλεια και την προστασία προσωπικών δεδομένων.
	Π3.19.2 Τεχνική και λειτουργική τεκμηρίωση	Εγχειρίδια χρήσης και διαχείρισης λογισμικού
Λύση Διαχείρισης Δικαιωμάτων Εγγράφων	Π3.20.1 Μελέτη εφαρμογής	Μελέτη υλοποίησης του λογισμικού, η οποία θα περιλαμβάνει κατ' ελάχιστο αρχιτεκτονική, ανάλυση ενδεχόμενων μηχανισμών διαλειτουργικότητας και προβλέψεις για την ασφάλεια και την προστασία προσωπικών δεδομένων.
	Π3.20.2 Τεχνική και λειτουργική τεκμηρίωση	Εγχειρίδια χρήσης και διαχείρισης λογισμικού
Λύση Διαχείρισης Λογαριασμών και Δικαιωμάτων Πρόσβασης Χρηστών	Π3.21.1 Μελέτη εφαρμογής	Μελέτη υλοποίησης του λογισμικού, η οποία θα περιλαμβάνει κατ' ελάχιστο αρχιτεκτονική, ανάλυση ενδεχόμενων μηχανισμών διαλειτουργικότητας και προβλέψεις για την ασφάλεια και την προστασία προσωπικών δεδομένων.
	Π3.21.2 Τεχνική και λειτουργική τεκμηρίωση	Εγχειρίδια χρήσης και διαχείρισης λογισμικού
Λύση Διαχείρισης Προνομιούχων Λογαριασμών Πρόσβασης	Π3.22.1 Μελέτη εφαρμογής	Μελέτη υλοποίησης του λογισμικού, η οποία θα περιλαμβάνει κατ' ελάχιστο αρχιτεκτονική, ανάλυση ενδεχόμενων μηχανισμών διαλειτουργικότητας και προβλέψεις για την ασφάλεια και την προστασία προσωπικών δεδομένων.
	Π3.22.2 Τεχνική και λειτουργική τεκμηρίωση	Εγχειρίδια χρήσης και διαχείρισης λογισμικού

7.1.7.2.1 Τμήμα 4

Στον παρακάτω πίνακα παρουσιάζονται τα παραδοτέα για κάθε λύση που περιλαμβάνεται στο τμήμα 4. Σημειώνεται ότι ανάλογα με το περιεχόμενο κάθε εκτελεστικής σύμβασης τα παραδοτέα είναι δυνατό, με τη σύμφωνη γνώμη της Αναθέτουσας Αρχής και του εκάστοτε φορέα, να συγχωνεύονται (για παράδειγμα εκπόνηση μίας μελέτης εφαρμογής για περισσότερες της μίας λύσεις λογισμικού).

Κατηγορία	Παραδοτέα	Περιεχόμενο παραδοτέων
Διαμόρφωση πολιτικών ασφαλείας κρίσιμων οντοτήτων με στόχο την ανάδειξη τεχνικών και οργανωτικών μέτρων για την προστασία τους από Κυβερνοαπειλές	Π4.1.1 Πολιτικές ασφαλείας κρίσιμων οντοτήτων	Σύμφωνα με το κεφάλαιο 7.1.6.2.6 του Παραρτήματος Ι
Διαμόρφωση πολιτικών ορθής χρήσης Πληροφοριακών συστημάτων και εφαρμογών	Π4.2.1 Πολιτικές ορθής χρήσης Πληροφοριακών συστημάτων και εφαρμογών	Σύμφωνα με το κεφάλαιο 7.1.6.2.1 του Παραρτήματος Ι
Διενέργεια δράσεων ενημέρωσης για τη μεταφορά τεχνογνωσίας και την διαμόρφωση κουλτούρας ενεργούς ευαισθητοποίησης για τους κινδύνους κυβερνοασφάλειας	Π4.3.1 Μεθοδολογία εκπαίδευσης	Σύμφωνα με τοσημείοI του κεφαλαίου 7.1.6.2.2 του Παραρτήματος Ι
	Π4.3.2 Εκπαιδευτικό υλικό	Σύμφωνα με τοσημείοI του κεφαλαίου 7.1.6.2.2 του Παραρτήματος Ι
	Π4.3.3 Ψηφιακή πλατφόρμα ασύγχρονης εκπαίδευσης	Σύμφωνα με τοσημείοII του κεφαλαίου 7.1.6.2.2 του Παραρτήματος Ι
	Π1.3.4 Δημιουργία εξειδικευμένου οδηγού Επικοινωνιακής Διαχείρισης Κρίσεων στον Κυβερνοχώρο	Σύμφωνα με κεφάλαιο 7.1.3.2.3 του Παραρτήματος Ι
Διαμόρφωση πλάνου ανάκαμψης από καταστροφές για κρίσιμες οντότητες	Π4.4.1 Πλάνο ανάκαμψης παό καταστροφή	Σύμφωνα με το κεφάλαιο 7.1.6.2.3 του Παραρτήματος Ι
Εκπόνηση Μελέτης εξωτερικού και εσωτερικού περιβάλλοντος και την ανάδειξη βέλτιστων πρακτικών	Π4.5.1 Μελέτη εξωτερικού και εσωτερικού περιβάλλοντος και την ανάδειξη βέλτιστων πρακτικών	Σύμφωνα με το κεφάλαιο 7.1.6.2.4 του Παραρτήματος Ι
Διαμόρφωση πολιτικής αντιγράφων ασφαλείας, που θα περιγράφει σκοπό, πεδίο εφαρμογής, ρόλους και ευθύνες	Π4.6.1 Πολιτικές αντιγράφων ασφαλείας	Σύμφωνα με το κεφάλαιο 7.1.6.2.5 του Παραρτήματος Ι

Κατηγορία	Παραδοτέα	Περιεχόμενο παραδοτέων
Διαμόρφωση Συστήματος Διαχείρισης της Ασφάλειας των Πληροφοριών (ΣΔΑΠ) με βάση το πρότυπο ISO 27001 & Εκπόνηση Μελέτης Ανάλυσης και Αξιολόγησης Κινδύνων	Π4.7.1 Σύστημα Διαχείρισης της Ασφάλειας των Πληροφοριών (ΣΔΑΠ)	Σύμφωνα με το κεφάλαιο 7.1.6.2.6 του Παραρτήματος Ι
	Π4.7.2 Μελέτη Ανάλυσης και Αξιολόγησης Κινδύνων	Σύμφωνα με το κεφάλαιο 7.1.6.2.6 του Παραρτήματος Ι
Διενέργεια ελέγχων διείσδυσης εξωτερικών δικτύων, εφαρμογών Ιστού, φυσικής ασφάλειας και διαρροής δεδομένων για τον εντοπισμό των ευπαθειών σε υποδομές, συσκευές και διακομιστές που είναι προσβάσιμοι από το διαδίκτυο	Π4.8.1 Αναφορά ελέγχων διείσδυσης εξωτερικών δικτύων	Αναλυτική περιγραφή της μεθοδολογίας διεξαγωγής και των ευρημάτων των ελέγχων, καθώς και συστάσεις για την αντιμετώπιση ενδεχόμενων ευπαθειών.
	Π4.8.2 Αναφορά ελέγχων διείσδυσης εφαρμογών ιστού	Αναλυτική περιγραφή της μεθοδολογίας διεξαγωγής και των ευρημάτων των ελέγχων, καθώς και συστάσεις για την αντιμετώπιση ενδεχόμενων ευπαθειών.
	Π4.8.3 Αναφορά ελέγχων φυσικής ασφάλειας	Αναλυτική περιγραφή της μεθοδολογίας διεξαγωγής και των ευρημάτων των ελέγχων, καθώς και συστάσεις για την αντιμετώπιση ενδεχόμενων ευπαθειών.
	Π4.8.4 Αναφορά ελέγχων διαρροής δεδομένων	Αναλυτική περιγραφή της μεθοδολογίας διεξαγωγής και των ευρημάτων των ελέγχων, καθώς και συστάσεις για την αντιμετώπιση ενδεχόμενων ευπαθειών.
Αξιοποίηση τεχνολογικής καινοτομίας και ερευνητικής πρωτοπορίας	Π4.9.1 Εξαμηνιαίες αναφορές τεχνολογικής καινοτομίας και ερευνητικής πρωτοπορίας	Παρουσίαση των καινοτομιών και ερευνητικών ευρημάτων στον τομέα της κυβερνοασφάλειας και προτάσεις για την αξιοποίησή τους.
Παροχή υπηρεσίαςSOC	Π4.10.1 Μελέτη εφαρμογής υπηρεσιών SOC	Σύμφωνα με το κεφάλαιο 7.1.6.5.1 του Παραρτήματος Ι
	Π4.10.2Τεκμηρίωση SOCaaS	Σύμφωνα με το κεφάλαιο 7.1.6.5.2 του Παραρτήματος Ι
	Π4.10.3 Αναφορές SOCaaS	Σύμφωνα με το κεφάλαιο 7.1.6.5.3 του Παραρτήματος Ι

Κατηγορία	Παραδοτέα	Περιεχόμενο παραδοτέων
Λύση Ddos	Π4.10.1 Εξοπλισμός και λογισμικό διαχείρισης	Σύμφωνα με τον πίνακα συμμόρφωσης 7.2.4.2
	Π4.10.2 Τεκμηρίωση εξοπλισμού και λογισμικού διαχείρισης	Εγχειρίδια χρήσης και διαχείρισης εξοπλισμού και λογισμικού διαχείρισης
Παροχή υπηρεσιών ανάκαμψης από καταστροφή & λήψης αντιγράφων ασφαλείας (disaster recovery as a service & data backup as a service)	Π4.11.1 Αναφορά υπηρεσιών ανάκαμψης από καταστροφή & λήψης αντιγράφων ασφαλείας	Αναλυτική αναφορά της παροχής υπηρεσιών συμπεριλαμβανομένου του πλήθους αντιγράφων ασφαλείας, του χρόνου που ελήφθησαν, καθώς και των τεχνικών τους χαρακτηριστικών.
Υπηρεσίες εγκατάστασης/παραμετροποίησης υπηρεσιών ανάκαμψης από καταστροφή & λήψης αντιγράφων ασφαλείας (disaster recovery as a service & data backup as a service)	Π4.12.1 Αναφορά εγκατάστασης / παραμετροποίησης υπηρεσιών ανάκαμψης από καταστροφή & λήψης αντιγράφων ασφαλείας	Αναλυτική αναφορά εγκατάστασης και παραμετροποίησης με τεκμηρίωση των παραμέτρων που ορίστηκαν και των σχετικών τιμών και ρυθμίσεων.
Πλατφόρμα Κυβερνοασφάλειας – Εκτεταμένης Ανίχνευσης & Απόκρισης (CyberSecurity)	Π4.13.1 Μελέτη εφαρμογής	Μελέτη υλοποίησης του λογισμικού, η οποία θα περιλαμβάνει κατ' ελάχιστο αρχιτεκτονική, ανάλυση ενδεχόμενων μηχανισμών διαλειτουργικότητας και προβλέψεις για την ασφάλεια και την προστασία προσωπικών δεδομένων.
	Π4.13.2 Τεχνική και λειτουργική τεκμηρίωση	Εγχειρίδια χρήσης και διαχείρισης λογισμικού
Λύση Διαβάθμισης και Σήμανσης Εγγράφων	Π4.14.1 Μελέτη εφαρμογής	Μελέτη υλοποίησης του λογισμικού, η οποία θα περιλαμβάνει κατ' ελάχιστο αρχιτεκτονική, ανάλυση ενδεχόμενων μηχανισμών διαλειτουργικότητας και προβλέψεις για την ασφάλεια και την προστασία προσωπικών δεδομένων.
	Π4.14.2 Τεχνική και λειτουργική τεκμηρίωση	Εγχειρίδια χρήσης και διαχείρισης λογισμικού
Λύση Προστασίας Δεδομένων από Διαρροή	Π4.15.1 Μελέτη εφαρμογής	Μελέτη υλοποίησης του λογισμικού, η οποία θα περιλαμβάνει κατ' ελάχιστο αρχιτεκτονική, ανάλυση

Κατηγορία	Παραδοτέα	Περιεχόμενο παραδοτέων
		ενδεχόμενων μηχανισμών διαλειτουργικότητας και προβλέψεις για την ασφάλεια και την προστασία προσωπικών δεδομένων.
	Π4.15.2 Τεχνική και λειτουργική τεκμηρίωση	Εγχειρίδια χρήσης και διαχείρισης λογισμικού
Λύση Διαχείρισης Δικαιωμάτων Εγγράφων	Π4.16.1 Μελέτη εφαρμογής	Μελέτη υλοποίησης του λογισμικού, η οποία θα περιλαμβάνει κατ' ελάχιστο αρχιτεκτονική, ανάλυση ενδεχόμενων μηχανισμών διαλειτουργικότητας και προβλέψεις για την ασφάλεια και την προστασία προσωπικών δεδομένων.
	Π4.16.2 Τεχνική και λειτουργική τεκμηρίωση	Εγχειρίδια χρήσης και διαχείρισης λογισμικού
Λύση Διαχείρισης Λογαριασμών και Δικαιωμάτων Πρόσβασης Χρηστών	Π4.17.1 Μελέτη εφαρμογής	Μελέτη υλοποίησης του λογισμικού, η οποία θα περιλαμβάνει κατ' ελάχιστο αρχιτεκτονική, ανάλυση ενδεχόμενων μηχανισμών διαλειτουργικότητας και προβλέψεις για την ασφάλεια και την προστασία προσωπικών δεδομένων.
	Π4.17.2 Τεχνική και λειτουργική τεκμηρίωση	Εγχειρίδια χρήσης και διαχείρισης λογισμικού
Λύση Διαχείρισης Προνομιούχων Λογαριασμών Πρόσβασης	Π4.18.1 Μελέτη εφαρμογής	Μελέτη υλοποίησης του λογισμικού, η οποία θα περιλαμβάνει κατ' ελάχιστο αρχιτεκτονική, ανάλυση ενδεχόμενων μηχανισμών διαλειτουργικότητας και προβλέψεις για την ασφάλεια και την προστασία προσωπικών δεδομένων.
	Π4.18.2 Τεχνική και λειτουργική τεκμηρίωση	Εγχειρίδια χρήσης και διαχείρισης λογισμικού

7.1.7.3 Όροι και προϋποθέσεις παραλαβών

Ανάλογα το είδος και τη φύση των παραδοτέων ισχύουν τα κάτωθι:

α) Μελέτες

Ελέγχονται ως προς τα ακόλουθα χαρακτηριστικά:

- Πληρότητα: Το Παραδοτέο πρέπει να καλύπτει όλες τις πτυχές του σκοπού για τον οποίο συντάχθηκε και ειδικότερα να ανταποκρίνεται στις απαιτήσεις περιεχομένου που έχουν ορισθεί γι' αυτό.
- Σαφήνεια/Εμβάθυνση: Το Παραδοτέο πρέπει να περιέχει πληροφορίες σε βάθος ανάλογα με το σκοπό του, και ταυτόχρονα πρέπει να έχει αποφευχθεί πλεονάζουσα λεπτομέρεια σε βαθμό που θα επισκιάζει τη σαφήνεια του Παραδοτέου.
- Σχετικότητα/ Λειτουργικότητα/ Αποτελεσματικότητα: Το Παραδοτέο πρέπει να ανταποκρίνεται στο σκοπό για τον οποίο έχει συνταχθεί και στις ανάγκες του Έργου.
- Τεκμηρίωση: Το Παραδοτέο πρέπει να είναι ακριβές και να αποτυπώνει την πραγματικότητα. Αυτό σημαίνει ότι πρέπει να βασίζεται σε επαρκώς τεκμηριωμένα στοιχεία και όπου απαιτείται να δίδονται σαφείς επεξηγήσεις.

β) Υπηρεσίες

Διενεργούνται οι κάτωθι έλεγχοι:

- Υπηρεσίες Εκπαίδευσης. Θα ελέγχεται η πληρότητα/εγκυρότητα των σχετικών απολογιστικών αναφορών οι οποίες θα πρέπει να αναφέρουν ημερομηνίες διενέργειας, τόπος, όνομα εκπαιδευτή και πρόγραμμα εκπαίδευσης, και να περιέχουν εκπαιδευτικό υλικό ή υλικό παρουσίασης, και παρουσιολόγια.
- Η καταλληλότητα του προγράμματος ελέγχεται στο πλάνο εκπαίδευσης, όπου αυτό υποβάλλεται.
- Υπηρεσίες on-site υποστήριξης. Θα ελέγχεται η πληρότητα/εγκυρότητα των σχετικών απολογιστικών αναφορών οι οποίες θα πρέπει να αναφέρουν ημερομηνίες διενέργειας, όνομα υποστηρικτή και παρουσιολόγια.
- Υπηρεσίες που υπόκεινται σε SLA. Έλεγχος τριμηνιαίων (ή της αντίστοιχης περιόδου που ορίζεται στη διακήρυξη) αναφορών και επιβολή ρητρών.
- Λοιπές υπηρεσίες. Οι εργασίες θα μπορούν να πιστοποιούνται ότι διενεργήθηκαν σε μεγάλο βαθμό κατά την εξέλιξη των εργασιών, ενώ θα ελέγχεται η πληρότητα/εγκυρότητα των σχετικών παραγόμενων παραδοτέων ή/και απολογιστικών αναφορών, ως αυτές ορίζονται στη διακήρυξη.

γ) έτοιμο λογισμικό

Διενεργούνται οι κάτωθι έλεγχοι:

- Έλεγχος versioning
- Έλεγχος modules που έχουν προσφερθεί
- Έλεγχος licenses
- Έλεγχος επιτυχούς εγκατάστασης και κατάλληλης προσαρμογής (configuration)

δ) Εξοπλισμός και υποδομές

Διενεργούνται οι κάτωθι έλεγχοι στα στοιχεία του κεντρικού εξοπλισμού και δικτύων:

- Έλεγχοι ποσότητας προσφερόμενων ειδών (vendor, model, p/n, s/n) συμπεριλαμβανομένων υποστηρικτικών συσκευών ή προϊόντων ως έχουν προσφερθεί.
- Μακροσκοπικός έλεγχος. Ελέγχονται να μην υπάρχουν φθορές/ζημιές που επηρεάζουν ή εν δυνάμει απειλούν την καταλληλότητα, μακροσκοπικοί έλεγχοι θυρών συνδεσιμότητας, τακτοποιημένη τοποθέτηση καλωδίων, κ.λπ.
- Πρακτική δοκιμασία αυτοτελούς λειτουργικότητας στοιχείων (εύρυθμη λειτουργία κ.λπ.).
- Έλεγχος τεχνικών προδιαγραφών
- Άδειες λογισμικών, όπου απαιτούνται μαζί με τον εξοπλισμό
- Έλεγχος συνέργειας και αρμονικής συλλειτουργίας μεταξύ εξοπλισμού και υποδομών

7.1.8 Περίοδος Εγγύησης Συντήρησης (ΠΕΣ)

Ως ΠΕΣ ορίζεται η συνολική Περίοδος Εγγύησης και Συντήρησης, με ολοκλήρωση του Έργου, η οποία έχει ελάχιστη χρονική διάρκεια τα τέσσερα (4) έτη, ενώ μπορεί να αυξηθεί αν ο Ανάδοχος προσφέρει Περίοδο Εγγύησης μεγαλύτερη της ελάχιστης ζητούμενης.

Ο Ανάδοχος είναι υποχρεωμένος να παρέχει δωρεάν υπηρεσίες Εγγύησης για τουλάχιστον ένα (1) έτος από την οριστική παραλαβή του έργου. Στην περίπτωση κατά την οποία ο Ανάδοχος έχει περιλάβει στην Προσφορά του Περίοδο Εγγύησης μεγαλύτερη της ελάχιστης ζητούμενης, αυτή θα πρέπει να καλύπτει το σύνολο των προϊόντων και υπηρεσιών για ακέραιο αριθμό ετών.

Η Περίοδος Συντήρησης ξεκινά με τη λήξη της προσφερθείσας δωρεάν Περιόδου Εγγύησης και λήγει με τη λήξη της ΠΕΣ.

Πριν τη λήξη της σύμβασης, ο Κύριος του Έργου δύναται να συνάψει Σύμβαση Εγγύησης - Συντήρησης με τον Ανάδοχο του Έργου. Στο πλαίσιο αυτό, ο Ανάδοχος υποχρεούται να συμβάλλεται με την Αναθέτουσα Αρχή/Κύριο του Έργου για την παροχή των δωρεάν υπηρεσιών εγγύησης και των υπηρεσιών Συντήρησης με τίμημα το προβλεπόμενο από την Προσφορά του σύμφωνα και με τους όρους της παρ. 4.5.1 της παρούσας.

Ειδικότερα, ο Ανάδοχος είναι υποχρεωμένος, εφόσον το επιθυμεί ο Φορέας για τον οποίο προορίζεται το Έργο, να υπογράψει Σύμβαση Συντήρησης στο πλαίσιο του δικαιώματος προαίρεσης συντήρησης, πριν από τη λήξη της σύμβασης, με τίμημα το κόστος συντήρησης που αναφέρεται στην Προσφορά του και διάρκεια έως τέσσερα (4) έτη περιλαμβανομένων και των ετών της περιόδου εγγύησης. Η διάρκεια της σύμβασης προαίρεσης Εγγύησης - Συντήρησης μπορεί να αυξηθεί αντίστοιχα, εφόσον ο Ανάδοχος έχει προσφέρει περίοδο εγγύησης μεγαλύτερη από την ελάχιστη ζητούμενη στην παρούσα. Η χρήση αυτού του Δικαιώματος προαίρεσης δεν είναι δεσμευτική για την Αναθέτουσα Αρχή/Κύριο του Έργου και σε καμία περίπτωση δεν υποχρεούται να ασκήσει το παραπάνω δικαίωμα, παρά μόνο εφόσον το κρίνει αναγκαίο και έως του ποσού του δικαιώματος προαίρεσης συντήρησης της παρ. 4.5.1.

Οι υπηρεσίες της Περιόδου Εγγύησης αφορούν στο σύνολο του Έργου, καλύπτουν το σύνολο των προϊόντων και υπηρεσιών, παρέχονται σε περιβάλλον Εγγυημένου Επιπέδου Υπηρεσιών (βλ. **7.1.8.2 Τήρηση Εγγυημένου Επιπέδου Υπηρεσιών – Ρήτρες**) και είναι αυτές που περιγράφονται στην παρ 7.1.8.1, αλλά παρέχονται δωρεάν.

7.1.8.1 Υπηρεσίες Περιόδου Εγγύησης-Συντήρησης

Οι υπηρεσίες της Περιόδου Εγγύησης αφορούν στο σύνολο του Έργου, παρέχονται σε περιβάλλον **Εγγυημένου Επιπέδου Υπηρεσιών** (βλ. παρ. 7.1.8.2 Τήρηση Εγγυημένου Επιπέδου Υπηρεσιών – Ρήτρες).

ΑΝΑΜΕΝΟΜΕΝΑ ΠΑΡΑΔΟΤΕΑ / ΑΠΟΤΕΛΕΣΜΑΤΑ ΠΕΡΙΟΔΟΥ:

ΑΝΤΙΚΕΙΜΕΝΟ / ΠΕΡΙΕΧΟΜΕΝΟ ΠΕΡΙΟΔΟΥ:

ΕΓΓΥΗΣΗ ΕΤΟΙΜΟΥ ΛΟΓΙΣΜΙΚΟΥ ή ΑΛΛΟΥ ΛΟΓΙΣΜΙΚΟΥ εφόσον έχει παραδοθεί στο πλαίσιο της παρούσας

1. Διασφάλιση καλής λειτουργίας έτοιμου λογισμικού.
2. Εντοπισμός αιτιών βλαβών/ δυσλειτουργιών και αποκατάσταση. Κατόπιν τεκμηριωμένης ειδοποίησης από τον Φορέα Λειτουργίας, ο Ανάδοχος είναι υποχρεωμένος να επιλύει τα προβλήματα εντός χρονικού διαστήματος από την αναγγελία (βλ. παρ. **7.1.8.2**) εφόσον αυτά δεν έχουν προκύψει από κακόβουλες ή άστοχες παρεμβάσεις τρίτων. Αν η πλήρης και οριστική επίλυση του προβλήματος δεν είναι εφικτή εντός του συγκεκριμένου χρονικού ορίου όπως προβλέπεται στην παρ. **7.1.8.2 Τήρηση Εγγυημένου Επιπέδου Υπηρεσιών – Ρήτρες**, επιβάλλονται οι προβλεπόμενες ρήτρες.
3. Βελτιστοποιήσεις στη δομή της βάσης, έτσι ώστε να εξασφαλίζεται η βέλτιστη απόδοση του συστήματος.
4. Παράδοση – εγκατάσταση τυχόν βελτιωτικών εκδόσεων λογισμικού, μετά από έγκριση της ΕΠΕ.
5. Εξασφάλιση ορθής λειτουργίας όλων των customizations, διεπαφών με άλλα συστήματα, κ.λπ., με τις βελτιωτικές εκδόσεις.
6. Παράδοση αντιτύπων όλων των μεταβολών ή των επανεκδόσεων ή τροποποιήσεων των εγχειριδίων λογισμικού.
7. Χρήση του Συστήματος Διαχείρισης Αιτημάτων Έργων (Ticket Management System) της Αναθέτουσας Αρχής από τον Ανάδοχο.

ΕΓΓΥΗΣΗ ΕΞΟΠΛΙΣΜΟΥ

8. Αποκατάσταση βλαβών εξοπλισμού. Οι ενέργειες (εργασίες και ανταλλακτικά) που απαιτείται να εκτελεστούν στον εξοπλισμό (hardware) προκειμένου να αποκατασταθούν οι προϋποθέσεις για την ομαλή λειτουργία τους μετά την εμφάνιση σχετικού προβλήματος.
9. Εξασφάλιση ανταλλακτικών. Υποχρέωση του Αναδόχου να έχει όλα τα απαραίτητα καινούργια ανταλλακτικά για την επισκευή και συντήρηση των συστημάτων.
10. Αντιμετώπιση σφαλμάτων– προβλημάτων όλου του εγκατεστημένου εξοπλισμού (ενεργού και παθητικού) τόσο σε επίπεδο υλικού όσο και λογισμικού.
11. Συντήρηση εξοπλισμού,: Ο Ανάδοχος στα πλαίσια των υπηρεσιών συντήρησης θα πρέπει να προβαίνει σε όλες τις αναβαθμίσεις λογισμικού που προβλέπονται από τους

κατασκευαστές (ενδεικτικά firmware, patches, drivers) για όλα τα ενεργά στοιχεία εξοπλισμού.

12. Ενημέρωση της Αναθέτουσας Αρχής για νέες εκδόσεις λογισμικού οι οποίες δεν παρέχονται δωρεάν από τον κατασκευαστή, με ανάλυση των νέων λειτουργιών.

ΥΠΗΡΕΣΙΕΣ/ΤΕΧΝΙΚΗ ΥΠΟΣΤΗΡΙΞΗ

1. Υπηρεσίες απομακρυσμένης Τεχνικής Υποστήριξης
2. On site υποστήριξη. Όταν τα αναφερόμενα προβλήματα δεν μπορούν να επιλυθούν απευθείας και οριστικά από το πρώτο επίπεδο παρέμβασης, πρέπει να προωθούνται σε ειδικούς οι οποίοι θα δίνουν την απαιτούμενη λύση επιτόπου.
3. Αντιμετώπιση λαθών και σφαλμάτων στη λειτουργία του συστήματος.
4. Προσαρμογή της βάσης που θα αναπτυχθεί στο πλαίσιο του παρόντος Έργου σε νέες απαιτήσεις που προκύπτουν από πιθανές τροποποιήσεις στην οργάνωση και τις λειτουργίες του Φορέα Λειτουργίας και σχετίζονται με το φυσικό αντικείμενο του παρόντος Έργου.
5. Αναβάθμιση του συστήματος σε νέες εκδόσεις του λειτουργικού συστήματος ή του συστήματος διαχείρισης βάσεων δεδομένων στα οποία βασίζεται το σύστημα.
6. Ενημέρωση των χειριστών του για τυχόν αλλαγές στη λειτουργικότητα του συστήματος.

Για τις ανωτέρω Υπηρεσίες 1, 2 και 3 θα πρέπει να παραδοθούν τα αντίστοιχα Παραδοτέα όπως αυτά περιγράφονται στο Αντικείμενο του Έργου της παρούσας.

Οι ΑΜ που θα διατεθούν κατά τη διάρκεια της περιόδου συντήρησης για τις εργασίες που περιγράφονται στο σημείο 1. ανωτέρω, δεν θα υπερβαίνουν κατ' έτος το 5% των ανθρωπομηνών που θα προσφερθούν από τον Ανάδοχο για την ανάπτυξη / παραμετροποίηση των εφαρμογών.

ΑΝΑΜΕΝΟΜΕΝΑ ΠΑΡΑΔΟΤΕΑ / ΑΠΟΤΕΛΕΣΜΑΤΑ ΠΕΡΙΟΔΟΥ:

Περίοδος Συντήρησης – Παραδοτέα (ελάχιστα):	
Τίτλος Παραδοτέου	Περιγραφή Παραδοτέου
Π1. Υπηρεσίες υποστήριξης και αποκατάστασης βλαβών	<p>Τεύχος αποτύπωσης υπηρεσιών που θα περιλαμβάνει:</p> <ul style="list-style-type: none"> • Αναλυτικό Πρόγραμμα ενεργειών προληπτικής συντήρησης, που υποβάλλεται με την έναρξη της σχετικής περιόδου • Αναλυτική Καταγραφή Πεπραγμένων Συντήρησης (Τακτικών – Έκτακτων Ενεργειών) • Τεκμηρίωση πρόσθετων προσαρμογών και παραμετροποιήσεων σε έτοιμο λογισμικό και εφαρμογών • Παράδοση αντιτύπων όλων των μεταβολών ή επανεκδόσεων ή τροποποιήσεων των εγχειριδίων του έτοιμου λογισμικού και εφαρμογών/ών

	<ul style="list-style-type: none"> • Τεκμηρίωση εγκαταστάσεων νέων εκδόσεων έτοιμου λογισμικού και εφαρμογής/ών • Έκθεση αξιολόγησης Περιόδου
--	---

7.1.8.2 Τήρηση Εγγυημένου Επιπέδου Υπηρεσιών – Ρήτρες

Ο Ανάδοχος υποχρεούται να υλοποιήσει το σύνολο του συστήματος παρέχοντας παράλληλα τις απαιτούμενες υπηρεσίες τεχνικής υποστήριξης, ώστε να τηρούνται τα ελάχιστα όρια διαθεσιμότητας που ορίζονται στη συνέχεια. Τονίζεται ότι οι όροι που αναφέρονται στην παρούσα παράγραφο ισχύουν για τις περιόδους εγγύησης και συντήρησης (για την τελευταία εφόσον υπογραφεί Σύμβαση Συντήρησης).

Ορισμοί:

- ✓ **Λογισμικό/Εφαρμογές:** το σύνολο των διακριτών μονάδων λογισμικού/εφαρμογών που παραδόθηκαν/αναπτύχθηκαν στο πλαίσιο της Σύμβασης (όπως περιγράφονται στην Παρ. **Error! Reference source not found.** του Παραρτήματος Ι), η εύρυθμη λειτουργία των οποίων στηρίζει τη λειτουργικότητα του συστήματος, δηλ., εφαρμογές υποσυστημάτων, εργαλεία ανάπτυξης.
- ✓ **Βλάβη:** ζημιά μέρους ή όλης της διακριτής μονάδας λογισμικού/εφαρμογών, η οποία επηρεάζει άμεσα και αρνητικά την διαθεσιμότητα ή απόδοση του εν λόγω στοιχείου και κατ' επέκταση τις προσφερόμενες υπηρεσίες του Συστήματος.
- ✓ **Δυσλειτουργία:** ζημιά μέρους ή όλης της διακριτής μονάδας λογισμικού/εφαρμογών, η οποία δεν επηρεάζει άμεσα και αρνητικά την διαθεσιμότητα ή απόδοση του εν λόγω στοιχείου και κατ' επέκταση τις προσφερόμενες υπηρεσίες του Συστήματος.
- ✓ **ΚΩΚ** (κανονικές ώρες κάλυψης): Το χρονικό διάστημα 07:30 – 17:00 για τις εργάσιμες ημέρες.
- ✓ **ΕΩΚ** (επιπλέον ώρες κάλυψης): Το υπόλοιπο χρονικό διάστημα.
- ✓ **Χρόνος αποκατάστασης βλάβης** είναι το μέγιστο επιτρεπόμενο χρονικό διάστημα από την αναγγελία της βλάβης μέχρι και την αποκατάστασή της. Σημειώνεται ότι, ανά διακριτή μονάδα, ο Χρόνος αποκατάστασης βλάβης προσμετράται **αθροιστικά σε μηνιαία βάση**. Ο χρόνος αυτός είναι:
 - έξι (6) ώρες από τη στιγμή της ανακοίνωσης της εμφάνισης της βλάβης αν η ανακοίνωση του προβλήματος πραγματοποιήθηκε εντός ΚΩΚ
 - έξι (6) ώρες οι οποίες θα προσμετρούνται από τις 07.30 της επόμενης εργάσιμης ημέρας, για τις λοιπές ώρες ανακοίνωσης προβλήματος βλάβης
- ✓ **Χρόνος αποκατάστασης δυσλειτουργίας** είναι το μέγιστο επιτρεπόμενο χρονικό διάστημα από την αναγγελία της δυσλειτουργίας μέχρι και την αποκατάστασή της. Σημειώνεται ότι, ανά διακριτή μονάδα, ο Χρόνος αποκατάστασης δυσλειτουργίας προσμετράται αθροιστικά σε μηνιαία βάση. Ο χρόνος αυτός είναι:
 - οκτώ (8) ώρες από τη στιγμή της ανακοίνωσης της εμφάνισης της δυσλειτουργίας αν η ανακοίνωση του προβλήματος πραγματοποιήθηκε εντός ΚΩΚ
 - είκοσι τέσσερις (24) ώρες οι οποίες θα προσμετρούνται από τις 07.30 της επόμενης εργάσιμης ημέρας, για τις λοιπές ώρες ανακοίνωσης προβλήματος δυσλειτουργίας

Μη διαθεσιμότητα – Ρήτρες:

Σε περίπτωση υπέρβασης του **μηνιαίου χρόνου αποκατάστασης βλάβης**, επιβάλλεται στον Ανάδοχο ρήτρα ίση με το μεγαλύτερο εκ των δύο ακόλουθων τιμών:

- **0,05%** επί του συμβατικού τιμήματος της μονάδας/τμήματος που είναι εκτός λειτουργίας
- **0,2%** επί του τρέχοντος ετήσιου κόστους συντήρησης του συνόλου του συστήματος.

για κάθε επιπλέον ώρα βλάβης (μη διαθεσιμότητας)/δυσλειτουργίας, εφόσον αυτή είναι εντός ΚΩΚ, ή το ήμισυ του ως άνω υπολογιζόμενου ποσού, εφόσον η ώρα είναι εκτός ΚΩΚ.

Σε περίπτωση υπέρβασης του **μηνιαίου χρόνου αποκατάστασης δυσλειτουργίας**, επιβάλλεται στον Ανάδοχο ρήτρα ίση με το μεγαλύτερο εκ των δύο ακόλουθων τιμών:

- **0,02%** επί του συμβατικού τιμήματος της μονάδας/τμήματος που είναι εκτός λειτουργίας
- **0,1%** επί του τρέχοντος ετήσιου κόστους συντήρησης του συνόλου του συστήματος.

για κάθε επιπλέον ώρα βλάβης (μη διαθεσιμότητας)/δυσλειτουργίας, εφόσον αυτή είναι εντός ΚΩΚ, ή το ήμισυ του ως άνω υπολογιζόμενου ποσού, εφόσον η ώρα είναι εκτός ΚΩΚ.

Διευκρινίζεται ότι:

- 1) Ένα σύστημα / υποσύστημα / υπηρεσία θεωρείται ολικά μη διαθέσιμο/η εάν είναι μη διαθέσιμο έστω και ένα μικρό μέρος της λειτουργικότητας που παρέχει.
- 2) Η μη διαθεσιμότητα μιας μονάδας επιφέρει τη μη διαθεσιμότητα όλων των μονάδων του Συστήματος (λογισμικό συστημάτων και εφαρμογών) που εξαρτώνται λειτουργικά από αυτήν, και συνυπολογίζεται στον προσδιορισμό της ρήτρας.

Επιπρόσθετες ρήτρες

- ✓ Αν μια μονάδα (λογισμικού/εφαρμογής) είναι μη διαθέσιμη (σε βλάβη ή δυσλειτουργία) για χρονική περίοδο άνω των 72 ωρών (είτε εντός ΚΩΚ είτε εκτός) αθροιστικά στο διάστημα ενός μήνα, πέραν των ως άνω αναφερόμενων ρητρών:
 - επιβάλλεται στον Ανάδοχο ρήτρα ίση με **0,02%** επί του συμβατικού τιμήματος της μονάδας/τμήματος που είναι εκτός λειτουργίας, κατά τη διάρκεια της περιόδου εγγύησης
 - δεν καταβάλλεται (για τον τρέχοντα μήνα) τίμημα συντήρησης για την μονάδα αυτή κατά τη διάρκεια της περιόδου συντήρησης (εφόσον υπογραφεί Σύμβαση Συντήρησης).

Οι ρήτρες της παρούσας παραγράφου δεν ισχύουν στην περίπτωση που εξοπλισμός ή λογισμικό του Κυβερνητικού Υπολογιστικού Νέφους H-Cloud (Government Cloud) ή/και του ΣΥΖΕΥΞΙΣ προκαλέσει αποδεδειγμένα δυσλειτουργία (τεκμαιρόμενη από τα εργαλεία και τις αναφορές διαθεσιμότητας των σχετικών πόρων / υπηρεσιών του H-Cloud) σε παραδοτέο του Έργου.

7.1.8.3 Προγραμματισμένες Διακοπές Υπηρεσίας

Επιτρέπεται η διενέργεια προγραμματισμένων διακοπών της Υπηρεσίας (Planned Outages), τόσο κατά την υλοποίηση του Έργου, σύμφωνα με τις παρακάτω συνθήκες:

- Κάθε προγραμματισμένη διακοπή της υπηρεσίας από τον Ανάδοχο θα ανακοινώνεται τουλάχιστον **15 ημερολογιακές ημέρες** νωρίτερα στο Φορέα, και θα πρέπει να τεκμηριώνεται κατάλληλα.
- Κάθε προγραμματισμένη διακοπή της υπηρεσίας θα πραγματοποιείται μόνο εφόσον ρητά συμφωνηθεί μεταξύ των δύο μερών.
- Η μέγιστη διάρκεια μίας προγραμματισμένης διακοπής υπηρεσιών θα συμφωνείται ρητά μεταξύ των δύο μερών.
- Θα πραγματοποιείται μόνο **σε ώρες ΕΩΚ** (όπως αυτές ορίζονται στην προηγούμενη ενότητα).
- Η χρονική περίοδος απώλειας της υπηρεσίας που οφείλεται σε προγραμματισμένη διακοπή δε θα υπολογίζεται στη μέτρηση των Ποιοτικών Κριτηρίων.

Σε περιπτώσεις όπου, η διάρκεια της προγραμματισμένης διακοπής υπηρεσίας υπερβεί την προσυμφωνημένη χρονική διάρκεια, και γι' αυτό ευθύνεται αποκλειστικά ο Ανάδοχος, τότε η επιπλέον χρονική διάρκεια απώλειας της υπηρεσίας θεωρείται ως βλάβη.

7.1.9 Σχήμα Διοίκησης Έργου

Οι οικονομικοί φορείς θα πρέπει να υποβάλλουν στην τεχνική τους προσφορά ολοκληρωμένη πρόταση για το σχήμα διοίκησης του έργου, το προσωπικό που θα διατεθεί για τη διοίκηση και υλοποίησή του, το αντικείμενο και το χρόνο απασχόλησης κάθε στελέχους στο έργο.

Επίσης θα πρέπει να περιγράψουν τις βασικές αρχές ενός ολοκληρωμένου συστήματος διοίκησης του έργου, καθορίζοντας τόσο την εσωτερική δομή, τους ρόλους, τα καθήκοντα και τις αρμοδιότητες και τις διαδικασίες επικοινωνίας της Ομάδας Έργου, όσο και τις εξωτερικές διεπαφές της και τον τρόπο συνεργασίας με τα στελέχη της Αναθέτουσας Αρχής.

Κάθε οικονομικός φορέας θα πρέπει να προβλέψει κατάλληλη Ομάδα Έργου η οποία θα απαρτίζεται από εξειδικευμένα στελέχη σύμφωνα με τα προβλεπόμενα στην Παρ. [2.2.6.2](#).

Τυχόν αλλαγή του προσωπικού θα τελεί υπό την έγκριση της Αναθέτουσας Αρχής μετά από σχετική εισήγηση της ΕΠΕ και οι σχετικές αποφάσεις θα αποτελούν αναπόσπαστο μέρος της συναφθείσας σύμβασης.

Την κύρια ευθύνη υλοποίησης του Έργου έχει ο Ανάδοχος, τη δε επίβλεψη και τον έλεγχο της εκτέλεσης της Σύμβασης και των παραδοτέων έχει η Αναθέτουσα Αρχή.

Ο Ανάδοχος θα συγκροτήσει Ομάδα Έργου, με κατάλληλο οργανωτικό σχήμα και επαρκή στελέχωση, για την παροχή των υπηρεσιών, που περιγράφονται αναλυτικά στη διακήρυξη.

7.1.9.1 Υπεύθυνος Έργου Αναδόχου

Ο υποψήφιος Ανάδοχος υποχρεούται να καθορίσει στην Προσφορά του τα στελέχη που θα αναλάβουν τους ρόλους:

- Του Υπευθύνου Έργου (project manager)
- Του αναπληρωτή Υπευθύνου Έργου

Οι ελάχιστες απαιτήσεις για τον Υπεύθυνο και τον Αναπληρωτή Υπεύθυνο Έργου βρίσκονται στην παρ. 2.2.6.

Συγκεκριμένα για τα δύο ανωτέρω στελέχη:

- Να περιγραφεί ο ρόλος τους στο προτεινόμενο από τον ανάδοχο σχήμα Διοίκησης
- Να δηλωθεί το γνωστικό αντικείμενο, που θα καλύψουν
- Να δηλωθεί το ποσοστό συμμετοχής τους στο Έργο και οι ανθρωπομήνες που θα αφιερώσουν ανά πακέτο εργασίας του Έργου.
- Να δηλωθεί η σχέση τους με τον υποψήφιο Ανάδοχο (υπάλληλος, στέλεχος αποκλειστικής απασχόλησης, εξωτερικός συνεργάτης, στέλεχος υπεργολάβου).

7.1.9.2 Μέλη Ομάδας Έργου

Ο υποψήφιος Ανάδοχος υποχρεούται επίσης να καθορίσει στην Προσφορά του τα στελέχη της Ομάδας Έργου.

Συγκεκριμένα, για όλα τα Μέλη της Ομάδας Έργου:

- Να περιγραφεί ο ρόλος τους στο προτεινόμενο Σχήμα Διοίκησης.

- Να δηλωθεί το γνωστικό αντικείμενο, που θα καλύψουν.
- Να δηλωθεί το ποσοστό συμμετοχής τους στο Έργο
- Να δηλωθεί η σχέση τους με τον υποψήφιο Ανάδοχο (στέλεχος Αναδόχου, στέλεχος υπεργολάβου, εξωτερικός συνεργάτης).

Οι ελάχιστες απαιτήσεις για την Ομάδα Έργου βρίσκονται στην παρ. [2.2.6.2](#).

7.1.10 Μεθοδολογία διοίκησης και διασφάλισης ποιότητας

Οι οικονομικοί φορείς πρέπει να αναλύσουν στην τεχνική τους προσφορά τη μεθοδολογία και τις τεχνικές διαχείρισης ποιότητας που εφαρμόζουν. Η διασφάλιση της ποιότητας του έργου είναι από τους πλέον κρίσιμους παράγοντες επιτυχίας του.

Η Διασφάλιση της Ποιότητας περιλαμβάνει όλες τις απαραίτητες ενέργειες/ελέγχους για την εξασφάλιση ότι το νέο Σύστημα θα ικανοποιεί όλες τις ποιοτικές απαιτήσεις του έργου.

Κάθε οικονομικός φορέας είναι υποχρεωμένος να συμπεριλάβει στην προσφορά του λεπτομερές χρονοδιάγραμμα υλοποίησης με τις κύριες δράσεις υλοποίησης, περιγραφές εργασιών και παραδοτέων, αναλυτικές χρονικές περιόδους υλοποίησης, ανθρώπινους πόρους (ρόλοι / ομάδες έργου) και αρμοδιότητες, καθώς και τα κύρια ορόσημα του Έργου.

Κατά τη διάρκεια υλοποίησης του Έργου, ο Ανάδοχος θα υποβάλλει Μηνιαίες Αναφορές Προόδου (progressreports) σχετικά με τις δράσεις του και τις διαδικασίες εκτέλεσης του Έργου, έτσι ώστε να διασφαλίζεται:

- η τήρηση του χρονοδιαγράμματος του Έργου
- η ορθή, και συμβατή με τις προδιαγραφές, εκτέλεση των υποχρεώσεων του Αναδόχου.

7.1.11 Μεθοδολογία διαχείρισης κινδύνων

Στο πλαίσιο του έργου οι οικονομικοί φορείς θα πρέπει να παρουσιάσουν αναλυτικό πλάνο και μεθοδολογία διαχείρισης κινδύνων / ρίσκων. Το πλάνο θα πρέπει να αντιμετωπίζει ρίσκα συνδεδεμένα τόσο με τεχνικές / τεχνολογικές πτυχές, όσο και με οργανωτικές / διαχειριστικές.

7.1.12 ΟΙΚΟΝΟΜΙΚΟ ΑΝΤΙΚΕΙΜΕΝΟ ΤΗΣ ΣΥΜΒΑΣΗΣ

Η εκτιμώμενη αξία της συμφωνίας-πλαίσιο ανέρχεται στο ποσό των εκατόν δύο εκατομμυρίων εκατόν εξήντα επτά χιλιάδων εννιακοσίων ενενήντα εννιά ευρώ και ενενήντα εννέα λεπτών (102.167.999,99 €) συμπεριλαμβανομένου ΦΠΑ 24 % (προϋπολογισμός χωρίς ΦΠΑ: 82.393.548,38 € ΦΠΑ: 19.774.451,61 €)

- Η εκτιμώμενη αξία της αρχικής συμφωνίας-πλαίσιο ανέρχεται στο ποσό των τριάντα οχτώ εκατομμυρίων εκατόν σαράντα πέντε χιλιάδων εκατόν εξήντα ενός ευρώ και είκοσι εννέα λεπτών (38.145.161,29 €) μη περιλαμβανομένου ΦΠΑ (προϋπολογισμός με ΦΠΑ: 47.300.000,00 €, ΦΠΑ 24% 9.154.838,71 €). Η πηγή χρηματοδότησης είναι το ΕΣΑΑ Ελλάδα 2.0, ΣΑΤΑ ΤΑΧΧΧΧΧ (Κωδ. Έργου: 2022ΤΑΧΧΧΧΧΧΧ).
- Το δικαίωμα προαίρεσης ως προς το φυσικό αντικείμενο ανέρχεται σε πενήντα τοις εκατό (50%) της αξίας της αρχικής συμφωνίας - πλαίσιο στο ποσό των δεκαεννέα εκατομμυρίων

εβδομήντα δύο χιλιάδων πεντακοσίων ογδόντα ευρώ και εξήντα τεσσάρων λεπτών (19.072.580,64 €) μη περιλαμβανομένου ΦΠΑ (προϋπολογισμός με ΦΠΑ: 23.650.000,00 €, ΦΠΑ 24% 4.577.419,35 €). Η προαίρεση δύναται να χρηματοδοτηθεί από οποιαδήποτε άλλη πηγή.

- Το δικαίωμα προαίρεσης ως προς τη συντήρηση ανέρχεται στο ποσό των είκοσι πέντε εκατομμυρίων εκατόν εβδομήντα πέντε χιλιάδων οχτακοσίων έξι ευρώ και σαράντα πέντε λεπτών (25.175.806,45 €) μη περιλαμβανομένου ΦΠΑ (προϋπολογισμός με ΦΠΑ: 31.218.000,00 €, ΦΠΑ 24% 6.042.193,55 €). Η προαίρεση δύναται να χρηματοδοτηθεί από οποιαδήποτε άλλη πηγή.

7.2 ΠΑΡΑΡΤΗΜΑ ΙΙ –Πίνακες Συμμόρφωσης

Οι υποψήφιοι ανάδοχοι καλούνται να συμπληρώσουν τον παρακάτω πίνακα συμμόρφωσης, ανά τμήμα του έργου:

7.2.1 Πίνακες Συμμόρφωσης Τμήματος 1 «Υπηρεσίες εξασφάλισης επιχειρησιακής συνέχειας, ασφάλειας διακίνησης δεδομένων και μέτρα και πολιτικές πρόληψης και αντιμετώπισης κινδύνων για τη Γ.Γ.Π.Σ.Δ.Δ.»

7.2.1.1 Υπηρεσίες Ransomware readiness assessment

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
1.	Να προσφερθεί Υπηρεσία Αξιολόγησης Ετοιμότητας Ransomware από διεθνή αναγνωρισμένη, εδραιωμένη και εξειδικευμένη ομάδα στο χώρο της κυβερνοασφάλειας.	ΝΑΙ		
2.	Η προσφερόμενη υπηρεσία θα αξιολογήσει την ετοιμότητα ανταπόκρισης και ανάκτησης από επιθέσεις ransomware.	ΝΑΙ		
3.	Η προσφερόμενη υπηρεσία θα εντοπίσει και θα παρουσιάσει κενά ελέγχου (controlgaps) στον οργανισμό της ΓΓΠΣ.	ΝΑΙ		
4.	Η προσφερόμενη υπηρεσία θα παρέχει πρακτικές συστάσεις (actionablerecommendations) για τη βελτίωση των δυνατοτήτων ανταπόκρισης σε συμβάντα ασφαλείας.	ΝΑΙ		
5.	Τα κριτήρια αξιολόγησης της υπηρεσίας θα βασίζονται σε βέλτιστες πρακτικές του κλάδου της κυβερνοασφάλειας και στην εμπειρία της εξειδικευμένης ομάδας να ανταποκρίνεται σε αντίστοιχα περιστατικά.	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
6.	Η ομάδα που θα διενεργήσει την αξιολόγηση θα προέρχεται από κατασκευαστή προϊόντων και υπηρεσιών, εδραιωμένο στο χώρο της κυβερνοασφάλειας με διεθνή βραβεία ώστε να αξιοποιηθούν οι βέλτιστες πρακτικές και η εμπειρία.			
7.	Το πεδίο εφαρμογής θα καλύπτει την τεχνική απόκριση, τη διαχείριση περιστατικών και τις δυνατότητες του οργανισμού που είναι απαραίτητες για την απόκριση σε σημαντικά περιστατικά ransomware.	ΝΑΙ		
8.	Ως παραδοτέα της προσφερόμενης υπηρεσίας θα περιλαμβάνονται κατ' ελάχιστο τα παρακάτω:			
9.	Έκθεση ευρημάτων και συστάσεων, συμπεριλαμβανομένων: <ul style="list-style-type: none"> - Περίληψη των κυριότερων σημείων - Ευρήματα αξιολόγησης για κάθε έναν από τους τομείς που αξιολογήθηκαν - Βαθμολογία ωριμότητας για κάθε έναν από τους τομείς που αξιολογήθηκαν Βραχυπρόθεσμες, μεσοπρόθεσμες και μακροπρόθεσμες συστάσεις για τη βελτίωση των δυνατοτήτων απόκρισης ransomware	ΝΑΙ		
10.	Επιτελική σύνοψη σε μορφή παρουσίασης που θα περιέχει τους τομείς ισχύος, των κενών και των βασικών κινδύνων, καθώς και συστάσεις για τη βελτίωση των δυνατοτήτων σε καθεμία από τις αξιολογούμενες λειτουργίες.	ΝΑΙ		

7.2.1.2 Μηχανισμός Ελέγχου Πρόσβασης Χρηστών Πολλαπλών Παραγόντων (MFA)

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
1.	Η προσφερόμενη πλατφόρμα θα πρέπει να υποστηρίζει εγγενώς τη σύνδεση τόσο με γνωστές εφαρμογές τρίτων τόσο και με customεφαρμογές και να είναι On-premise	ΝΑΙ		
2.	Να αναφερθεί το προσφερόμενο μοντέλο και ο κατασκευαστής			

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
3.	Να υποστηρίζεται εφαρμογή για κινητές συσκευές (app) Android, iOS	ΝΑΙ		
4.	Αριθμός απαιτούμενων αδειών χρηστών.	≥10.000		
5.	Η πλατφόρμα θα πρέπει να υποστηρίζει ειδοποιήσεις push για κινητά ως μηχανισμό πολλαπλών παραγόντων - ελέγχου ταυτότητας (multifactorauthentication)	ΝΑΙ		
6.	Η εφαρμογή να παράγει OTP (One time password)	ΝΑΙ		
7.	Η αδειοδότηση να είναι ανά χρήστη και να υποστηρίζει πολλαπλές συσκευές του χωρίς επιπρόσθετο κόστος	ΝΑΙ		
8.	Παροχή ενός selfserviceinterface στο οποίο ο χρήστης θα έχει εικόνα των προσβάσεων και των εφαρμογών στις οποίες μπορεί να ζητήσει πρόσβαση.	ΝΑΙ		
9.	Η προτεινόμενη πλατφόρμα θα πρέπει να διαθέτει authentication methods και out – of – the box connectors για authentication με εφαρμογές cloud χρησιμοποιώντας third party systems (Azure, Active Directory, ADFS)	ΝΑΙ		
10.	Να υποστηρίζεται SMS	ΝΑΙ		
11.	Η προτεινόμενη πλατφόρμα θα πρέπει να παρέχει πολλαπλούς μηχανισμούς ελέγχου ταυτότητας, συμπεριλαμβανομένων των παρακάτω: <ul style="list-style-type: none"> • Kerberos, • OAuth 2.0, • SAML 2.0, • OpenIDConnect, • OTP & TOTP One time password 	ΝΑΙ		
12.	Να αναφερθούν τα υποστηριζόμενα tokens	ΝΑΙ		
13.	Να υπάρχει δυνατότητα self-enrollment των χρηστών	ΝΑΙ		
14.	Ο διαχειριστής θα μπορεί να έχει εικόνα της διαστηριότητας των χρηστών και να μπορεί να βγάλει αναφορές.	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
15.	Η πλατφόρμα πρέπει προσφέρει δυνατότητα Single Sign-on.	ΝΑΙ		
16.	Η προϊοντική οικογένεια στην οποία ανήκει το προσφερόμενο προϊόν να αποτελεί την πιο πλήρη λύση στο κομμάτι Identity and Access Management της αγοράς με δυνατότητες όπως Single Sign-On (SSO), Multi-Factor Authentication (MFA), Identity Governance, Identity Analytics, Privileged Access Management και πολλά άλλα χωρίς τη χρήση 3ων λύσεων. Να περιγραφεί	ΝΑΙ		
17.	Η προσφερόμενη πλατφόρμα θα πρέπει να προσφέρει τη δυνατότητα δημιουργίας χρηστών με διαφορετικούς ρόλους και διαφορετικά δικαιώματα πρόσβασης.	ΝΑΙ		
18.	Η πλατφόρμα να έχει τη δυνατότητα ρύθμισης, ώστε να αναγκάζει τον χρήστη να αλλάξει κωδικό πρόσβασης κατά την πρώτη σύνδεση (όπου υποστηρίζεται από την εφαρμογή / σύστημα).	ΝΑΙ		
19.	Η πλατφόρμα θα πρέπει να προσφέρει δυνατότητα δημιουργίας διαφορετικών ομάδων (groups) χρηστών και ανάθεση διαφορετικών ρόλων και δικαιωμάτων ανά ομάδα.	ΝΑΙ		
20.	Η προτεινόμενη λύση θα πρέπει να παρέχει ένα πλαίσιο ελέγχου ταυτότητας χρησιμοποιώντας ένα reverse proxy.	ΝΑΙ		
21.	Η πλατφόρμα δεν θα πρέπει να στηρίζεται στην υιοθέτηση proprietary SDKs για την υποστήριξη νέων Authentication Providers	ΝΑΙ		
22.	Η πλατφόρμα να προσφέρει secure REST API	ΝΑΙ		
23.	Η πλατφόρμα πρέπει να παρέχει τη δυνατότητα σε έναν χρήστη να ξεκινήσει χειροκίνητα μια αίτηση πρόσβασης ή ενός δικαιώματος πρόσβασης μέσω μιας διεπαφής χρήστη. Η διεπαφή πρέπει να είναι φιλική προς τον χρήστη και να τον διευκολύνει στην αίτηση δικαιωμάτων πρόσβασης.	ΝΑΙ		
24.	Η πλατφόρμα θα πρέπει να παρέχει τη δυνατότητα delegation στη διαδικασία έγκρισης δικαιωμάτων πρόσβασης.	ΝΑΙ		
25.	Η πλατφόρμα θα έχει τη δυνατότητα να παρέχει, να ενεργοποιεί/απενεργοποιεί, να	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	πιστοποιεί και να συνδυάζει ταυτότητες, προσβάσεις και δικαιώματα σε πολλαπλά LDAP (ActiveDirectory).			
26.	Η προσφερόμενη λύση να μπορεί να ενσωματωθεί (integrate) με άλλες λύσεις του ίδιου κατασκευαστή συμπεριλαμβανομένων των SIEM, DatabaseMonitoring, PAM, UBA με απώτερο σκοπό την βέλτιστη άμυνα σε πιθανές επιθέσεις.	ΝΑΙ		

7.2.1.3 Παροχή υπηρεσιών ανάκαμψης από καταστροφή & λήψης αντιγράφων ασφαλείας (disaster recovery as a service & data backup as a service)

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
Γενικές Προδιαγραφές Παρόχου Δημοσίου Υπολογιστικού Νέφους				
1.	Το τμήμα Δημοσίου Υπολογιστικού Νέφους (Public Cloud) της προσφερόμενης λύσης θα πρέπει να παρέχει υπηρεσίες φιλοξενίας τύπου Cloud/Hosting, με υπηρεσίες υποδομής ως υπηρεσία (IaaS) και πλατφόρμας ως υπηρεσία (PaaS) από έναν πάροχο Δημοσίου Υπολογιστικού Νέφους.	ΝΑΙ		
2.	Η Αναθέτουσα Αρχή θα μπορεί να επιλέξει σε ποια γεωγραφική περιοχή (region) θα φιλοξενηθούν οι επιλεγόμενες υπηρεσίες.	ΝΑΙ		
3.	Ο πάροχος θα πρέπει να μπορεί να διαθέτει τις υπηρεσίες του από δύο τουλάχιστον γεωγραφικές περιοχές (regions), εντός Ευρωπαϊκής Ένωσης, με ελάχιστη απόσταση 500 χιλιομέτρων μεταξύ τους, τα οποία θα μπορούν να χρησιμοποιηθούν για την υλοποίηση υπηρεσιών που απαιτούν τον ύψιστο βαθμό υψηλής διαθεσιμότητας με χαρακτηριστικά ανάνηψης από καταστροφή (Disaster Recovery). Να αναφερθούν οι χώρες φιλοξενίας.	ΝΑΙ		
4.	Το τμήμα του δημοσίου υπολογιστικού νέφους (Public Cloud) της προσφερόμενης λύσης θα επιτρέπει τη διαμόρφωση υπηρεσιών υψηλής διαθεσιμότητας (high availability) και ανάκαμψης από καταστροφή (Disaster Recovery).	ΝΑΙ		
5.	Απαιτείται η ύπαρξη μηχανισμού παρακολούθησης και ελέγχου της κατάστασης (health) των	ΝΑΙ		



Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	χρησιμοποιούμενων πόρων σε συνάρτηση με την κατάσταση της υποδομής του παρόχου. Ο μηχανισμός να διαθέτει δυνατότητα μηχανισμού αποστολής ειδοποιήσεων κατά μόνος ή σε ομάδες, email, webhook βάσει κανόνων που τίθενται από το διαχειριστή.			
6.	Οι όροι SLA των υπηρεσιών να είναι δημοσιευμένοι στην επίσημη ιστοσελίδα του παρόχου. Να αναφερθεί η σχετική ιστοσελίδα.	ΝΑΙ		
7.	Για λόγους διαφάνειας και ελέγχου συμμόρφωσης με τα παρεχόμενα επίπεδα SLA η τρέχουσα κατάσταση λειτουργίας του συνόλου των υπηρεσιών θα πρέπει να είναι δημόσια διαθέσιμη στο επίσημο ιστότοπο του παρόχου. Να αναφερθεί η σχετική ιστοσελίδα.	ΝΑΙ		
8.	Ο πάροχος να διαθέτει δωρεάν υπηρεσίες για τη συνολική διακυβέρνηση – governance των πόρων που θα αξιοποιηθούν από τον φορέα λειτουργίας. Κατ'ελάχιστο απαιτούνται: <ul style="list-style-type: none">• δυνατότητα οργάνωσης και ελέγχου πρόσβασης στο σύνολο πολλαπλών λογαριασμών και συνδρομών• δυνατότητα διαμόρφωσης και εφαρμογής πολιτικών χρήσης των υπολογιστικών πόρων που περιλαμβάνονται σε λογαριασμούς και στις συνδρομές• καθορισμός πολλαπλών προϋπολογισμών με καθορισμό ορίων στο επιθυμητό επίπεδο εφαρμογής (scope) πόρων και δυνατότητα ενημέρωσης διαχειριστών μέσω email• εποπτεία και ανάλυση τρεχουσών χρεώσεων, ιστορικών χρεώσεων και πρόβλεψη της εξέλιξης τους	ΝΑΙ		
9.	Ο πάροχος να διαθέτει εγγενή μηχανισμό παροχής προτάσεων χωρίς επιπλέον κόστος, για βελτιστοποίηση της χρήσης των χρησιμοποιούμενων πόρων, στους τοείς της ασφάλειας, της διαθεσιμότητας, των επιδόσεων καθώς και του κόστους αυτών, κατά τις βέλτιστες πρακτικές του παρόχου υπολογιστικού νέφους.	ΝΑΙ		
10.	Να παρέχεται από τον πάροχο του δημοσίου υπολογιστικού νέφους ελεύθερα	ΝΑΙ		

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	προσπελάσιμος επίσημος ιστότοπος με πληροφορίες, οδηγούς και εγχειρίδια χρήσης, ρυθμίσεις, συχνές ερωτήσεις και παραδείγματα κώδικα για το σύνολο των υπηρεσιών του. Να αναφερθεί η σχετική ιστοσελίδα.			
11.	Να παρέχεται δωρεάν εκπαιδευτικό υλικό μέσω ηλεκτρονικής μάθησης σε επίσημο ιστότοπο του παρόχου με ενότητες στους εκάστοτε τομείς των υπηρεσιών υπολογιστικού νέφους. Να αναφερθεί η σχετική ιστοσελίδα.	ΝΑΙ		
Κανονιστική Συμμόρφωση Παρόχου Δημοσίου Υπολογιστικού Νέφους				
12.	Πιστοποίηση σε ισχύ που να αποδεικνύει τη συμμόρφωση της λειτουργίας του παρόχου με το πρότυπο διασφάλισης ποιότητας ISO/IEC 9001:2015. Να κατατεθεί αντίγραφο της πιστοποίησης.	ΝΑΙ		
13.	Πιστοποίηση σε ισχύ που να αποδεικνύει τη συμμόρφωση της λειτουργίας του παρόχου με το πρότυπο ασφάλειας ISO/IEC 27001:2013. Να κατατεθεί αντίγραφο της πιστοποίησης.	ΝΑΙ		
14.	Πιστοποίηση σε ισχύ που να αποδεικνύει τη συμμόρφωση της λειτουργίας του παρόχου με το πρότυπο ασφάλειας πληροφοριακών ελέγχων ISO/IEC 27017:2015. Να κατατεθεί αντίγραφο της πιστοποίησης.	ΝΑΙ		
15.	Πιστοποίηση σε ισχύ που να αποδεικνύει τη συμμόρφωση της λειτουργίας του παρόχου με το πρότυπο διασφάλισης της προστασίας προσωπικών δεδομένων ISO/IEC 27018:2019. Να κατατεθεί αντίγραφο της πιστοποίησης.	ΝΑΙ		
16.	Πιστοποίηση σε ισχύ που να αποδεικνύει τη συμμόρφωση της λειτουργίας του παρόχου με το πρότυπο ιδιωτικότητας πληροφοριών ISO/IEC 27701:2019. Να κατατεθεί αντίγραφο της πιστοποίησης.	ΝΑΙ		
17.	Πιστοποίηση σε ισχύ που να αποδεικνύει τη συμμόρφωση της λειτουργίας του παρόχου με το πρότυπο διασφάλισης της επιχειρησιακής συνέχειας ISO/IEC 22301:2019. Να κατατεθεί αντίγραφο της πιστοποίησης.	ΝΑΙ		
18.	Πιστοποίηση σε ισχύ που να αποδεικνύει τη συμμόρφωση της λειτουργίας του παρόχου με το πρότυπο διαχείρισης υπηρεσιών	ΝΑΙ		

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	πληροφοριακού συστήματος ISO/IEC 20000-1:2018			
19.	Συμμόρφωση της υποδομής του παρόχου κατά ServiceOrganizationControls (SOC) 1,2 και 3. Να κατατεθούν τα τρία σχετικά reports.	NAI		
20.	Συμμόρφωση της υποδομής του παρόχου κατά Payment Card Industry (PCI) Data Security Standards (DSS) έκδοση 3.2.1 - Level 1 . Να κατατεθεί η σχετική βεβαίωση.	NAI		
21.	Η υποδομή του παρόχου δημοσίου υπολογιστικού νέφους να διαθέτει benchmark με πρακτικές και προτάσεις καθοδήγησης, από το CenterforInternetSecurity (CIS) για την προστασία συστημάτων πληροφορικής ανεπτυγμένα στο δημόσιο υπολογιστικό νέφος έναντι κυβερνο-απειλών. Να κατατεθεί το σχετικό benchmark.	NAI		
22.	Το marketplace του παρόχου δημοσίου υπολογιστικού νέφους να διαθέτει ενισχυμένα -hardened- templates εικονικών μηχανών από το CenterforInternetSecurity (CIS).	NAI		
23.	Συμμόρφωση της λειτουργίας του παρόχου με το Cloud Control Matrix (CCM) του Cloud Security Alliance (CSA), με τη μορφή του Consensus Assessments Initiative Questionnaire (CAIQ) στην έκδοση 3.1 ή μεταγενέστερη. Να κατατεθεί το σχετικό αποδεικτικό αυτοαξιολόγησης (self assessment).	NAI		
24.	Πιστοποίηση σε ισχύ που να αποδεικνύει τη συμμόρφωση της λειτουργίας του παρόχου με το πρότυπο CSA-STAR του CloudSecurityAlliance (CSA). Να κατατεθεί αντίγραφο της πιστοποίησης.	NAI		
25.	Συμμόρφωση της υποδομής του παρόχου κατά EN 301 549. Να κατατεθεί το σχετικό αποδεικτικό.	NAI		
26.	Οι υπηρεσίες του παρόχου θα πρέπει να είναι συμβατές με τον Κανονισμό (ΕΕ) 2016/679 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα (GDPR Regulation).	NAI		
27.	Ο Πάροχος του Δημόσιου Υπολογιστικού Νέφους θα πρέπει να είναι μέλος του EUDataCentresEnergyEfficiencyCoC σύμφωνα με την λίστα που δημοσιεύεται	NAI		

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	στον παρακάτω σύνδεσμο: https://e3p.jrc.ec.europa.eu/node/575			
28.	Να αναφερθούν άλλα στοιχεία και μέτρα που αναλαμβάνει ο πάροχος ως προς την ασφάλεια και την κανονιστική συμμόρφωση.	ΝΑΙ		
Προδιαγραφές των Υπηρεσιών Αποκατάστασης Καταστροφών Παρόχου Δημοσίου Υπολογιστικού Νέφους				
29.	Υπηρεσία εξυπηρέτησης εγγενών φορτίων τεχνολογίας VMware με υποστήριξη τεχνολογιών vCenterServer, vSAN, vSphere και NSX-T, στην υποδομή του παρόχου υπολογιστικού νέφους. Ο Πάροχος να αποτελεί εγκεκριμένο προμηθευτή VMwareCloud τεχνολογιών.	ΝΑΙ		
30.	Παροχή μηνιαίου SLA για την υπηρεσία εξυπηρέτησης εγγενών φορτίων τεχνολογίας VMware, τουλάχιστον 99.9%.	ΝΑΙ		
31.	Η υπηρεσία εξυπηρέτησης εγγενών φορτίων τεχνολογίας VMware να προσφέρει υψηλό επίπεδο ασφάλειας και προστασίας δεδομένων των χρηστών, με δυνατότητες Role-BasedAccessControl και αυθεντικοποίησης μέσω SingleSignOn, αλλά και κρυπτογράφησης των καταχωρούμενων δεδομένων.	ΝΑΙ		
32.	Να προσφέρεται η δυνατότητα δικτύωσης στο περιβάλλον της υπηρεσίας εξυπηρέτησης εγγενών φορτίων τεχνολογίας VMware, τόσο από την τοπική υποδομή όσο και από το περιβάλλον υπολογιστικού νέφους.	ΝΑΙ		
33.	Να προσφέρεται η δυνατότητα ανάκαμψης από καταστροφή υφιστάμενης υποδομής VMware με χρήση VMwareSiteRecoveryManager (SRM) στην υπηρεσία εξυπηρέτησης εγγενών φορτίων τεχνολογίας VMware στο περιβάλλον υπολογιστικού νέφους μέσω αποκλειστικού κυκλώματος διασύνδεσης.	ΝΑΙ		
34.	Να προσφέρεται υπηρεσία αποκατάστασης φορτίων as-a-service από τον Πάροχο του Δημοσίου Υπολογιστικού Νέφους.	ΝΑΙ		
35.	Ο πάροχος της προσφερόμενης λύσης να αναφέρεται στη λίστα Leaders του φορέα αξιολόγησης Gartner στην κατηγορία DisasterRecoveryasaService (DRaaS).	ΝΑΙ		
36.	Μέσω της προσφερόμενης λύσης, να προσφέρεται προστασία υπολογιστικών	ΝΑΙ		

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	συστημάτων από καταστροφή μέσω συνεχούς replication, διαδικασία μετάπτωσης μετά καταστροφή καθώς και επανάκαμψης και επαναλειτουργίας.			
37.	Να προσφέρεται η δυνατότητα αποκατάστασης καταστροφών για τις εικονικές μηχανές που λειτουργούν σε περιβάλλον εικονικοποίησης VMware, vSphere/vCenter έκδοσης τουλάχιστον 6.0, μέσω της αναπαραγωγής τους σε περιβάλλον δημοσίου υπολογιστικού νέφους του κατασκευαστή της προσφερόμενης λύσης.	ΝΑΙ		
38.	Να προσφέρεται η δυνατότητα αποκατάστασης καταστροφών για τις εικονικές μηχανές που λειτουργούν σε περιβάλλον εικονικοποίησης Hyper-V έκδοσης τουλάχιστον 2012 R2, μέσω της αναπαραγωγής τους σε περιβάλλον δημοσίου υπολογιστικού νέφους του κατασκευαστή της προσφερόμενης λύσης.	ΝΑΙ		
39.	Να προσφέρεται η δυνατότητα αποκατάστασης καταστροφών για τους φυσικούς διακομιστές Linux και Windows, που λειτουργούν σε περιβάλλον τοπικής υποδομής μέσω της αναπαραγωγής τους, είτε σε μια δευτερεύουσα τοπική υποδομή είτε σε περιβάλλον δημοσίου υπολογιστικού νέφους του κατασκευαστή της προσφερόμενης λύσης.	ΝΑΙ		
40.	Να προσφέρεται η δυνατότητα αποκατάστασης καταστροφών για τις εικονικές μηχανές που λειτουργούν στο περιβάλλον δημοσίου νέφους του κατασκευαστή της προσφερόμενης λύσης μέσω της αναπαραγωγής τους σε μια δευτερεύουσα περιοχή του δημοσίου υπολογιστικού νέφους.	ΝΑΙ		
41.	Παροχή μηνιαίου SLA για την υπηρεσία αποκατάστασης φορτίων από τοπική υποδομή στο περιβάλλον δημοσίου υπολογιστικού νέφους, εντός 2 ωρών.	ΝΑΙ		
42.	Κατά την προστασία των εικονικών, η διαδικασία του replication να μην επηρεάζει τα πρωτότυπα δεδομένα.	ΝΑΙ		
43.	Να προσφέρεται η δυνατότητα πραγματοποίησης δοκιμαστικής αποκατάστασης καταστροφών, χωρίς να	ΝΑΙ		

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	προκαλούνται ανεπιθύμητες επιπτώσεις στις εφαρμογές και τα δεδομένα του Οργανισμού.			
44.	Να προσφέρεται η δυνατότητα πραγματοποίησης δοκιμαστικής αποκατάστασης καταστροφών, τόσο σε κάποια προγραμματισμένη χρονική στιγμή, όσο και σε κάποια η οποία δεν έχει προκαθοριστεί.	ΝΑΙ		
45.	Να προσφέρεται η δυνατότητα σχεδιασμού και παραμετροποίησης των σχεδίων αποκατάστασης από καταστροφή από τον Οργανισμό, καθώς και ομαδοποίησης και προτεραιοποίησης της αποκατάστασης των εφαρμογών στα σχέδια αυτά. Επιπλέον, να είναι δυνατή η ενσωμάτωση της προσφερόμενης λύσης με εξειδικευμένα για την εκάστοτε εφαρμογή σενάρια αποκατάστασης καταστροφών.	ΝΑΙ		
46.	Κατά την προστασία των εικονικών μηχανών να προσφέρεται η δυνατότητα applicationconsistent σημείων ανάκαμψης.	ΝΑΙ		
47.	Να προσφέρεται η δυνατότητα replication κατ'ελάχιστον για τις παρακάτω εφαρμογές τοπικής υποδομής: <ul style="list-style-type: none"> • Microsoft Active Directory • IIS • SQL • SharePoint υποστηρίζοντας τους εγγενείς μηχανισμούς υψηλής διαθεσιμότητας.	ΝΑΙ		
48.	Η προσφερόμενη λύση να διαθέτει παραμετροποίηση δικτυακών ρυθμίσεων των προστατευόμενων εικονικών μηχανών, καθώς και συνεργασία με δικτυακές υπηρεσίες του παρόχου υπολογιστικού νέφους.	ΝΑΙ		
49.	Ο πάροχος δημοσίου υπολογιστικού νέφους να προσφέρει κανάλι πρόσθετων επιλογών τύπου Marketplace, μέσω του οποίου να προσφέρονται εξειδικευμένες λύσεις αποκατάστασης καταστροφών από αντίστοιχους επίσημους συνεργάτες και κατασκευαστές λογισμικού.	ΝΑΙ		

7.2.1.4 Λύση δημιουργίας αντιγράφων ασφαλείας σε ταινίες με PhysicalAirGap – TrueAirGap 1.960PB χωρητικότητα

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	ΓΕΝΙΚΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ			
1.	Να προσφερθεί λύση προστασίας δεδομένων Physical Air Gap. Η λύση θα περιλαμβάνει δημιουργία επιπλέον αντιγράφων προστασίας δεδομένων σε σύστημα Tape Library και αποθήκευση σε κασέτες LTO	ΝΑΙ		
2.	Η λύση θα περιλαμβάνει λειτουργία κρυπτογράφησης δεδομένων	ΝΑΙ		
3.	Η λύση θα πρέπει να είναι συμβατή με το υπάρχον λογισμικό αντιγράφων ασφαλείας	ΝΑΙ		
4.	Η λύση θα περιλαμβάνει δύο (2) εξυπηρετητές για την υλοποίηση της λειτουργίας Physical Air Gap	ΝΑΙ		
5.	Να προσφερθεί εξωτερική συσκευή λήψης αντιγράφων ασφαλείας τύπου Tape Library	ΝΑΙ		
6.	Συνολικός αριθμός προσφερόμενων μονάδων	≥ 1		
7.	Εγκατάσταση σε υπάρχον rack cabinet 19"	ΝΑΙ		
8.	Ύψος μονάδας σε Rack Units	$\leq 12U$		
	ΤΕΧΝΙΚΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ			
9.	Αριθμός υποστηριζόμενων οδηγών ταινίας	≥ 12		
10.	Συνολικός αριθμός υποστηριζόμενων οδηγών ταινίας μετά από επέκταση	≥ 20		
11.	Αριθμός προσφερόμενων οδηγών ταινίας	≥ 12		
12.	Χωρητικότητα σε tape cartridges (slots)	≥ 200		
13.	Μέγιστος υποστηριζόμενος αριθμός tape cartridges (slots) μετά από επέκταση	≥ 270		
14.	Μέγιστη χωρητικότητα cartridge χωρίς συμπίεση (native)	≥ 12 TB ή ανώτερο		
15.	Τύπος Media	LTO8 ή ανώτερο		
16.	Ταχύτητα διαμεταγωγής δεδομένων ανά drive χωρίς συμπίεση (native)	≥ 300 MB/s ή ανώτερο		
17.	Fibre Channel διασύνδεση	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	ΓΕΝΙΚΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ			
18.	Ταχύτητα interface διασύνδεσης	≥ 8Gbps		
19.	Εφεδρικό τροφοδοτικό	ΝΑΙ		
20.	Να συνοδεύεται από αποθηκευτικά μέσα (LTO 8 cartridges)	≥ 180		
21.	Τα αποθηκευτικά μέσα θα συνοδεύονται από ετικέτες γραμμωτού κώδικα (bar code) συμβατές με το tape library	ΝΑΙ		
22.	Απαιτούμενος αριθμός Cleaning Cartridge	≥ 1		
23.	Διαχείριση του συστήματος με διεπαφή Web με πληροφορίες όπως κατάσταση βιβλιοθήκης, διαγνωστικά λειτουργίας, ρυθμίσεις καθώς και αναβάθμιση firmware	ΝΑΙ		
24.	Τα τμήματα που συνθέτουν τον εξοπλισμό πρέπει να ικανοποιούν το πρότυπο CE και ο κατασκευαστής το ISO 9001.	ΝΑΙ		
25.	Η εγγύηση του συστήματος αποθήκευσης θα πρέπει να προσφερθεί από τον κατασκευαστή για περίοδο 3 ετών με κάλυψη 24 x 7	ΝΑΙ		

7.2.1.5 Λύση δημιουργίας αντιγράφων ασφαλείας σε δίσκο Backup με Logical Air Gap για το 50% της χωρητικότητας

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	ΓΕΝΙΚΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ			
1.	Να προσφερθεί λύση προστασίας δεδομένων Logical Air Gap, πλήρως συμβατή με τα υπάρχοντα συστήματα αποθήκευσης δεδομένων SAN Storage (Block) IBM FlashSystem της ΓΤΠΣΔΔ, για την προστασία των παραγωγικών δεδομένων από Cyber attacks, ransomware, malware, corruption κτλ	ΝΑΙ		
2.	Με την προτεινόμενη λύση Logical Airgap απαιτείται να προστατευθούν παραγωγικά volumes που φιλοξενούν συστήματα (VMs, DBs, κτλ) με την υλοποίηση αντιγράφων ασφαλείας των volumes αυτών, τα οποία δεν θα μπορούν να διαγραφούν ή να αλλάξουν (space efficient immutable point in time image copies)	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	ΓΕΝΙΚΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ			
3.	Το μοντέλο και τα βασικά τμήματα του συστήματος θα πρέπει να βρίσκονται σε παραγωγή από τον κατασκευαστή τους την χρονική στιγμή υποβολής της προσφοράς. Δηλαδή δεν πρέπει να έχει σταματήσει η παραγωγή τους ή να βρίσκονται στην κατάσταση End Of Life.	ΝΑΙ		
4.	Να παρασχεθεί υψηλή διαθεσιμότητα σε επίπεδο ελεγκτών δίσκων, τροφοδοτικών, ανεμιστήρων κτλ.	ΝΑΙ		
5.	Να προσφερθεί λύση προστασίας δεδομένων Logical Air Gap για την προστασία παραγωγικών δεδομένων της τάξεως των 800TB και υποθέτοντας 1 ημερήσιο copy με 7 μέρες retention. Ο υπολογισμός της χωρητικότητας να γίνει με average daily change rate 5%.	ΝΑΙ		
6.	Στην χωρητικότητα Logical Air gap θα πρέπει να συμπεριληφθεί και ο χώρος που θα απαιτηθεί για τον έλεγχο των αντιγράφων ασφαλείας (recovery space) πριν την επαναφορά τους (restoration)	ΝΑΙ		
7.	Στην χωρητικότητα Logical Air gap θα πρέπει να συμπεριληφθεί και ο χώρος που θα απαιτηθεί στην περίπτωση που τα volumes γίνουν encrypt από τυχόν malware (στην περίπτωση αυτή ο υπολογισμός της χωρητικότητας θα γίνει υποθέτοντας ότι το τελευταίο backup θα είναι full backup)	ΝΑΙ		
8.	Να αναφερθεί η προσφερόμενη ωφέλιμη χωρητικότητα Logical AirGap μετά από υλοποίηση RAID6	ΝΑΙ		
9.	Τα αντίγραφα ασφαλείας των παραγωγικών volumes θα είναι isolated (δεν θα είναι ορατά και δεν θα γίνονται mount απευθείας από τους hosts)	ΝΑΙ		
10.	Τα αντίγραφα ασφαλείας των παραγωγικών volumes θα αποθηκεύονται σε δίσκους τεχνολογίας SSD για γρήγορη αποθήκευση, έλεγχο και επαναφορά τους όταν αυτό απαιτηθεί	ΝΑΙ		
11.	Για την ταχύτερη επαναφορά των αντιγράφων ασφαλείας είναι επιθυμητή η αποθήκευση τους στο ίδιο σύστημα αποθήκευσης δεδομένων σε	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	ΓΕΝΙΚΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ			
	απομονωμένο – isolated “logical Air Gap” περιβάλλον			
12	Θα πρέπει να παρέχεται πλήρης αυτοματοποίηση της διαδικασίας παραγωγής των αντιγράφων ασφαλείας σε προκαθορισμένα χρονικά διαστήματα καθώς και της διαδικασίας επαναφοράς τους	ΝΑΙ		
13	Η λύση θα πρέπει να παρέχει περιβάλλον διαχείρισης που θα παρέχει τις παρακάτω δυνατότητες : <ul style="list-style-type: none"> - Πλήρης προγραμματισμός της εκτέλεσης των αντιγράφων ασφαλείας (παραμετροποίηση της συχνότητας και της διάρκειας - backup retention) - Απεικόνιση των backup time points για προκαθορισμένα παραγωγικά volumes ή volume groups. - Δυνατότητα αυτοματοποίησης της εκτέλεσης διαδικασίας recovery και restoration των αντιγράφων ασφαλείας 	ΝΑΙ		
14	Η προτεινόμενη λύση θα πρέπει να υποστηρίζει έως 512 αντίγραφα ασφαλείας ανά volume group	ΝΑΙ		
15	Η λύση θα πρέπει να υποστηρίζει συνεργασία με λύσεις λογισμικού προληπτικής ανίχνευσης των κυβερνοεπιθέσεων	ΝΑΙ		
16	Η προτεινόμενη λύση δεν θα βασίζεται σε λύσεις που περιλαμβάνουν λήψη αντιγράφων ασφαλείας σε backup appliances, replication σε άλλα συστήματα κ.λ.π.	ΝΑΙ		
17	Η λύση θα πρέπει να υποστηρίζει τον ορισμό ρόλων χρηστών οι οποίοι ανάλογα με τον ρόλο τους θα μπορούν να ορίζουν τις πολιτικές backup, να δημιουργούν τα αντίγραφα ασφαλείας, να εκτελούν εργασίες recovery και restoration κ.λ.π.	ΝΑΙ		
18	Τα τμήματα που συνθέτουν τον εξοπλισμό πρέπει να ικανοποιούν κατ’ ελάχιστο τα πρότυπα CE και ο κατασκευαστής το ISO 9001.	ΝΑΙ		
19	Η εγγύηση του συστήματος αποθήκευσης θα πρέπει να προσφερθεί από τον κατασκευαστή για περίοδο 3 ετών με κάλυψη 24 x 7	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	ΓΕΝΙΚΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ			
20	Για την εγκατάσταση του συστήματος αποθήκευσης οι υπηρεσίες που αφορούν εγκατάστασης και παραμετροποίησης θα πρέπει να προσφερθούν από τον κατασκευαστή.	ΝΑΙ		
	ΤΕΧΝΙΚΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ			
21	Να προσφερθεί λύση παρακολούθησης και διαχείρισης περιστατικών ασφάλειας η οποία θα είναι πλήρως συμβατή με τη λύση προστασίας δεδομένων Logical Air Gap και με τα υπάρχοντα συστήματα αποθήκευσης δεδομένων SAN Storage (Block) IBM FlashSystem.	ΝΑΙ		
22	Η προσφερόμενη λύση θα συλλέγει logs, θα τα κανονικοποιεί, θα τα συσχετίζει με κανόνες ώστε να παράγει alerts σχετικά με περιστατικά ασφαλείας.	ΝΑΙ		
23	Ρυθμός συλλογής δεδομένων καταγραφής από τα υπό παρακολούθηση συστήματα	≥500 Events per Second		
24	Η προσφερόμενη λύση θα συλλέγει logs από τα συστήματα αποθήκευσης και από τα αντίστοιχα διαχειριστικά εργαλεία των συστημάτων αυτών.	ΝΑΙ		
25	Η λύση θα αναλύει τα παραπάνω Logs για τον εντοπισμό περιστατικών ασφάλειας και θα εκτελεί ενέργειες για την προστασία των δεδομένων.	ΝΑΙ		
26	Η προσφερόμενη λύση θα πρέπει να εγκατασταθεί σε εξειδικευμένη φυσική συσκευή (hardware appliance), ικανή να διαχειριστεί τον αριθμό των logs που θα παράγουν τα ως άνω συστήματα.	ΝΑΙ		
27	Η προσφερόμενη λύση να κατατάσσεται στους leaders του Gartner Magic Quadrant για πάνω από 11 χρόνια.	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	ΓΕΝΙΚΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ			
28	Η προσφερόμενη λύση θα είναι υπό τη μορφή all-in-one και θα εκτελεί τις παρακάτω λειτουργίες: <ul style="list-style-type: none"> - Σύστημα κεντροκοιμήμενης διαχείρισης όλων των υποσυστημάτων της λύσης - Σύστημα επεξεργασίας των γεγονότων ασφαλείας - Συστήματα συλλογής των γεγονότων καταγραφής 	ΝΑΙ		
29	Η προτεινόμενη λύση να διαθέτει ενσωματωμένο σύστημα User Behavior Analysis. Να υποστηρίζονται κατ' ελάχιστον τα απαιτούμενα χαρακτηριστικά: <ul style="list-style-type: none"> - Δείκτης επικινδυνότητας ανά χρήστη - Λίστα παρακολούθησης χρηστών - Dashboard - Δυναμική και στατική παραμετροποίηση του δείκτη επικινδυνότητας - Use Cases βασισμένα στην συμπεριφορά του χρήστη 	ΝΑΙ		
30	Η προτεινόμενη λύση να διαθέτει ενσωματωμένο σύστημα Machine Learning	ΝΑΙ		

7.2.1.6 Λύση προστασίας ηλεκτρονικού ταχυδρομείου Mail Security - 20.000 σταθμούς εργασίας

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
1.	Η λύση θα πρέπει να παρέχει μηχανισμό αποτροπής emails που περιέχουν κακόβουλα συνημμένα αρχεία είτε γνωστά είτε μηδενικού χρόνου (0-day).	ΝΑΙ		
2.	Η λύση θα πρέπει να ελέγχει emails τα οποία περιλαμβάνουν συνημμένα αρχεία και να τα παραδίδει σε πραγματικό χρόνο στο χρήστη σε καθαρή μορφή, από όπου έχει αφαιρεθεί οποιοδήποτε κακόβουλο περιεχόμενο (file scrubbing).	ΝΑΙ		
3.	Η λύση θα πρέπει να παρέχει μηχανισμό αποτροπής emails που έχουν σκοπό την παραπλάνηση του χρήστη μέσω ηλεκτρονικού "ψαρέματος" (anti-phishing).	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
4.	Η λύση θα πρέπει να παρέχει μηχανισμό ελέγχου και αποτροπής κακόβουλων emails που περιλαμβάνουν συνδέσμους (URLs) σε πραγματικό χρόνο.	ΝΑΙ		
5.	Η λύση θα πρέπει να τροποποιεί τους συνδέσμους (URLs) για την προστασία των χρηστών και να ελέγχει κατά πόσο είναι ασφαλείς κάθε φορά που κάποιος χρήστης τους ακολουθεί.	ΝΑΙ		
6.	Η λύση θα πρέπει να απαγορεύει στους χρήστες να ακολουθήσουν κάποιον κακόβουλο σύνδεσμο (URL) με δυνατότητα παράκαμψης της λειτουργίας αν το ορίζει η πολιτική του οργανισμού.	ΝΑΙ		
7.	Η λύση θα πρέπει να βάζει τα κακόβουλα emails σε καραντίνα με σκοπό να μην παραδίδονται στους χρήστες.	ΝΑΙ		
8.	Σε περίπτωση που ένα email μπαίνει σε καραντίνα, θα πρέπει να υπάρχει δυνατότητα ενημέρωσης του χρήστη.	ΝΑΙ		
9.	Η λύση θα πρέπει να ελέγχει τα εισερχόμενα emails καθώς και τα emails που αποστέλλονται εσωτερικά, μεταξύ των χρηστών του οργανισμού για την αποφυγή μετάδοσης κάποιας πιθανής μόλυνσης μεταξύ των χρηστών.	ΝΑΙ		
10.	Η λύση θα πρέπει να ανιχνεύει και να αποτρέπει περιπτώσεις μίμησης τρίτων οργανισμών (brand impersonation) ή χρηστών του οργανισμού τον οποίο προστατεύει (user/nickname impersonation).	ΝΑΙ		
11.	Η λύση θα πρέπει να παρέχει μηχανισμό ελέγχου και αποτροπής απώλειας ευαίσθητων δεδομένων (DLP).	ΝΑΙ		
12.	Η λύση θα πρέπει να παρέχει δυνατότητα επιβολής διαφορετικής πολιτικής ασφαλείας σε διαφορετικά τμήματα ενός οργανισμού.	ΝΑΙ		
13.	Η λύση θα πρέπει να παρέχει λεπτομερείς αναφορές και στατιστικά από όλες τις λειτουργίες για κάθε περιστατικό.	ΝΑΙ		
14.	Η λύση θα πρέπει να παρέχει τη δυνατότητα εξαγωγής των logs για διαχείριση και συσχέτισμό από κεντρικό σύστημα διαχείρισης ασφαλείας.	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
15.	Η λύση θα πρέπει να παρέχει γενικές αναφορές οι οποίες θα μπορούν να είναι συγκεντρωτικές και διαδραστικές, ώστε να παρέχουν χρήσιμες πληροφορίες στο διαχειριστή για όλες τις λειτουργίες ασφαλείας, χωρίς να χρειάζεται περεταίρω συσχετισμός των γεγονότων και αναζήτηση σε raw logs.	ΝΑΙ		
16.	Η λύση θα πρέπει να παράγει αυτόματα εβδομαδιαίες αναφορές οι οποίες θα αναπαριστούν τα κυριότερα περιστατικά ασφαλείας με γραφικό τρόπο και θα υπάρχει η δυνατότητα να αποστέλλονται αυτόματα ως email στον/στους διαχειριστή/ες.	ΝΑΙ		
17.	Η λύση θα πρέπει να παρέχει δυνατότητα αυτόματης ενεργοποίησης χωρίς την απαίτηση δημιουργίας κανόνων χειροκίνητα από το διαχειριστή στο domain.	ΝΑΙ		
18.	Η διαχείριση όλων των πολιτικών ασφαλείας θα πρέπει να γίνεται από το ίδιο διαχειριστικό περιβάλλον.	ΝΑΙ		

7.2.1.7 Λύση Endpoint Detection and Response - 20.000 σταθμούςεργασίας

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
1.	Η ζητούμενη πλατφόρμα πρέπει να αποτελεί μια ολοκληρωμένη λύση η οποία να εξασφαλίζει την κεντρική παρακολούθηση και διαχείριση.	ΝΑΙ.		
2.	Το σύστημα να βασίζεται σε λογισμικό που να παρέχεται και SaaS	ΝΑΙ		
3.	Αριθμός υποστηριζόμενων τελικών σημείων	>=20.000		
4.	Η προσφερόμενη λύση θα μπορεί να λειτουργήσει σε απομονωμένο air-gapped περιβάλλον προσφέροντας το ίδιο επίπεδο ανίχνευσης και προστασίας	ΝΑΙ		
5.	Η προσφερόμενη λύση θα επιτρέπει την απεγκατάσταση του agent στο endpoint απομακρυσμένα.	ΝΑΙ		
6.	Ο agent θα υποστηρίζεται κατ' ελάχιστο στα παρακάτω λειτουργικά:	Να αναφερθεί		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Windows 7 (SP1), 8, 8.1, 10, 10-POS Windows server 2008R2 (SP2), 2012, 2016, 2019 Linux Ubuntu 16, 18-Centos, 7-Debian 8, 10-RedHat 7, Mint 18+ MacOS Sierra+ onwards Android 4.2+ onwards			
7.	Η προσφερόμενη λύση θα έχει τη δυνατότητα ανίχνευσης κακόβουλου λογισμικού (malware) βάσει ανάλυσης συμπεριφοράς χωρίς τη χρήση υπογραφών.	ΝΑΙ		
8.	Η προσφερόμενη λύση θα προσφέρει λειτουργία antivirus ή θα μπορεί να συνυπάρξει με υπάρχουσα λύση antivirus.	ΝΑΙ		
9.	Για την ανίχνευση απειλών θα υλοποιούνται στο endpoint πάνω από εβδομήντα (70) behavioral models.	ΝΑΙ		
10.	Η προσφερόμενη λύση θα έχει δυνατότητα ομαδοποίησης για να διαχωρίζει διαφορετικά τελικά σημεία και να εφαρμόζει πολιτικές βάσει ομάδων.	ΝΑΙ		
11.	Ο agent θα πρέπει να υποστηρίζει (για τα λειτουργικά συστήματα που επιτρέπεται) τη δυνατότητα παρακολούθησης του λειτουργικού σε επίπεδο hypervisor ώστε να μην είναι δυνατή ο εντοπισμός και η απενεργοποίηση του agent σε περίπτωση επίθεσης.	ΝΑΙ		
12.	Η προσφερόμενη λύση να έχει κατ'ελάχιστο δυνατότητα ανίχνευσης των κακόβουλων συμπεριφορών: Keylogging, Dynamic Impersonation, Credential Harvesting, Kernel Exploits, Screen captures.	Να αναφερθεί		
13.	Η λύση δεν θα κάνει full logging, παρά μόνο αν παρουσιαστεί μία απειλή.	ΝΑΙ		
14.	Οι ανακτηθείσες εγκληματολογικές πληροφορίες (forensic information) από το τελικό σημείο θα προστατεύονται με κωδικό πρόσβασης και ο κωδικός πρόσβασης καθορίζεται από τον αναλυτή.	ΝΑΙ		
15.	Θα μπορεί να εμφανίζει behavioral tree που αποτελείται από την αλυσίδα επίθεσης,	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	επιλογές εξ αποστάσεως τερματισμού διαδικασίας, δημιουργία μαύρης λίστας και hunting για την ίδια διαδικασία εντός της υποδομής.			
16.	Θα παρέχει αντιστοίχιση MITRE στα συμβάντα που καταγράφονται.	ΝΑΙ.		
17.	Θα προσφέρει τη δυνατότητα απομόνωσης του τελικού σημείου από την κονσόλα διαχείρισης.	ΝΑΙ		
18.	Δυνατότητα scripting για τη δημιουργία νέων κανόνων και πολιτικών.	ΝΑΙ		
19.	Η προσφερόμενη λύση να υποστηρίζει αυτοματοποιημένη τεχνητή νοημοσύνη για τον εντοπισμό απειλών.	ΝΑΙ.		

7.2.1.8 Λύση που αφορά τον έλεγχο της πρόσβασης των εσωτερικών χρηστών στο Διαδίκτυο

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
1.	Η προσφερόμενη λύση θα πρέπει να είναι appliance ή software-based και να υποστηρίζει τη δυνατότητα εγκατάστασης σε εικονική υποδομή VMware, HyperV, KVM	ΝΑΙ		
2.	Η προσφερόμενη λύση θα πρέπει να παρέχει υπηρεσίες πιστοποίησης, εξουσιοδότησης και Λογιστικής (AAA) με βάση την ταυτότητα των χρηστών τους , συμμόρφωση με την πολιτική της εταιρίας και τον τύπο της συσκευής.	ΝΑΙ		
3.	Η εφαρμογή να προσφερθεί με άδεια για να καλύψει τουλάχιστον 20000 ταυτόχρονα συνδεδεμένες συσκευές	ΝΑΙ		
4.	Το λογισμικό θα πρέπει να χρησιμοποιεί ανοιχτά πρότυπα μέσω του πρωτοκόλλου IEEE 802.1x	ΝΑΙ		
5.	Δυνατότητα passive authentication, Easy Connect και 802.1x			
6.	Το λογισμικό θα πρέπει υποστηρίζει SAML			

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
7.	Το λογισμικό θα πρέπει υποστηρίζει TACACS+, TACACS+ proxy			
8.	Το λογισμικό θα πρέπει υποστηρίζει SecureSyslogRemoteLogging			
9.	Το λογισμικό θα πρέπει να αναγνωρίζει αυτόματα όλα τα είδη των δικτυακών συσκευών όπως desktops, laptops, smartphones, tablets, printers, ipphones, ipcameras κλπ.	NAI		
10.	Για την αναγνώριση αυτόματα όλων των συσκευών θα πρέπει να υποστηρίζονται τα ακόλουθα : netflow, DHCP, DNS, HTTP, Radius, NMAP, SNMP, AD			
11.	Αυτόματος εντοπισμός , αναφορά τοποθεσίας και έλεγχος οποιοδήποτε τύπου συστήματος που προσπαθεί να συνδεθεί στο δίκτυο, ανεξαρτήτως λειτουργικού συστήματος και είδους,	NAI		
12.	Η πιστοποίηση και πρόσβαση του τελικού χρήστη θα πρέπει να γίνεται ανεξάρτητα από λειτουργικά συστήματα ή τύπο IP δικτυακής συσκευής.	NAI		
13.	Να υπάρχει κεντρική διαχείριση της λύσης	NAI		
14.	Να υπάρχει διαδικασία onboarding και αυτόματης παραμετροποίησης μιας καινούργιας συσκευής.	NAI		
15.	Να αναφερθούν οι δυνατότητες του portal και οι αναλυτικές ενέργειες σύνδεσης μιας νέας συσκευής			
16.	Αυτόματη απεικόνιση και κεντρική εποπτεία της	NAI		
17.	Κατάσταση του δικτύου σχετικά με το ποιο σύστημα και τι είδους, αλλά και ποιος χρήστης είναι συνδεδεμένος			
18.	Τοποθέτηση των συστημάτων ανάλογα με την κατάσταση συμμόρφωσης τους σε πολλαπλά VLANs δυναμικά και βάσει της πολιτικής ασφαλείας καθώς και δυνατότητα downloadableaccess-list.	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
19.	Ο μηχανισμός καραντίνας θα πρέπει να απομονώνει αποτελεσματικά το μη συμμορφούμενο σύστημα από άλλα συστήματα και αναλόγως της πολιτικής να μπορεί να επικοινωνήσει μόνο με συγκεκριμένα συστήματα	ΝΑΙ		
20.	Ενοποίηση – συνεργασία με υποδομές MSActiveDirectory. Δυνατότητα σύνδεσης με πολλαπλά ActiveDirectorydomains που έχουν zerotrust μεταξύ τους.	ΝΑΙ		
21.	Το λογισμικό θα πρέπει υποστηρίζει ActiveDirectory, LDAP αλλά και internalDatabase			
22.	Καθορισμός πολιτικών ασφάλειας βάση των οποίων θα επιτρέπεται ή όχι η πρόσβαση σε συγκεκριμένα συστήματα. Να αναφερθούν αναλυτικά οι δυνατότητες πολιτικών Οι πολιτικές ασφάλειας θα πρέπει να παραμετροποιούνται βάσει του χρήστη/ομάδας ή ρόλου αλλά και Άλλων συνθηκών όπως είδος συσκευής, μέρα και ώρα, και τρόπο σύνδεσης στο δίκτυο	ΝΑΙ		
23.	Το λογισμικό θα πρέπει να υποστηρίζει internalCertificateAuthority			
24.	Το λογισμικό θα πρέπει να υποστηρίζει offlineCertificateProvisioning			
25.	Το λογισμικό θα πρέπει να υποστηρίζει CertificateProvisioning για VPNclients			
26.	Δυνατότητα integration με λύσεις Security Information and Event Management (SIEM) και ειδικότερα Qradar, Arcsight, RSA, Splunk			
27.	Δυνατότητα integration με λύση Next Generation Firewall ώστε να μπορεί να βάζει αυτόματα compromised endpoints σε καραντίνα			
28.	Το λογισμικό θα πρέπει να θέτει πολιτικές ανεξάρτητα με τον τρόπο σύνδεσης στο δίκτυο είτε είναι η σύνδεση είναι ενσύρματη, ασύρματη ή με τη χρήση VPN. Θα πρέπει να μπορούν να οριστούν	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	πολιτικές ανάλογα με τον τρόπο σύνδεσης ενός χρήστη.			
29.	Το λογισμικό θα πρέπει συνεργάζεται με CiscoASA για χρήση VPN και να υποστηρίζει ChangeofAuthorization			
30.	Το λογισμικό θα πρέπει να υποστηρίζει softwaredefinedsegmentation			
31.	Πρέπει να γίνεται συνεχώς αυτόματη ενημέρωση με νέα είδη συσκευών που θα χρησιμοποιεί η λύση. Η ενημέρωση θα πρέπει να γίνεται από διαπιστευμένη πηγή	NAI		
32.	Η προτεινόμενη λύση θα πρέπει να είναι εύκολα εφαρμόσιμη σε όλους τους χρήστες είτε είναι εσωτερικοί χρήστες είτε επισκέπτες. Να αναφερθεί η διαδικασία ένταξης νέων συστημάτων/χρηστών στο σύστημα	NAI		
33.	Καταγραφή γεγονότων και δημιουργία αναφορών. Να αναφερθούν οι δυνατότητες δημιουργίας αναφορών	NAI		
34.	Άμεση ενημέρωση του διαχειριστή για κάθε επιτυχημένη ή αποτυχημένη προσπάθεια καθώς και οι ενέργειες που πάρθηκαν ως αποτέλεσμα. Να αναφερθούν οι τρόποι ενημέρωση των χρηστών.	NAI		
35.	Υποστήριξη υψηλής διαθεσιμότητας	NAI		
36.	Δυνατότητα GuestSelfService - Portal για την εισαγωγή των επισκεπτών. Δυνατότητα Timebasedaccounts, για τη δημιουργία λογαριασμών με χρονική διάρκεια πρόσβασης.	NAI		
37.	Υποστήριξη Offline Portal Customization για το Guest Portal			
38.	Δυνατότητα εφαρμογής πολιτικών πρόσβασης των επισκεπτών καθώς και χρονικός περιορισμός στην πρόσβαση. Να αναφερθούν οι μηχανισμοί	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
39.	Δυνατότητα αναφορών ιστορικών και σε πραγματικό χρόνο για όλους τους χρήστες.	ΝΑΙ		
40.	Δυνατότητα πολλαπλών ρόλων για τους διαχειριστές με ποικίλους ρόλους και τρόπους πρόσβασης (i.e., NetworkAdmin, SecurityAdmin, HelpDesk, etc.)	ΝΑΙ		
41.	FIPS compliant	ΝΑΙ		
42.	Να προσφερθούν άδειες για 3 έτη	ΝΑΙ		

7.2.1.9 Λύση Ασφαλείας και προστασίας των χρηστών από απειλές του διαδικτύου (Web Security Gateway)

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
1.	Να προσφερθεί Σύστημα Ασφαλείας και προστασίας των χρηστών από απειλές του διαδικτύου (WebSecurityGateway)	Ναι		
	Τεχνικά χαρακτηριστικά			
2.	Η προσφερόμενη λύση να μπορεί να εγκατασταθεί σε υποδομή Vmware	ΝΑΙ		
3.	Να αναφερθεί Τύπος – Κατασκευαστής	ΝΑΙ		
4.	Η προσφερόμενη λύση θα πρέπει να υποστηρίζει τουλάχιστον 20000 χρήστες	ΝΑΙ		
5.	Η προσφερωμενη λύση πρέπει να ελέγχει την κίνηση HTTP, HTTPS και FTP από και προς το διαδίκτυο (Incoming&OutgoingWebtraffic), ανεξάρτητα από τις εφαρμογές που το χρησιμοποιούν. Να υποστηρίζει την inspection επιθεώρηση σε επίπεδο HTTP πρωτοκόλλου σε πραγματικό χρόνο (real-time).	ΝΑΙ		
6.	Η προσφερωμενη λύση να έχει τη δυνατότητα επιθεώρησης HTTPS πρωτοκόλλου.	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
7.	Η προσφερωμενη λύση να υποστηρίζει υπηρεσίες καταλόγου LDAP, ActiveDirectory κ.λ.π.	NAI		
8.	Δυνατότητα για τη δημιουργία και εφαρμογή πολιτικών ασφαλείας ανά: εφαρμογή, χρήστη (domainuser/group) και συνδυασμό χρήστη και εφαρμογής	NAI		
9.	Υποστήριξη λειτουργίας caching από το κάθε προσφερόμενο σύστημα	NAI		
10.	Υποστήριξη λειτουργίας TransparentProxy με χρήση πρωτοκόλλου WCCP, με την χρήση αρχείων proxgauto-config (PAC) από το κάθε προσφερόμενο σύστημα	NAI		
11.	Υποστήριξη δυνατότητας προσθήκης / φιλοξενίας αρχείων proxgauto-config (PAC) από το κάθε προσφερόμενο σύστημα	NAI		
12.	Η προσφερωμενη λύση να έχει ομαδοποιημένες κατηγορίες φίλτρων URL και ιστότοπων	NAI		
13.	Η προσφερωμενη λύση να υποστηρίζει αυτόματη ενημέρωση των φίλτρων URL και κατηγορίες ιστότοπων.	NAI		
14.	Δυνατότητα ενημέρωσης των φίλτρων URL και ένταξη ιστότοπων σε συγκεκριμένη κατηγορία, από τον διαχειριστή από το κάθε προσφερόμενο σύστημα	NAI		
15.	Χρήση διαφορετικών πολιτικών ασφαλείας ανά μέρα/ώρα από το κάθε προσφερόμενο σύστημα	NAI		
16.	Η προσφερωμενη λύση να κάνει υποστήριξη αυτόματης κατηγοριοποίησης ιστοσελίδων (real-time categorization) που δεν ανήκουν ήδη σε κάποια κατηγορία με βάση το περιεχόμενο τους	NAI		
17.	Η δυνατότητα άρνησης συνδέσεων σε επίπεδο πρωτοκόλλου ελέγχου μετάδοσης (TCPsession) να είναι αυτόματη όπως π.χ να βασίζεται σε τεχνικές "φίλτρων φήμης" (reputationfilters) από το κάθε προσφερόμενο σύστημα.	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Ο διαχειριστής να μπορεί να ρυθμίζει τον τρόπο συμπεριφοράς της συσκευής ανάλογα με την "φήμη".			
18.	Η προσφερωμενη λύση να υποστηρίζει τη δημιουργία πολλαπλών λιστών white/black (customURLcategories) από τον διαχειριστή.	NAI		
19.	Η προσφερωμενη λύση να υποστηρίζει την εφαρμογή πολιτικών ασφαλείας περιεχομένου σε επίπεδο διακινούμενων αρχείων (download και upload) βάσει του payload του αρχείου και όχι της κατάληψής του (filetypeextension) από κάθε ελεγχόμενη συσκευή	NAI		
20.	Η προσφερωμενη λύση να υποστηρίζει την επιθεώρηση και την απαγόρευση αποστολής αρχείων π.χ μέσω Webmail	NAI		
21.	Η προσφερωμενη λύση να υποστηρίζει αναγνώριση εφαρμογών WEB 2.0 και εφαρμογή διαφορετικής πολιτικής ανά εφαρμογή από κάθε ελεγχόμενη συσκευή	NAI		
22.	Θα πρέπει να υπάρχει δυνατότητα AntiVirus με δυνατότητα επιλογής ανάμεσα από διαφορετικούς κατασκευαστές.	NAI		
23.	Να αναφερθούν οι υποστηριζόμενοι κατασκευαστές.			
24.	Η προσφερωμενη λύση να υποστηρίζει την ταυτόχρονη λειτουργία διαφορετικών AntiVirus μηχανισμών. (Αρκεί να προσφερθεί τουλάχιστον ένας μηχανισμός antivirus).	NAI		
25.	Η προσφερωμενη λύση πρέπει να περιλαμβάνει ένα σύγχρονο σύστημα προστασίας από κακόβουλο λογισμικό με διάφορες υπηρεσίες φήμης και sandboxing για την εισερχόμενη κίνηση εκτός από τον AV μηχανισμό	NAI		
26.	Να υποστηρίζεται ο εντοπισμός zerodaythreat με χρήση sandboxing. Θα πρέπει να μπορούν να αναλυθούν μέχρι και 2000 διαφορετικά samples την ημέρα.	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
27.	Το κάθε προσφερόμενο σύστημα πρέπει να μπορεί να κάνει αποκρυπτογράφηση κίνησης τύπου ManInTheMiddle (MITM) με εγγενή αποκρυπτογράφηση TLS1.3 και 1.2.	NAI		
28.	Η προσφερωμενη λύση πρέπει να μπορεί να έχει τη δυνατότητα να ενσωματωθεί με υπηρεσίες απομόνωσης απομακρυσμένου προγράμματος περιήγησης (RBI) που βασίζονται σε σύννεφο, εάν απαιτηθεί στο μέλλον.	NAI		
29.	Η προσφερωμενη λύση πρέπει να έχει τη δυνατότητα να υλοποιηθεί με τους παρακάτω τρόπους χωρίς επιπλέον κόστος Explicit ή Transparentproxy: <ul style="list-style-type: none"> σε διάταξη εφεδρείας με χρήση load balancing Μηχανισμών (με WCCP ή explicit proxy λειτουργία) ή σε διάταξη λειτουργίας VRRP βασισμένη σε Active / Standby υλοποίηση εφεδρείας. 	NAI		
30.	Η προσφερωμενη λύση πρέπει να υποστηρίζει HTTP, HTTPS, FTP, SOCKSproxy	NAI		
31.	Η αδειοδότηση της προσφερωμενης λύσης πρέπει να επιτρέπει την επέκταση των πόρων proxy (το μέγεθος και τον αριθμό των εικονικών διακομιστών μεσολάβησης) χωρίς επιπλέον κόστος και αγορά άδειας	NAI		
32.	Η προσφερωμενη λύση Webproxy πρέπει να μπορεί να ενσωματωθεί με το παρεχόμενο σύστημα SOAR (XDR) για κεντρική διαχείριση πολλαπλών προϊόντων, αυτοματοποιημένη έρευνα απειλών και αυτοματοποιημένη απόκριση συμβάντων.	NAI		
33.	Η προσφερωμενη λύση πρέπει να κάνει έλεγχο του Bandwidth για ειδικούς τύπους περιεχομένου (streamingmedia)	NAI		
34.	Η προσφερωμενη λύση πρέπει να μπορεί να κάνει χρήση διαφορετικών πολιτικών ασφαλείας ανά μέρα/ώρα	NAI		
35.	Η προσφερωμενη λύση πρέπει να μπορεί να κάνει έλεγχο της πρόσβασης των χρηστών με χρήση time-quota και bandwidth-quota	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
36.	Η προσφερόμενη λύση NGFW, SOAR και WebProxy, προτείνεται να είναι του ίδιου κατασκευαστή ώστε να επιτρέπει την μέγιστη διαλειτουργικότητα	ΝΑΙ		
37.	Εγγύηση – Υπηρεσίες			
38.	Η προσφερόμενη λύση να συνοδεύεται από 3ετή εγγύηση (με δωρεάν συντήρηση του κατασκευαστή του για το λογισμικό).	ΝΑΙ		
39.	Να δοθούν τα σχετικά από τον κατασκευαστή αποδεικτικά στοιχεία, όταν αυτά γίνουν διαθέσιμα, και σε κάθε περίπτωση πριν την προσωρινή παραλαβή του έργου.			
40.	Τηλεφωνική υποστήριξη 24x7 κατά τη διάρκεια της εγγύησης	ΝΑΙ		
41.	Να συνοδεύεται από τις κατάλληλες άδειες 3 ετών, για συνεχείς ενημερώσεις όλου του λογισμικού.	ΝΑΙ		
42.	Εγκατάσταση, παραμετροποίηση και προσαρμογή του υπό προμήθεια εξοπλισμού στο δίκτυο	ΝΑΙ		
43.	Η προσφερόμενη τεχνική υποστήριξη (περιλαμβάνεται και η παροχή και εγκατάσταση νέων ενημερώσεων, αναβαθμίσεων λογισμικού, και drivers) θα παρέχεται από κατάλληλα πιστοποιημένα πρόσωπα από τον κατασκευαστή.	ΝΑΙ		
	Λύση κεντρικής διαχείρισης websecurity (συσκευή/appliance)			
	<i>Γενικά χαρακτηριστικά</i>			
44.	Ενιαία και εξειδικευμένη εφαρμογή κεντρικής διαχείρισης για την προσφερωμενη λύση proxy	ΝΑΙ		
45.	Εγκατάσταση σε υποδομή VM	ΝΑΙ		
	<i>Βασικές Λειτουργίες</i>			
46.	Κοινή διαχείριση των κανόνων ασφάλειας και αναφορών για την λύση websecurity	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
47.	Να έχει δυνατότητα κεντρικής διαχείρισης μέσω γραφικού περιβάλλοντος (GUI) όλων των virtual συσκευών websecurity	ΝΑΙ		
48.	Υποστήριξη Logging με δυνατότητα τοπικού φιλτραρίσματος και αποθήκευσης.	ΝΑΙ		
49.	Να υποστηρίζει ενσωματωμένο μηχανισμό παραγωγής αναφορών σε επίπεδο Χρήστη, URL φίλτρων, TopusageReports (Users/Filters/Malware κ.λ.π).	ΝΑΙ		
50.	Να υποστηρίζει ενσωματωμένο μηχανισμό παραγωγής αναφορών σχετικά με τη χρήση εύρους ζώνης (bandwidth) συνολικά και ανά χρήστη.	ΝΑΙ		
51.	Να υποστηρίζει ενσωματωμένο μηχανισμό παραγωγής αναφορών σχετικά με τον τύπο της δικτυακής κίνησης ενός χρήστη (OSILayerL4 trafficmonitoring)	ΝΑΙ		
52.	Κατά τη διάρκεια ενημέρωσης της συσκευής, οι ενεργοποιημένες υπηρεσίες να συνεχίζουν να λειτουργούν.	ΝΑΙ		
53.	Να διαθέτει ευέλικτο σχήμα αδειών για την μελλοντική αναβάθμιση των χαρακτηριστικών ή/και του αριθμού των υποστηριζόμενων χρηστών.	ΝΑΙ		
54.	Να προσφέρεται τεχνική υποστήριξη από τον κατασκευαστή 24x7,	≥ 3 χρόνια		
55.	Να συνοδεύεται από τις κατάλληλες άδειες 3 ετών , για συνεχείς ενημερώσεις όλων των βάσεων και του λειτουργικού για 20.000 χρήστες	ΝΑΙ		

7.2.2 Πίνακες Συμμόρφωσης Τμήματος 2 «Εξειδικευμένες λύσεις και υπηρεσίες ασφάλειας για την Η.ΔΙ.Κ.Α. Α.Ε.»

7.2.2.1 Λύση Διαβάθμισης και Σήμανσης Εγγράφων

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
1.	Οι endpointagents του Συστήματος Διαβάθμισης Δεδομένων, πρέπει να είναι συμβατοί με Λειτουργικά Συστήματα: Windows 10, WindowsServer 2008 R2,	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	2012, 2016, 2019 , , MacOS / X, AndroidEnterprise, IOS.			
2.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να καλύπτει χίλια (1.000) τερματικά του οργανισμού	ΝΑΙ		
3.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να έχει δυνατότητα να θέτει σήμανση σε έγγραφα της ακόλουθης μορφής: 1. ΣουίταMS Office (π.χ. Word, Excel, Power Point, Visio, Microsoft Project, OneNote). 2. Outlook email (π.χ. msg, pst, ost) 3.Αρχεία PDF 4. Αρχείακειμένου (π.χ. TXT, ASC, ANS, ACL, HTML, XML, ODM, OTT, INFO, PAP, PAGES) 5. Συμπιεσμένααρχεία (π.χ. ZIP, 7zip, RAR, WinRAR, BZip, Gzip, Tar, Bz2) 6. Αρχείαβίντεο (π.χ. mpg, mp4, amv, wmv, mov, avi, mkv) 7. Αρχείαήχου (π.χ. mp3, wma, wav, DVR-MS, WTV) 8. Αρχείαεικόνas (π.χ. JPEG, TIFF, GIF, BMP, PNG, AI, CDR, ADT, PSD, PUB) 9. Αρχείαβάσηςδεδομένων (π.χ. ACCDB, ADT, DB, MDB, MYD, MYI, ORA, SQL, SDF, sqlite, 10. Κρυπτογραφημένααρχεία (π.χ. ssh, pub, rpkr, cert, crt, der, p7b, PEM, PFX, AXX, EEA, TC, BPW, KDB, KDBX) 11. Άλλοιτύποιαρχείων (π.χ. CMD, BAT, JSP, PL, PHP, ASP, PYO, VBS)	ΝΑΙ		
4.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να διαβαθμίζει τα έγγραφα με τρόπο, ώστε η πληροφορία για το επίπεδο διαβάθμισης (π.χ. πληροφορίες μεταδεδομένων) να μην μπορεί να διαγραφεί ή τροποποιηθεί από τον απλό χρήστη.	ΝΑΙ		
5.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να επιβάλλει πολιτικές σχετικά με το αρχικό επίπεδο διαβάθμισης που θα έχει κάθε νέο έγγραφο (π.χ. οποιοδήποτε νέο έγγραφο δημιουργείται πρέπει να διαβαθμίζεται αυτόματα ως Εσωτερικό).	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
6.	Η πληροφορία για το επίπεδο διαβάθμισης πρέπει να ακολουθεί ένα διαβαθμισμένο έγγραφο κατά τη διάρκεια κάθε είδους μεταφοράς (π.χ. μέσω email, μέσω διαδικτύου, εφαρμογών cloud, μέσω FTP / SFTP, αντιγραφή σε οποιονδήποτε τύπο αφαιρούμενου μέσου, εάν κρυπτογραφεί και αποκρυπτογραφεί, σε περίπτωση συμπίεσης)	ΝΑΙ		
7.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να είναι σε θέση να επιβάλλει τουλάχιστον 4 διαφορετικά επίπεδα ταξινόμησης (π.χ. Δημόσιο, Εσωτερικό, Εμπιστευτικό και αυστηρά Εμπιστευτικό) και να έχει δυνατότητα να υποστηρίξει έως και πρακτικά απεριόριστα επίπεδα διαβάθμισης	ΝΑΙ		
8.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει επίσης να μπορεί να διαφοροποιεί και να επιβάλλει διαφορετικές πολιτικές σε διαφορετικά επίπεδα διαβάθμισης εγγράφων (υποκατάταξη) με βάση τα τμήματα του οργανισμού, όπως αποτυπώνονται στο κέντρικό κατάλογο χρηστών του οργανισμού (ActiveDirectory). Για παράδειγμα, θα μπορούσε να έχει ένα διαβαθμισμένο έγγραφο ως Εμπιστευτικό / Τμήμα Οικονομικών και άλλο έγγραφο, ως Εμπιστευτικό / Τμήμα εξυπηρέτησης κοινού, κ.λπ.	ΝΑΙ		
9.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να μπορεί να καθορίζει την πολιτική χρονικής διατήρησης ανάλογα με το επίπεδο διαβάθμισης και τον τύπο του εγγράφου	ΝΑΙ		
10.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να έχει δυνατότητες σάρωσης των εγγράφων και εντοπισμού χαρακτηριστικών σημείων του περιεχομένου π.χ. λέξεις-κλειδιά, regular expressions, περιεχόμενα λεξικών κ.λπ.	ΝΑΙ		
11.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να μπορεί να υποστηρίξει και να επιβάλλει διαφορετικές τεχνικές διαβάθμισης, όπως οι ακόλουθες:	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	<p>1. Χειροκίνητη Διαβάθμιση (π.χ. με ένα κλικ ενός κουμπιού, επιλέγοντας μεταξύ των 4 διαφορετικών επιπέδων και υπο-επιπέδων.</p> <p>2. Ημιαυτόματη ταξινόμηση (π.χ. με βάση το περιεχόμενο του εγγράφου για να δώσει κάποιες ενδείξεις στον χρήστη για το τι επίπεδο διαβάθμισης πρέπει να θέσει)</p> <p>Μαζική ταξινόμηση (Το εργαλείο πρέπει να ταξινομήσει όλα τα αρχεία σε έναν συγκεκριμένο folder με βάση το απαιτούμενο επίπεδο διαβάθμισης ή με βάση τη σάρωση περιεχομένου, π.χ. σε περίπτωση που ανακαλύπτει προσωπικά δεδομένα σε αυτό κ.λπ.)</p>			
12.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να έχει δυνατότητα ρύθμισης για το αν επιτρέπεται ή όχι η αλλαγή του επιπέδου διαβάθμισης από τους χρήστες (π.χ. αναβάθμιση ή υποβάθμιση).	ΝΑΙ		
13.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να δίνει την δυνατότητα αυτόματης διαβάθμισης εγγράφων κατά την αποθήκευση των εγγράφων .	ΝΑΙ		
14.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να εκτελεί μαζική σάρωσης εγγράφων που είναι αποθηκευμένα είτε σε τοπικούς servers είτε σε εφαρμογές αποθήκευσης εγγράφων στο νέφος και αυτόματης διαβάθμισης με βάση το περιεχόμενό τους. Η διαχείριση των σχετικών ενεργειών πρέπει να εκτελείται από την κεντρική κονσόλα του συστήματος.	ΝΑΙ		
15.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να μπορεί να σαρώνει μεγάλο όγκο εγγράφων ώστε να διαβαθμίσουν έγγραφα που έχουν παραχθεί στο παρελθόν και διατηρούνται στα πληροφοριακά συστήματα του ΔΕΔΔΗΕ.	ΝΑΙ		
16.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να εκτελεί αυτόματο καθορισμό των επιπέδων διαβάθμισης με βάση τον	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	εντοπισμό χαρακτηριστικών λέξεων και φράσεων στο περιεχόμενο των εγγράφων.			
17.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να εκτελεί αυτόματο καθορισμό των επιπέδων διαβάθμισης με βάση τον εντοπισμό σειρών χαρακτήρων που ακολουθούν συγκεκριμένους κανόνες (regular expressions). Η διαχείριση των σχετικών ενεργειών πρέπει να εκτελείται από την κεντρική κονσόλα του συστήματος.	ΝΑΙ		
18.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να μπορεί να επιβάλει την αλλαγή του επιπέδου διαβάθμισης με βάση την ημερομηνία δημιουργίας ή τροποποίησης του εγγράφου (πχ αλλαγή επιπέδου διαβάθμισης από «εμπιστευτικό» σε «δημόσιο» μετά από καθορισμένο χρόνο από την ημερομηνία δημιουργίας ενός εγγράφου).	ΝΑΙ		
19.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να παρέχει στατιστικά για την εξέλιξη της αυτόματης διαβάθμισης των υφιστάμενων εγγράφων από την κεντρική κονσόλα της λύσης.	ΝΑΙ		
20.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να συντάσσει καταλόγο (inventory) με τα έγγραφα που έχουν εντοπιστεί με βάση κάποια πολιτική η οποία λαμβάνει υπ όψιν το περιεχόμενο τους ή/και τα επίπεδα διαβάθμισης τους. Η διαχείριση των σχετικών ενεργειών πρέπει να εκτελείται από την κεντρική κονσόλα του συστήματος.	ΝΑΙ		
21.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να είναι σε θέση να σαρώσει, να αναγνωρίσει και να διαβαθμίσει δεδομένα που είναι αποθηκευμένα σε συστήματα διαμοιρασμού εγγράφων: <ul style="list-style-type: none"> • Sharepoint • OneDrive • Dropbox • Box • Windows Filesharing 			

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
22.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να μπορεί να τοποθετεί οπτική σήμανση χαρακτηριστικής του επιπέδου διαβάθμισης εντός των εγγράφων της οικογένειας MsOffice (word, exec, powerpoint)	ΝΑΙ		
23.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να μπορεί να θέτει αυτόματα σήμανση εντός των εγγράφων με βάση το επίπεδο ταξινόμησής τους (π.χ. υδατογράφημα, υποσέλιδο, κεφαλίδα κ.λπ.)	ΝΑΙ		
24.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να μπορεί να προσαρμόζει τη σήμανση στις απαιτήσεις του ΔΕΔΔΗΕ (πχ χρώματα, λεκτικά, θέση, κλπ)	ΝΑΙ		
25.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να μπορεί να τοποθετεί σήμανση χαρακτηριστική του επιπέδου διαβάθμισης εντός μηνυμάτων ηλεκτρονικής αλληλογραφίας της εφαρμογής MsOutlook.	ΝΑΙ		
26.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να μπορεί να θέτει αυτόματα σήμανση στα εικονίδια εγγράφων (π.χ. τα εικονίδια επιφάνειας εργασίας κάθε εγγράφου) με βάση το επίπεδο διαβάθμισης τους (π.χ. κόκκινη ετικέτα για αυστηρά εμπιστευτικό, πορτοκαλί ετικέτα για εμπιστευτικό, κίτρινη ετικέτα Εσωτερικό και πράσινη ετικέτα για Δημόσιας χρήσης).	ΝΑΙ		
27.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να μπορεί να επισημάνει τα έγγραφα με μεταδεδομένα (metadata) στα οποία περιλαμβάνονται όλες οι πληροφορίες για τα επίπεδα και υποεπίπεδα διαβάθμισης των εγγράφων	ΝΑΙ		
28.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να μπορεί να προσθέσει στα μεταδεδομένα κάθε εγγράφου και πληροφορία για την πολιτική διατήρησης ανάλογα με το επίπεδο διαβάθμισης και τον τύπο του εγγράφου.	ΝΑΙ		
29.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να προστατεύει τα μεταδεδομένα από	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	διαγραφή ή τροποποίηση από τον απλό χρήστη.			
30.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να μπορεί να διατηρεί τα μεταδεδομένα επί του εγγράφου κατά τη διάρκεια κάθε είδους μεταφοράς (π.χ. μέσω email, μέσω διαδικτύου, εφαρμογών cloud, ftp/sftp, αντιγραφής, κρυπτογράφησης/αποκρυπτογράφησης, συμπίεσης, κλπ).	ΝΑΙ		
31.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να είναι απολύτως συμβατό με το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) (π.χ. τα μεταδεδομένα τα σχετικά με το επίπεδο διαβάθμισης πρέπει να αναγνωρίζονται από το εργαλείο DLP το οποίο θα εφαρμόζει κατάλληλες πολιτικές ελέγχου).	ΝΑΙ		
32.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να είναι πλήρως συμβατό με την λύση IRM του ΔΕΔΔΗΕ. Τα μεταδεδομένα σχετικά με το επίπεδο διαβάθμισης πρέπει να αναγνωρίζονται από την λύση IRM.	ΝΑΙ		
33.	Το Σύστημα Διαβάθμισης Δεδομένων θα πρέπει να συνεργάζεται με εργαλεία Εξωτερικής κρυπτογράφησης.	ΝΑΙ		
34.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να έχει χαρακτηριστικά ανοικτής αρχιτεκτονικής ώστε να εξασφαλίζεται η διαλειτουργικότητα του με τα υφιστάμενα πληροφοριακά συστήματα του ΔΕΔΔΗΕ.	ΝΑΙ		
35.	Μετά από μαζική σάρωση εγγράφων σε servers ή σε εφαρμογές αποθήκευσης εγγράφων (πχ sharepoint), το Σύστημα Διαβάθμισης Δεδομένων πρέπει να παράγει αναφορές και στατιστικά καθώς και τα αντίστοιχα γραφήματα τους .	ΝΑΙ		
36.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να μπορεί να εξάγει τις αναφορές υπό μορφή αρχείου.	ΝΑΙ		
37.	Η κονσόλα διαχείρισης του Συστήματος Διαβάθμισης Δεδομένων θα πρέπει να	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	<p>συλλέγει καταγραφές συμβάντων (logs) από τα τερματικά χρηστών, στις ακόλουθες περιπτώσεις:</p> <p>1. Εάν ένας χρήστης αλλάξει το επίπεδο ταξινόμησης ενός εγγράφου (π.χ. μείωση του επιπέδου ταξινόμησης)</p> <p>2. Εάν έχει σταλεί προειδοποίηση για κάποια ενέργεια (alert) ή έχει ζητηθεί αιτιολόγηση από τον χρήστη για κάποια ενέργεια.</p>			
38.	Το Σύστημα Διαβάθμισης Δεδομένων θα έχει την Δυνατότητα μεταφοράς των καταγραφών των ενεργειών χρηστών σε syslogserver.	ΝΑΙ		
39.	Το Σύστημα Διαβάθμισης Δεδομένων θα πρέπει να υποστηρίζει πλήρως την ελληνική γλώσσα, (π.χ. πληροφορίες αναδυόμενων παραθύρων, ενσωματωμένα κουμπιά σε εφαρμογές του Office κ.λπ.).	ΝΑΙ		
40.	Η αρχιτεκτονική του Συστήματος Διαβάθμισης Δεδομένων, θα πρέπει να περιλαμβάνει μια κεντρική κονσόλα διαχείρισης από την οποία δημιουργούνται και προωθούνται οι κατάλληλες πολιτικές στα τερματικά των χρηστών.	ΝΑΙ		
41.	Ο agent του Συστήματος Διαβάθμισης Δεδομένων δεν πρέπει να καταναλώνει περισσότερο από 5% των πόρων σταθμού εργασίας / διακομιστή, βάσει δεδομένων και έγκυρων μετρήσεων.	ΝΑΙ		
42.	Θα πρέπει να υπάρχει δυνατότητα ελέγχου και εντοπισμού κακόβουλης απενεργοποίησης του agent .	ΝΑΙ		
43.	Μετά από μαζική σάρωση εγγράφων σε servers ή σε εφαρμογές αποθήκευσης εγγράφων (πχ sharepoint), το Σύστημα Διαβάθμισης Δεδομένων πρέπει να μπορεί να αρχειοθετεί αυτόματα τα διαβαθμισμένα έγγραφα που φτάνουν στην ημερομηνία λήξης σύμφωνα με την πολιτική διατήρησης.	ΝΑΙ		
44.	Η σειρά εφαρμογής ή προτεραιότητα των πολιτικών διαβάθμισης, θα πρέπει να είναι	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	σαφής και να καθορίζεται είτε από την σειρά της δήλωσής τους.			
45.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να υποστηρίζει λειτουργίες διαχείρισης πολιτικής όπως, μεταξύ άλλων, προσθήκη πολιτικής, κατάργηση πολιτικής, ενεργοποίηση πολιτικής, απενεργοποίηση πολιτικής, προσθήκη, κατάργηση και αλλαγή κανόνων πολιτικής, αλλαγή παραμέτρων πολιτικής, σύνδεση πολιτικής με συγκεκριμένους agents, πολιτική δοκιμών κ.λπ.	ΝΑΙ		
46.	Ο ανάδοχος πρέπει να παρέχει διαγράμματα αρχιτεκτονικής για το πώς θα υλοποιηθεί το Σύστημα και τους υπολογιστικούς πόρους που απαιτούνται για τη φιλοξενία του Συστήματος και για την Πρόληψη απώλειας δεδομένων.	ΝΑΙ		
47.	Ο ανάδοχος θα είναι υπεύθυνος για την εγκατάσταση της πλήρους υποδομής που απαιτείται για την υλοποίηση του Συστήματος (π.χ. εγκατάσταση λογισμικού και λειτουργικού συστήματος, DB, εφαρμογής κ.λπ.).	ΝΑΙ		
48.	Ο ανάδοχος θα είναι υπεύθυνος να εγκαταστήσει τους απαιτούμενους agents στους τερματικούς σταθμούς εργασίας των χρηστών.	ΝΑΙ		
49.	Ο ανάδοχος θα είναι υπεύθυνος για τη δημιουργία όλων των συμφωνημένων πολιτικών διαβάθμισης με βάση τις ανάγκες του αναθέτοντος οργανισμού και τις αντίστοιχες πολιτικές της εταιρείας αλλά και τα αποτελέσματα της μελέτης αξιολόγησης.	ΝΑΙ		
50.	Ο ανάδοχος πρέπει να παρέχει την κατάλληλη εκπαίδευση σε υπεύθυνους πληροφορικής του αναθέτοντος οργανισμού σχετικά με την λειτουργία του Συστήματος, αλλά και στο σύνολο των χρηστών της εταιρείας ώστε όλοι οι χρήστες να γνωρίζουν πως μπορούν να χρησιμοποιήσουν το σύστημα, σύμφωνα με τις απαιτήσεις της	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	παραγράφου Error! Reference source not found..			

7.2.2.2 Λύση Προστασίας Δεδομένων από Διαρροή

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
1.	Οι agents του συστήματος αποτροπής διαρροής δεδομένων που εγκαθίστανται στα τερματικά (endpoints), πρέπει να είναι συμβατοί με Λειτουργικά Συστήματα: Windows 10, WindowsServer 2008 R2, 2012, 2016, 2019 , , MacOS / X,	NAI		
2.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) πρέπει να έχει τέλεια συμβατότητα με το εργαλείο διαβάθμισης και σήμανσης εγγράφων και με την λύση IRM .	NAI		
3.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να καλύπτει χίλια (1.000) τερματικά του οργανισμού	NAI		
4.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να μπορεί να ανιχνεύει την ενέργεια και να λαμβάνει μέτρα (πχ αποτροπή / αιτιολόγηση / ενημέρωση) εάν ένας χρήστης αντιγράψει και επικολλήσει δεδομένα σε έναν μη έμπιστο προορισμό.	NAI		
5.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) πρέπει να μπορεί να επιθεωρεί την κυκλοφορία SSL (SSLinspection) εάν απαιτείται αλλά και να υποστηρίζει εξαίρεσεις (targetswhitelisting).	NAI		
6.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να μπορεί να παρέχει σε πραγματικό χρόνο καταγραφών της διακίνησης των δεδομένων στα πληροφοριακά συστήματα.	NAI		
7.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να μπορεί να καταγράφει τις κινήσεις που δεν είναι	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	συμβατές με την αποδεκτή πολιτική διακίνησης δεδομένων,			
8.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να παρακολουθεί μέσω κεντρικής κονσόλα διαχείρισης την συνολική εικόνα διακίνησης των δεδομένων δηλ. ποια είδη δεδομένων χρησιμοποιούνται, ή διαβιβάζονται και από ποιους	NAI		
9.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να ανιχνεύει τις κινήσεις που αφορούν ενέργειες επί των δεδομένων στα τελικά σημεία όπως για παράδειγμα copy/paste σε εξωτερική μονάδα δίσκου ή USBstick, εκτυπώσεις αρχείων, λειτουργία printscreen.	NAI		
10.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να ανιχνεύει την διακίνηση δεδομένων από μέσα προς τα έξω, μέσω των κεντρικών δικτυακών υποδομών και μέσω των διαφόρων πρωτοκόλλων επικοινωνίας ftp, http, https, smtp, αλλά και στιγμιαίο μήνυμα (IM).	NAI		
11.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να δημιουργεί incidents τα οποία πρέπει να διαβαθμίζονται αυτόματα σε διάφορα επίπεδα διαβάθμισης (πχ low, high, serious), με βάση τις πολιτικές και την κατηγοριοποίηση των δεδομένων.	NAI		
12.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει αποστέλλει ενημερώσεις ασφαλείας με διάφορα μέσα επικοινωνίας παραβίασης (πχ. Email, sms, κλπ)	NAI		
13.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να είναι σε θέση να σαρώσει, να εντοπίσει και να αποτρέψει τη διαρροή (με βάση τις πολιτικές) που είναι αποθηκευμένα στις ακόλουθες μορφές: 1. Αρχεία Excel 2. Αρχεία με οριοθετημένες στήλες (συγκεκριμένη γραμμογράφηση)	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	<p>3. Δεδομένα που αποθηκεύονται σε γνωστές βάσεις δεδομένων όπως Oracle, MS-SQL, PostgreSQL, MongoDB, DB2 και χρησιμοποιεί η εταιρεία.</p> <p>4. Δεδομένα που αποθηκεύονται σε συστήματα διαμοιρασμού εγγράφων:</p> <ul style="list-style-type: none"> • Filenet • Sharepoint • OneDrive • OwnCloud • Windows Filesharing 			
14.	<p>Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) πρέπει να περιέχει δυνατότητες αναγνώρισης δεδομένων σε όλα τα πληροφοριακά συστήματα του οργανισμού, βάσει πολιτικών περιεχομένου (π.χ. λέξεις-κλειδιά, regular expressions, περιεχόμενα λεξικών κ.λπ.). Ο εγκαταστάτης θα πρέπει να παρέχει υπηρεσίες ανάπτυξης Regular expressions οι οποίες να καλύπτουν την αναγνώριση των ακόλουθων δεδομένων:</p> <ol style="list-style-type: none"> 1. Αριθμοί Φορολογικού Μητρώου (ΑΦΜ) 2. Τηλεφωνικά νούμερα (Ελληνικά κινητά ή σταθερά τηλέφωνα) 3. Αριθμοί Ελληνικών Ταυτοτήτων. 4. Ελληνικά ονόματα (π.χ. πιθανώς με τεχνική λεξικού) 5. Διευθύνσεις (π.χ. πιθανώς με τεχνική λεξικού) 6. Αριθμοί πιστωτικών ή χρεωστικών καρτών 7. Αριθμοί λογαριασμών IBAN 8. Αριθμός Παροχής 9. Αριθμός Μητρώου Μισθωτού 	ΝΑΙ		
15.	<p>Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα ανακαλύπτει τα δεδομένα που αποθηκεύονται σε διάφορους τύπους πληροφοριακών συστημάτων ενός δικτύου (discovery), όπως σε Fileservers ή κεντρικά storage καθώς και πάνω σε σταθμούς εργασίας (endpoints).</p>	ΝΑΙ		
16.	<p>Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα παρέχει πληροφορίες για το περιεχόμενο των δεδομένων και για</p>	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	την διακίνηση τους, που θα δώσουν στους διαχειριστές ασφάλειας του ΔΕΔΔΗΕ πλήρη εποπτεία για το ποιος μπορεί να διακινήσει, ποιες πληροφορίες, από ποιο σημείο, και με ποιον τρόπο.			
17.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα καθορίζει πολιτικές αναζήτησης με βάση τα χαρακτηριστικά ή το περιεχόμενο των αρχείων.	ΝΑΙ		
18.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα καθορίζει με βάση τις απαιτήσεις του οργανισμού ποιες αναζητήσεις μπορούν να γίνουν σε εργάσιμες ώρες, και ποιες λόγω όγκου και επιβάρυνσης του δικτύου, πρέπει να γίνονται σε προγραμματισμένες μη εργάσιμες ώρες.	ΝΑΙ		
19.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα καθορίζει τις περιοχές καθώς και των Τελικών Σημείων που θα εκτελείται η αναζήτηση δεδομένων.	ΝΑΙ		
20.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) πρέπει να αποτρέπει τη διαρροή εταιρικών πληροφοριών, που είναι: 1. Αποθηκευμένες σε Πληροφοριακά Συστήματα (in rest) 2. Σε διαμετακόμιση (in transit) 3. Σε χρήση (in use)	ΝΑΙ		
21.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) πρέπει να καλύπτει τις ακόλουθες ανάγκες του οργανισμού: 1. Πρόληψη απώλειας δεδομένων προς τον ιστό (forward Proxy) 2. Πρόληψη απώλειας δεδομένων στο email 3. Πρόληψη απώλειας δεδομένων στο OWA - Outlook Web Access (web mail reverse proxy) 4. Πρόληψη απώλειας δεδομένων στο δίκτυο / VPN 5. Πρόληψη απώλειας δεδομένων από τα τερματικά (π.χ. αποτροπή εξαγωγής δεδομένων σε αφαιρούμενες συσκευές)	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
22.	<p>Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) πρέπει να έχει δυνατότητα να εφαρμόσει τους ακόλουθους κανόνες / τύπους ενεργειών επί των δεδομένων :</p> <ol style="list-style-type: none"> 1. Επιτρεπτή ενέργεια (allow) 2. Αποτροπή (block) 3. προειδοποίηση και αιτιολόγηση (π.χ. αίτημα προς τον τελικό χρήστη να περιγράψει τον λόγο για τον οποίο θέλει να κάνει την ενέργεια) 4. Καραντίνα 5. Κρυπτογράφηση <p>Ο Οργανισμός θα μπορεί να επιλέξει για ποιες από τις παραπάνω ενέργειες θα πρέπει να δημιουργούνται άμεσα alerts σε καθορισμένους ρόλους</p>	ΝΑΙ		
23.	<p>Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να μπορεί να ανιχνεύει και να αποτρέπει τη διαρροή δεδομένων (βάσει πολιτικών), μέσω οποιοδήποτε πιθανού καναλιού επικοινωνίας δεδομένων, και οπωσδήποτε από τα ακόλουθα:</p> <ol style="list-style-type: none"> 1. HTTP / HTTPS 2. FTP / FTPS 3. SMB (Κοινή χρήση αρχείων) 4. SSH / Telnet 5. VPN / OpenVPN (TLS / SSL / IPSEC / PPTP / PPTPS) 6. RDP 7. POP / POP3 / IMAP / IMAP4 / SMTP 8. IRC / SNMP 9. RPC / NFS 10. Rsync 	ΝΑΙ		
24.	<p>Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να μπορεί να εντοπίζει και να αποτρέπει διαρροές δεδομένων ηλεκτρονικού ταχυδρομείου μέσω:</p> <ol style="list-style-type: none"> 1. Microsoft Outlook 2. Outlook Web Anywhere (OWA) 3. Outlook Active Sync 	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
25.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP), θα πρέπει να μπορεί να εντοπίζει και να αποτρέπει διαρροές δεδομένων από τους τερματικούς σταθμούς που επιχειρούνται μέσω των ακόλουθων καναλιών: 1. Wi-Fi 2. USB 3. Κάρτες Micro / Mini / Midi SD 4. CD / DCD 5. NFS / SMB	ΝΑΙ		
26.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να μπορεί να ανιχνεύει και να αποτρέπει διαρροές δεδομένων μέσω οποιοδήποτε τύπου εφαρμογών cloud, όπως: 1. Skype / Skype for business 2. DropBox 3. Evernote 4. OneDrive 5. iCloud 6. GoogleDrive 7. OneNote 8. Yammer 9. Jabber 10. Logmein 11. Citrix 12. TeamViewer 13. WebEx 14. Gmail 15. Facebook 16. Twitter 17. Instagram 18. Yammer 19. Wettransfer 20. Γιουσέντιτ 21. YouTransfer 22. Sendanywhere	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	23. FileDrop 24. BOX25. Filenet 26. Sharepoint 27. Teams 28. Etc.			
27.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να μπορεί να αναγνωρίζει, να ταξινομεί και να αποτρέπει τη διαρροή (βάσει πολιτικών) εγγράφων της ακόλουθης μορφής: 1. Σουίταγραφείου (π.χ. Word, Excel, Power Point, Visio, Microsoft Project, one-note κ.λπ.). 2. Email Outlook (π.χ. msg, pst, ost, κλπ) 3. Αρχεία PDF 4. Αρχείακειμένου (π.χ. TXT, ASC, ANS, ACL, 0, HTML, XML, ODM, OTT, INFO, PAP, PAGES κ.λπ.) 5. Συμπιεσμένα αρχεία (π.χ. ZIP, 7zip, RAR, WinRAR, BZip, Gzip, Tar, Bz2 κ.λπ.) 6. Αρχείαβίντεο (π.χ. mpg, mp4, amv, wmv, mov, avi, mkv κ.λπ.) 7. Αρχείαήχου (π.χ. mp3, wma, wav, DVR-MS, WTV κ.λπ.) 8. Αρχείαεικόνας (π.χ. JPEG, TIFF, GIF, BMP, PNG, AI, CDR, ADT, PSD, PUB κ.λπ.) 9. Αρχείαβάσηςδεδομένων (π.χ. ACCDB, ADT, DB, MDB, MYD, MYI, ORA, SQL, SDF, sqlite, 10. Κρυπτογραφημένα αρχεία (π.χ. ssh, pub, rpkr, cert, crt, der, p7b, PEM, PFX, AXX, EEA, TC, BPW, KDB, KDBX κ.λπ.) 11. Άλλοι τύποι αρχείων (π.χ. CMD, BAT, JSP, PL, PHP, ASP, PYO, VBS κ.λπ.)	ΝΑΙ		
28.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να μπορεί να ανιχνεύει την ενέργεια και να λαμβάνει μέτρα (πχ αποτροπή / αιτιολόγηση / ενημέρωση) εάν ένας χρήστης προσπαθήσει να εκτυπώσει ή να αντιγράψει την οθόνη (printscreen)	ΝΑΙ		
29.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να έχει	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	ενσωματωμένη δυνατότητα να φιλτράρει την δικτυακή κίνηση, να ανιχνεύει την ενέργεια και να λαμβάνει μέτρα (πχ αποτροπή / αιτιολόγηση / ενημέρωση) εάν ένα έγγραφο με τύπο εικόνας περιέχει διαβαθμισμένες πληροφορίες (π.χ. δυνατότητες OCR)			
30.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) προστατεύει τα δεδομένα, με συγκεκριμένες διαδικασίες και με προκαθορισμένες αυτοματοποιημένες πολιτικές βασισμένες πάνω στις πολιτικές ασφαλείας που ορίζει η εταιρεία αλλά και με εκτεταμένο εύρος ενσωματωμένων πολιτικών ανά γεωγραφική περιοχή και επιχειρηματική δραστηριότητα.	ΝΑΙ		
31.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα εκτελεί συγκεκριμένες κινήσεις όταν οι ενέργειες του χρήστη παραβαίνουν την πολιτική ασφάλειας του Οργανισμού.	ΝΑΙ		
32.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα καταγράφει την ενέργεια του χρήστη (Monitor)	ΝΑΙ		
33.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα προειδοποιεί τον χρήστη (Alert)	ΝΑΙ		
34.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα αποτρέπει αυτόματα μία ενέργειας του χρήστη (Block),	ΝΑΙ		
35.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα μπορεί να απαιτεί από τον χρήστη αιτιολόγησης μίας ενέργειας (Justify).	ΝΑΙ		
36.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα μπορεί να παραμετροποιεί τους κανόνες που καθορίζουν το είδος της ενέργειας που θα εκτελέσει το σύστημα DLP, ώστε να λαμβάνουν υπ όψιν την ταυτότητα του χρήστη που επιχειρεί την διακίνηση των δεδομένων, το είδος των δεδομένων, τον	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	υπο διακίνηση δεδομένων, τον όγκο των υπο διακίνηση δεδομένων, την πηγή και τον αποδέκτη των δεδομένων, κλπ.			
37.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να κατηγοριοποιεί δεδομένα των εφαρμογών συνολικά	ΝΑΙ		
38.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα μπορεί να δημιουργεί κανόνες ελέγχου για συγκεκριμένες κατηγορίες τελικών σημείων	ΝΑΙ		
39.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) δεν θα έχει περιορισμούς στον αριθμό των κανόνων ελέγχου και θα μπορεί να εφαρμόζει πολλαπλούς κανόνες	ΝΑΙ		
40.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα εφαρμόζει κανόνες με βάση το σύστημα/εφαρμογή που προέρχονται τα δεδομένα	ΝΑΙ		
41.	<p>Η κονσόλα διαχείρισης του Συστήματος Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να συλλέγει δεδομένα από οποιονδήποτε αισθητήρα DLP (με βάση agents ή με βάση το δίκτυο) και θα πρέπει να μπορεί να παρέχει τις ακόλουθες αναφορές:</p> <ol style="list-style-type: none"> 1. Χρήστες οι οποίοι έχουν τον μεγαλύτερο αριθμό ενεργοποίησης κανόνων (triggered policies). 2. Συμβάντα για τα οποία ενεργοποιήθηκε η πολιτική αποτροπής (Block) 3. Συμβάντα για τα οποία ενεργοποιήθηκε αιτιολόγησης (Justify) 6. Προσπάθειες (επιτυχείς ή ανεπιτυχείς) που έχουν γίνει για την απομάκρυνση εταιρικών δεδομένων όταν το τερματικό ήταν εκτός εταιρικού δικτύου ή όταν ήταν συνδεδεμένο στο εταιρικό δίκτυο. 7. Περιστατικά για τα οποία ενεργοποιήθηκε Καραντίνα 8. Αναφορές ανά κανόνα ή ανά πολιτική 	ΝΑΙ		
42.	Οι αναφορές και τα στατιστικά στοιχεία θα πρέπει να είναι διαθέσιμα σε μορφή excel ή	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	CSV και επιπλέον να περιλαμβάνουν γραφήματα.			
43.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) πρέπει να παράγει αρχεία καταγραφής συμβάντων από τις ενέργειες των χρηστών (logs), τα οποία θα πρέπει να μεταφέρονται εύκολα σε πλατφόρμα SIEM (να περιγραφεί ο τρόπος διασύνδεσης). Επίσης, το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) πρέπει να έχει τη δυνατότητα αποστολής μόνο ανώνυμων δεδομένων (απόκρυψη του ονόματος χρήστη).	ΝΑΙ		
44.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα μπορεί να δημιουργεί αναφορές σε διάφορα επίπεδα συμπεριλαμβανομένου πλήρες ιστορικού ανά ένδειξη/περιστατικό	ΝΑΙ		
45.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα μπορεί να δημιουργεί αναφορές που καλύπτουν τις απαιτήσεις του Νομοθετικού/Κανονιστικού πλαισίου	ΝΑΙ		
46.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα μπορεί να δημιουργεί αναφορές ανά χρήστη, τελικό σημείο, κατηγορία ένδειξης/περιστατικού, κλπ	ΝΑΙ		
47.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα μπορεί να δημιουργεί αναφορές που δίνουν την αποτύπωση της συνολικής εικόνα των εγκαταστάσεων της εφαρμογής σε επίπεδο εταιρείας και στατιστικών στοιχείων των κανόνων	ΝΑΙ		
48.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα έχει την δυνατότητα να μεταφέρει αυτοματοποιημένα τις καταγραφές σε συστήματα SIEM.	ΝΑΙ		
49.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) πρέπει να έχει ενσωματωμένη δυνατότητα να εντοπίζει και να απεικονίζει στην κονσόλα πληροφορία βασισμένη σε αποδεκτά στατιστικά μοντέλα			

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	για ποιοι είναι οι πιο επικίνδυνοι χρήστες για διαρροή δεδομένων.			
50.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) να υποστηρίζει μέσω παραμετροποίησης την ελληνική γλώσσα (π.χ. πληροφορίες αναδυόμενων παραθύρων)	ΝΑΙ		
51.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να αναγνωρίζει εάν ένας σταθμός εργασίας είναι συνδεδεμένος στο εταιρικό δίκτυο ή εκτός σύνδεσης εταιρικού δικτύου και να λαμβάνει τα κατάλληλα μέτρα σε κάθε περίπτωση (βάσει των πολιτικών DLP)	ΝΑΙ		
52.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να είναι σε θέση να αναγνωρίζει οποιονδήποτε τύπο κρυπτογραφημένων αρχείων και να δίνει την δυνατότητα αποτροπής αποστολή τους εκτός της εταιρείας.	ΝΑΙ		
53.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) πρέπει να είναι σε θέση να κρυπτογραφεί (βάσει πολιτικών) έγγραφα που έχουν χαρακτηριστεί ως εμπιστευτικά (μέσω εφαρμογής διαβάθμισης εγγράφων), όταν επιχειρείται η εξαγωγή τους από τον σταθμό εργασίας (endpoint) σε αποσπώμενα μέσα αποθήκευσης (USB).	ΝΑΙ		
54.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) πρέπει να έχει δυνατότητα ψευδοανωνυμοποίησης σχετικά με τα λεπτομερή αποτελέσματα των ενεργειών των χρηστών. Τα αποτελέσματα της ανάλυσης θα πρέπει να προβάλλονται μόνο μετά από αίτημα παροχής στοιχείων σε περίπτωση συμβάντος και με την τεχνική splitknowledge (π.χ. διαπιστευτήρια του CISO και του διευθυντή IT).	ΝΑΙ		
55.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να υποστηρίζει την ελληνική γλώσσα, σε αναδυόμενα παράθυρα (pop-us). Επιπλέον, θα πρέπει να	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	αναγνωρίζει ελληνικούς χαρακτήρες που μπορεί να περιλαμβάνονται σε έγγραφα.			
56.	Ο agent του Συστήματος Αποτροπής Διαρροής Δεδομένων (DLP) δεν πρέπει να καταναλώνει περισσότερο από 5% των πόρων σταθμού εργασίας / διακομιστή, βάσει δεδομένων και έγκυρων μετρήσεων.	ΝΑΙ		
57.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) πρέπει να είναι απολύτως συμβατό με το Σύστημα Διαβάθμισης Δεδομένων (π.χ. τα μεταδεδομένα τα σχετικά με το επίπεδο διαβάθμισης οποιουδήποτε αρχείου πρέπει να αναγνωρίζονται, από το εργαλείο DLP το οποίο θα εφαρμόζει κατάλληλες πολιτικές ελέγχου) και με τα υπόλοιπα συστήματα του Οργανισμού.	ΝΑΙ		
58.	Ο agent που εγκαθίσταται στο τερματικό χρήστη πρέπει να προστατεύεται από περιπτώσεις κακόβουλης απενεργοποίησης. Θα πρέπει να υπάρχει άμεση ενημέρωση (alert) σε περίπτωση που εντοπιστεί περίπτωση μη εξουσιοδοτημένης απενεργοποίησης	ΝΑΙ		
59.	Η σειρά εφαρμογής ή προτεραιότητα των κανόνων / πολιτικών θα πρέπει να είναι σαφής και να καθορίζεται είτε από την σειρά της δήλωσής τους ή ρητά με αριθμό προτεραιότητας ή σπουδαιότητας.	ΝΑΙ		
60.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) πρέπει να υποστηρίζει λειτουργίες διαχείρισης πολιτικής όπως, μεταξύ άλλων, προσθήκη πολιτικής, κατάργηση πολιτικής, ενεργοποίηση πολιτικής, απενεργοποίηση πολιτικής, προσθήκη, κατάργηση και αλλαγή κανόνων πολιτικής, αλλαγή παραμέτρων πολιτικής, σύνδεση πολιτικής με συγκεκριμένους agents, πολιτική δοκιμών κ.λπ.	ΝΑΙ		
61.	Το "UserInterface" του συστήματος πρέπει να καθορίζεται με βάση τους ρόλους του συστήματος. Πρέπει να διακρίνονται κατ'	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	ελάχιστον οι ρόλοι (α) διαχειριστής, (β) υπεύθυνος ασφαλείας, (γ) κοινός χρήστης			
62.	Ο agent του συστήματος Αποτροπής Διαρροής Δεδομένων (DLP) θα μπορεί να εγκαθίσταται εξ αποστάσεως και θα είναι συμβατός με άλλα εργαλεία που λειτουργούν στα τελικά σημεία (antivirus κλπ)	ΝΑΙ		
63.	Οι agents του Συστήματος Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να είναι δυνατόν να εγκατασταθούν στα τελικά σημεία (endpoint) εξ αποστάσεως	ΝΑΙ		
64.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα έχει την δυνατότητα εγκατάστασης δικτυακών στοιχείων για την παρακολούθηση της διακίνησης δεδομένων μέσω του κεντρικού δικτύου,	ΝΑΙ		
65.	Οι κανόνες θα εφαρμόζονται τόσο σε online όσο και offline κατάσταση του τελικού σημείου	ΝΑΙ		
66.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα δίνει την δυνατότητα Ενεργοποίηση/Απενεργοποίηση κανόνων εξ αποστάσεως μόνο από συγκεκριμένους εξουσιοδοτημένους χρήστες	ΝΑΙ		
67.	Οι άμεσες ενημερώσεις θα διαχειρίζονται εύκολα και κεντροποιημένα	ΝΑΙ		
68.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να μπορεί να διακρίνει ρόλους χρηστών στην κεντρική κονσόλα διαχείρισης	ΝΑΙ		
69.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) δεν θα πρέπει να δίνει την δυνατότητα απενεργοποίησης της εφαρμογής από τον τελικό χρήστη	ΝΑΙ		
70.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να υποστηρίζει διεπαφές (RESTAPI) ώστε να εξασφαλίζεται η διαλειτουργικότητα του με τα υφιστάμενα πληροφοριακά συστήματα του ΔΕΔΔΗΕ.	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
71.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να μπορεί να διαχειρίζεται μεγάλο όγκου δεδομένων	ΝΑΙ		
72.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να είναι επεκτάσιμο	ΝΑΙ		
73.	Ο ανάδοχος πρέπει να παρέχει διαγράμματα αρχιτεκτονικής για το πώς θα υλοποιηθεί το Σύστημα και τους υπολογιστικούς πόρους που απαιτούνται για τη φιλοξενία του Συστήματος και για την Πρόληψη απώλειας δεδομένων.	ΝΑΙ		
74.	Ο ανάδοχος θα είναι υπεύθυνος για την εγκατάσταση της πλήρους υποδομής που απαιτείται για την υλοποίηση του Συστήματος (π.χ. εγκατάσταση λογισμικού και λειτουργικού συστήματος, DB, εφαρμογής κ.λπ.).	ΝΑΙ		
75.	Ο ανάδοχος θα είναι υπεύθυνος να εγκαταστήσει τους απαιτούμενους agents στους τερματικούς σταθμούς εργασίας των χρηστών.	ΝΑΙ		
76.	Ο ανάδοχος θα είναι υπεύθυνος για τη δημιουργία όλων των συμφωνημένων πολιτικών διαβάθμισης με βάση τις ανάγκες του φορέα.	ΝΑΙ		
77.	Ο ανάδοχος πρέπει να παρέχει την κατάλληλη εκπαίδευση σχετικά με τη λειτουργία του Συστήματος ώστε όλοι οι χρήστες να γνωρίζουν πως μπορούν να χρησιμοποιήσουν το σύστημα	ΝΑΙ		

7.2.2.3 Λύση Διαχείρισης Δικαιωμάτων Εγγράφων

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
1.	Η λύση πρέπει να επιτρέπει τον καθορισμό του είδους των δικαιωμάτων που έχει κάθε χρήστης επί του εγγράφου (πχ μόνο ανάγνωση, επεξεργασία, ορισμός δικαιούχων, κλπ)	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
2.	Η λύση πρέπει να επιτρέπει στους διαχειριστές να παρακολουθούν τις ενέργειες πρόσβασης (επιτυχείς ή αποτυχημένες) από τελικούς χρήστες.			
3.	Η λύση πρέπει να επιτρέπει σε επιλεγμένους χρήστες να παρακολουθούν τις ενέργειες πρόσβασης (επιτυχείς ή αποτυχημένες) από τελικούς χρήστες.			
4.	Η λύση πρέπει να δίνει τη δυνατότητα εξ αποστάσεως αναίρεσης των δικαιωμάτων που έχουν παραχωρηθεί σε χρήστες ή διαγραφής ενός εγγράφου	ΝΑΙ		
5.	Η λύση πρέπει να δίνει τη δυνατότητα ορισμού ημερομηνιών λήξης της ισχύος των δικαιωμάτων πρόσβασης.	ΝΑΙ		
6.	Η λύση πρέπει να δίνει τη δυνατότητα σε διαχειριστές να καθορίζουν πολιτικές πρόσβασης και σε χρήστες να εφαρμόζουν αυτές τις πολιτικές πρόσβασης σε έγγραφα.	ΝΑΙ		
7.	Η λύση Λύση Διαχείρισης Δικαιωμάτων Εγγράφων θα πρέπει να προσφερθεί για καλύπτει χίλιους (1000) χρήστες	ΝΑΙ		
8.	Η λύση πρέπει να έχει την δυνατότητα να αποδίδει συγκεκριμένα δικαιώματα πρόσβασης είτε σε μεμονωμένους χρήστες είτε σε ομάδες χρηστών.	ΝΑΙ		
9.	Η λύση πρέπει να έχει την δυνατότητα να εφαρμόζει πολιτικές απόδοσης δικαιωμάτων πρόσβασης τόσο σε επίπεδο εταιρείας όσο και σε συγκεκριμένους χρήστες.			
10.	Η λύση πρέπει να επιτρέπει σε επιλεγμένους χρήστες (όχι μόνο διαχειριστές) να διαχειρίζονται πολιτικές απόδοσης δικαιωμάτων πρόσβασης.			
11.	Η λύση πρέπει να δίνει την δυνατότητα καθορισμού των διαδικτυακών διευθύνσεων από τις οποίες επιτρέπεται η πρόσβαση στα έγγραφα.	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
12.	Η λύση πρέπει να αναγνωρίζει και να αυθεντικοποιεί τους χρήστες που ανήκουν στον οργανισμό μέσω πλήρους λειτουργικής διασύνδεσης με το AD του οργανισμού.	ΝΑΙ		
13.	Η λύση πρέπει να έχει την δυνατότητα απόδοσης συγκεκριμένων δικαιωμάτων πρόσβασης σε χρήστες που ανήκουν σε συγκεκριμένες ομάδες του οργανισμού (ActiveDirectorygroups).	ΝΑΙ		
14.	Η λύση πρέπει να δίνει την δυνατότητα να καθορίζονται ονομαστικά οι χρήστες (εσωτερικοί ή εξωτερικοί) στους οποίους επιτρέπεται η πρόσβαση σε έγγραφα του οργανισμού καθώς και το είδος της πρόσβασης που παρέχεται.	ΝΑΙ		
15.	Η λύση πρέπει να δίνει την δυνατότητα να καθορίζονται ομάδες χρηστών στις οποίες επιτρέπεται η πρόσβαση σε έγγραφα του οργανισμού.			
16.	Η λύση πρέπει να έχει την δυνατότητα αποστολής ειδοποιήσεων/προσκλήσεων (invitations) σε εξωτερικούς χρήστες στους οποίους παραχωρείται πρόσβαση σε ένα έγγραφο.	ΝΑΙ		
17.	Οι χρήστες στους οποίους αποδίδεται δικαίωμα πρόσβασης σε ένα έγγραφο πρέπει να μπορούν να διαχειρίζονται το έγγραφο χωρίς την χρήση ειδικών προγραμμάτων (transparency).	ΝΑΙ		
18.	Η λύση πρέπει να δίνει την δυνατότητα καθορισμού δικαιωμάτων πρόσβασης σε οποιονδήποτε τύπο αρχείου			
19.	Η λύση πρέπει να δίνει την δυνατότητα καθορισμού δικαιωμάτων πρόσβασης είτε σε διακριτά έγγραφα είτε σε όλα τα έγγραφα που διατηρούνται σε συγκεκριμένα διακριτά σημεία διατήρησης (φακέλους ή μέσα αποθήκευσης).	ΝΑΙ		
20.	Η λύση πρέπει να δίνει δυνατότητα καθορισμού δικαιωμάτων πρόσβασης σε αρχεία που διατηρούνται σε τοπικούς	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	σταθμούς εργασίας, servers, σε εφαρμογές νέφους (Office365, Sharepoint, OneDrive, κλπ).			
21.	Ο τρόπος διαχείρισης των δικαιωμάτων πρόσβασης των εγγράφων θα πρέπει να είναι ίδιος ανεξάρτητα από το μέσο διατήρησης των αρχείων.	ΝΑΙ		
22.	Η λύση πρέπει να έχει πλήρη συμβατότητα με τις εφαρμογές του Office 365 και να δίνει δυνατότητα στους χρήστες των εφαρμογών να καθορίζουν τα δικαιώματα επί των δεδομένων μέσα από το περιβάλλον των ίδιων των εφαρμογών ή μέσω της εφαρμογής.	ΝΑΙ		
23.	Η λύση πρέπει να έχει πλήρη συμβατότητα με τις εφαρμογές Outlook και Exchange.	ΝΑΙ		
24.	Η λύση πρέπει να έχει δυνατότητα καθορισμού δικαιωμάτων πρόσβασης σε αρχεία pdf.	ΝΑΙ		
25.	Η λύση πρέπει να έχει την δυνατότητα λειτουργικής διασύνδεσης με την λύση DLP του Οργανισμού (DataLossPrevention) και τη λύση Διαβάθμισης Εγγράφων καθώς και τις υπόλοιπες εφαρμογές του Οργανισμού.	ΝΑΙ		
26.	Δυνατότητα Διασύνδεσης με το SIEM του οργανισμού	ΝΑΙ		
27.	Ο ανάδοχος πρέπει να παρέχει την κατάλληλη εκπαίδευση σχετικά με τη λειτουργία του Συστήματος ώστε όλοι οι χρήστες να γνωρίζουν πως μπορούν να χρησιμοποιήσουν το σύστημα	ΝΑΙ		

7.2.2.4 Λύση Διαχείρισης Λογαριασμών και Δικαιωμάτων Πρόσβασης Χρηστών

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Να αναφερθεί το όνομα, η έκδοση, η ημερομηνία ανακοίνωσης και ο κατασκευαστής της προσφερόμενης πλατφόρμας.	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Ο κατασκευαστής της προσφερόμενης πλατφόρμας λογισμικού Identity&AccessRightsManagement IAM θα πρέπει να διαθέτει τοπική παρουσία με τοπικό γραφείο εκπροσώπησης / θυγατρική στην Ελλάδα	ΝΑΙ		
	ΗπροσφερόμενηΛύσηIdentity&AccessRightsManagementIAM θακαλύπτειχιλίους (1.000) λογαριασμούς.	ΝΑΙ		
	Η προτεινόμενη αρχιτεκτονική υλοποίησης της πλατφόρμας θα πρέπει να περιλαμβάνει λειτουργία σε διάταξη υψηλής διαθεσιμότητας.	ΝΑΙ		
	Η προτεινόμενη αρχιτεκτονική υλοποίησης της πλατφόρμας θα πρέπει να υποστηρίζει λειτουργία 24x7.	ΝΑΙ		
	Χρήση μιας κεντρικής ενιαίας σχεσιακής βάσης δεδομένων για την διαχείριση του συνόλου των δεδομένων της προτεινόμενης πλατφόρμας.	ΝΑΙ		
	Η προτεινόμενη αρχιτεκτονική υλοποίησης της πλατφόρμας θα πρέπει να προσφέρει τη δυνατότητα οριζόντιας και κάθετης κλιμάκωσης.	ΝΑΙ		
	Η δυνατότητα οριζόντιας κλιμάκωσης θα προβλέπει δυναμική προσθήκη επιπλέον κόμβων στη βάση δεδομένων και στους εξυπηρετητές εφαρμογών της πλατφόρμας χωρίς καμιά διακοπή της υπηρεσίας. Κάθε νέος κόμβος που θα προστίθεται θα γίνεται άμεσα ενεργός και θα αναλαμβάνει μέρος του φόρτου εργασίας και των συνδέσεων των εφαρμογών.	ΝΑΙ		
	Οι προσφερόμενες άδειες χρήσης λογισμικού της πλατφόρμας IAM θα επιτρέπουν στον Φορέα εάν το επιθυμεί να μεταφέρει και να λειτουργήσει την πλατφόρμα IAM σε υποδομές PublicCloud. Η προσφερόμενη λύση θα πρέπει να μπορεί να μεταφερθεί και να λειτουργήσει κατ'ελάχιστων στις ακόλουθες υποδομές Δημόσιου Νέφους (PublicCloudInfrastructure): α)Microsoft Azure, β) Amazon Web Services.			
	Όλα τα δομικά συστατικά της προτεινόμενης πλατφόρμας λογισμικού θα πρέπει να λειτουργούν σε διάταξη υψηλής διαθεσιμότητας και ισοκατανομής φόρτου εργασίας	ΝΑΙ		
	Υποστήριξη κεντροποιημένης πολιτικής με χρήση των ακόλουθων στοιχείων:	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	<ul style="list-style-type: none"> Χρήστες (users) Ρόλοι χρηστών (roles) Δικαιώματα (permissions) Εφαρμογές (applications) Εξαιρέσεις (exclusions) Κίνδυνοι (risks) <p>Οργανισμοί (organizations)</p>			
	Υποστήριξη εκχώρησης της δυνατότητας εκτέλεσης των διαθέσιμων διαχειριστικών ενεργειών στο σύστημα είτε απευθείας σε χρήστες, είτε σε ομάδες χρηστών (delegatedadministration).	ΝΑΙ		
	Εργαλείο αναζήτησης βάση πολλαπλών κριτηρίων.	ΝΑΙ		
	Δυνατότητα επαναφοράς του συνθηματικού χρήστη στις εφαρμογές από τον χρήστη, χωρίς τη διαμεσολάβηση διαχειριστή (self-servicepasswordreset).	ΝΑΙ		
	Η πλατφόρμα θα πρέπει να υποστηρίζει πολλαπλά πρωτόκολλα για αυθεντικοποίηση και εξουσιοδότηση (Active Directory/ADFS, LDAP, OpenID, OAuth, Identity Management Systems etc).	ΝΑΙ		
	Να περιγραφεί η διαδικασία εξουσιοδότησης και συγκεκριμένα η διαδικασία δημιουργίας ρόλων και ανάθεσης δικαιωμάτων εξουσιοδότησης.	ΝΑΙ		
	Η πλατφόρμα θα πρέπει να παρέχει δυνατότητες προσαρμογής της διεπαφής χρήσης καθώς και των connectors και των διαδικασιών.	ΝΑΙ		
	Η πλατφόρμα θα πρέπει να υποστηρίζει την παραμετροποίηση τήρησης των αποθηκευμένων διαπιστευτηρίων (saved/cachedcredentials).	ΝΑΙ		
	Η πλατφόρμα θα πρέπει να υποστηρίζει SingleSign-On (SSO) για αυθεντικοποίηση χρηστών.	ΝΑΙ		
	Η πλατφόρμα θα πρέπει να διασφαλίζει την εξουσιοδοτημένη πρόσβαση σε υπηρεσίες και δεδομένα.	ΝΑΙ		
	Η πλατφόρμα θα πρέπει να παρέχει τη δυνατότητα ανάθεσης μόνο των τελείως απαραίτητων δικαιωμάτων σε κάθε χρήστη ανάλογα με τον ρόλο του και εφαρμόζοντας την αρχή του LeastPrivilege.	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Η πλατφόρμα θα πρέπει να υποστηρίζει το RESTAPIs για εισερχόμενες διεπαφές με τρίτα συστήματα.	ΝΑΙ		
	Να διατεθούν και να υλοποιηθούν adapters με τον ActiveDirectory και με μία βάση (Oracle ή MSSQL) του Φορέα	ΝΑΙ		
	Η προτεινόμενη πλατφόρμα θα πρέπει να έχει τη δυνατότητα διασύνδεσης με ActiveDirectory για την παραμετροποίηση των ρόλων των χρηστών.	ΝΑΙ		
	Η πλατφόρμα θα πρέπει να υποστηρίζει το RoleBasedAccessControl (RBAC) μοντέλο. Θα πρέπει να ανατεθούν σε χρήστες επιχειρησιακοί ρόλοι που θα μεταφράζονται σε δικαιώματα εφαρμογών και θα ανταποκρίνονται στη θέση τους στον οργανισμό.	ΝΑΙ		
	Η πλατφόρμα θα πρέπει να υποστηρίζει MultiFactorAuthentication.	ΝΑΙ		
	<p>Δυνατότητα δημιουργίας ρόλων αιτημάτων χρήσης μέσω γραφικού περιβάλλοντος, με τα παρακάτω χαρακτηριστικά:</p> <ul style="list-style-type: none"> Υποστήριξη παράλληλων και σειριακών διεργασιών με αιτήματα έγκρισης από ευέλικτα καθοριζόμενους χρήστες (approvaltasks). Δυνατότητα προώθησης συγκεκριμένων αιτημάτων έγκρισης σε άλλους χρήστες. Δυνατότητα προσωρινής εκχώρησης των δικαιωμάτων έγκρισης σε άλλο χρήστη (και με ημερομηνία λήξης). Δυνατότητα παρακολούθησης της κατάστασης ενός αιτήματος (και για χρήστες μη εγγεγραμμένους στο σύστημα). Δυνατότητα έγκρισης/απόρριψης ενός αιτήματος από το e-mail του χρήστη. <p>Δυνατότητα έναρξης αιτημάτων για δημιουργία λογαριασμού χωρίς την ανάγκη κατοχής λογαριασμού χρήσης στο σύστημα.</p>	ΝΑΙ		
	Δυνατότητα υποστήριξης αυτόματων μεταβολών στις προσβάσεις ενός χρήστη ανάλογα με τις κινήσεις που γίνονται στο trustedsource (HRMS) σύστημα (πρόσληψη, μετακίνηση, αλλαγή θέσης, τερματισμός).	ΝΑΙ		
	Αυτοματοποιημένη μεταβολή των δικαιωμάτων πρόσβασης στα συνδεδεμένα (connected) συστήματα.	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Δυνατότητα αποδοχής ή άρνησης των αιτήσεων πρόσβασης στις εφαρμογές.	ΝΑΙ		
	Δυνατότητα προσωρινής εκχώρησης των δικαιωμάτων έγκρισης σε άλλο χρήστη (και με ημερομηνία λήξης).	ΝΑΙ		
	Δυνατότητα παρακολούθησης της κατάστασης ενός αιτήματος (και για χρήστες μη εγγεγραμμένους στο σύστημα).	ΝΑΙ		
	Να παρέχεται έτοιμο λογισμικό, χωρίς την ανάγκη ανάπτυξης κώδικα, για τη σύνδεση με συστήματα αποθήκευσης χρηστών (userrepositories). Να αναφερθούν τα υποστηριζόμενα συστήματα	ΝΑΙ		
	Να παρέχονται εύκολα παραμετροποιήσιμοι οδηγοί (wizards) για την σύνδεση και διαχείριση χρηστών σε συστήματα ευρέως χρησιμοποιούμενων τεχνολογιών (π.χ CSV αρχεία, συστήματα με webservices διεπαφές, πίνακες σε βάσεις δεδομένων με ειδική μορφή).	ΝΑΙ		
	Δυνατότητα διασύνδεσης εφαρμογών ως disconnected, με την αποστολή εργασίας (task) στον διαχειριστή ενός συστήματος, ώστε να μπορούν να συνδεθούν δυναμικά όλες οι εφαρμογές του οργανισμού.	ΝΑΙ		
	Η πλατφόρμα θα πρέπει να διαθέτει connectors τα οποία θα πρέπει να υποστηρίζουν εργασίες για το provisioning (δημιουργία, ενημέρωση, κατάργηση) των χρηστών στα διασυνδεδεμένα συστήματα καθώς και το reconciliation αυτών (ανάκτηση χρήστη και των δικαιωμάτων του). Οι προσβάσεις που έχουν αποδοθεί εκτός των διαδικασιών της λύσης, θα πρέπει να έχουν την αντίστοιχη ένδειξη για να μπορούν να ληφθούν αποφάσεις είτε χειροκίνητα (κατάργηση τους από τον διαχειριστή του συστήματος) είτε αυτόματα (κατάργηση τους μέσω διεργασίας).	ΝΑΙ		
	Ορισμός πολιτικών εξαιρέσεων και διαχωρισμού των προσβάσεων ανάλογα με τον ρόλο του χρήστη (SegregationofDuties). Θα πρέπει να εφαρμόζονται οι πολιτικές κατά το αίτημα ενός χρήστη για πρόσβαση καθώς και να μπορεί να προγραμματιστεί περιοδικός έλεγχος που θα αναθέτει μια εργασία αποκατάστασης (remediationtask) σε εξουσιοδοτημένους χρήστες.	ΝΑΙ		
	Καταγραφή του συνόλου των γεγονότων του συστήματος και παραγωγή έτοιμων αναφορών (outoftheboxreports) κατ'ελάχιστον για τα ακόλουθα:	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	<ul style="list-style-type: none"> Πολιτικές πρόσβασης ανά ρόλο χρηστών και συνδεδεμένο σύστημα Κατάσταση αιτημάτων έγκρισης και εγκριτικών ροών εργασίας Κατάσταση χρηστών ανά σύστημα και ρόλο χρηστών <p>Δικαιώματα πρόσβασης ανά χρήστη, ρόλο, οργανισμό, και συνδεδεμένο σύστημα</p>			
	Το σύστημα θα πρέπει να υποστηρίζει τον σχεδιασμό νέων αναφορών μέσω wizards.	ΝΑΙ		
	Η πλατφόρμα θα πρέπει να προσφέρει δυνατότητες καταγραφής.	ΝΑΙ		
	Θα πρέπει να διαλειτουργεί με κεντρική logging ή SIEM υποδομή.	ΝΑΙ		
	Υποστήριξη κατηγοριοποίησης γεγονότων βασιζόμενοι σε τύπο (π.χ. error, warning, information, debugetc.) και σημαντικότητα (π.χ. critical, major, normal etc.) με τρόπο που να είναι εύκολο το φιλτράρισμα σε αναφορές.	ΝΑΙ		
	Το επίπεδο καταγραφής θα πρέπει να είναι προσαρμόσιμο.	ΝΑΙ		
	<p>Να περιγράφουν οι δυνατότητες καταγραφής της πλατφόρμας αναφέροντας:</p> <ul style="list-style-type: none"> ενέργειες και γεγονότα που καταγράφονται τεχνολογίες που χρησιμοποιούνται <p>εκτυπωτικές δυνατότητες</p>	ΝΑΙ		
	Η πλατφόρμα θα πρέπει να διατηρεί ιστορικά αρχεία (logs) με ασφαλή τρόπο που να αποτρέπει οποιαδήποτε απόπειρα τροποποίησης.	ΝΑΙ		
	Η γραφική διεπαφή της προσφερόμενης πλατφόρμας θα πρέπει να είναι διαθέσιμη σε πολλαπλά είδη συσκευών (desktop, tablet, mobile).	ΝΑΙ		
	Η γραφική διεπαφή της προσφερόμενης πλατφόρμας θα πρέπει να διατίθεται μέσω webbrowser.	ΝΑΙ		
	Υποστήριξη Single-Sign On μεταξύ των προστατευόμενων web/application servers.	ΝΑΙ		
	Υποστήριξη πολιτικών πρόσβασης με βάση τα παρακάτω κριτήρια: <ul style="list-style-type: none"> Εφαρμογή για την οποία ζητείται η πρόσβαση 	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	<ul style="list-style-type: none"> • Ταυτότητα χρήστη • Ομάδα χρήστη • IP διεύθυνση <p>Ώρα εισόδου</p>			
	<p>Δυνατότητα υποστήριξης πολλαπλών μηχανισμών αυθεντικοποίησης όπως:</p> <ul style="list-style-type: none"> • Αναγνωριστικό Χρήστη/Κωδικός Πρόσβασης • One Time Password <p>Passwordless Authentication</p>	ΝΑΙ		
	Δυνατότητα καθορισμού χρόνου λήξης ανενεργού συνόδου χρήσης (idlelogout).	ΝΑΙ		
	Καταγραφή και αναφορά της IP διεύθυνσης των συνδεδεμένων χρηστών.	ΝΑΙ		
	Παροχή API για την δημιουργία κατά παραγγελία μεθόδων αυθεντικοποίησης (customauthenticationmodules).	ΝΑΙ		
	Υψηλή διαθεσιμότητα αξιοποιώντας εγγενώς τεχνολογίες caching, διαμοιρασμού φορτίου, failover.	ΝΑΙ		
	Δυνατότητα ορισμού επιπέδων αυθεντικοποίησης μεταξύ των διαφόρων μεθόδων αυθεντικοποίησης (multi-levelauthentication) και αντιστοίχιση των επιπέδων με τις προσφερόμενες υπηρεσίες. Στην περίπτωση απόπειρας πρόσβασης σε υπηρεσία υψηλότερου επιπέδου από το τρέχον επίπεδο αυθεντικοποίησης του χρήστη, ο χρήστης θα πρέπει να προτρέπει για επιπρόσθετη αυθεντικοποίηση, (step-upauthentication).	ΝΑΙ		
	Υποστήριξη δυνατοτήτων κληρονόμησης δικαιωμάτων από χρήστες ή ομάδες.	ΝΑΙ		
	Υποστήριξη του πρωτοκόλλου SAML 2.0.	ΝΑΙ		
	Υποστήριξη αυτόματης αντιστοίχισης της ταυτότητας μεταξύ ενός απομακρυσμένου και ενός τοπικού χρήστη (accountmapping).	ΝΑΙ		
	Δυνατότητα προτροπής της συγκατάβασης από τον χρήστη, για την σύνδεση ή όχι μεταξύ της τοπικής και απομακρυσμένης ταυτότητας (opt-in, opt-outsso)	ΝΑΙ		
	Υποστήριξη single-signon και singlelogout μεταξύ απομακρυσμένων συστημάτων.	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Να αναφερθούν λεπτομερώς οι δυνατότητες ολοκλήρωσης με υποδομή LDAP καταλόγου.	ΝΑΙ		
	Η πλατφόρμα πρέπει να προσφέρει ένα RoleMining εργαλείο για την ανάλυση των useraccounts και των entitlements σε εφαρμογές και να προτείνει υποψήφιους επιχειρησιακούς ρόλους.	ΝΑΙ		
	Το RoleMining εργαλείο θα πρέπει να διαλειτουργεί με την πλατφόρμα για να: <ul style="list-style-type: none"> Φορτώνει δεδομένα από IDM πλατφόρμα που είναι απαραίτητα για ανάλυση Δημοσιεύει τον υποψήφιο ρόλο σε IDM πλατφόρμα για να γίνει διαθέσιμη σε αιτήσεις χρηστών	ΝΑΙ		
	Το RoleMining εργαλείο θα πρέπει να επιτρέπει κλιμακωτή φόρτωση υποψήφιων ρόλων σε IDM πλατφόρμα για να ενημερωθούν αλλαγές σε ρόλους αλλά και να φορτωθούν νέοι ρόλοι που δημιουργήθηκαν μετά το αρχικό load.	ΝΑΙ		
	Το RoleMining εργαλείο θα πρέπει προσφέρει τη δυνατότητα σύγκρισης υποψήφιων ρόλων με τους υφιστάμενους ρόλους για τον εντοπισμό πιθανών διπλών ρόλων.	ΝΑΙ		
	Το RoleMining εργαλείο θα πρέπει προσφέρει τη δυνατότητα συγκέντρωσης δεδομένων από διαφορετικές πηγές (IDM και CSV αρχεία).	ΝΑΙ		
	Το RoleMining εργαλείο θα πρέπει προσφέρει δυνατότητες analysis πριν δημοσιεύσει τους ρόλους σε IDM πλατφόρμα.	ΝΑΙ		
	Να αναφερθεί το όνομα, η έκδοση του προσφερόμενου Συστήματος Διαχείρισης Βάσεων Δεδομένων (Σ.Δ.Β.Δ.) και η χρονολογία διάθεσης της προσφερόμενης έκδοσης	ΝΑΙ		
	Υποστηριζόμενες πλατφόρμες υλικού και λογισμικού: <ul style="list-style-type: none"> - Unix και Linux - Windows 	ΝΑΙ		
	Συνοπτική περιγραφή της αρχιτεκτονικής του προσφερόμενου Σ.Δ.Β.Δ., του τρόπου συνεργασίας με το Λ.Σ. και του τρόπου αξιοποίησης της φυσικής αρχιτεκτονικής του συστήματος	ΝΑΙ		
	Ο ανάδοχος πρέπει να παρέχει την κατάλληλη εκπαίδευση, ώστε όλοι οι χρήστες να γνωρίζουν πως μπορούν να χρησιμοποιήσουν το σύστημα	ΝΑΙ		

7.2.2.5 Λύση Διαχείρισης Προνομιούχων Λογαριασμών Πρόσβασης

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
1.	Να αναφερθεί το λογισμικό και ο κατασκευαστής.	ΝΑΙ		
2.	Αριθμός Υποστηριζόμενων Διαχειριστών	≥ 100		
3.	Αριθμός υποστηριζόμενων συνεργατών (namedusers)	≥ 50		
4.	Η προσφερόμενη λύση θα πρέπει να υποστηρίζει μηχανισμούς υψηλής διαθεσιμότητας.	ΝΑΙ		
5.	Η προσφερόμενη λύση θα πρέπει να υποστηρίζει διατάξεις Active/ Active και Active/ Passive.	ΝΑΙ		
6.	Η προσφερόμενη λύση θα πρέπει να υποστηρίζει την δυνατότητα οριζόντιας κλιμάκωσης σε περιπτώσεις υψηλού φόρτου.	ΝΑΙ		
7.	Η προσφερόμενη λύση θα πρέπει να υποστηρίζει την κλιμακούμενη αύξηση του αριθμού των χρηστών και των υποστηριζόμενων συστημάτων.	ΝΑΙ		
8.	Η προσφερόμενη λύση δεν θα πρέπει να χρειάζεται ενδιάμεσους "jumpservers" για την διαχείριση των συνδέσεων με τα υπό διαχείριση συστήματα.			
9.	Η πρόσβαση στην προσφερόμενη λύση θα πρέπει να υλοποιείται με χρήση διεθνών αναγνωρισμένων μηχανισμών κρυπτογράφησης .	ΝΑΙ		
10.	Η προσφερόμενη λύση θα πρέπει να υποστηρίζει, κατ' ελάχιστα, την διασύνδεση με τα ακόλουθα συστήματα: <ul style="list-style-type: none"> • Windows • (Windows 10, Windowsserver 2012, 2016 και 2019 και μεταγενέστερες). • Unix / Linux (Oracle Enterprise Linux, RHEL, AIX, Ubuntu). • Databases (DB2, Oracle, MSSQL, MongoDB, PostgreSQL). • Network devices (Checkpoint, Fortigate firewalls, HP και Cisco 	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	switches, routers, Cisco balancers, κτλ.) • Εικονικά Συστήματα. • Εφαρμογές Web.			
11.	Η προσφερόμενη λύση θα πρέπει να υποστηρίζει την εφαρμογή διαφορετικών πολιτικών συνθηματικών καθώς και εναλλαγής/ διαχείρισης περιόδων σύνδεσης.	NAI		
12.	Η προσφερόμενη λύση θα πρέπει να υποστηρίζει την εφαρμογή ελέγχου ταυτότητας πολλαπλών παραγόντων (MFA) για τους διαχειριστές καθώς και μηχανισμούς ελέγχου ενός παράγοντα για όλες τις εταιρικές εφαρμογές ιστού και κινητών.	NAI		
13.	Η προσφερόμενη λύση θα πρέπει να υποστηρίζει μηχανισμούς ελέγχου ταυτότητας βασισμένους στον βαθμό επικινδυνότητας του χρήστη.	NAI		
14.	Η προσφερόμενη λύση θα πρέπει να διαθέτει μηχανισμό προ-ελέγχου ταυτότητας για τις εφαρμογές που ανακτούν κωδικούς από ασφαλή αποθετήριο (securestore).	NAI		
15.	Η προσφερόμενη λύση θα πρέπει να διαθέτει μηχανισμό ελέγχου πρόσβασης σε οποιοδήποτε σύστημα, υπηρεσία ή/ και εφαρμογή, που συνδέονται χρήστες με αυξημένα δικαιώματα καθώς και να παρέχει την δυνατότητα περιορισμού των δικαιωμάτων "superuser".	NAI		
16.	Η προσφερόμενη λύση θα πρέπει να παρέχει την δυνατότητα σύνδεσης με αυξημένα δικαιώματα σε συστήματα, υπηρεσίες και εφαρμογές όταν αυτό απαιτείται.	NAI		
17.	Η προσφερόμενη λύση θα πρέπει παρέχει την δυνατότητα εκχώρησης ρόλων στους λογαριασμούς χρηστών με σκοπό την διασφάλιση της αρχής του ελάχιστου δικαιώματος (leastprivilege) και αποφυγή	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	παραχώρησης αυξημένων δικαιωμάτων πρόσβασης όταν δεν απαιτείται.			
18.	Η προσφερόμενη λύση θα πρέπει να παρέχει την δυνατότητα τερματισμού ή αποκλεισμού μιας συνόδου (session) η οποία έχει υλοποιηθεί με λογαριασμό με αυξημένα δικαιώματα είτε λόγω αδράνειας είτε μετά από αίτημα του διαχειριστή.	NAI		
19.	Η προσφερόμενη λύση θα πρέπει να παρέχει την δυνατότητα περιορισμού απομακρυσμένης πρόσβασης και ενεργειών σε συστήματα, υπηρεσίες ή/και εφαρμογές του οργανισμού.	NAI		
20.	Η προσφερόμενη λύση θα πρέπει να παρέχει ένα ενοποιημένο περιβάλλον για τη διαχείριση πολλαπλών απομακρυσμένων συνδέσεων RemoteDesktop και SSH από την ίδια κονσόλα.	NAI		
21.	Η προσφερόμενη λύση θα πρέπει να υποστηρίζει την δημιουργία συνεδρίας αυξημένων δικαιωμάτων για σύνδεση των διαχειριστών σε συστήματα Linux και συσκευές δικτύου μέσω SSH.	NAI		
22.	Η προσφερόμενη λύση θα πρέπει να υποστηρίζει την δημιουργία συνεδρίας αυξημένων δικαιωμάτων για σύνδεση των διαχειριστών σε συστήματα Windows μέσω RDP.	NAI		
23.	Τα δεδομένα της προσφερόμενης λύσης θα πρέπει να διατηρούν τα ίδια επίπεδα ασφάλειας και κρυπτογράφησης κατά την διαδικασία λήψης αντίγραφου ασφαλείας	NAI		
24.	Η προσφερόμενη λύση θα πρέπει να διαθέτει διαδικτυακή πύλη μέσω της οποίας οι χρήστες (εξωτερικοί και εσωτερικοί) θα αποκτούν πρόσβαση στα εξουσιοδοτημένα συστήματα.	NAI		
25.	Η προσφερόμενη λύση θα πρέπει να διαθέτει υποσύστημα για κινητές συσκευές μέσω της οποίας θα είναι διαθέσιμη η αποδοχή ή απόρριψη ροών έγκρισης.	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
26.	Η προσφερόμενη λύση θα πρέπει να διαθέτει εφαρμογή για κινητές συσκευές η οποία θα λειτουργεί σαν εναλλακτική μέθοδος σύνδεσης κάνοντας χρήση λογαριασμού με αυξημένα δικαιώματα.	NAI		
27.	Η προσφερόμενη λύση θα πρέπει να παρέχει την δυνατότητα ανάκτησης κωδικού πρόσβασης μέσω SDK. Τα διαπιστευτήρια που σχετίζονται με την εφαρμογή θα πρέπει να αποθηκεύονται σε ένα ασφαλές αποθηκευτικό χώρο.	NAI		
28.	Η βάση δεδομένων της προσφερόμενης λύσης θα πρέπει να χρησιμοποιεί κρυπτογράφηση με κλειδί AES256 (AdvancedEncryptionStandards).	NAI		
29.	Η προσφερόμενη λύση θα πρέπει να παρέχει δυνατότητα αναβάθμισης.	NAI		
30.	Η προσφερόμενη λύση θα πρέπει να διασυνδέεται με κεντρικό κατάλογο χρηστών (ActiveDirectory). Να αναφερθούν οι δυνατότητες	NAI		
31.	Η προσφερόμενη λύση θα πρέπει να παρέχει δυνατότητα αυθεντικοποίησης διαχειριστών που δεν ανήκουν στον Φορέα (εξωτερικοί συνεργάτες)	NAI		
32.	Η πρόσβαση στην προσφερόμενη λύση θα πρέπει να επιτυγχάνεται με την χρήση των τρεχόντων διαπιστευτηρίων των χρηστών και χωρίς την ύπαρξη λογισμικού (agentless) στους σταθμούς εργασίας τους.	NAI		
33.	Η προσφερόμενη λύση θα πρέπει να υποστηρίζει την δημιουργία κατά απαίτηση (adhoc) σύνδεσης με συγκεκριμένο τύπου τερματικού στην περίπτωση έλλειψης προεπιλεγμένης διασύνδεσης.	NAI		
34.	Η προσφερόμενη λύση θα πρέπει να διαχειρίζεται διαπιστευτήρια βασισμένα στις πολιτικές που ορίζονται στα τελικά συστήματα καθώς και να επιτρέπει την διαχείριση των κλειδιών SSH και API για περιβάλλοντα νέφους.	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
35.	Η προσφερόμενη λύση θα πρέπει να εντοπίζει, να εισάγει και να διαχειρίζεται λογαριασμούς σε όλο το περιβάλλον του οργανισμού.	ΝΑΙ		
36.	Κατά τη δημιουργία νέου λογαριασμού με αυξημένα δικαιώματα, η προσφερόμενη λύση θα πρέπει να εντοπίζει και να ενημερώνει για την ύπαρξη προηγούμενου λογαριασμού με το ίδιο αναγνωριστικό σε οποιοδήποτε σύστημα, εφαρμογή και/ ή υπηρεσία, για την αποφυγή επαναχρησιμοποίησης του.	ΝΑΙ		
37.	Η προσφερόμενη λύση θα πρέπει να προστατεύει τις πληροφορίες που είναι απαραίτητες για την αυθεντικοποίηση των χρηστών με αυξημένα δικαιώματα για την αποφυγή μια πιθανής εκμετάλλευσης από μη εξουσιοδοτημένους χρήστες.	ΝΑΙ		
38.	Η προσφερόμενη λύση θα πρέπει να μπορεί να περιορίζει τις αποτυχημένες προσπάθειες σύνδεσης για την αποφυγή επιθέσεων τύπου bruteforce/ dictionaryattack και να ενημερώνει αυτόματα συγκεκριμένους χρήστες εντός της εταιρείας.	ΝΑΙ		
39.	Να αναφερθούν οι μηχανισμοί ασφαλείας.	ΝΑΙ		
40.	Η προσφερόμενη λύση θα πρέπει να υποστηρίζει την κρυπτογράφηση των αποθηκευμένων διαπιστευτηρίων χρησιμοποιώντας διεθνώς αναγνωρισμένους αλγόριθμους κρυπτογράφησης όπως AES-256, RSA-2048 κ.λπ.	ΝΑΙ		
41.	Η προσφερόμενη λύση θα πρέπει να χρησιμοποιεί κρυπτογραφημένο κανάλι επικοινωνίας για την μεταφορά των δεδομένων από/ προς το αποθετήριο.			
42.	Η προσφερόμενη λύση θα πρέπει να μπορεί να αλλάζει αυτόματα, τα συνθηματικά που εισάγονται στο αποθετήριο.			
43.	Η προσφερόμενη λύση θα πρέπει να διασφαλίζει την εναλλαγή των	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	συνθηματικών των λογαριασμών των χρηστών με υψηλά προνόμια.			
44.	Η προσφερόμενη λύση θα πρέπει να διασφαλίζει την εναλλαγή των συνθηματικών, όπου η ύπαρξη των λογαριασμών με αυξημένα δικαιώματα είναι απαραίτητη π.χ. κώδικας σε αρχεία παραμετροποίησης, συνδέσεις με βάσεις δεδομένων κ.λπ.			
45.	Η προσφερόμενη λύση θα πρέπει να παρέχει δυνατότητα αποθήκευσης στο αποθετήριο, διαπιστευτήρια που δεν πρέπει να γίνουν αλλαγή (π.χ. λογαριασμοί έκτακτης ανάγκης).			
46.	Η προσφερόμενη λύση θα πρέπει να παρέχει τη δυνατότητα αλλαγής των συνθηματικών που ανήκουν σε συστήματα καταλόγου, όπως και σε εκείνα που ανήκουν σε συστήματα Windows και Linux.	NAI		
47.	Η προσφερόμενη λύση θα πρέπει να μπορεί να περιορίσει το χρόνο ισχύος των συνθηματικών που χρησιμοποιούνται από λογαριασμούς με αυξημένα προνόμια επιτρέποντας την δημιουργία εξαιρέσεων στην γενική πολιτική.	NAI		
48.	Η προσφερόμενη λύση θα πρέπει να επιτρέπει την δημιουργία συνθηματικών μίας χρήσης και να διατηρεί ιστορικό των διαπιστευτηρίων για την αποφυγή επαναχρησιμοποίησης τους σύμφωνα με τους περιορισμούς χρόνου που έχει θέσει ο οργανισμός.	NAI		
49.	Για περιστασιακές περιπτώσεις, η προσφερόμενη λύση θα πρέπει να διαθέτει μηχανισμό αυτόματης αλλαγής συνθηματικών.	NAI		
50.	Η προσφερόμενη λύση θα πρέπει να δυνατότητα επιβολής της πολιτικής ασφάλειας του ΔΕΔΔΗΕ σχετικά με τους κωδικούς πρόσβασης και δυνατότητα να			

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	υποστηρίζει τις σχετικές κανονιστικές απαιτήσεις και τις βέλτιστες πρακτικές.			
51.	Η προσφερόμενη λύση θα πρέπει να επιβάλει κανόνες για την συνθετότητα των κωδικών, που περιλαμβάνουν μήκος κωδικών, μίξη αλφανουμερικών και ειδικών χαρακτήρων, διάκριση μεταξύ κεφαλαίων και μικρών (upper και lower).			
52.	Η προσφερόμενη λύση θα πρέπει να δίνει την δυνατότητα στους administrators για αλλαγή των κωδικών <ul style="list-style-type: none"> • σε συγκεκριμένα διαστήματα με βάση την πολιτική του οργανισμού. • σε περιοδική βάση, • μετά από κάθε πρόσβαση εφόσον κριθεί αναγκαίο • κωδικών κατ' εντολή. 	ΝΑΙ		
53.	Η προσφερόμενη λύση θα πρέπει να παρέχει τους απαραίτητους μηχανισμούς παρακολούθησης, καταγραφής και ελέγχου της χρήσης των λογαριασμών με αυξημένα δικαιώματα σε οποιοδήποτε σύστημα, εφαρμογή και/ ή υπηρεσία.	ΝΑΙ		
54.	Η προσφερόμενη λύση θα πρέπει υποστηρίζει την προώθηση όλων των ενεργειών των χρηστών στο SIEM της εταιρείας .	ΝΑΙ		
55.	Η προσφερόμενη λύση θα πρέπει να παρέχει τους απαραίτητους μηχανισμούς προστασίας από διαγραφή ή/ και τροποποίηση των συμβάντων ασφαλείας.	ΝΑΙ		
56.	Η προσφερόμενη λύση θα πρέπει να παρέχει την δυνατότητα παρακολούθησης των συνοδών SSH που πραγματοποιούνται από τον τελικό χρήστη σε διακομιστή Linux ή άλλη δικτυακή συσκευή, με δυο διαφορετικούς τρόπους: <ul style="list-style-type: none"> • καταγραφή της περιόδου λειτουργίας σε δευτερόλεπτα για όσο διάστημα είναι ενεργή η σύνδεση 	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	<ul style="list-style-type: none"> καταγραφή όλων των εντολών και ενεργειών που εκτελούνται κατά τη διάρκεια της συνόδου 			
57.	Η προσφερόμενη λύση θα πρέπει να παρέχει την δυνατότητα εύρεσης των εντολών που εκτέλεσε ο χρήστης μέσω των καταγραφών της συνόδου SSH	ΝΑΙ		
58.	<p>Η προσφερόμενη λύση θα πρέπει να παρέχει την δυνατότητα παρακολούθησης των συνόδων RDP που πραγματοποιούνται από τον τελικό χρήστη σε διακομιστή Windows με δυο διαφορετικούς τρόπους:</p> <ul style="list-style-type: none"> καταγραφή της συνόδου σε δευτερόλεπτα για όσο διάστημα είναι ενεργή καταγραφή όλων των εντολών και ενεργειών που εκτελούνται κατά τη διάρκεια της συνόδου 	ΝΑΙ		
59.	Δυνατότητα καταγραφής (videorecording) των ενεργειών των χρηστών και για νομικές/κανονιστικές απαιτήσεις			
60.	Όλες οι ενέργειες του διαχειριστή της εφαρμογής θα πρέπει να υπάρχει η δυνατότητα να αποστέλλονται στο SIEM			
61.	<p>Η προσφερόμενη λύση θα πρέπει να παρέχει στους διαχειριστές της λύσης την δυνατότητα</p> <ul style="list-style-type: none"> δυναμικής παροχής πρόσβασης - πχ. χρονικού περιορισμού της πρόσβασης (πχ. Πρόσβαση για τις επόμενες Χ ώρες) διακοπής πρόσβασης μέσω του Συστήματος εφόσον κριθεί αναγκαίο έγκρισης της πρόσβασης από τρίτον χρήστη πολλαπλών τρόπων έγκρισης για άμεση ενεργοποίηση 	ΝΑΙ		
62.	Η προσφερόμενη λύση θα μπορεί να επιβάλει επιπλέον κανόνων ελέγχου πρόσβασης που δεν καθορίζονται μόνο από το ρόλο του χρήστη όπως ο χρόνος της πρόσβασης (ημέρα, βράδυ, εργάσιμες ημέρες αργίες).	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
63.	Η προσφερόμενη λύση θα μπορεί να περιορίζει την πρόσβαση από συγκεκριμένα δικτυακά σημεία.	NAI		
64.	Η προσφερόμενη λύση θα μπορεί να μεσολαβεί μεταξύ του διαχειριστή και του υπό διαχείριση συστήματος προωθώντας εντολές του διαχειριστή χωρίς ο ίδιος να γνωρίζει τον κωδικό πρόσβασης στο υπό διαχείριση σύστημα (sessionproxy).	NAI		
65.	Δυνατότητα πλήρους καταγραφής των ενεργειών του διαχειριστή ώστε να αποδεικνύεται η συμμόρφωση με Νομικές/Κανονιστικές απαιτήσεις.	NAI		
66.	Η προσφερόμενη λύση θα πρέπει διαθέτει μηχανισμούς ανάλυσης της συμπεριφοράς των χρηστών, με σκοπό τον εντοπισμό των ανωμαλιών ή των περιπτώσεων απόκλισης από την συνηθισμένη ασυνήθιστη δραστηριότητα ή ανωμαλιών σε πραγματικό χρόνο. Και να ενημερώνει αυτόματα συγκεκριμένους ρόλους και θέσεις εντός της εταιρείας.	NAI		
67.	Η προσφερόμενη λύση θα πρέπει να υποστηρίζει την δημιουργία προτύπου αναφοράς (baseline) σύμφωνα με την συμπεριφορά των χρηστών. Το ως άνω πρότυπο θα βασίζεται σε αλγόριθμους μηχανικής εκμάθησης που αναλύουν την συμπεριφορά σε βάθος χρόνου, τη συμπεριφορά πρόσβασης, την σπουδαιότητα των διαπιστευτηρίων και την συμπεριφορά των απλών χρηστών. Μόλις ένας χρήστης παρεκκλίνει από το ως άνω πρότυπο, θα βαθμολογείται η επικινδυνότητα σε πραγματικό χρόνο.	NAI		
68.	Η προσφερόμενη λύση θα πρέπει να βαθμολογεί την συμπεριφορά των χρηστών βάσει της επικινδυνότητας.	NAI		
69.	Η προσφερόμενη λύση θα πρέπει να καταγράφει τους λογαριασμούς με αυξημένα δικαιώματα και τους χρήστες που έχουν πρόσβαση σε αυτούς. Επιπλέον οι χρήστες ή/ και τα διαπιστευτήρια θα πρέπει	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	να μπορούν να ομαδοποιηθούν ώστε να μπορεί να διαπιστωθεί εάν ένα διαπιστευτήριο περιέχεται σε μια ομάδα ή εάν οι χρήστες έχουν πρόσβαση σε διαπιστευτήρια ή στοιχεία που ανήκουν σε άλλα τμήματα.			
70.	Η Λύση Διαχείρισης Προνομιούχων Λογαριασμών Πρόσβασης θα μπορεί να ανακαλύπτει λογαριασμούς με αυξημένα δικαιώματα ώστε να αποφεύγεται το ενδεχόμενο ύπαρξης κάποιου λογαριασμού ο οποίος δεν έχει πέσει στην αντίληψη της ομάδας πληροφορικής και οποίος ενδεχομένως χρησιμοποιείται κακόβουλα ώστε να παρακάμψει τα εφαρμοζόμενα μέτρα προστασίας και λογοδοσίας (auditing).	NAI		
71.	Η Λύση Διαχείρισης Προνομιούχων Λογαριασμών Πρόσβασης θα μπορεί να διαχειρίζεται κεντρικά και αυτοματοποιημένα τους λογαριασμούς με αυξημένα δικαιώματα σε όλα τα συστήματα με τα οποία θα διασυνδεθεί.	NAI		
72.	Η Λύση Διαχείρισης Προνομιούχων Λογαριασμών Πρόσβασης θα μπορεί να εντοπίζει εύκολα τα διαπιστευτήρια των διαχειριστών που δεν ελέγχονται μέσω του Συστήματος	NAI		
73.	Η Λύση Διαχείρισης Προνομιούχων Λογαριασμών Πρόσβασης θα μπορεί να εντοπίζει εύκολα τα διαπιστευτήρια εντός εφαρμογών (hard-coded/embedded application credentials) και περιορισμό αυτών.	NAI		
74.	Η Λύση Διαχείρισης Προνομιούχων Λογαριασμών Πρόσβασης θα μπορεί να εκδίδει ειδοποιήσεις (alerts) σε κάθε περίπτωση που θα διαπιστωθεί η ύπαρξη κάποιου μη αναμενόμενου λογαριασμού.	NAI		
75.	Η προσφερόμενη λύση θα διατηρεί λεπτομερείς αναφορές σχετικά με την χρήση	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	των κωδικών πρόσβασης από τους διαχειριστές των συστημάτων (logging).			
76.	Η προσφερόμενη λύση θα διατηρεί λεπτομερείς αναφορές με το ποια πολιτική διαχείρισης κωδικών εφαρμόζεται σε κάθε σύστημα και ποιες εξαιρέσεις ισχύουν.	ΝΑΙ		
77.	Η προσφερόμενη λύση θα διατηρεί λεπτομερείς αναφορές σε διάφορα επίπεδα συμπεριλαμβανομένου πλήρους ιστορικού ενεργειών ανά διαχειριστή/σύστημα.	ΝΑΙ		
78.	Η προσφερόμενη λύση θα διατηρεί λεπτομερείς αναφορές για το ποιος απέκτησε πρόσβαση με αυξημένα δικαιώματα, πότε και για ποιον λόγο.	ΝΑΙ		
79.	Η προσφερόμενη λύση θα παρέχει Δυνατότητα αποστολής των καταγραφών σε σύστημα SIEM	ΝΑΙ		
80.	Ο ανάδοχος πρέπει να παρέχει την κατάλληλη εκπαίδευση ώστε όλοι οι χρήστες να γνωρίζουν πως μπορούν να χρησιμοποιήσουν το σύστημα	ΝΑΙ		

7.2.2.6 Λύση μηχανισμών ισχυρής ταυτοποίησης

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Η προσφερόμενη πλατφόρμα θα πρέπει να υποστηρίζει εγγενώς τη σύνδεση τόσο με γνωστές εφαρμογές τρίτων τόσο και με customεφαρμογές και να είναι On-premise	ΝΑΙ		
	Να αναφερθεί το προσφερόμενο μοντέλο και ο κατασκευαστής			
	Να υποστηρίζεται εφαρμογή για κινητές συσκευές (app) Android, iOS	ΝΑΙ		
	Αριθμός απαιτούμενων αδειών χρηστών.	≥500		
	Η πλατφόρμα θα πρέπει να υποστηρίζει ειδοποιήσεις push για κινητά ως μηχανισμό πολλαπλών παραγόντων - ελέγχου ταυτότητας (multifactorauthentication)	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Η εφαρμογή να παράγει OTP (One time password)	ΝΑΙ		
	Η αδειοδότηση να είναι ανά χρήστη και να υποστηρίζει πολλαπλές συσκευές του χωρίς επιπρόσθετο κόστος	ΝΑΙ		
	Παροχή ενός selfserviceinterface στο οποίο ο χρήστης θα έχει εικόνα των προσβάσεων και των εφαρμογών στις οποίες μπορεί να ζητήσει πρόσβαση.	ΝΑΙ		
	Η προτεινόμενη πλατφόρμα θα πρέπει να διαθέτει authentication methods και out – of – the box connectors για authentication με εφαρμογές cloud χρησιμοποιώντας third party systems (Azure, Active Directory, ADFS)	ΝΑΙ		
	Να υποστηρίζεται SMS	ΝΑΙ		
	Η προτεινόμενη πλατφόρμα θα πρέπει να παρέχει πολλαπλούς μηχανισμούς ελέγχου ταυτότητας, συμπεριλαμβανομένων των παρακάτω: <ul style="list-style-type: none"> • Kerberos, • OAuth 2.0, • SAML 2.0, • OpenIDConnect, OTP & TOTP One time password	ΝΑΙ		
	Να αναφερθούν τα υποστηριζόμενα tokens	ΝΑΙ		
	Να υπάρχει δυνατότητα self-enrollment των χρηστών	ΝΑΙ		
	Ο διαχειριστής θα μπορεί να έχει εικόνα της διαστηριότητας των χρηστών και να μπορεί να βγάλει αναφορές.	ΝΑΙ		
	Η πλατφόρμα πρέπει προσφέρει δυνατότητα Single Sign-on.	ΝΑΙ		
	Η προϊόντική οικογένεια στην οποία ανήκει το προσφερόμενο προϊόν να αποτελεί την πιο πλήρη λύση στο κομμάτι Identity and Access Management της αγοράς με δυνατότητες όπως Single Sign-On (SSO), Multi-Factor Authentication (MFA), Identity Governance, Identity Analytics, Privileged Access Management και πολλά άλλα χωρίς τη χρήση 3ων λύσεων. Να περιγραφεί	ΝΑΙ		
	Η προσφερόμενη πλατφόρμα θα πρέπει να προσφέρει τη δυνατότητα δημιουργίας χρηστών με διαφορετικούς ρόλους και διαφορετικά δικαιώματα πρόσβασης.	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Η πλατφόρμα να έχει τη δυνατότητα ρύθμισης, ώστε να αναγκάζει τον χρήστη να αλλάξει κωδικό πρόσβασης κατά την πρώτη σύνδεση (όπου υποστηρίζεται από την εφαρμογή / σύστημα).	ΝΑΙ		
	Η πλατφόρμα θα πρέπει να προσφέρει δυνατότητα δημιουργίας διαφορετικών ομάδων (groups) χρηστών και ανάθεση διαφορετικών ρόλων και δικαιωμάτων ανά ομάδα.	ΝΑΙ		
	Η προτεινόμενη λύση θα πρέπει να παρέχει ένα πλαίσιο ελέγχου ταυτότητας χρησιμοποιώντας ένα reverseproxy.	ΝΑΙ		
	Η πλατφόρμα δεν θα πρέπει να στηρίζεται στην υιοθέτηση proprietary SDKs για την υποστήριξη νέων Authentication Providers	ΝΑΙ		
	Η πλατφόρμα να προσφέρει secure REST API	ΝΑΙ		
	Η πλατφόρμα πρέπει να παρέχει τη δυνατότητα σε έναν χρήστη να ξεκινήσει χειροκίνητα μια αίτηση πρόσβασης ή ενός δικαιώματος πρόσβασης μέσω μιας διεπαφής χρήστη. Η διεπαφή πρέπει να είναι φιλική προς τον χρήστη και να τον διευκολύνει στην αίτηση δικαιωμάτων πρόσβασης.	ΝΑΙ		
	Η πλατφόρμα θα πρέπει να παρέχει τη δυνατότητα delegation στη διαδικασία έγκρισης δικαιωμάτων πρόσβασης.	ΝΑΙ		
	Η πλατφόρμα θα έχει τη δυνατότητα να παρέχει, να ενεργοποιεί/απενεργοποιεί, να πιστοποιεί και να συνδυάζει ταυτότητες, προσβάσεις και δικαιώματα σε πολλαπλά LDAP (ActiveDirectory).	ΝΑΙ		
	Η προσφερόμενη λύση να μπορεί να ενσωματωθεί (integrate) με άλλες λύσεις του ίδιου κατασκευαστή συμπεριλαμβανομένων των SIEM, Database Monitoring, PAM, UBA με απώτερο σκοπό την βέλτιστη άμυνα σε πιθανές επιθέσεις.	ΝΑΙ		

7.2.2.7 Υπηρεσίες ανάκαμψης από καταστροφή και λήψης αντιγράφων ασφαλείας

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Το τμήμα Δημοσίου Υπολογιστικού Νέφους (PublicCloud) της προσφερόμενης λύσης θα πρέπει να παρέχει υπηρεσίες φιλοξενίας τύπου Cloud/Hosting, με υπηρεσίες υποδομής ως υπηρεσία (IaaS) και πλατφόρμας ως υπηρεσία (PaaS) από έναν πάροχο Δημοσίου Υπολογιστικού Νέφους.	ΝΑΙ		
	Η Αναθέτουσα Αρχή θα μπορεί να επιλέξει σε ποια γεωγραφική περιοχή (region) θα φιλοξενηθούν οι επιλεγόμενες υπηρεσίες.	ΝΑΙ		
	Ο πάροχος θα πρέπει να μπορεί να διαθέτει τις υπηρεσίες του από δύο τουλάχιστον γεωγραφικές περιοχές (regions), εντός Ευρωπαϊκής Ένωσης, με ελάχιστη απόσταση 500 χιλιομέτρων μεταξύ τους, τα οποία θα μπορούν	ΝΑΙ		

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	να χρησιμοποιηθούν για την υλοποίηση υπηρεσιών που απαιτούν τον ύψιστο βαθμό υψηλής διαθεσιμότητας με χαρακτηριστικά ανάνηψης από καταστροφή (DisasterRecovery). Να αναφερθούν οι χώρες φιλοξενίας.			
	Το τμήμα του δημοσίου υπολογιστικού νέφους (PublicCloud) της προσφερόμενης λύσης θα επιτρέπει τη διαμόρφωση υπηρεσιών υψηλής διαθεσιμότητας (highavailability) και ανάκαμψης από καταστροφή (DisasterRecovery).	ΝΑΙ		
	Απαιτείται η ύπαρξη μηχανισμού παρακολούθησης και ελέγχου της κατάστασης (health) των χρησιμοποιούμενων πόρων σε συνάρτηση με την κατάσταση της υποδομής του παρόχου. Ο μηχανισμός να διαθέτει δυνατότητα μηχανισμού αποστολής ειδοποιήσεων κατά μόνας ή σε ομάδες, email, webhook βάσει κανόνων που τίθενται από το διαχειριστή.	ΝΑΙ		
	Οι όροι SLA των υπηρεσιών να είναι δημοσιευμένοι στην επίσημη ιστοσελίδα του παρόχου. Να αναφερθεί η σχετική ιστοσελίδα.	ΝΑΙ		
	Για λόγους διαφάνειας και ελέγχου συμμόρφωσης με τα παρεχόμενα επίπεδα SLA η τρέχουσα κατάσταση λειτουργίας του συνόλου των υπηρεσιών θα πρέπει να είναι δημόσια διαθέσιμη στο επίσημο ιστότοπο του παρόχου. Να αναφερθεί η σχετική ιστοσελίδα.	ΝΑΙ		
	Ο πάροχος να διαθέτει δωρεάν υπηρεσίες για τη συνολική διακυβέρνηση – governancetων πόρων που θα αξιοποιηθούν από τον φορέα λειτουργίας. Κατ'ελάχιστο απαιτούνται: <ul style="list-style-type: none"> • δυνατότητα οργάνωσης και ελέγχου πρόσβασης στο σύνολο πολλαπλών λογαριασμών και συνδρομών • δυνατότητα διαμόρφωσης και εφαρμογής πολιτικών χρήσης των υπολογιστικών πόρων που περιλαμβάνονται σε λογαριασμούς και στις συνδρομές • καθορισμός πολλαπλών προϋπολογισμών με καθορισμό ορίων στο επιθυμητό επίπεδο εφαρμογής (scope) πόρων και δυνατότητα ενημέρωσης διαχειριστών μέσω email εποπτεία και ανάλυση τρεχουσών χρεώσεων, ιστορικών χρεώσεων και πρόβλεψη της εξέλιξης τους	ΝΑΙ		
	Ο πάροχος να διαθέτει εγγενή μηχανισμό παροχής προτάσεων χωρίς επιπλέον κόστος, για βελτιστοποίηση της χρήσης των χρησιμοποιούμενων πόρων, στους τοείς της ασφάλειας, της διαθεσιμότητας, των επιδόσεων καθώς και του κόστους αυτών, κατά τις βέλτιστες πρακτικές του παρόχου υπολογιστικού νέφους.	ΝΑΙ		
	Να παρέχεται από τον πάροχο του δημοσίου υπολογιστικού νέφους ελεύθερα προσπελάσιμος επίσημος ιστότοπος με πληροφορίες, οδηγούς και εγχειρίδια χρήσης, ρυθμίσεις, συχνές ερωτήσεις και παραδείγματα κώδικα για το σύνολο των υπηρεσιών του. Να αναφερθεί η σχετική ιστοσελίδα.	ΝΑΙ		
	Να παρέχεται δωρεάν εκπαιδευτικό υλικό μέσω ηλεκτρονικής μάθησης σε επίσημο ιστότοπο του παρόχου με ενότητες στους εκάστοτε τομείς των υπηρεσιών υπολογιστικού νέφους. Να αναφερθεί η σχετική ιστοσελίδα.	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Πιστοποίηση σε ισχύ που να αποδεικνύει τη συμμόρφωση της λειτουργίας του παρόχου με το πρότυπο διασφάλισης ποιότητας ISO/IEC 9001:2015. Να κατατεθεί αντίγραφο της πιστοποίησης.	NAI		
	Πιστοποίηση σε ισχύ που να αποδεικνύει τη συμμόρφωση της λειτουργίας του παρόχου με το πρότυπο ασφάλειας ISO/IEC 27001:2013. Να κατατεθεί αντίγραφο της πιστοποίησης.	NAI		
	Πιστοποίηση σε ισχύ που να αποδεικνύει τη συμμόρφωση της λειτουργίας του παρόχου με το πρότυπο ασφάλειας πληροφοριακών ελέγχων ISO/IEC 27017:2015. Να κατατεθεί αντίγραφο της πιστοποίησης.	NAI		
	Πιστοποίηση σε ισχύ που να αποδεικνύει τη συμμόρφωση της λειτουργίας του παρόχου με το πρότυπο διασφάλισης της προστασίας προσωπικών δεδομένων ISO/IEC27018:2019. Να κατατεθεί αντίγραφο της πιστοποίησης.	NAI		
	Πιστοποίηση σε ισχύ που να αποδεικνύει τη συμμόρφωση της λειτουργίας του παρόχου με το πρότυπο ιδιωτικότητας πληροφοριών ISO/IEC 27701:2019. Να κατατεθεί αντίγραφο της πιστοποίησης.	NAI		
	Πιστοποίηση σε ισχύ που να αποδεικνύει τη συμμόρφωση της λειτουργίας του παρόχου με το πρότυπο διασφάλισης της επιχειρησιακής συνέχειας ISO/IEC 22301:2019. Να κατατεθεί αντίγραφο της πιστοποίησης.	NAI		
	Πιστοποίηση σε ισχύ που να αποδεικνύει τη συμμόρφωση της λειτουργίας του παρόχου με το πρότυπο διαχείρισης υπηρεσιών πληροφοριακού συστήματος ISO/IEC 20000-1:2018	NAI		
	Συμμόρφωση της υποδομής του παρόχου κατά ServiceOrganizationControls (SOC) 1,2 και 3. Να κατατεθούν τα τρία σχετικά reports.	NAI		
	Συμμόρφωση της υποδομής του παρόχου κατά Payment Card Industry (PCI) Data Security Standards (DSS) έκδοση 3.2.1 - Level 1 . Να κατατεθεί η σχετική βεβαίωση.	NAI		
	Η υποδομή του παρόχου δημοσίου υπολογιστικού νέφους να διαθέτει benchmark με πρακτικές και προτάσεις καθοδήγησης, από το CenterforInternetSecurity (CIS) για την προστασία συστημάτων πληροφορικής ανεπτυγμένα στο δημόσιο υπολογιστικό νέφος έναντι κυβερνο-απειλών. Να κατατεθεί το σχετικό benchmark.	NAI		
	Το marketplace του παρόχου δημοσίου υπολογιστικού νέφους να διαθέτει ενισχυμένα -hardened- templates εικονικών μηχανών από το CenterforInternetSecurity (CIS).	NAI		
	Συμμόρφωση της λειτουργίας του παρόχου με το Cloud Control Matrix (CCM) του Cloud Security Alliance (CSA), με τη μορφή του Consensus Assessments Initiative Questionnaire (CAIQ) στην έκδοση 3.1 ή μεταγενέστερη. Να κατατεθεί το σχετικό αποδεικτικό αυτοαξιολόγησης (self assessment).	NAI		
	Πιστοποίηση σε ισχύ που να αποδεικνύει τη συμμόρφωση της λειτουργίας του παρόχου με το πρότυπο CSA-STAR του CloudSecurityAlliance (CSA). Να κατατεθεί αντίγραφο της πιστοποίησης.	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Συμμόρφωση της υποδομής του παρόχου κατά EN 301 549. Να κατατεθεί το σχετικό αποδεικτικό.	NAI		
	Οι υπηρεσίες του παρόχου θα πρέπει να είναι συμβατές με τον Κανονισμό (ΕΕ) 2016/679 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα (GDPR Regulation).	NAI		
	Ο Πάροχος του Δημόσιου Υπολογιστικού Νέφους θα πρέπει να είναι μέλος του EU Data Centres Energy Efficiency CoC σύμφωνα με την λίστα που δημοσιεύεται στον παρακάτω σύνδεσμο: https://e3p.jrc.ec.europa.eu/node/575	NAI		
	Να αναφερθούν άλλα στοιχεία και μέτρα που αναλαμβάνει ο πάροχος ως προς την ασφάλεια και την κανονιστική συμμόρφωση.	NAI		
	Υπηρεσία εξυπηρέτησης εγγενών φορτίων τεχνολογίας VMware με υποστήριξη τεχνολογιών vCenter Server, vSAN, vSphere και NSX-T, στην υποδομή του παρόχου υπολογιστικού νέφους. Ο Πάροχος να αποτελεί εγκεκριμένο προμηθευτή VMware Cloud τεχνολογιών.	NAI		
	Παροχή μηνιαίου SLA για την υπηρεσία εξυπηρέτησης εγγενών φορτίων τεχνολογίας VMware, τουλάχιστον 99.9%.	NAI		
	Η υπηρεσία εξυπηρέτησης εγγενών φορτίων τεχνολογίας VMware να προσφέρει υψηλό επίπεδο ασφάλειας και προστασίας δεδομένων των χρηστών, με δυνατότητες Role-Based Access Control και αυθεντικοποίησης μέσω Single Sign On, αλλά και κρυπτογράφησης των καταχωρούμενων δεδομένων.	NAI		
	Να προσφέρεται η δυνατότητα δικτύωσης στο περιβάλλον της υπηρεσίας εξυπηρέτησης εγγενών φορτίων τεχνολογίας VMware, τόσο από την τοπική υποδομή όσο και από το περιβάλλον υπολογιστικού νέφους.	NAI		
	Να προσφέρεται η δυνατότητα ανάκαμψης από καταστροφή υφιστάμενης υποδομής VMware με χρήση VMware Site Recovery Manager (SRM) στην υπηρεσία εξυπηρέτησης εγγενών φορτίων τεχνολογίας VMware στο περιβάλλον υπολογιστικού νέφους μέσω αποκλειστικού κυκλώματος διασύνδεσης.	NAI		
	Να προσφέρεται υπηρεσία αποκατάστασης φορτίων as-a-service από τον Πάροχο του Δημοσίου Υπολογιστικού Νέφους.	NAI		
	Ο πάροχος της προσφερόμενης λύσης να αναφέρεται στη λίστα Leaders του φορέα αξιολόγησης Gartner στην κατηγορία Disaster Recovery as a Service (DRaaS).	NAI		
	Μέσω της προσφερόμενης λύσης, να προσφέρεται προστασία υπολογιστικών συστημάτων από καταστροφή μέσω συνεχούς replication, διαδικασία μετάπτωσης μετά καταστροφή καθώς και επανάκαμψης και επαναλειτουργίας.	NAI		
	Να προσφέρεται η δυνατότητα αποκατάστασης καταστροφών για τις εικονικές μηχανές που λειτουργούν σε περιβάλλον εικονικοποίησης VMware, vSphere/vCenter έκδοσης τουλάχιστον 6.0, μέσω της	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	αναπαραγωγής τους σε περιβάλλον δημοσίου υπολογιστικού νέφους του κατασκευαστή της προσφερόμενης λύσης.			
	Να προσφέρεται η δυνατότητα αποκατάστασης καταστροφών για τις εικονικές μηχανές που λειτουργούν σε περιβάλλον εικονικοποίησης Hyper-V έκδοσης τουλάχιστον 2012 R2, μέσω της αναπαραγωγής τους σε περιβάλλον δημοσίου υπολογιστικού νέφους του κατασκευαστή της προσφερόμενης λύσης.	NAI		
	Να προσφέρεται η δυνατότητα αποκατάστασης καταστροφών για τους φυσικούς διακομιστές Linux και Windows, που λειτουργούν σε περιβάλλον τοπικής υποδομής μέσω της αναπαραγωγής τους, είτε σε μια δευτερεύουσα τοπική υποδομή είτε σε περιβάλλον δημοσίου υπολογιστικού νέφους του κατασκευαστή της προσφερόμενης λύσης.	NAI		
	Να προσφέρεται η δυνατότητα αποκατάστασης καταστροφών για τις εικονικές μηχανές που λειτουργούν στο περιβάλλον δημοσίου νέφους του κατασκευαστή της προσφερόμενης λύσης μέσω της αναπαραγωγής τους σε μια δευτερεύουσα περιοχή του δημοσίου υπολογιστικού νέφους.	NAI		
	Παροχή μηνιαίου SLA για την υπηρεσία αποκατάστασης φορτίων από τοπική υποδομή στο περιβάλλον δημοσίου υπολογιστικού νέφους, εντός 2 ωρών.	NAI		
	Κατά την προστασία των εικονικών, η διαδικασία του replication να μην επηρεάζει τα πρωτότυπα δεδομένα.	NAI		
	Να προσφέρεται η δυνατότητα πραγματοποίησης δοκιμαστικής αποκατάστασης καταστροφών, χωρίς να προκαλούνται ανεπιθύμητες επιπτώσεις στις εφαρμογές και τα δεδομένα του Οργανισμού.	NAI		
	Να προσφέρεται η δυνατότητα πραγματοποίησης δοκιμαστικής αποκατάστασης καταστροφών, τόσο σε κάποια προγραμματισμένη χρονική στιγμή, όσο και σε κάποια η οποία δεν έχει προκαθοριστεί.	NAI		
	Να προσφέρεται η δυνατότητα σχεδιασμού και παραμετροποίησης των σχεδίων αποκατάστασης από καταστροφή από τον Οργανισμό, καθώς και ομαδοποίησης και προτεραιοποίησης της αποκατάστασης των εφαρμογών στα σχέδια αυτά. Επιπλέον, να είναι δυνατή η ενσωμάτωση της προσφερόμενης λύσης με εξειδικευμένα για την εκάστοτε εφαρμογή σενάρια αποκατάστασης καταστροφών.	NAI		
	Κατά την προστασία των εικονικών μηχανών να προσφέρεται η δυνατότητα application consistent σημείων ανάκαμψης.	NAI		
	Να προσφέρεται η δυνατότητα replication κατ'ελάχιστον για τις παρακάτω εφαρμογές τοπικής υποδομής: <ul style="list-style-type: none"> • Microsoft Active Directory • IIS • SQL • SharePoint υποστηρίζοντας τους εγγενείς μηχανισμούς υψηλής διαθεσιμότητας.	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Η προσφερόμενη λύση να διαθέτει παραμετροποίηση δικτυακών ρυθμίσεων των προστατευόμενων εικονικών μηχανών, καθώς και συνεργασία με δικτυακές υπηρεσίες του παρόχου υπολογιστικού νέφους.	ΝΑΙ		
	Ο πάροχος δημοσίου υπολογιστικού νέφους να προσφέρει κανάλι πρόσθετων επιλογών τύπου Marketplace, μέσω του οποίου να προσφέρονται εξειδικευμένες λύσεις αποκατάστασης καταστροφών από αντίστοιχους επίσημους συνεργάτες και κατασκευαστές λογισμικού.	ΝΑΙ		

7.2.2.8 Ddos

A.A	Προδιαγραφή	Απαίτηση	Απάντηση	Παραπομπή
1.	Να περιγραφεί η γενική προσέγγιση της προτεινόμενης on premise και Cloud-based λύσης προστασίας από κατανεμημένες επιθέσεις άρνησης υπηρεσίας (DDoS) και με ποιο τρόπο προστατεύει την επιχειρησιακή συνέχεια (business continuity) και τη διαθεσιμότητα των υπηρεσιών (Δικτυακή δομή -Website - Portal) τους από τις επιθέσεις DDoS	ΝΑΙ		
2.	Αποφυγή Inbound (Εντός εσωτερικού δικτύου) και Outbound απειλές (Από εξωτερικά δίκτυα). Ελάχιστο network traffic το οποίο μπορεί να προστατευτεί από την cloud DDoS λύση ≥ 200 Mbps. Να περιγραφεί αναλυτικά.	ΝΑΙ		
3.	Αποφυγή των γνωστών (μέχρι σήμερα) τύπων DDoS επιθέσεων (DNS, NTP, Chargen, SSDP, SNMP, Portmap, MSSQL, SYN, Slow Rate Attacks, SIP, Volumetric, RFC) amplification attacks, TCP, UDP State exhaustion. Να περιγραφούν άλλοι τύποι επιθέσεων που μπορούν να αποτραπούν και παρατεθούν στοιχεία (π.χ. από ENISA ή άλλο διεθνή οργανισμό).	ΝΑΙ		
4.	Ελάχιστο inspected throughput	<u>200</u> Mbps		
5.	Η συσκευή προστασίας DDoS που θα εγκατασταθεί θα πρέπει να παρέχει τη δυνατότητα μετριασμού (mitigation) 6 Gbps, ανεξάρτητα από την άδεια χρήσης.	ΝΑΙ		
6.	Η συσκευή προστασίας DDoS θα πρέπει να παρέχει τη δυνατότητα αναβάθμισης της άδειας χρήσης για προστασία έως και 5	ΝΑΙ		

	Gbps καθαρής κίνησης χωρίς την ανάγκη αντικατάστασης υλικού. Αρχικά να προσφερθεί με αδειά για 2Gbp aggregate καθαρή κίνηση			
7.	Η προσφερόμενη λύση θα πρέπει να παρέχει τη δυνατότητα application layer και state exhausting attacks, εκτός από τις προαναφερόμενες.	NAI		
8.	Η προσφερόμενη λύση θα πρέπει να παρέχει τη δυνατότητα IPV4/IPV6 Header checks, fragmentation checks, layer 4 checks. Να περιγραφούν οι δυνατότητες οι οποίες περιλαμβάνονται.	NAI		
9.	Η DDoS συσκευή που θα προσφερθεί θα πρέπει να εγκατασταθεί στο Data center της ΗΔΙΚΑ	NAI		
10.	Η προτεινόμενη συσκευή θα πρέπει να υποστηρίζει 6 copper Ethernet θύρες και 2xSFP+	NAI		
11.	Η προτεινόμενη συσκευή θα πρέπει να μπορεί με υποστηρίζει λειτουργία IP mode και transparent λειτουργία	NAI		
12.	Η προτεινόμενη DDoS συσκευή θα πρέπει να είναι εξειδικευμένη συσκευή για DDoS Και όχι firewall ή load balancer	NAI		
13.	Η προτεινόμενη συσκευή θα πρέπει να υποστηρίζει τη αντιμετώπιση Day Burst Attacks με υπογραφή η οποία δημιουργείται αυτόματα.	NAI		
14.	<ul style="list-style-type: none"> Η προτεινόμενη συσκευή θα πρέπει να υποστηρίζει μηδενικό χρόνο για τον μετριάσμο των επιθέσεων Burst, ξεκινώντας από το πρώτο χτύπημα burst. 	NAI		
15.	Η προτεινόμενη συσκευή θα πρέπει να παρέχει προστασίας behavioral-DoS χρησιμοποιώντας υπογραφές πραγματικού χρόνου που δημιουργούνται με βάση πολλαπλές παραμέτρους σε κεφαλίδες πακέτων L3 έως L7, αντί για αποκλεισμό διεύθυνσης IP προέλευσης ή περιορισμό ρυθμού	NAI		
16.	Η προτεινόμενη συσκευή θα πρέπει να υποστηρίζει behavioral DDoS προστασία για DNS τόσο σε TCP και UDP.	NAI		

17.	Η προτεινόμενη συσκευή θα πρέπει να υποστηρίζει bahavioral based application layer HTTP DDoS προστασία	NAI		
18.	Η προτεινόμενη συσκευή θα πρέπει να υποστηρίζει προστασία από zero day επιθέσεις	NAI		
19.	Η προτεινόμενη συσκευή θα πρέπει να υποστηρίζει mitigation SLA 18 sec από τον εντοπισμό	NAI		
20.	Η προτεινόμενη συσκευή θα πρέπει να υποστηρίζει IPS.	NAI		
21.	Η προτεινόμενη συσκευή θα πρέπει να υποστηρίζει εβδομαδιαίες ενημερώσεις για signatures feeds για προστασία από νέες επιθέσεις	NAI		
22.	<ul style="list-style-type: none"> Η προτεινόμενη συσκευή θα πρέπει να υποστηρίζει χιλιάδες υπογραφές ταυτόχρονα 	NAI		
23.	Η προτεινόμενη συσκευή θα πρέπει να υποστηρίζει προστασία σε επίπεδο SSL/TLS	NAI		
24.	Η προσφερόμενη λύση θα πρέπει να έχει τη δυνατότητα δημιουργίας Protection Groups. Κάθε PG να μπορεί να αντιστοιχεί σε διαφορετική υποδομή του δικτύου ή server.	NAI		
25.	Η on-premise συσκευή θα πρέπει να έχει τη δυνατότητα εκμάθησης κανονικών επιπέδων κυκλοφορίας και να προτείνει κατάλληλα όρια προστασίας για κάθε υπό παρακολούθηση στοιχείο.	NAI		
26.	<p>Να δοθεί αναλυτική περιγραφή της αρχιτεκτονικής και της λειτουργικότητας της προσφερόμενης λύσης με τη λογική ότι υφίσταται ήδη firewall.</p> <p>Να αναλυθεί το γεγονός ότι η προσφερόμενη λύση DDoS προστατεύει από άλλου τύπου επιθέσεις σε περίπτωση που το υφιστάμενο firewall παρέχει βασικές IPS/IDS λειτουργίες.</p>	NAI		
27.	<p>Η προτεινόμενη συσκευή θα πρέπει να παρέχει SSL προστασία με τους παρακάτω τρόπους</p> <ul style="list-style-type: none"> Keyless SSL Protection (χωρίς certificate και χωρίς decryption) 	NAI		



	<ul style="list-style-type: none">• First Request SSL Protection (με decryption Μόνο του πρώτου https request και μόνο κατά τη διάρκεια επίθεσης που εντοπίστηκε μέσω IP reputation)• Selective Full SSL Protection (με πλήρη decryption κατά τη διάρκεια επίθεσης και για τις ύποπτες συνδέσεις)• Full SSL Protection			
28.	Θα πρέπει να υποστηρίζονται οι ακόλουθοι τρόποι λειτουργίας (Modes), κατ' ελάχιστον: inline, SPAN.	NAI		
29.	Η on-premise συσκευή θα πρέπει να υποστηρίζει τις ενσωματωμένες επιλογές παράκαμψης για αστοχία ανοίγματος και αποτυχία κλεισίματος.	NAI		
30.	Η προσφερόμενη λύση θα πρέπει να παρουσιάζει τις πληροφορίες σε ένα φιλικό προς το χρήστη περιβάλλον (GUI).	NAI		
31.	Η προσφερόμενη λύση θα πρέπει παρέχει τη δυνατότητα whitelisting και blacklisting IP διευθύνσεων (Δυνατότητα IPV4 και IPV6.	NAI		
32.	Η προσφερόμενη λύση θα πρέπει να συνοδεύεται από τις απαραίτητες άδειες λειτουργίας οι οποίες θα πρέπει να αφορούν τόσο το λειτουργικό σύστημα, εάν αυτό απαιτεί ξεχωριστή άδεια χρήσης όσο και το λογισμικό. Όλες οι άδειες θα βαρύνουν τον ανάδοχο	NAI		
33.	Η Υποστήριξη του λογισμικού και οι αναβαθμίσεις σε νεότερες εκδόσεις του θα πρέπει παρέχονται από τον ανάδοχο στο πλαίσιο του έργου.	NAI		

34.	Υποστήριξη IPv4 και IPv6 και prefix matching.	ΝΑΙ		
35.	Υποστήριξη τουλάχιστον SNMP v2 & v3.	ΝΑΙ		
36.	Η προσφερόμενη λύση θα πρέπει να υποστηρίζει το RESTful API για τη διαμόρφωση του στοιχείου εσωτερικής εγκατάστασης και την παρακολούθηση του στοιχείου cloud.	ΝΑΙ		
37.	Δυνατότητα για SSL. Να αναφερθούν οι SSL decryption επιλογές	ΝΑΙ		
38.	Να αναφερθούν τα πρωτόκολλα που χρησιμοποιούνται την προστασία από DDOS επιθέσεις.	ΝΑΙ		
39.	Η on-premise συσκευή θα πρέπει να υποστηρίζει από τον κατασκευαστή ενημερώσεις για DDos και botnet intelligence.	ΝΑΙ		
40.	Η On premise συσκευή θα πρέπει να υποστηρίζει εισαγωγή threat feeds (pm IP reputation, active attackers) του κατασκευαστή.	ΝΑΙ		
41.	Γραφικό περιβάλλον για παρακολούθηση και παραμετροποίηση.	ΝΑΙ		
42.	Η προσφερόμενη λύση θα πρέπει να έχει τη δυνατότητα για notifications SNMP trap, syslog, email.	ΝΑΙ		
43.	Να αναφερθούν οι υποστηριζόμενοι φυλλομετρητές (browsers).	ΝΑΙ		
44.	Η προσφερόμενη λύση θα πρέπει να παρέχει δυνατότητα αναγγελίας συμβάντος μέσω ηλεκτρονικού ταχυδρομείου (email)	ΝΑΙ		

	για σοβαρά συμβάντα, συστημικά συμβάντα ή άλλα θέματα κίνησης.			
45.	Η προσφερόμενη λύση θα πρέπει να παράγει μηνύματα συμβάντων εξαιτίας λάθους του συστήματος/ κατάσταση υπερφόρτωσης (πχ. Λάθος επεξεργασίας, φόρτωση CPU, υψηλή κατανάλωση μνήμης.)	NAI		
46.	Η προσφερόμενη λύση θα πρέπει να παρέχει αναφορές real-time για πληροφορίες IPV4 και IPV6, total traffic, passed/ blocked traffic, top URL, domain, κλπ.	NAI		
47.	Η προσφερόμενη λύση θα πρέπει να εξάγει δεδομένα σε πολλαπλές μορφές συμπεριλαμβανομένου των παρακάτω δημοφιλών τύπων αρχείων: CSV, XML, PDF, etc.	NAI		
48.	VLAN Tagging support (IEEE 802.1q)	NAI		
49.	Η προσφερόμενη λύση θα πρέπει να δημιουργεί αναγγελίες συμβάντων (alerts) όταν μία τιμή έχει ξεπεράσει το κατώφλι, δείχνοντας: συνολικό traffic, το ποσοστό αποκλεισμένου και το botnet traffic	NAI		
50.	Η προσφερόμενη λύση θα πρέπει να παρέχει μετριάσμο προστασίας OnDemand / AlwaysON έναντι ογκομετρικών (volumetric) επιθέσεων σε πραγματικό χρόνο.	NAI		
51.	Η προσφερόμενη λύση θα πρέπει να μπορεί να ανιχνεύσει και να μετριάσει DDoS επιθέσεις από επίπεδο 3 στο επίπεδο7 του OSI μοντέλου. Στην περίπτωση της Cloud υπηρεσίας η συνολική χωρητικότητα των mitigation κέντρων να είναι 10Tbps.	NAI		
52.	Να περιγράφει ο τρόπος με τον οποίο θα ελαχιστοποιηθεί ο κίνδυνος τοπικής συμφόρησης κάθε Mitigation κέντρο της cloud υπηρεσίας να υποστηρίζει τουλάχιστον 200gbps.	NAI		
53.	Η υπηρεσία cloud θα πρέπει να υποστηρίζει περιοδικές δοκιμές από άκρη σε άκρη της υπηρεσίας, χωρίς επιπλέον κόστος.	NAI		
54.	Η προσφερόμενη cloud λύση θα πρέπει να προστατεύει από volumetric και application DDoS επιθέσεις.	NAI		

55.	Η προσφερόμενη λύση θα πρέπει να βασίζεται στο cloud και σε υβριδικό μοντέλο (λύση που ενσωματώνει εντοπισμό και μετριάσμο on premise εγκατάστασης με volumetric καθαρισμό επιθέσεων βάσει cloud)	NAI		
56.	Η προσφερόμενη cloud DDOS λύση θα πρέπει να ενσωματώνεται με παρόχους Public Cloud για αυτόματη ανίχνευση και εκτροπή στο Cloud Scrubbing Center	NAI		
57.	Η προσφερόμενη λύση cloud DDoS θα πρέπει να αξιοποιεί προσφερόμενη On premise λύση του ίδιου κατασκευαστή	NAI		
58.	Η προσφερόμενη cloud DDoS λύση θα πρέπει να υποστηρίζει SSL encrypted επιθέσεις.	NAI		
59.	Η προσφερόμενη cloud DDoS λύση θα πρέπει να παρέχει προστασία χωρίς να κάνει decrypt πλήρως όλη την κίνηση	NAI		
60.	Η προσφερόμενη cloud DDoS λύση θα πρέπει να είναι πιστοποιημένη σύμφωνα με τα παρακάτω πρότυπα: <ul style="list-style-type: none"> ○ ISO/IEC 27017:2015 (Information Security for Cloud Services) ○ ISO/ IEC 27018:2014 (Information Security Protection of Personally Identifiable Information (PII) in Public Clouds). ○ PCI-DSS v3.1 (Payment Card Industry Data Security Standard) ○ ISO/IEC 27001:2013 (Information Security Management Systems) ○ ISO/IEC 27032:2012 (Security Techniques -- Guidelines for Cybersecurity) ○ ISO 28000:2007 (Supply Chain Security Management System) ○ ISO 9001:2015 (Quality Management System) ○ ISO 14001:2015 (Environment Management System) 	NAI		
61.	Η προσφερόμενη λύση θα πρέπει να είναι ανεξάρτητη του υφιστάμενου παρόχου τηλεπικοινωνιών.	NAI		
62.	Να περιγραφεί ο τρόπος με τον οποίο η προσφερόμενη λύση θα προκαλέσει	NAI		

	μετριάσμούς On premise και με ποιον τρόπο θα αναδρομολογεί κίνηση στο cloud.			
63.	Η λύση θα πρέπει να υποστηρίζει εκτροπή κίνησης βάση on BGP Και DNS	NAI		
64.	Η προσφερόμενη λύση θα πρέπει να υποστηρίζει πολυεπίπεδη προστασία DDoS με σηματοδότηση από μηχανή σε μηχανή από εσωτερική συσκευή μετριάσμού DDoS στο cloud όταν απαιτείται μετριάσμός. Ο χρήστης να μπορεί να διαμορφώσει τη σηματοδότηση χειροκίνητα ή αυτόματα, όπως επιθυμεί.	NAI		
65.	Η υπηρεσία θα πρέπει να μπορεί να παρακολουθεί την εσωτερική συσκευή μετριάσμού DDoS μέσω heartbeat και να ανιχνεύει εάν αυτή η συσκευή δεν είναι πλέον προσβάσιμη.	NAI		
66.	Να περιγραφεί ο τρόπος με τον οποίο η προσφερόμενη λύση θα εκτρέπει την κίνηση.	NAI		
67.	Να περιγραφεί ο τρόπος με τον οποίο η προσφερόμενη λύση θα επαναφέρει την κυκλοφορία	NAI		
68.	Η λύση θα πρέπει να υποστηρίζει asymmetric traffic και symmetric traffic for DDOS τεχνικές μετριάσμού ανάλογα με το μοντέλο ανάπτυξης.	NAI		
69.	Η προσφερόμενη λύση να προστατεύει από DNS flood επιθέσεις			
70.	Η προσφερόμενη λύση θα πρέπει να εντοπίζει και προστατεύει από όλα τα zero-day DNS floods	NAI		
71.	Η λύση πρέπει να μπορεί να προστατεύει από οριζόντιες (all IP and same IP scan) και κατακόρυφες (σε καταστάσεις "σάρωσης".	NAI		
72.	Η λύση πρέπει να μπορεί να προστατεύει από τις ακόλουθες καταστάσεις flood: <ul style="list-style-type: none"> • UDP • TCP ICMP	NAI		
73.	Η λύση θα πρέπει να υποστηρίζει την ανίχνευση της συμπεριφοράς και τον μετριάσμό με μεγάλη ακρίβεια κατά τυχαίων sub-domain flood (για παράδειγμα: Mirai DNS Water Torisation)	NAI		

74.	Η προσφερόμενη λύση θα πρέπει να παρέχει τη δυνατότητα αποκλεισμού της κυκλοφορίας βάσει συγκεκριμένων υπογραφών botnet / επιθέσεων και / ή δακτυλικών αποτυπωμάτων και /ή στην ανάλυση συμπεριφοράς και τη μηχανική μάθηση	ΝΑΙ		
75.	Η προσφερόμενη λύση θα πρέπει να επιτρέπει την προ-διαμόρφωση προτύπων μετριάσμου για τους πελάτες κατά την αρχική παροχή βάσει των λεπτομερειών των υπηρεσιών που προστατεύονται και άλλων συγκεκριμένων πληροφοριών για τους πελάτες. Οι χρήστες να έχουν τη δυνατότητα να ενημερώνουν αυτά τα πρότυπα περιοδικά. Αυτά τα πρότυπα πρέπει να εφαρμόζονται σε μετριάσμούς όταν ξεκινά ένας μετριάσμός.	ΝΑΙ		
76.	Η προσφερόμενη λύση θα πρέπει να παρέχει πληροφορίες σχετικά με τον αριθμό των κέντρων μετριάσμου που περιλαμβάνονται στη λύση και τη γεωγραφική θέση των κέντρων μετριάσμου.	ΝΑΙ		
77.	Η προσφερόμενη λύση θα πρέπει να παρέχει μια ειδική πύλη (portal) η οποία να περιλαμβάνει πληροφορίες σε πραγματικό χρόνο σχετικά με την κυκλοφορία που πέρασε, την κυκλοφορία η οποία μειώθηκε κατά τη διάρκεια συμβάντων μετριάσμου, και να επιτρέπει στο χρήστη να επιλέξει τη χρονική περίοδο και τα δεδομένα τα οποία τον αφορούν.	ΝΑΙ		
78.	Η υπηρεσία μετριάσμου cloud θα πρέπει να μην απαιτεί χρέωση ρύθμισης.	ΝΑΙ		
79.	Η λύση cloud θα πρέπει περιλαμβάνει 24/7 SOC πρόσβαση χωρίς επιπλέον κόστος.	ΝΑΙ		
80.	Ο Ανάδοχος ν θα πρέπει α παρέχει τα κάτωθι: i. Σεμινάρια κατασκευαστή. ii. Οδηγίες χρήσης και γνώση των προϊόντων. iii. Τεκμηρίωση της προσφοράς.	ΝΑΙ		



	iv. Γνωσιακή βάση με γνωστά προβλήματα λογισμικού / υλικού και τρόπους αντιμετώπισής τους. v. Ενημέρωση για επερχόμενες αλλαγές (σφάλματα, επιδιορθώσεις).			
81.	Η προσφερόμενη λύση θα πρέπει να επιτρέπει παραμετροποίηση των δικαιωμάτων των ομάδων Χρηστών (User Account Groups).	NAI		
82.	Η προσφερόμενη λύση θα πρέπει να διαθέτει Menu κεντρικής διαχείρισης συμβάντων και σφαλμάτων και δυνατότητα αποστολής ειδοποιήσεων μέσω SNMP, Email, syslog.	NAI		
83.	Η διαχείριση της λύσης θα πρέπει να γίνεται μέσω ενός αποκλειστικού συστήματος διαχείρισης που ανήκει στον ίδιο προμηθευτή της ίδιας της συσκευής.	NAI		
84.	<p>Η ολοκληρωμένη λύση διαχείρισης πρέπει να υποστηρίζει συγκεκριμένα τα ακόλουθα:</p> <ul style="list-style-type: none">• κεντρική διαχείριση των διαμορφώσεων συστήματος των συσκευών Hw (Διαχείριση Διαμόρφωσης).• Συγκεντρωτικό καθορισμό και διανομή των Πολιτικών Ασφαλείας σε διαχειριζόμενες συσκευές.• κεντρική συλλογή και συσχέτιση πληροφοριών (καταγραφής) διαχειριζόμενων συσκευών.• εκτέλεση της εγκληματολογικής ανάλυσης των πληροφοριών που συλλέγονται (ημερολόγιο).• Μηχανισμό εξουσιοδότησης διαφορετικών προφίλ διαχείρισης που βασίζονται σε ρόλους (RBAC - Role Based Access Control). <p>δημιουργία προκαθορισμένων ή προσαρμοσμένων αναφορών που σχετίζονται με τον διαχειριζόμενο εξοπλισμό. Οι αναφορές που δημιουργούνται πρέπει να εξαχθούν σε μορφές "CSV", "PDF" ή "XML".</p>	NAI		



85.	Σε περίπτωση σφάλματος (bug) στο λογισμικό, η πλήρης αποκατάσταση του σφάλματος με κατάλληλη διορθωτική έκδοση (patch/fix) θα πρέπει να ολοκληρώνεται εντός μιας (1) ημερολογιακής εβδομάδας. Να περιγραφεί η διαδικασία που θα πρέπει ακολουθείται για την αποκατάσταση των προβλημάτων και να αναφερθεί το μέσο και μέγιστο χρόνο αποκατάστασης.	ΝΑΙ		
86.	Η προσφερωμενη λύση θα πρέπει να προσφερθεί με subscription και υποστηρίζει για 36 μήνες.	ΝΑΙ		
87.	Η προσφερόμενη λύση θα πρέπει να διαθέτει κεντρικό μενού με εύκολη πλοήγηση προς όλες τις πληροφορίες και τις αναφορές.	ΝΑΙ		
88.	Η προσφερόμενη λύση θα πρέπει να έχει τη δυνατότητα προγραμματισμού για ημερήσιες, εβδομαδιαίες ή μηνιαίες αναφορές και δυνατότητα είτε παρακολούθησης από αντίστοιχη ιστοσελίδα είτε εξαγωγής τους σε αρχείο XML, PDF, CSV.	ΝΑΙ		

7.2.2.9 NGFW για το Data Center, για την πρόσβαση των εσωτερικών χρηστών στο Διαδίκτυο και την ανάλυση των επικοινωνιών τους και για την απομακρυσμένη πρόσβαση. Άδειες για προστασία IPS, antimalware, Application Control. Διαχειριστικό εργαλείο για τα firewall

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
1.	Ενιαία και εξειδικευμένη εφαρμογή κεντρικής διαχείρισης για όλα τα προσφερόμενα συστήματα υλικού, εικονικού και λογικού τείχους προστασίας. Το σύστημα πρέπει να διαθέτει δυνατότητες ενσωμάτωσης με τα άλλα εξαρτήματα ασφαλείας που προσφέρονται.	ΝΑΙ		
2.	Εγκατάσταση/πόμολογηση hardware appliance σε HA (active/standby). Να προσφερθούν 2 συσκευές.	ΝΑΙ		
3.	Το κάθε προσφερόμενο appliance να μπορεί να εξυπηρετήσει πλήθος IPSevents	>=300.000.000		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
4.	Οι προσφερόμενες συσκευές διαχείρισης πρέπει να έχουν τη δυνατότητα να κανουν Ingest και να αναλύουν τα ακόλουθα συμβάντα από τις διαχειριζόμενες συσκευές Τείχους προστασίας χωρίς πρόσθετους διακομιστές: - Εκδηλώσεις σύνδεσης. - Συμβάντα ασφαλείας (IPS, κακόβουλο λογισμικό). - Hostdiscovery (fingerprinting) events.	YES		
5.	Το κάθε προσφερόμενο appliance να υποστηρίζει πλήθος evets/sec	>=3.2 TB		
6.	Το κάθε προσφερόμενο appliance να υποστηρίζει 10 GbpsSFP+ με 10BASE-SR οπτικά	>=20,000 event/sec		
7.	Το κάθε προσφερόμενο appliance να υποστηρίζει διπλά τροφοδοτικά 1+1 και hotswappable	>=2		
8.	Το κάθε προσφερόμενο appliance να υποστηρίζει πλήρη και ενοποιημένη διαχείριση όλων των λειτουργιών των συστημάτων: Firewall, ApplicationControl, IntrusionPrevention (IPS και Malware)	NAI		
9.	Να υποστηρίζει κεντρική διαχείριση: Κεντρική διαμόρφωση, καταγραφή, παρακολούθηση και αναφορά	NAI		
10.	Να υποστηρίζει διαχείριση γεγονότων (events) και πολιτικών (policies)	NAI		
11.	Να υποστηρίζει προσαρμοζόμενα (custom) dashboards	NAI		
12.	Να υποστηρίζει προσαρμοζόμενες (custom) και προ-εγκατεστημένες (template-based) αναφορές (reports)	NAI		
13.	Να υποστηρίζει αυτοματοποιημένες συστάσεις (recommendations) για τις IPS πολιτικές που θα πρέπει να ενεργοποιηθούν για την αποφυγή falsepositives ενώ βελτιώνουν την αποδοχή και εξασφαλίζουν το επιθυμητό securityprotection επιπεδο	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Οι συστάσεις θα πρέπει να βασίζονται στην πληροφορία γνώσης του περιβάλλοντος και να είναι σχετικές, (για παράδειγμα) με τα λειτουργικά συστήματα που βρίσκονται στο δίκτυο.			
14.	Να υποστηρίζει γνώση του δικτυακού περιβάλλοντος (hosts, OS-Versions κ.τ.λ.) μέσω deerpaketinspection της κίνησης που περνάει μέσα από τις προσφερόμενες NGFW συσκευές.	NAI		
15.	Να υποστηρίζει αυτοματοποιημένες συστάσεις για securityevents που πρέπει να διερευνηθούν	NAI		
16.	Το σύστημα πρέπει να μπορεί να διαφοροποιεί συμβάντα IoC και να τα συσχετίζει με τον παραβιασμένο κεντρικό υπολογιστή, καθώς και να υπολογίζει τα επίπεδα επιπτώσεων ειδοποίησης ασφαλείας με βάση το λογισμικό και το προφίλ υπηρεσίας και τις πληροφορίες ευπάθειας που έχουν αντιστοιχιστεί στον κεντρικό υπολογιστή-στόχο.	NAI		
17.	Τα alerts να αναλύονται στον προσφερόμενο εξοπλισμό με βάση την επίπτωση κάθε απειλής (impactanalysis) και διαχωρισμό των απειλών σε διαφορετικές κατηγορίες.	NAI		
18.	Να υποστηρίζει συσχέτιση (correlation) επιθέσεων πραγματικού χρόνου.	NAI		
19.	Να υποστηρίζει εργαλεία ανίχνευσης (track) μολύνσεις μολύνσεων από κακόβουλο λογισμικό (malwareinfections), με δυνατότητα προβολής της πορείας του αρχείου διαμέσου των υπολογιστών του δικτύου (trajectory).	NAI		
20.	Υποστηρίξη ενός unified, time-based file και malware trajectory view το οποίο επιτρέπει την επιτάχυνση των file based malware investigations και παρέχει τουλάχιστον τα παρακάτω data points: - το File hash ως unique file identifier και primary search criteria;	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	<ul style="list-style-type: none"> - File disposition και security score; - File traversal path across hosts including the transit protocol; - Endpoint client application και nd web application data; - User information; - Information on potential malicious file transactions from the endpoint telemetry agent. 			
21.	Να υποστηρίζει Υποστήριξη μηχανισμού παραγωγής αναφορών σε επίπεδο χρήστη, εφαρμογής, και IPSevents.	ΝΑΙ		
22.	<p>Να έχει την δυνατότητα IoCs (Indication of Compromise): που να προσδιορίζουν τους πιθανώς παραβιασμένους εξυπηρετητές μέσω της συσχέτισης πολλαπλών συμβάντων από πολλές πηγές.</p> <p>Θα πρέπει να υποστηρίζεται η συσχέτιση των απειλών ανάλογα με χρήστη, συσκευή, υπηρεσία και εφαρμογή.</p>	ΝΑΙ		
23.	Το σύστημα πρέπει να μπορεί να ανακτήσει χαρακτηριστικά ετικετών (tag attributes) από το Azure, το AWS, το Office 365 και το AzureServiceTags, για να ενεργοποιηθούν οι αλλαγές πολιτικής στα NGFW χωρίς την πραγματική ανάγκη ανάπτυξης πολιτικής.	ΝΑΙ		
24.	Το σύστημα πρέπει να μπορεί να συλλέγει επαρκή συμφραζόμενα δεδομένα για τη δημιουργία σύνθετων προφίλ κεντρικού υπολογιστή (host profiles) που περιλαμβάνουν πληροφορίες σχετικά με τις εκδόσεις και τις υπηρεσίες του λειτουργικού συστήματος που εκτελούνται και τις ανοιχτές θύρες των hosts.	ΝΑΙ		
25.	Τα προαναφερθέντα host profiles πρέπει να συγκρίνονται με μια ενσωματωμένη βάση δεδομένων ευπάθειας του προσφερόμενου εξοπλισμού, ή/και δεδομένα συστήματος εξωτερικού σαρωτή ευπάθειας (external scanner).	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
26.	Τα δεδομένα hostprofiles πρέπει να χρησιμοποιούνται για τον εντοπισμό ανωμαλιών του προφίλ ενός κεντρικού υπολογιστή και να χρησιμοποιούνται για τη βελτίωση των υπολογισμών του βαθμού αντίκτυπου των ειδοποιήσεων IPS καθώς και του αυτοματοποιημένου συντονισμού της πολιτικής IPS.	ΝΑΙ		
27.	Τα δεδομένα προφίλ του κεντρικού υπολογιστή (hostprofile) πρέπει να χρησιμοποιούνται για τον εντοπισμό ανωμαλιών του προφίλ του κεντρικού υπολογιστή και να χρησιμοποιούνται για τη βελτίωση των υπολογισμών του βαθμού αντίκτυπου των ειδοποιήσεων IPS καθώς και του αυτοματοποιημένου συντονισμού της πολιτικής IPS.	ΝΑΙ		
28.	Το σύστημα πρέπει να συσχετίζει security, connnection και anomalyevents	ΝΑΙ		
29.	Οι ενημερώσεις IoCs πρέπει να επισημαίνουν συγκεκριμένα συμβάντα δικτύου που απαιτούν στενότερη παρακολούθηση.	ΝΑΙ		
30.	Να υποστηρίζει Υποστήριξη Structured Threat Information Expression (STIX™) για την ανταλλαγή cyber threat intelligence (CTI) με άλλες πηγές.	ΝΑΙ		
31.	Η συσκευή διαχείρισης πρέπει να υποστηρίζει διασύνδεση με λύση NetworkAccessControl για αυτοματοποιημένη απομάκρυνση παραβιασμένων συσκευών (compromisedendpoints) από το δίκτυο.	ΝΑΙ		
32.	Το σύστημα πρέπει να παρέχει δυναμικές προβολές χαρτών δικτύου με λεπτομερή ανάλυση και δυνατότητες φιλτραρίσματος τουλάχιστον για τα ακόλουθα θέματα: · Ιεραρχική προβολή χάρτη δικτύου · Παρουσίαση των συστημάτων, με σύνοψη του λειτουργικού συστήματος, της κρισιμότητας και πληροφοριών NetBIOS	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	<ul style="list-style-type: none"> Εμφανίζει τους υπολογιστές που έχουν παραβιαστεί, οργανωμένους με βάση indications of compromise (IOC) Σύνοψη εφαρμογών και συγκεντρωτικών πινάκων συσχέτισης με υπολογιστές Σύνοψη υπηρεσιών διακομιστών και συγκεντρωτικοί πίνακες με πληροφορίες Προσαρμοσμένες προβολές χαρακτηριστικών υπολογιστών σε συγκεντρωτικούς πίνακες Αντιστοίχιση ευπαθειών και λιστών ευπαθειών εξωτερικών πηγών σε συσχέτιση με τους προστατευμένους υπολογιστές 			
33.	<p>Το σύστημα πρέπει να παρέχει τις ακόλουθες δυνατότητες συντονισμού IPS: Χειροκίνητος συντονισμός των παραμέτρων αξιολόγησης υπογραφής IPS, όπως κατώφλια και ενέργειες ενεργοποίησης ειδοποίησης. Δυνατότητες δημιουργίας προσαρμοσμένων υπογραφών χρησιμοποιώντας τη μορφή υπογραφής Snortv3.</p> <p>Αυτοματοποιημένη ενεργοποίηση και απενεργοποίηση υπογραφής με βάση το επιθυμητό επίπεδο προστασίας / απαιτήσεις απόδοσης έναντι μιας συγκεκριμένης Πολιτικής IPS. Αυτοματοποιημένος συντονισμός πολιτικής IPS με βάση την απογραφή των προστατευόμενων περιουσιακών στοιχείων, λαμβάνοντας υπόψη τα προφίλ λογισμικού και υπηρεσιών αυτών των κεντρικών υπολογιστών. Παράλληλη χρήση πολλαπλών πολιτικών IPS με διαφορετικά σύνολα υπογραφών, μηχανισμό προεπεξεργαστή και ρυθμίσεις μεταβλητών συνόλων. Κατά προτίμηση το σύστημα πρέπει να επιτρέπει την επιλογή μιας πολιτικής IPS για έναν κανόνα πολιτικής ελέγχου προσβασης</p>	NAI		
34.	Ο προμηθευτής πρέπει να μπορεί να προσφέρει μια πλατφόρμα SOAR στην οποία το σύστημα μπορεί να στείλει	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	συμβάντα ασφαλείας και τα σχετικά συμβάντα σύνδεσης. Η πλατφόρμα SOAR πρέπει να μπορεί να προωθεί ορισμένα συμβάντα ασφαλείας σε Συμβάντα με βάση τα παρεχόμενα από τον προμηθευτή κριτήρια και προσαρμοσμένα κριτήρια φιλτραρίσματος συμβάντων.			
35.	Να προσφέρεται τεχνική υποστήριξη από τον κατασκευαστή του εξοπλισμού 24x7, και δυνατότητα RMA την επόμενη εργάσιμη μέρα.	≥ 3 χρόνια		

7.2.2.10 Switches για τη διασύνδεση των firewalls

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
1.	Αριθμός μεταγωγών	2		
2.	Να αναφερθεί μοντέλο και εταιρεία κατασκευής για κάθε έναν από τους μεταγωγούς	NAI		
3.	Αριθμός πορτών 40/100GbpsQSFP28 ανα μεταγωγέα	>=12		
4.	Αριθμός πορτών 1/10/25GbpsSFP/SFP+ ανα μεταγωγέα	>=48		
5.	Αριθμός πορτών για διαχειριστικούς λόγους ανα μεταγωγέα	>=2		
6.	Αριθμός USB πορτών	>=1		
7.	Δυνατότητα διαχείρισης μέσω consoleport (RS-232 port)	NAI		
8.	Συνολική αθροιστική ταχύτητα μεταγωγής κάθε μεταγωγού Layer 2 και Layer 3	≥4.8 Tbps		
9.	Ικανότητα διαμεταγωγής πακέτων ανά δευτερόλεπτο	≥2.5 bpps		
10.	Ο μεταγωγέας θα πρέπει να υποστηρίζει διόρθωση των μεταδιδόμενων λαθών (FC-FEC&RS-FEC)	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
11.	Όλες οι πόρτες πρέπει να υποστηρίζουν MACSEC κρυπτογράφηση	ΝΑΙ		
12.	Εισαγωγή καθυστέρησης μεταγωγής πακέτων (Latency)	<=1 microsecond		
13.	Να υποστηρίζονται καλώδια τύπου Directattachcable (DAC) για την διασύνδεση : 40/100 GbpsEthernet Θύρες	ΝΑΙ		
14.	Να υποστηρίζονται καλώδια τύπου Directattachcable (DAC) για την διασύνδεση :10 GbpsEthernet Θύρες ανα μεταγωγό ή SFP+ SR 10Gbps ανάλογα με την κάρτα που θα προσφερθεί στους εξυπηρετητές	ΝΑΙ		
15.	Δυνατότητα προσαρμογής στο Rack με την εισαγωγή του αέρα από την πλευρά των θυρών , είτε με την εξαγωγή του αέρα από την πλευρά των θυρών με την αντίστοιχη αλλαγή/προμήθεια των ανεμιστήρων και των τροφοδοτικών	ΝΑΙ		
16.	Υποστήριξη εφεδρικού τροφοδοτικού και εφεδρικών ανεμιστήρων	ΝΑΙ		
17.	Δυνατότητα αντικατάστασης τροφοδοτικού και ανεμιστήρων χωρίς διακοπή λειτουργίας του μεταγωγέα.	ΝΑΙ		
18.	Υποστήριξη σε λειτουργία VXLANEVPNfabric	ΝΑΙ		
19.	Υποστήριξη δυναμικών πρωτοκόλλων δρομολόγησης OSPF,BGP	ΝΑΙ		
20.	Δυνατότητα διαχείρισης του μεταγωγέα μέσω πλατφόρμας διαχείρισης	ΝΑΙ		
21.	Δυνατότητα αποστολής δεδομένων τηλεμετρίας σε εργαλείο ανάλυσης	ΝΑΙ		
22.	Μέγιστος αριθμός υποστηριζόμενων MACaddresses εγγραφών	>=256000		
23.	Μέγιστος αριθμός υποστηριζόμενων ECMP διαδρομών	64		
24.	Μέγεθος Buffer	>=40 MB		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
25.	Μέγιστος Αριθμός δικτυακών διαδρομών (IProutes)	≥ 896000		
26.	Μέγιστος Αριθμός Multicast Routes	≥ 128000		
27.	Μέγιστος Αριθμός VRFs	≥ 16000		
28.	Μέγιστος Αριθμός port Channels	≥ 512		
29.	Μέγιστος αριθμός συνδέσεων σε portchannel	≥ 32		
30.	Μέγιστος Αριθμός NAT entries	≥ 1023		
31.	Μέγιστος Αριθμός Multiple Spanning Tree (MST) instances	≥ 64		
32.	Αριθμός υποστηριζόμενων VLANs	≥ 4096		
33.	Δυνατότητα παραμετροποίησης 2 μεταγωγών με τέτοιο τρόπο ώστε να μπορεί να δημιουργηθεί ένα λογικό κανάλι που θα ομαδοποιεί ανά δύο (2) και ανά υποσύστημα μεταγωγής τις θύρες Ethernet του κάθε εξυπηρετητή ή του κάθε μεταγωγέα που δύναται να συνδεθεί με τους διακομιστές, μέσω IEEE 802.3adLinkAggregation. Μέσα από το κανάλι αυτό ο εξυπηρετητής θα επικοινωνεί μέσω IEEE 802.1QVLANtagging, ώστε να συμμετέχει σε άνω του ενός VLAN. (Multichassisportchannel). Η προηγούμενη δυνατότητα να υποστηρίζεται χωρίς την ενοποίηση του controlplane των μεταγωγών (stacking)	NAI		
34.	Μέγιστος αριθμός active SPAN Sessions	≥ 4		
35.	Υποστήριξη HSRP ή αντίστοιχο	NAI		
36.	Μέγιστος αριθμός HSRP Groups	≥ 490		
37.	Μέγιστος αριθμός Access List Entries – ingress	≥ 5000		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
38.	Μέγιστος αριθμός Access List Entries – egress	>=2000		
39.	Ο προσφερόμενος αριθμός θυρών πρέπει να καλύπτει πλήρως τις ανάγκες της συνδεσμολογίας	ΝΑΙ		
40.	Να αναφερθεί ο χώρος που καταλαμβάνεται στο Rack	ΝΑΙ		

7.2.2.11 Virtual firewall Για 10 tenants με High availability Καιάδειες IPS και antimalware

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
1.	Να προσφερθεί Virtual Next Generation Firewall και Next Generation Intrusion Prevention System Platform που να υποστηρίζει: προστασία από κακόβουλο λογισμικό, FW, NAT, IPS, λειτουργία προστασίας από κακόβουλο λογισμικό και έλεγχο παρακολούθησης εφαρμογών (application control, visibility)	ΝΑΙ		
2.	Ο προμηθευτής πρέπει να προσφέρει ευελιξία στις δυνατότητες αδειοδότησης και να επιτρέπει τη φορητότητα αδειών χρήσης τόσο σε privatecloud και όσο και σε publiccloud καθώς και σε virtualmachineinstances. Παρακαλούμε αναλύστε τις δυνατότητες εγκατάστασης της προσφερόμενης λύσης	ΝΑΙ		
3.	Ο κατασκευαστής θα πρέπει να είναι σε θέση να προσφέρει πολλαλές βαθμίδες επιδόσεων των virtualfirewalls, που να είναι κοινές μεταξύ των πλατφόρμών, αλλάζοντας μόνο τις απαιτήσεις των πόρων των εικονικών μηχανημάτων.	ΝΑΙ		
4.	Η πολιτική αδειοδότησης θα πρέπει να είναι υπο τη μορφή subscription διάρκειας 3 ετών	ΝΑΙ		
5.	Εκτός από standard REST API, ο προμηθευτής πρέπει να έχει Terraform templates, καθώς και εγγενή IaC templates για AWS και Azure (CF και ARM templates αντίστοιχα).	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
6.	Υποστήριξη SR-IOV.	NAI		
7.	Το σύστημα πρέπει να υποστηρίζει τις ακόλουθες πλατφόρμες : VMware, KVM, AWS, Azure, OCI, GCP, Cisco HyperFlex, Nutanix, OpenStack, Alibaba Cloud.	NAI		
8.	Εκτός από το Threatintelligencefeed και τις υπογραφές του ίδιου του κατασκευαστή, το σύστημα θα πρέπει να είναι σε θέση να χρησιμοποιεί και να αξιολογεί τις ακόλουθες μορφές πληροφοριών και υπογραφών: <ul style="list-style-type: none"> Υπογραφές STIX IoC μέσω χειροκίνητης αποστολής, αυτοματοποιημένης κατανάλωσης από κοινόχρηστα στοιχεία δικτύου και μέσω του πρωτοκόλλου TAXII. Μορφοποιημένες υπογραφές IPS Snort v3 Προδιαγραφές OpenAppID AVC Κατηγοριοποιημένη λίστα κακόβουλων IPs, domain και URLs που βρίσκονται σε αρχεία κειμένου. 	NAI		
9.	Το σύστημα πρέπει να συσχετίζει για τα προστατευμένα assets τα χαρακτηριστικά του λειτουργικού τους και του software τους με μια ενσωματωμένη βάση δεδομένων ευπαθειών.	NAI		
10.	Το σύστημα πρέπει να είναι σε θέση να δίνει προτεραιότητα στις ειδοποιήσεις ασφαλείας με βάση τα χαρακτηριστικά του λειτουργικού συστήματος και του λογισμικού του host καθώς και να εντοπίζει συσχετισμένες ευπάθειες των παραπάνω με ενσωματωμένες (outofthebox) λειτουργίες	NAI		
11.	Το σύστημα πρέπει να υποστηρίζει hardwareacceleration της κρυπτογράφησης σε περιβάλλοντα VMware και KVM. Παρακαλούμε επεξηγήστε τις δυνατότητες, τους περιορισμούς και τις απαιτήσεις υλικού (hardwarerequirements) του hypervisorhost.	NAI		
12.	Το σύστημα πρέπει να παρέχει τις ακόλουθες δυνατότητες ρύθμισης IPS: <ul style="list-style-type: none"> Χειροκίνητη ρύθμιση των παραμέτρων αξιολόγησης των IPS 	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	<p>signatures , όπως alert triggers και ενέργειες.</p> <ul style="list-style-type: none"> Δημιουργία custom signatures μετο format Snort v3 Αυτοματοποιημένη ενεργοποίηση και απενεργοποίηση υπογραφών IPS με βάση το επιθυμητό επίπεδο προστασίας / απαιτήσεις απόδοσης έναντι μιας συγκεκριμένης πολιτικής IPS. Αυτοματοποιημένη προσαρμογή της πολιτικής IPS με βάση το inventory των προστατευμένων assets, λαμβάνοντας υπόψη το προφίλ λογισμικού και υπηρεσιών των hosts. Παράλληλη χρήση πολλών πολιτικών IPS με διαφορετικά σύνολα υπογραφών, ρυθμίσεις μηχανισμού προεπεξεργαστή και συνόλου μεταβλητών. Κατά προτίμηση, το σύστημα θα πρέπει να επιτρέπει την επιλογή μιας πολιτικής IPS για έναν κανόνα πολιτικής ελέγχου πρόσβασης. 			
13.	Τα virtualNGFW / NGIPS πρέπει να μοιράζονται τη λύση κεντρικής διαχείρισης με την κύρια hardware πλατφόρμα NGFW.	NAI		
14.	Τα προτεινόμενα virtualNGFW/NGIPS πρέπει να έχουν πανομοιότυπες δυνατότητες ενσωμάτωσης SOAR με την προτεινόμενη κύρια πλατφόρμα NGFW.	NAI		
15.	Ο κατασκευαστής θα πρέπει να μπορεί να προσφέρει μια πλατφόρμα SOAR στην οποία το σύστημα μπορεί να στέλνει συμβάντα ασφαλείας και τα σχετικά συμβάντα σύνδεσης.	NAI		
16.	<p>Το προτεινόμενο σύστημα θα πρέπει να υποστηρίζει τη λειτουργία του ως RemoteAccessVPNconcentrator με τα ακόλουθα χαρακτηριστικά:</p> <ul style="list-style-type: none"> Υποστήριξη πρωτοκόλλου IPsec IKEv2, TLS και DTLS . SAML ως κύρια μέθοδος ελέγχου ταυτότητας. Ως εναλλακτική λύση του SAML - θα πρέπει να υποστηρίζονται 	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	<p>τουλάχιστον δύο μέθοδοι ελέγχου ταυτότητας βάσει ονόματος χρήστη και κωδικού πρόσβασης που μπορούν να χρησιμοποιήσουν πεδία τοπικής βάσης δεδομένων, RADIUS ή LDAP ή συνδυασμό τους.</p> <ul style="list-style-type: none"> • Προαιρετικό πεδίο authorization που υποστηρίζει μόνο RADIUS ή LDAP. • Τουλάχιστον δύο μέθοδοι ελέγχου ταυτότητας που βασίζονται σε ψηφιακά πιστοποιητικά και εκτελούνται σε μια ακολουθία μέσα σε μία μόνο περίοδο λειτουργίας ελέγχου ταυτότητας που μπορούν να συνδυαστούν με SAML ή με τις προαναφερθείσες μεθόδους που βασίζονται σε όνομα χρήστη και κωδικό πρόσβασης. • Υποστήριξη RADIUS Change of Authorization • Υποστήριξη διάφορων χαρακτηριστικών εξουσιοδότησης RADIUS, συμπεριλαμβανομένων των downloadable ACLs και των Security Group Tags (SGTs). 			
17.	<p>Το προτεινόμενο σύστημα πρέπει να είναι σε θέση να υλοποιεί κανόνες πολιτικής τείχους προστασίας με βάση την ταυτότητα χρήστη, μέσω integration με το activedirectory (με native τρόπο ή μέσω ενσωμάτωσης με passive τρόπο με connector)</p>	NAI		
18.	<p>Το σύστημα κεντρικής διαχείρισης των virtualfirewalls πρέπει να είναι ίδιο με το σύστημα διαχείρισης των NGFW appliances και πρέπει να είναι σε θέση:</p> <ul style="list-style-type: none"> • Να παρέχει κεντρική διαμόρφωση και παρακολούθηση των διαχειριζόμενων συσκευών. • Να αναλύει συμβάντα σύνδεσης και ασφάλειας, αλλά παράλληλα είναι σε θέση να κάνει trigger τις συσκευές ώστε να στέλνουν secure syslog events σε εξωτερικά συστήματα SIEM. 	NAI		



A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	<ul style="list-style-type: none">• Να κάνει proxy και μετασχηματισμό συμβάντων σε SNMP και σε summarized SMTP alerts.• Να παρέχει ένα πλήρως προσαρμόσιμο dashboard παρακολούθησης.• Να παρέχει προεπιλεγμένα και προσαρμοσμένα dashboards / event tables με δυνατότητες για εκβάθυνση στα workflows• Να μετατρέπει κάθε ενσωματωμένο και προσαρμοσμένο πίνακα σε reporting templates μέσω του GUI χωρίς να χρειάζεται programming developement ή δημιουργία ερωτήματων SQL.• Να μπορεί να προγραμματίζει: δημιουργία αντιγράφων ασφαλείας, δημιουργία αναφορών, αναβάθμιση και εργασίες ενημέρωσης εργασιών.• Ενοποίηση με το σύστημα SOAR που προσφέρεται με τρόπο τέτοιο ώστε το περιβάλλον εργασίας περιστατικού, έρευνας και ειδοποίησης του συστήματος SOAR να είναι ορατό στην κύρια κονσόλα με τα δικαιώματα χρήση διαχειριστή να λαμβάνονται υπόψη και για τα δύο συστήματα.• Να διαθέτει δυνατότητες SOAR και εκκίνησης (cross launch) UI άλλων κατασκευαστών.• Να διαθέτει time -based προβολές malware συμβάντων μέσω του integration με endpoint agent συστήματα για ενημέρωση επι συγκεκριμένων events• Να συσχετίζει εσωτερικά συμβάντα IPS, IoC, Intelligence, Malware και connection events με πληροφορίες σύνδεσης χρήστη, host OS και υπηρεσιών εφαρμογών σε ένα προφίλ host.• Να διαθέτει δυνατότητες ανίχνευσης ανωμαλιών σε επιπεδο			

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	<p>κίνησης δικτύου και επιπεδο host profile</p> <ul style="list-style-type: none"> • Να υποστήριζει τη συσχέτιση ανωμαλιών, συμβάντων ασφάλειας και σύνδεσης σε συμβάντα μετα-δεδομένων και ενεργοποίηση αυτοματοποιημένων διαδικασιών εξωτερικής αποκατάστασης. • Οι αυτοματοποιημένες διαδικασίες αποκατάστασης πρέπει να είναι σε θέση να ζητήσουν καραντίνα στο προτεινόμενο σύστημα ελέγχου πρόσβασης στο δίκτυο (NAC) για να χρησιμοποιηθούν πρώτα στο πλαίσιο RAVPN και στη συνέχεια να επεκταθούν για τα δίκτυα LAN και WLAN. • Δυνατότητα δημιουργίας custom remediation scripts. 			
19.	Η λύση κεντρικής διαχείρισης πρέπει να μπορεί να προσλαμβάνει, να αποθηκεύει και να αναλύει τα συμβάντα, με προαιρετική δυνατότητα προσθήκης προηγούμενου διατηρητέου storage εκ των υστέρων	NAI		
20.	Η προτεινόμενη λύση πρέπει να είναι σε θέση να συλλέγει τα γενικά συμβάντα αρχείων και IoC από τα endpoints και να τα ενσωματώνει σε μια χρονολογική συνάρτηση απεικόνισης της τροχιάς του αρχείου (filetrajectory).	NAI		
21.	Η προτεινόμενη λύση πρέπει να είναι σε θέση να συσχετίσει συμβάντα IoC με συμβάντα NGFW ή NGIPS.	NAI		
22.	Η προτεινόμενη λύση πρέπει να ενσωματώνεται με το σύστημα SOAR στο οποίο τα παρατηρήσιμα δεδομένα από συμβάντα NGFW ή NGIPS μπορούν να ερευνηθούν πλήρως σε μια λεπτομερή βάση δεδομένων τηλεμετρίας τελικού σημείου με πλήρως αυτοματοποιημένο τρόπο.	NAI		
23.	Το προτεινόμενο συστήματα πρέπει να διαθέτει άδεια χρήσης για δυνατότητες	NAI		



A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Firewall, AVC, IPS και Anti-Malware με ανάλυση αρχείων σε cloudsandbox			
24.	<p>Το προτεινόμενο σύστημα πρέπει να διαθέτει ολοκληρωμένες δυνατότητες ελέγχου λογισμικού κακόβουλης λειτουργίας και αρχείων όπως:</p> <ul style="list-style-type: none">• Εντοπισμός του πραγματικού τύπου αρχείων και αποκλεισμός αρχείων με βάση τον πραγματικό τύπο και το πρωτόκολλο τους - ελεγχοντάς τα με ένα ευέλικτο μοντέλο πολιτικής, το οποίο επιτρέπει τη χρήση διαφορετικών πολιτικών ελέγχου αρχείων ανά κανόνα πολιτικής ελέγχου πρόσβασης.• Τουλάχιστον ένας μηχανισμός αναζήτησης file reputation και heuristic fingerprint, ο οποίος παρέχει αποτελεσματικές δυνατότητες ανίχνευσης κακόβουλου λογισμικού• Τουλάχιστον ένας τοπικός μηχανισμός AV ροής.• Προαιρετικές δυνατότητες για την υποβολή αρχείων σε on premises ή cloud sandbox. Παρακαλούμε αναλύστε τις προσφερόμενες δυνατότητες.	ΝΑΙ		
25.	<p>Θα πρέπει να υποστηρίζονται οι παρακάτω βαθμίδες απόδοσης:</p> <ul style="list-style-type: none">• Βαθμίδα 1:<ul style="list-style-type: none">○ Fw, IPS, AVC (combined throughput) : 100 Mbps○ Μέγιστος αριθμός ταυτόχρονων περιόδων λειτουργίας: 100000○ Νέες συνδέσεις ανά δευτερόλεπτο: 12500○ Μέγιστος αριθμός VPN peers: 250.○ IPsec VPN throughput: 100 Mbps. <p>Να προσφερθούν 20 Virtual firewalls Βαθμίδας 1 ώστε να υλοποιηθούν σε active/standby υλοποίηση για 10</p>			

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	<p>tenants με διάρκεια subscription και υποστήριξης IPS, FW, Application control 3 χρόνια</p> <ul style="list-style-type: none"> Βαθμίδα 2: <ul style="list-style-type: none"> Fw, IPS, AVC (combined throughput) : 1 Gbps Μέγιστος αριθμός ταυτόχρονων περιόδων λειτουργίας: 100000 Νέες συνδέσεις ανά δευτερόλεπτο: 20000 Μέγιστος αριθμός VPN peers: 250. IPsec VPN throughput: 1 Gbps <p>Να προσφερθούν 20 Virtual firewalls Βαθμίδας 2 ώστε να υλοποιηθούν σε active/standby υλοποίηση για 10 tenants με διάρκεια subscription και υποστήριξης IPS, FW, Application control 3 χρόνια</p>			

7.2.2.12 Λύση Microsegmentation

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Η λύση θα πρέπει να υποστηρίζει microsegmentation σε επίπεδο workload (VM ή baremetals server ή container)	ΝΑΙ		
	Η Λύση θα πρέπει να διαθέτει γραφικό περιβάλλον που να δείχνει συμπεριφορά των διαδικασιών (processbehavior) και την συμπεριφορά forensic	ΝΑΙ		
	Η λύση θα πρέπει να υποστηρίζει την αναγνώριση των τρωτών σημείων του λογισμικού (softwarevulnerabilities)	ΝΑΙ		
	Η λύση θα πρέπει να υποστηρίζει την ανίχνευση ανωμαλιών επικοινωνίας σε επίπεδο δικτύου	ΝΑΙ		
	Η λύση θα πρέπει να υποστηρίζει την αναγνώριση της ανοικτής επιφάνειας επίθεσης, συνδιάζοντας πληροφορία σχετική με θύρες επικοινωνίας, διαδικασίες και στοιχεία κίνησης (trafficvolume) για παραδειγμα να μπορεί να εντοπίζει εάν γνωστές θύρες είναι ανοικτές για 2 βδομάδες και δεν χρησιμοποιούνται.	ΝΑΙ		
	Η Λύση θα πρέπει να υποστηρίζει όλες τις λειτουργίες 1.1 - 1.5 σε εικονικές μηχανές, σε servers που είναι baremetal και σε workloads που βρίσκονται σε containers	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Η λύση θα πρέπει να προσφέρθει με άδειες για 500 endpoint και 600 εικονικές μηχανές.			
	Η λύση θα πρέπει να υποστηρίζει όλες τις λειτουργίες ενός εικονικού περιβάλλοντος ανεξάρτητα από το περιβάλλον hypervisor.	NAI		
	Η λύση θα πρέπει να είναι cloudagnostic δηλαδή να υποστηρίζει όλες τις λειτουργίες υανεξάρτητα από την επιλογή δημόσιο cloud (AWS, GCP, Azure) και ανεξάρτητα από το που βρίσκεται το ιδιωτικό cloud.	NAI		
	Η λύση θα πρέπει να υποστηρίζει την παρακάτω λίστα λειτουργικών συστημάτων για διακομιστές Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012R2, Windows Server 2012, Windows Server 2008R2, Windows Storage Server 2016, Windows 10 Enterprise LTSC 2019, Windows 10 Enterprise LTSC 2019, Windows 11 with x86_64 architecture. ubuntu 16.04, 18.04, 20.04, 14.04, oracle linux 7.x, 8.x, 6.1, AIX 7.1, 7.2, 7.3, 6.1 (ppc architecture), Centos 7.x, 8.x, 6.1, Red Hat Enterprise Linux 7.x, 8.x, 6.1	NAI		
	Η πλατφόρμα θα πρέπει να έχει τη δυνατότητα να συλλέγει τηλεμετρία με εναλλακτικές επιλογές όπου δεν είναι δυνατή η εγκατάσταση agent λογισμικού. Παρακαλούμε να αναφέρετε τις εναλλακτικές επιλογές με την προσθήκη επιπλέον αδειών και υποδομής virtual, εάν χρειάζεται. Οι επιπλέον άδειες και υποδομή δεν απαιτείται να προσφερθεί στην παρούσα προσφορά	NAI		
	Η λύση θα πρέπει να υποστηρίζει τη μελλοντική επέκταση και να λαμβάνει τηλεμετρία με Netflowv9 και IPFIX με προσθήκη επιπλέον αδειών και εξαρτημάτων, εάν χρειάζεται	NAI		
	Η λύση θα πρέπει να συλλέγει τηλεμετρία και μοτίβα επικοινωνίας σε πραγματικό χρόνο από τους φόρτους εργασίας (workloads)	NAI		
	Η λύση θα πρέπει να παρέχει μια επιλογή για τον έλεγχο της χρήσης της CPU που επιτρέπεται στον agent της λύσης	NAI		
	Η λύση θα πρέπει να υποστηρίζει λειτουργίες που επιτρέπουν στο διαχειριστή να ρυθμίζει διαφορετικά όρια CPU που μπορεί να χρησιμοποιεί ο agent της λύσης ανάλογα με το περιβάλλον του διακομιστή. Για παράδειγμα, η λύση θα πρέπει να υποστηρίζει να μπορούν να ορίζονται διαφορετικά όρια CPU για διακομιστές Linux έναντι διακομιστών Microsoft Windows.	NAI		
	Περιγράψτε λεπτομερώς το επίπεδο ορατότητας που παρέχουν ο agent της λύσης για τον κεντρικό υπολογιστή, στον οποίο εκτελείται.	NAI		
	Περιγράψτε λεπτομερώς όλες τις πληροφορίες τηλεμετρίας που καταγράφονται από τους agent λογισμικού σε κάθε host	NAI		
	Πρέπει να είναι δυνατή η διαχείριση της αναβάθμισης δυνατοτήτων ορατότητας, επιβολή πολιτικής χωρίς την εκ νέου εγκατάσταση λογισμικού στο φόρτο εργασίας	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Η λύση θα πρέπει να είναι συμβατή με IPv4, IPv6 addressing σε όλα τα στοιχεία της (agent λογισμικού και πλατφόρμα SaaS)	ΝΑΙ		
	Η λύση θα πρέπει να προσφέρεται ως SaaS υπηρεσία	ΝΑΙ		
	η λύση θα πρέπει να ενσωματωθεί με το IBMQRadar για συσχέτιση συμβάντων και ειδοποιήσεις.	ΝΑΙ		
	Λειτουργίες ορατότητας και χαρτογράφηση εξάρτησεων εφαρμογών (applicationdependency mapping)	ΝΑΙ		
	Η πλατφόρμα θα πρέπει να παρέχει μια ενοποιημένη προβολή για κάθε διακομιστή που εμφανίζει λεπτομέρειες σχετικά με: τις διεργασίες που εκτελούνται, τα εγκατεστημένα πακέτα λογισμικού, τις πολιτικές που επιβάλλονται, τη γεωγραφική θέση όπου επικοινωνούν τα workloads (εαν εαν server επικοινωνεί με κάποια συγκεκριμένη χώρα)	ΝΑΙ		
	Περιγράψτε τον τρόπο με τον οποίο μπορεί να γίνει αναζήτηση για το πλήρες inventory ενός host για χαρακτηριστικά όπως: Πλατφόρμα λειτουργικού συστήματος, διεργασίες εκτέλεσης (συμπεριλαμβανομένης της γραμμής εντολών, binaryhash), εγκατεστημένα πακέτα λογισμικού, λίστα ευπαθών	ΝΑΙ		
	Η λύση θα πρέπει να παρέχει την εικόνα όλων των επικοινωνιών σε επίπεδο host με χρονική σειρά (timeseriesviews)	ΝΑΙ		
	Η λύση θα πρέπει να διατηρεί πλήρη ανάλυση των λεπτομερειών συνομιλίας κατά τη διάρκεια της μέγιστης περιόδου διατήρησης σε πλήρη κλίμακα πλατφόρμας Δηλαδή ακόμα και όταν κάνει Scale σε περισσότερα VM (1000+) στο μέλλον	ΝΑΙ		
	Η λύση θα πρέπει να υποστηρίζει αναζήτηση για όλες τις λεπτομέρειες συνομιλίας με βάση πολλαπλά χαρακτηριστικά, όπως διευθύνσεις IP, hostnames, θύρες, ονόματα διεργασιών, αυθαίρετες ετικέτες (TAGS) κ.λπ.;	ΝΑΙ		
	η λύση θα πρέπει να μπορεί να ενσωματωθεί με εξωτερικά συστήματα όπως vCenter, Kubernetes, RedHatOpenshift, Δημόσια Σύννεφα, IPAM ή CMDB για να έχει περισσότερη πληροφορία (context) για κάθε διεύθυνση IP ή υποδίκτυο	ΝΑΙ		
	η λύση θα πρέπει να υποστηρίζει περισσότερα από 32 χαρακτηριστικά (attributes)/μεταδεδομένα (metadata) καθορισμένα από το χρήστη από τα εν λόγω εξωτερικά συστήματα. Αυτά τα χαρακτηριστικά μεταδεδομένων θα πρέπει να ορίζονται από το χρήστη	ΝΑΙ		
	η λύση θα πρέπει να έχει ενσωμάτωση με τείχη προστασίας για τον εντοπισμό και τη συρραφή ροών που διέρχονται από αυτά όταν χρησιμοποιείται NAT	ΝΑΙ		
	Η λύση θα πρέπει να παρέχει αυτόματη αντιστοίχιση εξάρτησης εφαρμογών (applicationdependency mapping) και αυτόματη δημιουργία πολιτικής με βάση δεδομένα συνομιλίας και επεξεργασίας	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Η λύση θα πρέπει να ανακαλύψει όλες τις εξαρτήσεις σε μια εφαρμογή είτε είναι υλοποιημένη σε onpremise datacenter είτε στο δημόσιο cloud είτε σε υβριδικό datacenter	NAI		
	Η λύση θα πρέπει να έχει τη δυνατότητα αυτόματης ομαδοποίησης workloads με παρόμοια συμπεριφορά βάση κίνησης και διαδικασιών σε ομάδες πολιτικής (μη επιτηρημένη μηχανική μάθηση - unsupervised ML)	NAI		
	Η λύση θα πρέπει να παρέχει μια ένδειξη ακρίβειας της ομαδοποίησης των workloads σε policy groups.	NAI		
	Η λύση θα πρέπει να δημιουργήσει αυτόματα πολιτική whitelist για τμηματοποίηση (segmentation), με βάση χάρτες εξάρτησης εφαρμογών χωρίς τη χρήση προτύπων (με εστίαση σε περιβάλλοντα Brownfield)	NAI		
	Η λύση θα πρέπει να χρησιμοποιεί AI/ML για να ανακαλύπτει και να δημιουργεί πολιτικές ασφαλείας	NAI		
	Η λύση θα πρέπει να χρησιμοποιεί πρότυπα εφαρμογών για να επιταχύνει την εφαρμογή των πολιτικών τμηματοποίησης (πχ sharepoint, activedirectory, sqltemplates κτλ)	NAI		
	Η λύση θα πρέπει να επιτρέπει τον καθορισμό πολιτικής ανώτερης τάξης για απαιτήσεις infosec ή κανονιστικής συμμόρφωσης, οι οποίες διαφέρουν από τις πολιτικές εφαρμογής που ανακαλύφθηκαν. Περιγράψτε τα επίπεδα ιεραρχίας πολιτικής που υποστηρίζονται. Η διαχείριση της ιεραρχίας πολιτικής πρέπει να ελέγχεται με βάση τους ρόλους και τα προνόμια των χρηστών της πλατφόρμας (RBAC)	NAI		
	Η λύση θα πρέπει να επιτρέπει τη βελτιστοποίηση της πολιτικής ασφαλείας μηδενικής εμπιστοσύνης που ανακαλύφθηκε, ώστε να επιτρέπονται ή να απαγορεύονται οι επικοινωνίες για ορισμένες ροές μέσω συγκεκριμένων υποδοχών (sockets)	NAI		
	Η λύση θα πρέπει να υποστηρίζει τη δημιουργία ομάδων πολιτικής και πολιτικών τμηματοποίησης εφαρμογών με βάση χαρακτηριστικά, ετικέτες ή ετικέτες VM	NAI		
	Η λύση θα πρέπει να εμφανίζει τις διαφορές μεταξύ διαφορετικών εκδόσεων πολιτικής	NAI		
	Η λύση θα πρέπει να παρέχει πλήρη καταγραφή όλων των προσβάσεων στο σύστημα και των εφαρμοζόμενων αλλαγών.	NAI		
	Η λύση θα πρέπει να υποστηρίζει προσομοιώσεις αλλαγής πολιτικής πριν από την επιβολή τους	NAI		
	Η λύση θα πρέπει να δείχνει τις επιπτώσεις μιας αλλαγής πολιτικής στα ιστορικά δεδομένα με αλλαγές πολιτικής	NAI		
	Η λύση θα πρέπει να παρέχει τη δυνατότητα προσομοίωσης των πολιτικών με τη χρήση δεδομένων σχεδόν σε πραγματικό χρόνο, χωρίς να χρειάζεται να εφαρμόζεται η πολιτική	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Η λύση δεν θα πρέπει να απαιτεί οποιεσδήποτε αλλαγές στους κανόνες του τείχους προστασίας κεντρικού υπολογιστή κατά τον εντοπισμό πολιτικής και την προσομοίωση/δοκιμή	ΝΑΙ		
	Η λύση πρέπει να υλοποιήσει την τμηματοποίηση εφαρμογών σε κεντρικούς υπολογιστές χρησιμοποιώντας τα εγγενή τείχη προστασίας λειτουργικού συστήματος, όπως IPtables/IPSets, Windows firewall.	ΝΑΙ		
	Η λύση θα πρέπει να εντοπίζει, να διορθώνει και να κοινοποιεί κάθε προσπάθεια παράκαμψης της εφαρμογής της πολιτικής τμηματοποίησης (αντίμετρα παραποίησης)	ΝΑΙ		
	Η λύση θα πρέπει να υποστηρίζει τον ορισμό πολιτικής σε μορφή φυσικής γλώσσας για τμηματοποίηση που είναι ανεξάρτητη από τη διεύθυνση IP ενός φόρτου εργασίας ή το VLAN ή το hostname.	ΝΑΙ		
	η λύση θα πρέπει να υποστηρίζει τη συνεπή επιβολή της πολιτικής ασφάλειας εφαρμογών σε πολλαπλά περιβάλλοντα cloud (σε onpremise datacenter, ιδιωτικά και δημόσια cloud)	ΝΑΙ		
	Η λύση θα πρέπει να βελτιώνει την πολιτική microsegmentation για να συμπεριλάβει χαρακτηριστικά εμπλουτισμένων τελικών σημείων και συσκευών χωρίς να εγκατασταθούν επιπλέον πράκτορες	ΝΑΙ		
	η πλατφόρμα λαμβάνει τα συμφραζόμενα δεδομένα και την τηλεμετρία ροής από τους απομακρυσμένους χρήστες που έχουν πρόσβαση στο δίκτυο μέσω της προτεινόμενης λύσης απομακρυσμένης πρόσβασης σε πραγματικό χρόνο, έτσι ώστε κάθε φορά που μια νέα συσκευή συνδέεται στο VPN, η λύση για microsegmentation πρέπει να μπορεί να λαμβάνει : Πληροφορίες τερματικού συμπεριλαμβανομένης της τηλεμετρίας ροής, των πληροφοριών διεργασίας, των εφαρμογών που χρησιμοποιούνται και των πληροφοριών ταυτότητας χρήστη.	ΝΑΙ		
	η πλατφόρμα λαμβάνει τα συμφραζόμενα δεδομένα από το προτεινόμενο NAC σε πραγματικό χρόνο, έτσι ώστε κάθε φορά που μια νέα συσκευή συνδέεται στο NAC, η λύση για μικροτμηματοποίηση πρέπει να μπορεί να λαμβάνει: Προφίλ τελικού σημείου, posture συσκευής	ΝΑΙ		
	Η λύση μικροτμηματοποίησης θα πρέπει να μπορεί να προσαρμόζει δυναμικά τις πολιτικές ασφαλείας με βάση τις αλλαγές στο posture του τελικού χρήστη ή της συσκευής	ΝΑΙ		
	Παράδειγμα πολιτικής που βασίζεται στον τύπο της συσκευής (καθορίζεται από το προφίλ τελικού σημείου της: Ένα σύστημα ελέγχου HVAC δεν μπορεί να συνδεθεί σε οτιδήποτε άλλο εκτός από την εφαρμογή HVAC.	ΝΑΙ		
	2. Παράδειγμα πολιτικής που βασίζεται στο posture της συσκευής: Ένας χρήστης που χρησιμοποιεί ένα iPhone που έχει σπάσει από τη	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	φυλακή δεν μπορεί να έχει πρόσβαση σε εφαρμογές που σχετίζονται με τη συμμόρφωση.			
	Η λύση θα πρέπει να μπορεί να επιλέγει ποια χαρακτηριστικά LDAP-AD που σχετίζονται με το τελικό σημείο και τον χρήστη θα ληφθούν και θα υποβληθούν σε επεξεργασία (τουλάχιστον 6 χαρακτηριστικά, για παράδειγμα ldapcommonname, ldapdistinguishedname, sAMAccountName κ.λπ.)	NAI		
	Η λύση θα πρέπει να επιτρέπει την αναζήτηση ιδιοτήτων τελικού χρήστη ή συσκευής ή στάσης στη βάση δεδομένων αποθέματος (π.χ. εμφάνιση όλων των iPhone που είναι συνδεδεμένα σε μια εφαρμογή)	NAI		
	Η λύση θα πρέπει να παρακολουθεί την γενεαλογία δέντρου διεργασίας για κάθε διακομιστή και να διατηρεί μια ιστορική καταγραφή του δέντρου διεργασιών με την πάροδο του χρόνου	NAI		
	η λύση θα πρέπει να υποστηρίζει λειτουργίες για τον εντοπισμό αποκλίσεων από τη βασική συμπεριφορά (ανωμαλίες), όπως η εκτέλεση κακόβουλου κώδικα ή εντολές οι οποίες δεν έχουν ξαναδωθεί σε φόρτους εργασίας	NAI		
	Η λύση θα πρέπει να αποστέλλει ειδοποιήσεις με βάση μη εγκεκριμένη πρόσβαση σε εμπιστευτικά αρχεία, όπως αρχεία κωδικού πρόσβασης	NAI		
	Η λύση θα πρέπει να εντοπίζει κλιμακώσεις δικαιωμάτων (privilegeescalations) και τις εκτελέσεις shellcode στους διακομιστές	NAI		
	Η λύση θα πρέπει να παρακολουθεί οποιαδήποτε δραστηριότητα δημιουργίας rawsocket στους διακομιστές	NAI		
	η λύση θα πρέπει να ανιχνεύει ασυνεπείς μεταξύ hash διεργασιών για παρόμοιες διεργασίες στο περιβάλλον εφαρμογής	NAI		
	η λύση θα πρέπει να εντοπίζει κακόβουλη συμπεριφορά με βάση την απόκλιση από τη γνωστή καλή συμπεριφορά	NAI		
	Η λύση θα πρέπει εγγενώς να εντοπίζει ευπάθειες λογισμικού και να παρέχει λεπτομέρειες σχετικά με τα ευάλωτα πακέτα λογισμικού	NAI		
	Η λύση θα πρέπει να υποστηρίζει δυνατότητες τμηματοποίησης με βάση τις πολιτικές για φόρτους εργασίας με ευάλωτα πακέτα λογισμικού, είτε πρόκειται για την καρτρίνα των διακομιστών είτε για τη δυνατότητα να επιτρεπονται ροές προς διακομιστές αποκατάστασης	NAI		
	Η λύση θα πρέπει να παρέχει έναν τρόπο ανίχνευσης ανωμαλιών ροής δεδομένων που μπορεί να υποδεικνύουν συμβάντα διαρροής δεδομένων (dataexfiltration)	NAI		
	Η λύση θα πρέπει να παρέχει ορατότητα για Bogon, IP και φήμη τομέα με ενσωμάτωση με κορυφαίες τροφοδοσίες απειλών της βιομηχανίας	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Η λύση θα πρέπει να παρέχει αξιολόγηση της επιφάνειας επίθεσης μέσω του εντοπισμού ανοικτών, αλλά αχρησιμοποίητων υποδοχών και συναφών διεργασιών στον κεντρικό υπολογιστή	ΝΑΙ		
	Η λύση θα πρέπει να ενσωματωθεί με τις ροές STIX/TAXII	ΝΑΙ		
	Η λύση θα πρέπει να είναι του ιδίου κατασκευαστή με την λύση firewall για καλύτερη διαλειτουργικότητα			
	η λύση θα πρέπει να παρέχει σύνθετη αξιολόγηση security posture σε επίπεδο οργανισμού, εφαρμογής και κεντρικού υπολογιστή	ΝΑΙ		
	Η λύση θα πρέπει να αναλύει για να διαπιστώσει ποιοι διακομιστές αντιμετωπίζουν σημαντικά ζητήματα ασφαλείας. Αυτό θα πρέπει να συνδέεται με μια συγκεκριμένη εφαρμογή	ΝΑΙ		
	Να προσφερθούν άδειες / συνδρομές που απαιτούνται	≥ 36 μήνες		

7.2.2.13 Λύση Ασφαλείας και προστασίας των χρηστών από απειλές του διαδικτύου (Web Security Gateway) - 250 χρήστες και Συσκευές υλικού (HW appliances)

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
1.	Σύστημα Ασφαλείας και προστασίας των χρηστών από απειλές του διαδικτύου (WebSecurityGateway)			
2.	Να προσφερθεί Σύστημα Ασφαλείας και προστασίας των χρηστών από απειλές του διαδικτύου (WebSecurityGateway)	Ναι		
3.	Τεχνικά χαρακτηριστικά			
4.	Το προσφερόμενο Σύστημα να μπορεί να εγκαθίσταται σε υποδομή με φυσικά HW appliances του κατασκευαστή	ΝΑΙ		
5.	Να προσφερθούν ΔΥΟ (2) Συσκευές σε σύνδεση active/standby, και με δυνατότητα σύνδεσης active/active χωρίς την ανάγκη επιπλέον αδειών λογισμικού/εξοπλισμού.	ΝΑΙ		
6.	Να αναφερθεί Τύπος – Κατασκευαστής			
7.	Το κάθε προσφερόμενο σύστημα θα πρέπει να υποστηρίζει τουλάχιστον 250 χρήστες	≥ 250 χρήστες		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
8.	Το κάθε προσφερόμενο σύστημα πρέπει να ελέγχει την κίνηση HTTP, HTTPS και FTP από και προς το διαδίκτυο (Incoming&OutgoingWebtraffic), ανεξάρτητα από τις εφαρμογές που το χρησιμοποιούν.	ΝΑΙ		
9.	Να υποστηρίζει την inspection επιθεώρηση σε επίπεδο HTTP πρωτοκόλλου σε πραγματικό χρόνο (real-time).			
10.	Το κάθε προσφερόμενο σύστημα να έχει την δυνατότητα επιθεώρησης HTTPS πρωτοκόλλου.	ΝΑΙ		
11.	Το κάθε προσφερόμενο σύστημα να υποστηρίζει υπηρεσίες καταλόγου LDAP, ActiveDirectory κ.λ.π.	ΝΑΙ		
12.	Η υλοποίηση λύσης LDAP να επιτρέπει την δημιουργία πολιτικών ανά χρήστη ή ομάδα χρηστών. Σκοπός είναι να επιτρέπεται η διαμόρφωση πολιτικών σε επίπεδο τμημάτων ή διευθύνσεων του οργανισμού	ΝΑΙ		
13.	Δυνατότητα για την δημιουργία και εφαρμογή πολιτικών ασφαλείας ανά: εφαρμογή, χρήστη (domainuser/group) και συνδυασμό χρήστη και εφαρμογής	ΝΑΙ		
14.	Υποστήριξη λειτουργίας caching από το κάθε προσφερόμενο σύστημα	ΝΑΙ		
15.	Υποστήριξη λειτουργίας TransparentProxy με χρήση πρωτοκόλλου WCCP, με την χρήση αρχείων proxgauto-config (PAC) από το κάθε προσφερόμενο σύστημα	ΝΑΙ		
16.	Υποστήριξη δυνατότητας προσθήκης / φιλοξενίας αρχείων proxgauto-config (PAC) από το κάθε προσφερόμενο σύστημα	ΝΑΙ		
17.	Το κάθε προσφερόμενο σύστημα να έχει ομαδοποιημένες κατηγορίες φίλτρων URL και ιστότοπων	ΝΑΙ		
18.	Το κάθε προσφερόμενο σύστημα να υποστηρίζει αυτόματη ενημέρωση των φίλτρων URL και κατηγορίες ιστότοπων.	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
19.	Δυνατότητα ενημέρωσης των φίλτρων URL και ένταξη ιστότοπων σε συγκεκριμένη κατηγορία, από τον διαχειριστή από το κάθε προσφερόμενο σύστημα	ΝΑΙ		
20.	Χρήση διαφορετικών πολιτικών ασφαλείας ανά μέρα/ώρα από το κάθε προσφερόμενο σύστημα	ΝΑΙ		
21.	Το κάθε προσφερόμενο σύστημα να κάνει υποστήριξη αυτόματης κατηγοριοποίησης ιστοσελίδων (real-time categorization) που δεν ανήκουν ήδη σε κάποια κατηγορία με βάση το περιεχόμενο τους	ΝΑΙ		
22.	Η δυνατότητα άρνησης συνδέσεων σε επίπεδο πρωτοκόλλου ελέγχου μετάδοσης (TCP session) να είναι αυτόματη όπως π.χ να βασίζεται σε τεχνικές "φίλτρων φήμης" (reputation filters) από το κάθε προσφερόμενο σύστημα. Ο διαχειριστής να μπορεί να ρυθμίζει τον τρόπο συμπεριφοράς της συσκευής ανάλογα με την "φήμη".	ΝΑΙ		
23.	Το κάθε προσφερόμενο σύστημα να υποστηρίζει την δημιουργία πολλαπλών λιστών white/black (custom URL categories) από τον διαχειριστή.	ΝΑΙ		
24.	Το κάθε προσφερόμενο σύστημα να υποστηρίζει την εφαρμογή πολιτικών ασφαλείας περιεχομένου σε επίπεδο διακινούμενων αρχείων (download και upload) βάσει του payload του αρχείου και όχι της κατάληψής του (file type extension) από κάθε ελεγχόμενη συσκευή	ΝΑΙ		
25.	Το κάθε προσφερόμενο σύστημα να υποστηρίζει την επιθεώρηση και την απαγόρευση αποστολής αρχείων π.χ μέσω Webmail	ΝΑΙ		
26.	Το κάθε προσφερόμενο σύστημα να υποστηρίζει αναγνώριση εφαρμογών WEB 2.0 και εφαρμογή διαφορετικής πολιτικής ανά εφαρμογή από κάθε ελεγχόμενη συσκευή	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
27.	Θα πρέπει να υπάρχει δυνατότητα AntiVirus με δυνατότητα επιλογής ανάμεσα από διαφορετικούς κατασκευαστές. Να αναφερθούν οι υποστηριζόμενοι κατασκευαστές.	NAI		
28.	Το κάθε προσφερόμενο σύστημα να υποστηρίζει την ταυτόχρονη λειτουργία διαφορετικών AntiVirus μηχανισμών. (Αρκεί να προσφερθεί τουλάχιστον ένας μηχανισμός antivirus).	NAI		
29.	Το κάθε προσφερόμενο σύστημα πρέπει να περιλαμβάνει ένα σύγχρονο σύστημα προστασίας από κακόβουλο λογισμικό με διάφορες υπηρεσίες φήμης και sandboxing για την εισερχόμενη κίνηση εκτός από τους δύο προαναφερθέντες AV μηχανισμούς	NAI		
30.	Να υποστηρίζεται ο εντοπισμός zerodaythreat με χρήση sandboxing	NAI		
31.	Το κάθε προσφερόμενο σύστημα πρέπει να μπορεί να κάνει αποκρυπτογράφηση κίνησης τύπου ManInTheMiddle (MITM) με εγγενή αποκρυπτογράφηση TLS1.3 και 1.2.	NAI		
32.	Το κάθε προσφερόμενο σύστημα πρέπει να μπορεί να έχει τη δυνατότητα να ενσωματωθεί με υπηρεσίες απομόνωσης απομακρυσμένου προγράμματος περιήγησης (RBI) που βασίζονται σε σύννεφο, εάν απαιτηθεί στο μέλλον.	NAI		
33.	Το κάθε προσφερόμενο σύστημα πρέπει να έχει τη δυνατότητα να υλοποιηθεί με τους παρακάτω τρόπους χωρίς επιπλέον κόστος Explicit ή Transparentproxy: <ul style="list-style-type: none">σε διάταξη εφεδρείας με χρήση load balancing Μηχανισμών (με WCCP ή explicit proxy λειτουργία) ήσε διάταξη λειτουργίας VRRP βασισμένη σε Active / Standby υλοποίηση εφεδρείας.	NAI		
34.	Το κάθε προσφερόμενο σύστημα πρέπει να υποστηρίζει HTTP, HTTPS, FTP, SOCKSproxy	NAI		
35.	Η αδειοδότηση του συστήματος πρέπει να επιτρέπει την επέκταση των πόρων proxy (το	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	μέγεθος και τον αριθμό των εικονικών διακομιστών μεσολάβησης) χωρίς επιπλέον κόστος και αγορά άδειας			
36.	Το κάθε προσφερόμενο σύστημα Webproxy πρέπει να μπορεί να ενσωματωθεί με το παρεχόμενο σύστημα SOAR (XDR) για κεντρική διαχείριση πολλαπλών προϊόντων, αυτοματοποιημένη έρευνα απειλών και αυτοματοποιημένη απόκριση συμβάντων.	NAI		
37.	Το κάθε προσφερόμενο σύστημα πρέπει να κάνει έλεγχο του Bandwidth για ειδικούς τύπους περιεχομένου (streamingmedia)	NAI		
38.	Το κάθε προσφερόμενο σύστημα πρέπει να μπορεί να κάνει χρήση διαφορετικών πολιτικών ασφαλείας ανά μέρα/ώρα	NAI		
39.	Το κάθε προσφερόμενο σύστημα πρέπει να μπορεί να κάνει έλεγχο της πρόσβασης των χρηστών με χρήση time-quota και bandwidth-quota	NAI		
40.	Η προσφερόμενη λύση NGFW, SOAR και WebProxy, προτείνεται να είναι του ίδιου κατασκευαστή ώστε να επιτρέπει την μέγιστη διαλειτουργικότητα	NAI		
41.	Το κάθε προσφερόμενο σύστημα να συνοδεύεται από 3ετή εγγύηση (με δωρεάν συντήρηση του κατασκευαστή του για το λογισμικό). Να δοθούν τα σχετικά από τον κατασκευαστή αποδεικτικά στοιχεία, όταν αυτά γίνουν διαθέσιμα, και σε κάθε περίπτωση πριν την παραλαβή της λύσης.	NAI		
42.	Τηλεφωνική υποστήριξη 24x7 κατά τη διάρκεια της εγγύησης	NAI		
43.	Να συνοδεύεται από τις κατάλληλες άδειες 3 ετών, για συνεχείς ενημερώσεις όλου του λογισμικού.	NAI		
44.	Εγκατάσταση, παραμετροποίηση και προσαρμογή του υπό προμήθεια εξοπλισμού στο δίκτυο	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
45.	Η προσφερόμενη τεχνική υποστήριξη (περιλαμβάνεται και η παροχή και εγκατάσταση νέων ενημερώσεων, αναβαθμίσεων λογισμικού, και drivers) θα παρέχεται από κατάλληλα πιστοποιημένα πρόσωπα από τον κατασκευαστή.	NAI		
	Τεχνικά Χαρακτηριστικά των HWarpliances (proxy)			
46.	Να υποστηρίζουν τις λειτουργίες που αναγράφονται παραπάνω στον παρόντα πίνακα συμμόρφωσης			
47.	Υποστηριζόμενη μνήμη 16GB ανα συσκευή	NAI		
48.	Υποστηριζόμενο Storage: τεσσερα 600 GB hard disk drives (2.5" 12G SAS 10K RPM) ανα συσκευή	NAI		
49.	Το καθε προσφερομενο appliance να υποστηρίζει 1Gbps θύρες ανα συσκευή	>=6		
50.	Το καθε προσφερομενο appliance να υποστηρίζει διπλά τροφοδοτικά 1+1 και hotswappable ανα συσκευή	NAI		
51.	κοινή διαχείριση των κανόνων ασφάλειας και αναφορών από τις δυο συσκευές websecurity	NAI		
52.	Να έχει δυνατότητα κεντρικής διαχείρισης μέσω γραφικού περιβάλλοντος (GUI) όλων των συσκευών websecurity	NAI		
53.	Υποστήριξη Logging με δυνατότητα τοπικού φιλτραρίσματος και αποθήκευσης.	NAI		
54.	Να υποστηρίζει ενσωματωμένο μηχανισμό παραγωγής αναφορών σε επίπεδο Χρήστη, URL φίλτρων, TopusageReports (Users/Filters/Malware κ.λ.π).	NAI		
55.	Να υποστηρίζει ενσωματωμένο μηχανισμό παραγωγής αναφορών σχετικά με την χρήση εύρους ζώνης (bandwidth) συνολικά και ανά χρήστη.	NAI		
56.	Να υποστηρίζει ενσωματωμένο μηχανισμό παραγωγής αναφορών σχετικά με τον τύπο της δικτυακής κίνησης ενός χρήστη (OSILayerL4 trafficmonitoring)	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
57.	Κατά τη διάρκεια ενημέρωσης της συσκευής, οι ενεργοποιημένες υπηρεσίες να συνεχίζουν να λειτουργούν.	ΝΑΙ		
58.	Να διαθέτει ευέλικτο σχήμα αδειών για την μελλοντική αναβάθμιση των χαρακτηριστικών ή/και του αριθμού των υποστηριζόμενων χρηστών.	ΝΑΙ		
59.	Να προσφέρεται τεχνική υποστήριξη από τον κατασκευαστή του εξοπλισμού 24x7, και δυνατότητα RMA την επόμενη εργάσιμη μέρα.	≥ 3 χρόνια		
60.	Να συνοδεύεται από τις κατάλληλες άδειες 3 ετών , για συνεχείς ενημερώσεις όλων βάσεων και του λειτουργικού για 250 χρήστες	ΝΑΙ		

7.2.2.14 Λύση Αυστηρής πιστοποίησης για την απομακρυσμένη πρόσβαση (MFA, Zero Trust)

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
1.	Η λύση πρέπει να είναι SaaS και να προσφέρεται από το Cloud	ΝΑΙ		
2.	Η λύση θα πρέπει να προσφερθεί για χρήστες	≥250		
3.	Η λύση θα πρέπει να επιτρέπει στους χρήστες να εγγραφούν πολλαπλές συσκευές για πιστοποίηση	ΝΑΙ		
4.	Η λύση θα πρέπει να επιτρέπει στους χρήστες να ορίζουν ποια συσκευή είναι η προτιμητέα για πιστοποίηση	ΝΑΙ		
5.	Η λύση θα πρέπει να επιτρέπει στους χρήστες να επιλέγουν ποια είναι η εναλλακτική συσκευή που έχει οριστεί για αυτό το χρήστη ώστε να χρησιμοποιείται όταν η πρωτεύουσα συσκευή δεν είναι διαθέσιμη (primary)	ΝΑΙ		
6.	Η λύση θα πρέπει να επιτρέπει στους χρήστες να διαχειρίζονται τις συσκευές τους ώστε να μειωθεί το διαχειριστικό κόστος	ΝΑΙ		
7.	Η λύση θα πρέπει να επιτρέπει πολλαπλούς τρόπους πιστοποίησης Mobile Push, Soft Token, SMS, Phone Call, U2F, Wearables, Biometrics and Hardware Tokens	ΝΑΙ		
8.	Η λύση θα πρέπει να hardware token συμβατό με OATH	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
9.	Η λύση θα πρέπει να υποστηρίζει Yubikeytokens	NAI		
10.	Η λύση θα πρέπει να υποστηρίζει πιστοποίηση με onetimepasscode που παρέχεται από την εφαρμογή της λύσης που θα τρέχει στο κινητό τηλέφωνο	NAI		
11.	Η λύση θα πρέπει να υποστηρίζει προσωρινούς κωδικούς παρακαμψης για πιστοποίηση (bypasspasscode) για contractors και εταιρικούς χρήστες	NAI		
12.	Η λύση θα πρέπει να υποστηρίζει οι χρήστες για εγγράφουν πολλαπλές συσκευές για πιστοποίηση	NAI		
13.	Η λύση θα πρέπει να υποστηρίζει την παροχή δεύτερου παράγοντα για πιστοποίηση που να μπορεί να χρησιμοποιηθεί ακόμα και όταν δεν υπάρχει πρόσβαση στο δίκτυο	NAI		
14.	Η λύση θα πρέπει να παρέχει εργαλεία παραμετροποίησης ώστε να είναι δυνατός ο συγχρονισμός χρηστών από Activedirectory	NAI		
15.	Η λύση θα πρέπει να υποστηρίζει οι χρήστες να μπορούν να προστεθούν μέσω CSV αρχείου	NAI		
16.	Η λύση θα πρέπει να επιτρέπει οι χρήστες να μπορούν να εγγραφούν οι ίδιοι ώστε να μειώνεται ο χρόνος υλοποίησης	NAI		
17.	Η λύση θα πρέπει να υποστηρίζει οι administrators να μπορούν να δημιουργούν one-time κωδικούς	NAI		
18.	The solution should support the operating systems: Apple iOS, Google Android, and windows 10, windows 11	NAI		
19.	Η λύση θα πρέπει να υποστηρίζει να εξαγει τα logs σε thirdpartySIEM	NAI		
20.	η λύση θα πρέπει να υποστηρίζει rolebased ελεγχους (rolebasedadministrationcontrols) για τους διαχειριστές	NAI		
21.	η λύση θα πρέπει να υποστηρίζει να μπαίνει το logo της εταιρείας	NAI		
22.	Η λύση θα πρέπει να υποστηρίζει τις παρακατω εφαρμογες.	NAI		
23.	Cisco ASAFTD IPSEC and SSL VPN με anyconnect client	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
24.	OWA (supporting Exchange Server 2008, 2010 and 2013)	NAI		
25.	Citrix Netscaler and Access Gateway	NAI		
26.	Integration with Microsoft RDP and support for below operating systems: -Windows Vista SP2 and Windows Server 2008 SP2 -Windows Server 2008 R2 SP1 -Windows 8 and Windows Server 2012 -Windows 8.1 and Windows Server 2012 R2 -Windows 10, 11	NAI		
27.	Integration with Microsoft Local Login, for below operating systems -Windows Vista SP2 and Windows Server 2008 SP2 - Windows Server 2008 R2 SP1 -Windows 8 and Windows Server 2012 -Windows 8.1 and Windows Server 2012 R2 -Windows 11	NAI		
28.	Integration με Unix με SSH utility και PAM integration	NAI		
29.	Integration με Oracle PeopleSoft	NAI		
30.	integration με VMWare View	NAI		
31.	integration με BOMGAR, Tthycotic, Lastpass, Jira, Docusign, WordPress	NAI		
32.	integration Με άλλες λύσεις VPN άλλων κατασκευαστών (Checkpoint, Forti, Palo Alto, Juniper κτλ)	NAI		
33.	integration Με Office 365, Microsoft remote desktop Web Access, Microsoft RD Web	NAI		
34.	Integration με Microsoft Routing and Remote Access Server (RRAS)	NAI		
35.	Η Λύση θα πρέπει να υποστηρίζει RESTAPI για πιστοποίηση, εγγραφή και διαχείριση	NAI		
36.	Η λύση θα πρέπει να υποστηρίζει RADIUS για πιστοποίηση	NAI		
37.	Η λύση θα πρέπει να υποστηρίζει LDAP για πιστοποίηση	NAI		
38.	Η Λύση θα πρέπει να υποστηρίζει SAML 2.0 για πιστοποίηση	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
39.	Η λύση θα πρέπει να έχει Integration Με εφαρμογές όπως Box, Salesforce, Office 365	NAI		
40.	όλο τα τεχνικά εγχειρίδια θα πρέπει να είναι διαθέσιμα στο διαδίκτυο χωρίς κωδικούς για ευκολία στην πρόσβαση	NAI		
41.	Η Λύση θα πρέπει να υποστηρίζει singlesignon με πολλαπλά ActiveDirectoryDomains με και χωρίς ADtrust	NAI		
42.	Η λύση επιτρέπει ελεγχο προσβασης σε εφαρμογες με χρήση πολιτικών και περιορίζει την πρόσβαση όταν μία συσκευή δεν πληρεί τις απαιτήσεις ασφαλείας	NAI		
43.	Υποστηρίξτε τη λειτουργία αυτο-εγγραφής (autoenrolment) για τους τελικούς χρήστες της λύσης	NAI		
44.	Η λύση είναι σε θέση να υπενθυμίζει την τελευταία μέθοδο που χρησιμοποιήθηκε στον πελάτη για την επιλογή MFA της εφαρμογής web.	NAI		
45.	Υποστήριξη μηχανισμών ελέγχου ταυτότητας εφαρμογών που βασίζονται στο webSDK.	NAI		
46.	Υποστήριξη για έλεγχο ταυτότητας εκτός σύνδεσης Windows και MAC, όταν η σύνδεση δικτύου δεν είναι διαθέσιμη	NAI		
47.	Η εφαρμογή Solution για κινητά πρέπει να μπορεί να δημιουργεί αντίγραφα ασφαλείας και να επαναφέρει προστατευμένους λογαριασμούς, OTP 3rdparty, λογαριασμούς 3rdparty για λειτουργικά συστήματα Android και IOS	NAI		
48.	Η λύση θα πρέπει να επιτρέπει την ενεργοποίηση του MFA για SSH, RDP			
49.	Υποστήριξη πρόσβασης passwordless για εφαρμογές με ενεργοποιημένη τη δυνατότητα singlesignon και που υποστηρίζουν SAMLOIDC			
50.	Η λύση πρέπει να επιβάλει πολιτικές με βάση την θέση του χρήστη (userlocation)	NAI		
51.	Η λύση πρέπει να υποστηρίζει αποτροπή πιστοποίησης που γίνονται από άγνωστες IP διευθύνσεις όπως αυτές που παρέχονται από TOR, HTTP/HTTPSproxy ή anonymousVPN εφαρμογες	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
52.	Η λύση θα πρέπει να υποστηρίζει IPwhitelisting/geolocation	NAI		
53.	Η λύση θα πρέπει να υποστηρίζει διαμορφώσιμες πολιτικές που να μπλοκάρουν χρήστες από συγκεκριμένες χώρες ώστε να μειώσουν το ρίσκο για συγκεκριμένο group χρηστών ή εφαρμογές	NAI		
54.	Η λύση θα πρέπει να υποστηρίζει διαμορφωση πολιτικής που μπλοκάρει χρήστες οι οποίοι χρησιμοποιούν συσκευές οι οποίες είναι jailbroken ώστε να μειώσουν το ρίσκο για συγκεκριμένο group χρηστών ή εφαρμογές	NAI		
55.	Η λύση πρέπει να παρέχει ορατότητα στην υγεία της ασφάλειας των φορητών υπολογιστών και των desktop			
56.	Η Λύση θα πρέπει να πιστοποιεί την καταστασης ασφαλείας της συσκευής πριν την παροχή πρόσβαση σε ένα χρήστη ελέγχοντας τα παρακάτω κριτήρια για τη συσκευή την οποία χρησιμοποιεί ο χρήστης. Για laptop: <ul style="list-style-type: none"> • OS version, Browser, Pluggins, endpoint security agent • HD encryption, χρήση firewall για κινητό <ul style="list-style-type: none"> • OS version, Tampered, biometric, encryption 	NAI		
57.	Η λύση πρέπει να επιβάλλει πολιτικές με βάση την τοποθεσία του χρήστη	NAI		
58.	Η λύση πρέπει να παρέχει μια επισκόπηση του πίνακα εργαλείων των συσκευών που διατρέχουν κίνδυνο με βάση μη ενημερωμένα λειτουργικά συστήματα, προγράμματα περιήγησης ή plugins	NAI		
59.	Η λύση πρέπει να επιτρέπει τη δημιουργία πολιτικών ασφαλείας για μη διαχειριζόμενες συσκευές που έχουν πρόσβαση σε συγκεκριμένες εφαρμογές	NAI		
60.	Η λύση πρέπει να είναι ικανή να επιτρέπει στους χρήστες να έχουν πρόσβαση σε ιστότοπους, εφαρμογές και διακομιστές SSH εντός εγκατάστασης	NAI		



A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
61.	Η λύση θα πρέπει να υποστηρίζει την ορατότητα της υγείας της συσκευής πριν από την παραχώρηση πρόσβασης, όπως η δυνατότητα ελέγχου για κινητή συσκευή, π.χ.: το λειτουργικό σύστημα είναι root ή jailbreak ή παλιά έκδοση, έλεγχος προγράμματος περιήγησης, επιλογή βιομετρικής σύνδεσης, κλείδωμα οθόνης κινητής συσκευής, ρυθμίσεις 2FA. Για πληροφορίες λειτουργικού συστήματος προσωπικών υπολογιστών, έλεγχος προσθηκών, ρυθμίσεις προγράμματος περιήγησης.	NAI		
62.	Η λύση θα πρέπει να ελέγξει την έκδοση των προγραμμάτων περιήγησης, τις εκδόσεις των προσθηκών java και Flash. Εάν οι εκδόσεις είναι ξεπερασμένες λύσεις που μπορούν να ανακατευθύνουν για αποκατάσταση ή να αρνηθούν τα αιτήματα πρόσβασής τους στα συστήματα	NAI		
63.	Η λύση πρέπει να υποστηρίζει ελεγχους posture χωρίς agent	NAI		
64.	Η λύση πρέπει να παρέχει πληροφορίες υγιεινής σε συσκευές MacOS	NAI		
65.	Η λύση πρέπει να παρέχει πληροφορίες υγείας σε συσκευές Windows, MacOS και Linux	NAI		
66.	Η λύση MFA θα πρέπει να υποστηρίζει verifiedpush ως εργαλείο ελέγχου ταυτότητας (π.χ. ο χρήστης θα πρέπει να παρέχει 3-δψήφιο αριθμό για να αποφύγει την κόπωση MFA)	NAI		
67.	Η λύση θα πρέπει να μπορεί στο μέλλον να υποστηρίξει με αναβάθμιση άδειών τις παρακατω λειτουργίες σε μία ενιαία κονσόλα: <ul style="list-style-type: none"> • Η λύση πρέπει να μπορεί να εντοπίζει μη διαχειριζόμενες συσκευές (μη εταιρικές δηλαδή BYOD) που έχουν πρόσβαση σε εσωτερικές εφαρμογές με αναβάθμιση άδειες στο μέλλον • Η λύση πρέπει να παρέχει αναφορές σχετικά με διαχειριζόμενες και μη διαχειριζόμενες συσκευές που έχουν πρόσβαση σε οποιεσδήποτε εφαρμογές εσωτερικού χώρου και σε cloud με αναβάθμιση άδειες στο μέλλον • Η λύση πρέπει να ενσωματωθεί με την υπάρχουσα λύση MDM για τον εντοπισμό αξιόπιστων και μη διαχειριζόμενων 	NAI		



A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	<p>συσκευών με αναβαθμιση αδειες στο μελλον</p> <ul style="list-style-type: none"> • Η λύση πρέπει να προσδιορίζει τις εταιρικές συσκευές και το BYOD με αναβαθμιση αδειας στο μελλον • Η λύση πρέπει να προσδιορίζει εάν ένας 3rdpartyagent είναι ενεργοποιημενος στη συσκευή με αναβαθμιση αδειας στο μελλον με αναβαθμιση αδειας στο μελλον • Ενοποίηση με λύσεις EDR. Μπορεί να επιβάλει πολιτικές και να επιτρέπει αξιόπιστα τελικά σημεία με έλεγχο στάσης σε συνδυασμό με MDM, EMM, AD και άλλες ενσωματώσεις με αναβαθμιση αδειας στο μελλον • Η λύση πρέπει να παρέχει VPNless προσβαση για εφαρμογές RDP, SSH, Http, https, SMBforVPNlessaccess με αναβαθμιση αδειας στο μελλον • Η λύση πρέπει να λειτουργεί passwordless για RDP, SSH με αναβαθμιση αδειας στο μελλον 			

7.2.2.15 Λύση Cloud Proxy προστασίας απομακρυσμένων χρηστών

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Γενικά			
1.	Να αναφερθεί ο κατασκευαστής και το εμπορικό όνομα / προϊόν της προτεινόμενης λύσης	ΝΑΙ		
2.	Η προτεινόμενη λύση να καλύπτει τουλάχιστον 250 απομακρυσμένους εταιρικού χρήστες	ΝΑΙ		
3.	Ελάχιστη διάρκεια προσφερόμενης υπηρεσίας	≥ 3 χρόνια		
	Αρχιτεκτονική			
4.	Η λύση να παρέχει την πρώτη γραμμή άμυνας στην πρόσβαση στο Διαδίκτυο, ανεξάρτητα από τη θέση των χρηστών,	ΝΑΙ		
5.	Η προτεινόμενη λύση ασφάλειας να είναι βασισμένη στην υπηρεσία DNS και να υποστηρίζει αναδρομική ανάλυση (recursiveDNS).	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
6.	Η λύση πρέπει να βασίζεται στο cloud και να υποστηρίζεται από ένα παγκόσμιο δίκτυο κέντρων δεδομένων.	ΝΑΙ		
7.	Το κέντρο δεδομένων, που φιλοξενεί την προτεινόμενη λύση cloud, πρέπει να βρίσκεται σε χώρα που ανήκει στην Ευρωπαϊκή Ένωση	ΝΑΙ		
8.	Η υπηρεσία να υποστηρίζεται από ThreatIntelligence, που θα φιλοξενείται στις υποδομές του κατασκευαστή.	ΝΑΙ		
9.	Η προτεινόμενη λύση πρέπει να έχει ελάχιστο αντίκτυπο στην υφιστάμενη υποδομή, να μην απαιτεί εγκατάσταση φυσικού εξοπλισμού / υλικού και να χρησιμοποιεί τόσο την υπάρχουσα υποδομή διαδικτύου όσο και την προτεινόμενη υποδομή από τον παρόν διαγωνισμό.	ΝΑΙ		
10.	Η λύση πρέπει να προσφέρει πολλαπλές επιλογές υλοποίησης, τουλάχιστον τις ακόλουθες: α) τον επίσημο (authoritative) DNS του Πανεπιστημίου β) εσωτερικό διακομιστή μεσολάβησης DNS (ProxyDNS) γ) agent σε μια τερματική συσκευή (χωρίς επιπλέον φυσικό υλικό)	ΝΑΙ		
11.	Η λύση να μπορεί να εφαρμόζεται σε χρήστες που συνδέονται τόσο στα ενσύρματα και όσο και στα ασύρματα δίκτυα του ΙΔΙΚΑ, με δυνατότητα καθορισμού διαφορετικών πολιτικών βάσει διαφορετικών δημόσιων IP ή/και εσωτερικών δικτύων.	ΝΑΙ		
12.	Η λύση θα πρέπει αρχικά να εφαρμοστεί στους χρήστες περιαγωγής (roamingusers) με χρήση agent και να επιτρέπει την ενεργοποίηση πολιτικών ανά χρήστη περιαγωγής, εάν χρειάζεται.	ΝΑΙ		
	Τεχνικά Χαρακτηριστικά			

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
13.	Η λύση να μπορεί να εντοπίζει και να αποκλείει κακόβουλο λογισμικό χρησιμοποιώντας πρωτόκολλα και διαφορετικά από HTTP / HTTPS.	ΝΑΙ		
14.	Η λύση πρέπει να είναι σε θέση να εντοπίζει και να αποκλείει κακόβουλο λογισμικό που χρησιμοποιείται τόσο για ευκαιριακές επιθέσεις όσο και για στοχευμένες επιθέσεις για έναν συγκεκριμένο οργανισμό.	ΝΑΙ		
15.	Η λύση πρέπει να προστατεύει τουλάχιστον από τις ακόλουθες κατηγορίες κακόβουλου λογισμικού: botnets, exploitkits, drive-by.	ΝΑΙ		
16.	Η λύση πρέπει να προστατεύει τουλάχιστον από τις ακόλουθες κατηγορίες κακόβουλου περιεχομένου: phishing, newly seen domains, δυνητικά επιβλαβής domains, cryptomining, dns tunnelling, command & control επικοινωνία.	ΝΑΙ		
17.	Η λύση να επιτρέπει στον διαχειριστή να καθορίζει πολιτικές πρόσβασης σε εφαρμογές που θα επιλέγονται από ένα κατάλογο εφαρμογών. Η επιλογή του διαχειριστή να μπορεί να γίνει σε επίπεδο συγκεκριμένης εφαρμογής αλλά και κατηγορίας εφαρμογών.	ΝΑΙ		
18.	Η λύση πρέπει να είναι σε θέση να αποτρέπει μολύνσεις, να αποκλείει τα αιτήματα DNS προς τομείς διανομής κακόβουλου λογισμικού, να γνωρίζει τις προϋπάρχουσες μολύνσεις, και να αποκλείει τις αιτήσεις DNS προς υποδομές εντολών και ελέγχου (command&control).	ΝΑΙ		
19.	Η λύση πρέπει να βασίζεται σε αλγορίθμους μηχανικής μάθησης, στατιστικά μαθηματικά μοντέλα και ανάλυση τεράστιου όγκου δεδομένων απειλών (και όχι σε μαύρες λίστες (blacklists) ή βάσεις δεδομένων φήμης)	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	ώστε να επιτρέπει τον εντοπισμό γνωστών αλλά και αναδυόμενων απειλών.			
20.	Η προγνωστική νοημοσύνη της υπηρεσίας θα πρέπει να δημιουργηθεί μέσω ανάλυσης κίνησης DNS σε παγκόσμια κλίμακα. Παρέχετε στοιχεία ότι η επισκεψιμότητα προέρχεται από ένα δίκτυο καταμετρημένων κέντρων δεδομένων (πάνω από 10) που φιλοξενούν λύσεις επίλυσης DNS και επεξεργάζονται καθημερινά τουλάχιστον 400 δισεκατομμύρια αιτήματα DNS από εκατομμύρια χρήστες	NAI		
21.	Η λύση πρέπει να είναι λειτουργική για τους απομακρυσμένους χρήστες χωρίς να υπάρχει ανάγκη παρουσίας υπηρεσίας VPN (SSL ή IPSEC)	NAI		
22.	Οι πολιτικές φιλτραρίσματος και ασφάλειας ιστού πρέπει να επιτρέπουν τη δημιουργία γενικών εξαιρέσεων για διάφορους τομείς (domains) μέσω προσαρμοσμένων λευκών ή μαύρων λιστών (whiteorblacklists).	NAI		
23.	Η πρόληψη επιθέσεων κακόβουλου λογισμικού, Phishing και Command&Control (C2) Callbacks, Cryptomining πρέπει να υποστηρίζεται σε οποιαδήποτε πόρτα ή πρωτόκολλο.	NAI		
24.	Δυνατότητα επιβολής λειτουργίας «Ασφαλούς Αναζήτησης» (SafeSearch) στις γνωστές μηχανές αναζήτησης στο Διαδίκτυο, τουλάχιστον Google, Bing&YouTube.	NAI		
25.	Να είναι δυνατή η προσαρμογή της σελίδας αποκλεισμού σε μια καταχώριση της σχετικής πολιτικής ώστε να περιλαμβάνει τουλάχιστον δυνατότητα καθορισμού ενός προσαρμοσμένου μηνύματος, προσαρμοσμένου λογότυπου ή διεύθυνσης email διαχειριστή.	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
26.	Δυνατότητα δοκιμής/προσομοίωσης των πολιτικών πριν από την εφαρμογή τους σε κανονική λειτουργία.	NAI		
27.	Η χρήση agent πρέπει να υποστηρίζει τουλάχιστον τις ακόλουθες επιλογές εγκατάστασης: WindowsGPO και MDM/EMM	NAI		
	Διαχείριση	NAI		
28.	Η διαχείριση της υπηρεσίας να γίνεται μέσω ενός γραφικού, web-based περιβάλλοντος.	NAI		
29.	Η διεπαφή διαχείρισης να επιτρέπει τη δημιουργία διαφορετικών προφίλ χρήστη (ρόλοι) με διαφορετικά επίπεδα δικαιωμάτων. Να υποστηρίζονται τουλάχιστον οι ακόλουθοι ρόλοι: - Διαχειριστή - Χρήστη με δικαίωμα δημιουργίας αναφορών - Χρήστη χωρίς δικαιώματα επεξεργασίας	NAI		
30.	Το γραφικό περιβάλλον ορισμού πολιτικών θα πρέπει να δίνει τη δυνατότητα δημιουργίας πολιτικών ασφαλείας που βασίζονται σε ταυτότητες, όπως δίκτυα, χρήστες, υπολογιστές.	NAI		
31.	Οι πολιτικές ασφαλείας πρέπει να επιτρέπουν τη δημιουργία διακριτών προφίλ ασφάλειας και φιλτραρίσματος ιστού.	NAI		
32.	Να υπάρχει δυνατότητα δοκιμής και επαλήθευσης των ταυτοτήτων που ταιριάζουν με μια πολιτική ασφαλείας, μέσω μίας δοκιμαστικής συνάρτησης, πριν από την ανάπτυξη της πολιτικής σε παραγωγή.	NAI		
33.	Να επιτρέπεται ο ορισμός μιας ιστοσελίδας για τις αποκλεισμένες συνδέσεις DNS και η προώθηση μιας αποκλεισμένης σύνδεσης σε εσωτερική διεύθυνση URL του Πανεπιστημίου.	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
34.	Να επιτρέπεται ο καθορισμός μιας διαφορετικής σελίδας αποκλεισμού για κάθε ταυτότητα και κατηγορία συμβάντων (για παράδειγμα μια σελίδα αποκλεισμού για συμβάντα που σχετίζονται με την ασφάλεια, μια σελίδα αποκλεισμού για μπλοκ φιλτραρίσματος ιστού κ.λπ.)	ΝΑΙ		
35.	Να επιτρέπει τη δημιουργία χρηστών, σε μια τοπική βάση δεδομένων, με δυνατότητα παράκαμψης των αποκλεισμένων σελίδων.	ΝΑΙ		
36.	Να επιτρέπει τη δημιουργία ειδικών κωδικών που να επιτρέπουν την παράκαμψη των αποκλεισμένων σελίδων.	ΝΑΙ		
37.	Τα συμβάντα που σχετίζονται με όλα τα DNS ερωτήματα (queries) που αναλύθηκαν πρέπει να εμφανίζονται σε πραγματικό χρόνο, με τη δυνατότητα διαμόρφωσης φίλτρων βάσει ταυτότητας, προορισμού, IP προέλευσης, τύπου απόκρισης και ημερομηνίας.	ΝΑΙ		
38.	Να επιτρέπεται η επαναταξινόμηση ενός τομέα (domain), που σχετίζεται με ένα συμβάν ασφαλείας, μέσω αιτήματος (άνοιγμα ticket) προς την ομάδα έρευνας του κατασκευαστή/προμηθευτή της υπηρεσίας ασφαλείας.	ΝΑΙ		
39.	Να εμφανίζει μια επισκόπηση όλης της κυκλοφορίας του τοπικού οργανισμού, με τη δυνατότητα αναγνώρισης και αναφοράς του αποκλεισμού κίνησης DNS στα πλαίσια προληπτικού περιορισμού, στα πλαίσια περιορισμού μολύνσεων ασφαλείας και στα πλαίσια της πολιτική φιλτραρίσματος ιστού (webfiltering)	ΝΑΙ		
40.	Η πλατφόρμα διαχείρισης πρέπει να διαθέτει προηγμένες δυνατότητες για τον εντοπισμό εφαρμογών cloud ή συσκευών ShadowIT προκειμένου να προσδιορίσει υπηρεσίες χρησιμοποιούνται εντός του Πανεπιστημίου και να εντοπίσει ανωμαλίες στη χρήση τους.	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
41.	Η πλατφόρμα διαχείρισης να επιτρέπει τη δημιουργία τουλάχιστον των ακόλουθων αναφορών: - Σύνολο αιτημάτων DNS - Όγκος δραστηριότητας για αποκλεισμένα αιτήματα ανά κατηγορία - Domains με τη μεγαλύτερη χρήση - Κατηγορίες με τη μεγαλύτερη χρήση - Ταυτότητες με τη μεγαλύτερη χρήση	NAI		
42.	Όλες οι δραστηριότητες που πραγματοποιούνται από τους διαχειριστές πρέπει να καταγράφονται σε μια αναφορά καταγραφής ελέγχου διαχειριστή.	NAI		
43.	Ως πρόσθετη μέθοδο ελέγχου ταυτότητας που μπορεί να ενεργοποιηθεί, οι χρήστες διαχειριστών πρέπει να είναι σε θέση να ενεργοποιήσουν τους μηχανισμούς SSO.	NAI		
44.	Η λύση θα πρέπει να περιλαμβάνει όχι μόνο αναζητήσεις ευφυΐας DNS, αλλά ανάλυση σε πραγματικό χρόνο σε ερωτήματα DNS με εφαρμογή μηχανικής μάθησης και ικανότητας στατιστικής εκμάθησης και Μηχανικής μάθησης για τον εντοπισμό υπαρχουσών και αναδυόμενων απειλών. Οι αλγόριθμοι ανάλυσης πρέπει να χρησιμοποιούν ανιχνευτές πρόβλεψης πολλαπλών επιπέδων. Η λύση θα πρέπει να περιλαμβάνει, ενδεικτικά, να σταματήσει να σταματήσει το κακόβουλο λογισμικό, το ηλεκτρονικό ψάρεμα, το C&c και παρόμοιες συμπεριφορές επίθεσης.	NAI		
45.	Δυνατότητα εντοπισμού και αποκλεισμού domain που εμφανίστηκαν πρόσφατα (newlyseendomain) για προστασία από νέες καμπάνιες κακόβουλο λογισμικού	NAI		
46.	Η πλατφόρμα πρέπει να έχει δικό της threatintelligence/research για απειλές	NAI		
47.	Η πύλη ασφαλείας cloud της πλατφόρμας πρέπει να παρέχει δυνατότητες βασισμένες σε σύννεφο για προστασία επιπέδου DNS και DNStunneling έναντι domain που σχετίζονται με κακόβουλο	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	λογισμικό, ransomware, phishing, botnet, εντολές και έλεγχο σε όλες τις θύρες και τα πρωτόκολλα			
48.	Η λύση πρέπει να υποστηρίζει cloudproxy	ΝΑΙ		
49.	Η λύση πρέπει να παρέχει αποκρυπτογράφηση SSL στο cloud χωρίς όριο αριθμού αρχείων/επισκεψιμότητας που πρέπει να αποκρυπτογραφηθούν.	ΝΑΙ		
50.	Η πύλη ασφαλείας cloud της πλατφόρμας πρέπει να παρέχει προσαρμοσμένες blockpages και επιλογές παράκαμψης (bypassoptions)	ΝΑΙ		
51.	Η λύση πρέπει να παρέχει δυνατότητες που βασίζονται σε σύννεφο για τον αποκλεισμό αρχείων που βασίζονται σε AVEngine και προστασία από κακόβουλο λογισμικό	ΝΑΙ		
52.	Η λύση πρέπει να παρέχει ενσωματωμένο sandboxing βάσει cloud για άγνωστα αρχεία με υποστήριξη για πολλούς τύπους αρχείων, όπως exe, dll, bat, docx, xlsx, pdf, zip	ΝΑΙ		
53.	η λύση πρέπει να παρέχει δυνατότητες που βασίζονται σε σύννεφο για αποκρυπτογράφηση και inspection της κίνησης HTTPS	ΝΑΙ		
54.	Η λύση πρέπει να παρέχει ασφάλεια σε επίπεδα με χρήση DNS και cloudproxy	ΝΑΙ		
55.	Η λύση πρέπει να παρέχει δυνατότητες που βασίζονται σε σύννεφο για τον εντοπισμό και την αφαίρεση κακόβουλου λογισμικού από εφαρμογές που βασίζονται σε σύννεφο	ΝΑΙ		
56.	Η λύση πρέπει να παρέχει δυνατότητες που βασίζονται σε σύννεφο για την απομόνωση της κυκλοφορίας ιστού (isolationofwebtraffic) μεταξύ της συσκευής χρήστη και τυχόν απειλών που βασίζονται σε πρόγραμμα περιήγησης	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	τόσο σε εφαρμογές όσο και σε ιστότοπους			
57.	Η πύλη ασφαλείας cloud της πλατφόρμας πρέπει να παρέχει δυνατότητες που βασίζονται σε σύννεφο για να αποκλείει/επιτρέπει την πρόσβαση σε συγκεκριμένες εφαρμογές βάσει κατηγοριών ανά χρήστη/συσκευή/τοποθεσία	NAI		
58.	Η πύλη ασφαλείας cloud της πλατφόρμας πρέπει να παρέχει δυνατότητες που βασίζονται σε σύννεφο για τον αποκλεισμό τύπων αρχείων (π.χ. αποκλεισμό λήψης αρχείων .exe)	NAI		
59.	Η πύλη ασφαλείας cloud της πλατφόρμας πρέπει να παρέχει δυνατότητες βασισμένες σε σύννεφο για περιορισμούς cloudtenants για τον έλεγχο των παρουσιών εφαρμογών SaaS στις οποίες μπορούν να έχουν πρόσβαση όλοι οι χρήστες ή συγκεκριμένες ομάδες/άτομα (tenantcontrol για o365)	NAI		
60.	Η πύλη ασφαλείας cloud της πλατφόρμας πρέπει να παρέχει δυνατότητες που βασίζονται σε σύννεφο για τον αναλυτικό έλεγχο των εφαρμογών αποθήκευσης cloud για να επιτρέψει τον αποκλεισμό upload δεδομένων σε αυτές τις εφαρμογές.	NAI		
	Ολοκλήρωση			
61.	Η λύση πρέπει να διαθέτει έναν ενοποιημένο agent για την Ασφάλεια DNS, tocontentfiltering το EndpointEDR, Posturing, για συσκευές Windows 11.	NAI		
62.	Η λύση πρέπει να είναι σε θέση να επεκτείνει την προστασία και εκτός δικτύου μέσω της εγκατάστασης ενός agent σε συσκευές Windows και OSX.	NAI		
63.	Ο agent πρέπει να είναι σε θέση να επιβάλει ένα αποκλειστικό σύνολο πολιτικών ασφαλείας και φιλτραρίσματος	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	ιστού για τους εξωτερικούς χρήστες ή επίσης να επεκτείνει με διαφάνεια τις εσωτερικές εταιρικές πολιτικές όταν το τερματικό βρίσκεται εκτός του δικτύου του οργανισμού.			
64.	Η λύση πρέπει να είναι σε θέση να εξάγει τα αρχεία καταγραφής ελέγχου (logs) σε εξωτερικά συστήματα αποθήκευσης, από όπου θα μπορούν να τροφοδοτηθούν λύσεις SIEM. Καθορίστε τη μεθοδολογία και τις μορφές που υποστηρίζονται.	NAI		
65.	Η λύση θα πρέπει να παρέχει ένα API για ενοποίηση με 3rdparty λύσεις	NAI		
66.	Η λύση πρέπει να ενσωματώνεται με την Κεντρική Πλατφόρμα Ενορχήστρωσης Ασφαλείας, Αυτοματοποίησης και Απόκρισης (SOAR) αφενός για να την τροφοδοτεί με πληροφορίες για την τοπική ασφάλεια και αφετέρου για δυνατότητα άμεσου αποκλεισμού τομέων (domains).	NAI		
	Ανθεκτικότητα και αξιοπιστία			
67.	Η υπηρεσία DNS πρέπει να υποστηρίζει EDNSClientSubnet (ECS)	NAI		
68.	Το δίκτυο που χρησιμοποιείται για την υπηρεσία ασφαλείας DNS πρέπει να χρησιμοποιεί Anycast.	NAI		
69.	Το δίκτυο που χρησιμοποιείται για την υπηρεσία ασφαλείας DNS πρέπει να συνδέεται απευθείας με πάροχους υπηρεσιών Διαδικτύου (ISPs) Tier 1/2/3, τουλάχιστον με 500 διαφορετικούς σε παγκόσμιο επίπεδο.	NAI		
70.	Το δίκτυο που χρησιμοποιείται για την υπηρεσία ασφαλείας DNS πρέπει να έχει ετήσια διαθεσιμότητα (uptime) τουλάχιστον 99,999.	NAI		

7.2.2.16 Λύση Antimalware απομακρυσμένων χρηστών (AV,EDR, XDR)

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
1.	Να προσφερθεί εξειδικευμένο λογισμικό προστασίας τερματικού και ανάλυσης επιθέσεων. Να αναφερθεί ο κατασκευαστής και το εμπορικό όνομα / προϊόν της προτεινόμενης λύσης	ΝΑΙ		
2.	Μέγιστος Αριθμός τελικών Σημείων >=500	ΝΑΙ		
	Γενικά χαρακτηριστικά			
3.	Το λογισμικό να διαθέτει ελαφρύ agent	ΝΑΙ		
4.	Το λογισμικό να παρέχει cloud-based analytics	ΝΑΙ		
5.	Το λογισμικό να παρέχει web-based management graphical user interface	ΝΑΙ		
6.	Το λογισμικό να παρέχει προηγμένες δυνατότητες προστασίας για την ασφάλεια τερματικών (εταιρικών/ΗΥ)	ΝΑΙ		
7.	Η προτεινόμενη λύση πρέπει να περιλαμβάνει προηγμένες δυνατότητες ανίχνευσης και απόκρισης απειλών	ΝΑΙ		
8.	Η προτεινόμενη λύση πρέπει να παρέχει δυνατότητες έρευνας και αναζήτησης (threat hunting) απειλών	ΝΑΙ		
9.	Η προτεινόμενη λύση πρέπει να υποστηρίζει αυτόματοποιημένη έρευνα και αναζήτηση απειλών με χρήση ενσωματωμένων SOAR χαρακτηριστικών	ΝΑΙ		
10.	Όλα τα χαρακτηριστικά EDR (Endpoint Detection & Response) πρέπει να καλύπτονται με τη χρήση ενός μοναδικού λογισμικού στο τερματικό σημείο, που θα έχει κεντρική διαχείριση	ΝΑΙ		
11.	Η προτεινόμενη λύση να προσφέρει δυνατότητες XDR (extended Detection & Response) και SOAR, που δεν περιορίζονται στις λύσεις του κατασκευαστή	ΝΑΙ		
12.	Το λογισμικό εφαρμογής (agent) πρέπει να λειτουργεί σε συνδυασμό με το cloud για αναλυτικά στοιχεία και διαχείριση και χωρίς επιπτώσεις στην απόδοση της συσκευής, εκτελώντας όλες τις αναλύσεις στο cloud	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
13.	Το κέντρο δεδομένων, που φιλοξενεί την προτεινόμενη λύση cloud, πρέπει να βρίσκεται σε datacenter που ανήκει στην Ευρωπαϊκή Ένωση	NAI		
14.	Η προτεινόμενη λύση να περιλαμβάνει cloudsandbox για αυτόματη ή χειροκίνητη έρευνα μέσα από την κονσόλα του EDR	NAI		
15.	Κάθε ζητούμενη λειτουργία που ακολουθεί να παρέχεται με λύσεις από τον ίδιο προμηθευτή πλήρως ενσωματωμένες	NAI		
	Λογισμικό Διαχείρισης			
16.	Η διαχείριση του λογισμικού γίνεται κεντρικά με χρήση κονσόλας Web	NAI		
17.	Η πρόσβαση στην κονσόλα διαχείρισης να υποστηρίζει έλεγχο ταυτότητας 2 παραγόντων (2-factor authentication)	NAI		
18.	Η λύση πρέπει να υποστηρίζει SSO (singlesignon) και να ενσωματώνεται με πάροχο SAML	NAI		
19.	Η λύση πρέπει να περιλαμβάνει το δικό του πάροχο SAML για ενοποιημένη σύνδεση μεταξύ διαφορετικών κονσολών του ίδιου προμηθευτή	NAI		
20.	Η κονσόλα διαχείρισης περιλαμβάνει ενσωματωμένο διαχειριστή περιστατικών με τουλάχιστον τις ακόλουθες δυνατότητες ανά περιστατικό: Σημειώσεις, ανάθεση σε αναλυτή, στιγμιότυπα έρευνας (snapshotsofInvestigation - XDR), τμηματική ανάλυση των περιστατικών, στόχων & πηγών	NAI		
21.	Ενσωματωμένη διαχείριση περιστατικών που υποστηρίζει τη χειροκίνητη δημιουργία περιστατικών από τον αναλυτή ή με αυτοματοποιημένο τρόπο χρησιμοποιώντας τις δυνατότητες SOAR της λύσης	NAI		
22.	Η λύση υποστηρίζει την κεντρική ενημέρωση των agents (windowsclients)	NAI		
23.	Η λύση υποστηρίζει την προγραμματισμένη ενημέρωση των agents με βάση την ομαδοποίηση των χρηστών	NAI		
24.	Η λύση επιτρέπει στο διαχειριστή να ορίζει λεπτομερή δικαιώματα σε λογαριασμό αναλυτή με κατ' ελάχιστον: ορατότητα	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	ομάδας, ορατότητα πολιτικής, δικαίωμα επιβολής, δικαίωμα λήψης αρχείου από τελικό σημείο, δικαίωμα απομόνωσης τελικού σημείου			
25.	Η λύση υποστηρίζει τον αποκλεισμό (exclusion) συγκεκριμένης μηχανής πρόληψης, βασισμένο σε πολιτική και χρησιμοποιώντας τουλάχιστον τα κριτήρια διαδρομή (path), κλειδί (hash) & wildcard	NAI		
26.	Η λύση επιτρέπει στο διαχειριστή να ορίσει ποιο λειτουργικό σύστημα θα χρησιμοποιηθεί για την αυτόματη ανάλυση των αρχείων στο sandbox	NAI		
27.	Η λύση υποστηρίζει την ειδοποίηση μέσω email σε περίπτωση περιστατικού (incident)	NAI		
28.	Η λύση πρέπει να υποστηρίζει ειδοποιήσεις για τα παρακάτω κατ'ελάχιστον - Άμεση ειδοποίηση όλων των γεγονότων σε συγκεκριμένο χρονικό παράθυρο (σύννοψη) - Άμεση ειδοποίηση ως ένα email ανά event - Ωριαία, ημερήσια, εβδομαδιαία και μηνιαία ειδοποίηση			
29.	Η λύση θα πρέπει να επιτρέπει στον διαχειριστή να εξάγει τις ρυθμίσεις διαμόρφωσης πολιτικής ως αρχείο XML			
30.	Η λύση υποστηρίζει προσαρμοσμένη (custom) ειδοποίηση σε σύστημα συνεργασίας [MSTeams / Webex]	NAI		
31.	Η λύση περιλαμβάνει τεκμηριωμένο RESTAPI για επιβολή ενέργειας (enforcementAPI)	NAI		
32.	Η λύση περιλαμβάνει ένα τεκμηριωμένο RESTAPI για διερεύνηση	NAI		
33.	Η λύση περιλαμβάνει ένα τεκμηριωμένο RESTAPI για διαχείριση	NAI		
34.	Η λύση περιλαμβάνει ένα τεκμηριωμένο RESTAPI για υποβολή αρχείου σε sandbox για ανάλυση	NAI		
35.	Η λύση περιλαμβάνει ένα τεκμηριωμένο REST-API για τη χρήση των δυνατοτήτων XDR και SOAR που περιλαμβάνει	NAI		
	Υλοποίηση			

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
36.	Η προτεινόμενη λύση πρέπει να υποστηρίζει τουλάχιστον τα ακόλουθα λειτουργικά συστήματα: - MS Windows 7 (ESU) to Windows 11 - MS Windows Server from 2008R2 (ESU) to 2022 - Linux Centos - RHEL 6 to 9 - Oracle Linux RHCK/UEK 6 to 9 - AlmaLinux 8 & 9 - Amazon Linux 2 - Dabian 10 & 11 - Ubuntu 18 to 22.04 LTS - OpenSUSE Leap 15.1 to 15.3 - Rocky Linux 8 & 9 - Mac OSX 10.14 to 11.x - Android 8.0 and above - iOS 11.4 and above	NAI		
37.	Η λύση πρέπει να υποστηρίζει την εγκατάσταση του λογισμικού τερματικά σημεία με χρήση του MicrosoftSCCM	NAI		
38.	Η λύση να επιτρέπει στο τελικό σημείο τη λήψη ενημερώσεων υπογραφών antivirus από το cloud ή από τοπικό διακομιστή (λογισμικό) που παρέχεται με τη λύση	NAI		
39.	Η εφαρμογή λογισμικού στο τερματικό σημείο πρέπει να προστατεύεται με κωδικό πρόσβασης ώστε να μην επιτρέπεται η διακοπή της λειτουργίας και η απεγκατάσταση του (π.χ. από χάκερ ή μη εξουσιοδοτημένο χρήστη)	NAI		
40.	Όλα τα χαρακτηριστικά EDR (EndpointDetection&Response) καλύπτονται με τη χρήση ενός μοναδικού agent με κεντρική διαχείριση	NAI		
41.	Η λύση υποστηρίζει υλοποίηση στο νέφος (clouddeployment)	NAI		
42.	Η δυνατότητες EDR θα πρέπει επίσης να είναι διαθέσιμες σε ένα agent από τον ίδιο προμηθευτή, με κεντρική διαχείριση και να παρέχονται πρόσθετες δυνατότητες για την ασφάλεια του τελικού σημείου (VPN, 2MFA, InternetProtection) εάν απαιτηθούν στο μέλλον με επιπλέον άδεια για την περίπτωση του Windows 11 λειτουργικού	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
43.	Οποιαδήποτε άλλη μελλοντική λύση πρέπει να αξιοποιεί τον ίδιο παράγοντα (τελικό σημείο) για τα Windows 11	NAI		
44.	Η λύση πρέπει να υποστηρίζει multitenancy	NAI		
45.	Η λύση επιτρέπει στο τελικό σημείο να λαμβάνει την ενημέρωση των υπογραφών antivirus είτε από το cloud ή από ένα τοπικό διακομιστή ενημέρωσης που παρέχεται από το λογισμικό	NAI		
	Πρόληψη / ανίχνευση	NAI		
46.	Η λύση υποστηρίζει τη συνεχή και σε πραγματικό χρόνο προστασία/πρόληψη με χρήση ελέγχου φήμης (reputation) από το cloud για κάθε δραστηριότητα του συστήματος αρχείων, ανεξάρτητα από την κατηγοριοποίηση (maliciousorgood) του αρχείου χωρίς σάρωση (1-to-1 SignatureMatching).	NAI		
47.	Η λύση παρέχει προστασία/πρόληψη σε πραγματικό χρόνο κατά της εξέλιξης του κακόβουλου λογισμικού με χρήση μηχανικής μάθησης (machinelearningengine) μέσω cloud και σημαντικών δεδομένων εκπαίδευσης (trainingdata)	NAI		
48.	Η λύση περιλαμβάνει προστασία πραγματικού χρόνου έναντι πολυμορφικής παραλλαγής γνωστού κακόβουλου λογισμικού (polymorphicmalware) με τη χρήση προηγμένης τεχνικής όπως σύγκριση γενικών υπογραφών (1 to many matching)	NAI		
49.	Η λύση περιλαμβάνει μηχανισμό προστασίας από ιούς βασισμένο σε υπογραφές, με τακτική και προγραμματισμένη ενημέρωση υπογραφών	NAI		
50.	Η λύση παρέχει προστασία από προγράμματα root-kit	NAI		
51.	Η λύση παρέχει προστασία από κρυφές απειλές (stealth threats) με χρήση τεχνικών μηχανικής μάθησης	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
52.	Η λύση μπορεί να εντοπίσει memory-less ή file-lessmalware	ΝΑΙ		
53.	Η λύση παρέχει ορατότητα στα scripts που εκτελούνται στα τερματικά και να συμβάλει στην προστασία από επιθέσεις που γίνονται με scripts που χρησιμοποιούνται συχνά από επιθέσεις malware (scriptprotection)	ΝΑΙ		
54.	Η λύση περιλαμβάνει ανίχνευση συμπεριφοράς και προστασία από προγράμματα ransomware.	ΝΑΙ		
55.	Η λύση περιλαμβάνει την ικανότητα τερματισμού και καραντίνας διαδικασιών (process) που λειτουργούν ως ransomware πριν από την πλήρη κρυπτογράφηση του ασθενή μηδέν και τη διάδοσή τους.	ΝΑΙ		
56.	Η λύση περιλαμβάνει προηγμένη τεχνολογία για την αποτροπή της εκμετάλλευσης των ευπαθειών των εφαρμογών που βρίσκονται στα τερματικά (exploitprevention)	ΝΑΙ		
57.	Η λύση περιλαμβάνει μηχανισμούς ανάλυσης συμπεριφοράς (behavioralanalysis) παρακολουθώντας κατ'ελάχιστον τις δραστηριότητες του συστήματος αρχείων, του δικτύου, της γραμμής εντολών και του μητρώου για την προστασία του τελικού σημείου από στοιχεία παραβίασης	ΝΑΙ		
58.	Η λύση παρέχει προστασία μέσω μηχανισμού ανάλυσης της συμπεριφοράς (behavioralprotection). Ο μηχανισμός ανάλυσης συμπεριφοράς πρέπει να είναι σε θέση να εκτελεί αυτόματα κατ'ελάχιστον τις ακόλουθες ενέργειες: να βάζει σε καραντίνα ένα τερματικό, να τερματίζει διεργασίες και δέντρο διεργασιών, να ξεκινάει μία ανάλυση στο sandbox και να δημιουργεί forensicdump/snapshot	ΝΑΙ		
59.	Η λύση υποστηρίζει την πρόληψη στην εκτέλεση διεργασιών και σεναρίων (scripts) σε ενεργή ή παθητική λειτουργία (active/passivemode) βάσει πολιτικής	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
60.	Η λύση προστατεύει το σύστημα από τεχνικές που χρησιμοποιούνται για την προσπέλαση και αποθήκευση διαπιστευτηρίων όπως η mimikatz (systemprotection)	NAI		
61.	Η λύση προστατεύει το σύστημα από επιθέσεις χρησιμοποιώντας τεχνικές powershellscript (scriptprotection)	NAI		
62.	Η λύση χρησιμοποιεί το AMSI για την ακριβή ταυτοποίηση του script (scriptprotection)	NAI		
63.	Η λύση χρησιμοποιεί αναδρομική ασφάλεια επιπλέον της ανάλυσης σημείου στο χρόνο (retrospectivesecurity)	NAI		
64.	Η λύση υποστηρίζει αυτόματη καραντίνα αρχείου που ανιχνεύεται σε πραγματικό χρόνο ή αναδρομικά (retrospective)	NAI		
65.	Η λύση εντοπίζει και να αναφέρει ευάλωτες εφαρμογές μέσα στον οργανισμό	NAI		
66.	Η λύση εντοπίζει και να αναφέρει εφαρμογές χαμηλής συχνότητας (lowprevalence) μέσα στον οργανισμό	NAI		
67.	Η λύση υποστηρίζει την αυτόματη ανάλυση στο sandbox του επικίνδυνου κώδικα (payload) και dll που εκτελούνται μέσα στον οργανισμό	NAI		
68.	Η λύση περιλαμβάνει ανάλυση συμπεριφοράς για τον εντοπισμό κακόβουλης δραστηριότητας παρακολουθώντας κατ' ελάχιστον αλλά όχι περιοριζόμενη σε: σύστημα αρχείων, διεργασίες, δίκτυο, δραστηριότητες γραμμής εντολών, κλειδιά μητρώου, αρχεία καταγραφής συμβάντων των Windows	NAI		
69.	Η λύση παρέχει ουσιαστικές και αναλυτικές πληροφορίες σχετικά με το συμβάν που εντοπίστηκε, τουλάχιστον σε σχέση με το πλαίσιο MITTRE (Τεχνικές, βήματα και δευτερεύοντα βήματα)	NAI		
70.	Τα συμβάντα εντοπισμού πρέπει να περιλαμβάνουν τουλάχιστον 4 επίπεδα	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	σοβαρότητας για να καθορίζουν την προτεραιότητα περιστατικών			
	Εντοπισμός & αντιμετώπιση απειλών (ThreatHunting)			
71.	Η λύση εντοπισμού & αντιμετώπισης απειλών συλλέγει συνεχώς και σε πραγματικό χρόνο και συγκεντρώνει δεδομένα τηλεμετρίας σχετικά με τις δραστηριότητες στο τερματικό	NAI		
72.	Η λύση πρέπει να παρουσιάζει artifacts σε μια εύκολα κατανοητή μορφή	NAI		
73.	Όλα τα συμβάντα πρέπει να έχουν χρονοδιάγραμμα σε μορφή μήνα/ημερομηνία/ώρα/λεπτό/δευτ	NAI		
74.	Όλα τα artifacts και events πρέπει να απεικονίζονται και νωκαιοί συσχετίσεις μεταξύ των διεργασιών, δείχνοντας με σαφήνεια ποια διαδικασία προκάλεσε ποια άλλη διεργασία ή επηρέασε άλλες διεργασίες/στοιχεία, συμπεριλαμβανομένου του προφίλ χρήστη τη στιγμή της επίθεσης	NAI		
75.	Ο Αναλυτής Ασφαλείας θα πρέπει να μπορεί να βλέπει πώς εξελίσσονταν τα γεγονότα σε πραγματικό χρόνο μέσω μιας δυνατότητας έρευνας	NAI		
76.	Η λύση θα πρέπει να έχει ετοιμα queries	NAI		
77.	Τα δεδομένα τηλεμετρίας περιλαμβάνουν κατ' ελάχιστον, χωρίς όμως να περιορίζονται σε αυτά: δραστηριότητες συστήματος αρχείων (filesystemactivity), δραστηριότητες διεργασίας, δικτύου και γραμμής εντολών	NAI		
78.	Η τηλεμετρία είναι διαθέσιμη στην κονσόλα εντοπισμού & αντιμετώπισης απειλών για τουλάχιστον 30 ημέρες	NAI		
79.	Τα δεδομένα τηλεμετρίας είναι διαθέσιμα μέσω μιας ενσωματωμένης μηχανής αναζήτησης (elasticsearchengine)	NAI		
80.	Τα δεδομένα τηλεμετρίας είναι διαθέσιμα μέσω γραφικής και έγκαιρης αναπαράστασης με δυνατότητες	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	αναζήτησης και φιλτραρίσματος (devicetrajectory)			
81.	Η λύση πρέπει να επιτρέπει στον αναλυτή/διαχειριστή να ξεκινήσει μια εκτεταμένη έρευνα χρησιμοποιώντας τις παρεχόμενες δυνατότητες XDR απευθείας από οποιαδήποτε σελίδα της κονσόλας της λύσης EDR	NAI		
82.	Η λύση αναφέρει σχετικά με την κύρια αιτία της απειλής - rootcause (Πχ η εφαρμογή και διεργασία που εισάγουν λογισμικό κακόβουλης λειτουργίας στον οργανισμό)	NAI		
83.	Η λύση πρέπει να επιτρέπει στον αναλυτή/διαχειριστή να στρέφεται σε οποιοδήποτε αρχείο για να λάβει λεπτομερείς πληροφορίες που να περιλαμβάνουν τουλάχιστοντα ακόλουθα: τερματικό αημείο έναρξης (patientzero), δραστηριότητες δικτύου, ιδιότητα αρχείου και γνωστό όνομα, disposition του αρχείου, αριθμός και λίστα τερματικών που στοχοποιήθηκαν, γονική και θυγατρική διεργασία	NAI		
84.	Η λύση πρέπει να επιτρέπει στον αναλυτή/διαχειριστή να λαμβάνει (fetch) απομακρυσμένα αρχεία από το τερματικό σημείο	NAI		
85.	Η λύση επιτρέπει στον αναλυτή να αποστέλλει για ανάλυση στο sandbox οποιοδήποτε αρχείο που εμφανίζεται στο τελικό σημείο	NAI		
86.	Από την κονσόλα EDR, ο αναλυτής/διαχειριστής πρέπει να λαμβάνει άμεση και σε πραγματικό χρόνο την απόφαση/ετυμηγορία (threatintelligencevedrict/disposition) από πολλαπλές πηγές πληροφοριών απειλών για οποιαδήποτε εμφανιζόμενη ip, hash, domain κλπ	NAI		
87.	Η λύση επιτρέπει την αυτοματοποιημένη ή την χειροκίνητη λήψη dump/forensicsnapshot από ένα τερματικό	NAI		
88.	Η λύση πρέπει να περιλαμβάνει τη δυνατότητα ζωντανών ερωτημάτων πραγματικού χρόνου για τη συλλογή	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	πληροφοριών χαμηλού επιπέδου από το ίδιο το λειτουργικό σύστημα			
89.	Η λύση επιτρέπει την υποβολή ερωτήματος σε ένα τερματικό σημείο σε πραγματικό χρόνο για να δοθεί η πλήρης λίστα των εγκατεστημένων εφαρμογών και εγκατεστημένων patches του λειτουργικού συστήματος του τερματικού	NAI		
90.	Η λύση επιτρέπει το ερώτημα ενός, πολλών ή όλων των τερματικών σημείων σε πραγματικό χρόνο για τη λήψη πληροφοριών λογαριασμού χρήστη, όπως ο τρέχων συνδεδεμένος χρήστης, περίοδος λειτουργίας λογαριασμού (accountsession)	NAI		
91.	Η λύση περιλαμβάνει μια εσωτερική βάση δεδομένων πληροφοριών απειλών ώστε οι αναλυτές να μπορούν να αποθηκεύουν προσωπικές κρίσεις και δείκτες (indicators) για να εμπλουτίζουν τις περαιτέρω έρευνες	NAI		
92.	Η λύση επιτρέπει την αυτοματοποίηση των δραστηριοτήτων κυνηγιού απειλών (threathuntingactivities) χρησιμοποιώντας δεδομένα τηλεμετρίας και livequeries	NAI		
93.	Η λύση επιτρέπει την αυτοματοποίηση των δραστηριοτήτων αναζήτησης απειλών (threathuntingactivities) χρησιμοποιώντας δεδομένα τηλεμετρίας και livequeries	NAI		
94.	Η λύση παρέχει μονάδες ανάλυσης (analyzermodules) για τον εμπλουτισμό συμβάντων και τεχνουργημάτων (artifacts) με συνδρομές πληροφοριών απειλών και δεδομένα τηλεμετρίας/αναφοράς που προέρχονται από πολλαπλές λύσεις ασφάλειας του ίδιου ή άλλου κατασκευαστή	NAI		
95.	Το αποτέλεσμα του εμπλουτισμού θα πρέπει να παρουσιάζεται με γραφικό τρόπο επισημαίνοντας και συσχετίζοντας τις συνδέσεις μεταξύ των γεγονότων	NAI		
96.	Η λύση μπορεί να εντοπίσει το πρώτο τερματικό που μολύνθηκε από το κακόβουλο λογισμικό (patient 0)	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
97.	Η λύση να εμφανίζει λίστα ευάλωτων λογισμικών, τους υπολογιστές που περιέχουν αυτά τα λογισμικά και τους υπολογιστές που πιθανό να έχουν παραβιαστεί. Να παρουσιάζει τον αριθμό και τη σοβαρότητα ευάλωτων εφαρμογών και τον αριθμό των τερματικών στα οποία έχει εμφανιστεί μια ευάλωτη εφαρμογή. Να μπορούν να συνδεθούν οι ευπάθειες για κάθε εφαρμογή στις σχετικές καταχωρίσεις CVE	ΝΑΙ		
98.	Η λύση να έχει δυνατότητα συνεχούς παρακολούθησης της διάδοσης αρχείων, με την πάροδο του χρόνου, σε όλο το περιβάλλον προκειμένου να υπάρχει ορατότητα και να μειωθεί ο χρόνος που απαιτείται για την αντιμετώπιση μιας παραβίασης κακόβουλου λογισμικού.	ΝΑΙ		
99.	Εμφάνιση όλων των αρχείων που έχουν εκτελεστεί στον οργανισμό, ταξινομημένα κατά την επικράτηση από το χαμηλότερο στο υψηλότερο για την ανακάλυψη απειλών που δεν εντοπίστηκαν στο παρελθόν και παρατηρήθηκαν από μικρό αριθμό χρηστών. Τα αρχεία που εκτελούνται μόνο από λίγους χρήστες ενδέχεται να είναι κακόβουλα (για παράδειγμα, στοχευμένες προηγμένες επίμονες απειλές) ή αμφισβητήσιμες εφαρμογές	ΝΑΙ		
100	Το λογισμικό πρέπει να παρακολουθεί, αναλύει και καταγράφει όλη τη δραστηριότητα των αρχείων και των επικοινωνιών στα τερματικά σημεία. Εάν ένα υποτιθέμενο "καλό" ή "άγνωστο" αρχείο αρχίσει να συμπεριφέρεται κακόβουλα, η προτεινόμενη λύση θα πρέπει να μπορεί να ειδοποιήσει αναδρομικά τις ομάδες ασφαλείας. Οι ειδοποιήσεις θα πρέπει να είναι σε θέση να παρέχουν ένα καταγεγραμμένο ιστορικό δραστηριότητας αρχείων με λεπτομερείς πληροφορίες σχετικά με τη συμπεριφορά της απειλής. Αυτή η διαδικασία θα πρέπει να είναι ικανή να δώσει τουλάχιστον τα παρακάτω δεδομένα ασφαλείας: - Από πού προήλθε το κακόβουλο λογισμικό - Ποια ήταν η μέθοδος και το σημείο εισόδου - Πού ήταν και ποια συστήματα επηρεάστηκαν - Τι έκανε η απειλή και τι κάνει τώρα	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	- Πώς σταματάμε την απειλή και εξαλείφουμε τη βασική αιτία			
101	Η λύση θα πρέπει να υποστηρίζει endpointIoC (IndicationofCompromise), ώστε οι χρήστες θα πρέπει να μπορούν να υποβάλουν δικά τους IoC για να εντοπιστούν στοχευμένες επιθέσεις.	NAI		
	Δυνατότητες απόκρισης			
102	Η λύση πρέπει να υποστηρίζει χειρονακτική (manual) απομόνωση απομακρυσμένων τερματικών σημείων	NAI		
103	Ο αναλυτής θα πρέπει να έχει τη δυνατότητα να σταματήσει την απομόνωση ανά πάσα στιγμή από απόσταση	NAI		
104	Οι χρήστες θα πρέπει να έχουν τη δυνατότητα να σταματήσουν την απομόνωση μόνο με έναν κώδικα που δημιουργείται από τον διαχειριστή	NAI		
105	Η λύση υποστηρίζει την αυτόματη απομόνωση τελικού σημείου με έγκριση 2 επιπέδων ώστε κάποιος να μπορεί να εγκρίνει την απομόνωση	NAI		
106	Η λύση επιτρέπει στον αναλυτή να ορίζει προσαρμοσμένη μαύρη λίστα (customblacklist) βάσει hash και να την εφαρμόζει σε συγκεκριμένη ομάδα τερματικών	NAI		
107	Η λύση επιτρέπει στον αναλυτή να ορίζει προσαρμοσμένες (custom) υπογραφές AV-antivirus και να τις εφαρμόζει με αναλυτικότητα σε συγκεκριμένο τερματικό	NAI		
108	Η λύση επιτρέπει στον αναλυτή να ορίζει προσαρμοσμένη μαύρη λίστα εφαρμογών/διεργασιών (customapplication/processblacklist) για να αρνείται την εκτέλεση ανεπιθύμητων, ευάλωτων ή υποβαθμισμένων εφαρμογών και να τις εφαρμόζει αναλυτικά σε συγκεκριμένο τερματικό βάσει πολιτικής	NAI		
109	Η λύση πρέπει να επιτρέπει στον αναλυτή/διαχειριστή να ορίζει απλές ή προηγμένες προσαρμοσμένες ενέργειες	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	απόκρισης (customresponseactions) χρησιμοποιώντας δυνατότητες XDR και SOAR			
110	Η λύση υποστηρίζει αυτοματοποιημένες ενέργειες έρευνας και αντίδρασης (προκαθορισμένες και custom)	NAI		
111	Η λύση περιλαμβάνει μονάδες απόκρισης (respondermodules) για κεντρική εκτέλεση ενσωματωμένης ή προσαρμοσμένης ενέργειας απόκρισης σε πολλαπλές λύσεις ασφάλειας από τον ίδιο προμηθευτή και λύσεις ασφαλείας τρίτων	NAI		
112	Η λύση επιτρέπει την απόκριση σε άλλες λύσεις ασφαλείας όπως της προτεινόμενης λυσης ασφαλειας email από την κονσόλα εντοπισμού & αντιμετώπισης απειλών τερματικού (EDR) (μέσω ενσωμάτωσης με τη δυνατότητα XDR)	NAI		
	Δυνατότητες Sandbox			
113	Η προτεινόμενη λύση να περιλαμβάνει πλήρες cloudsandbox για αυτόματη ή χειροκίνητη έρευνα τόσο από την EDRconsole όσο και με απαυθείας σύνδεση στο sandbox	NAI		
114	Η λύση υποστηρίζει την ανάλυση της διεύθυνσης URL	NAI		
115	Η λύση λειτουργεί υπό ιδιόκτητο (proprietary) και μη εμπορικό hypervisor	NAI		
116	Η λύση περιλαμβάνει εικονικά μηχανήματα προσαρμοσμένα και συντηρούμενα από τον προμηθευτή με τακτική ενημέρωση	NAI		
117	Η λύση παρέχει άμεση πρόσβαση στην εικονική μηχανή κατά τη διάρκεια της ανάλυσης για αλληλεπίδραση με τον χρήστη	NAI		
118	Η λύση επιτρέπει την επιλογή διαφορετικής εξόδου δικτύου σε όλο τον κόσμο κατά την ανάλυση στο sandbox ενός αρχείου ή url	NAI		
119	Η λύση επιτρέπει την επιλογή της διάρκειας του χρόνου εκτέλεσης της ανάλυσης	NAI		
120	Η λύση υποστηρίζει πολλαπλά λειτουργικά συστήματα windows και προφίλ για το ίδιο	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	λειτουργικό σύστημα με ένα διαφορετικό σύνολο εφαρμογών και γλώσσας			
121	Η λύση επιτρέπει στους αναλυτές να εκτελούν προκαθορισμένα βιβλία αυτοματισμού (automationplaybooks) κατά τη διάρκεια της δυναμικής ανάλυσης στο sandbox	NAI		
122	Η λύση παρέχει πρόσβαση σε έναν κατάλογο δημόσιων αναλύσεων από την κοινότητα	NAI		
123	Η λύση επιτρέπει την εκτέλεση απλής και προηγμένης αναζήτησης στο πλαίσιο ιστορικής ανάλυσης με τη χρήση προσέγγισης πολλαπλών κριτηρίων (submissionsandanalysisdetails)	NAI		
124	Η λύση θα πρέπει να περιλαμβάνει images σύγχρονων λειτουργικών συστημάτων	NAI		
125	Η λύση πρέπει να δεχεται passwordprotectedsamples	NAI		
126	Η λύση θα πρέπει να επιτρέπει την πολλαπλή επανάληψη ανάλυσης ενός filesample. Ο αναλυτής θα πρέπει να μπορεί να επαναλαμβάνει τις αναλύσεις όσες φορές κρίνει σκόπιμο.	NAI		
	Δυνατότητες Ενσωμάτωσης με άλλες λύσεις			
127	Η λύση υποστηρίζει την ενσωμάτωση με SIEM	NAI		
128	Η λύση υποστηρίζεται πλήρως και να ενσωματώνεται με [SPLUNK/QRADAR] SIEM	NAI		
129	Η λύση υποστηρίζει την ενοποίηση με εξωτερικό σύστημα παρακολούθησης αιτημάτων (externalticketingsystem) για αυτόματη δημιουργία/ενημέρωση περιστατικών	NAI		
130	Η λύση θα πρέπει να ενσωματώνεται με συστήματα διαχείρισης περιστατικών ομάδων SOC, τουλάχιστον με TheHive ή ServiceNow	NAI		
131	Η λύση μπορεί να ενσωματωθεί με λύση 2-factorauthentication για να μην επιτρέπεται η πρόσβαση σε προστατευμένες εφαρμογές	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	από τερματικά σημεία που είναι compromised			
132	Η λύση υποστηρίζει ενσωμάτωση με λύση NAC ώστε να μπορούν να απομονωθούν και μέσω δικτύου τα μολυσμένα τερματικά	ΝΑΙ		
133	Το XDR θα πρέπει να περιλαμβάνει μια λίστα αποθέματος για να επιτρέπεται η ορατότητα σε όλες τις συσκευές του οργανισμού, είτε διαχειριζόμενες είτε χωρίς διαχείριση - Ποιοι τύποι συσκευών είναι συνδεδεμένοι στο περιβάλλον μας; -Ποιοι χρήστες είχαν πρόσβαση σε αυτές τις συσκευές; -Πού βρίσκονται αυτές οι συσκευές; -Ποιες ευπάθειες συνδέονται με κάθε συσκευή; -Ποιοι πράκτορες ασφαλείας είναι εγκατεστημένοι; -Είναι ενημερωμένο το λογισμικό ασφαλείας; "	ΝΑΙ		
134	Οποιαδήποτε προσαρμοσμένη ανίχνευση (fileblacklist) που έχει διαμορφωθεί από αναλυτή στην κονσόλα EDR πρέπει να εφαρμόζεται αυτόματα στην προτεινόμενη λύση ασφάλειας proxy	ΝΑΙ		
135	Κάθε αρχείο που εντοπίζεται ως κακόβουλο από την προτεινόμενη λύση ασφάλειας proxy θα πρέπει να κοινοποιείται με την ασφαλή λύση EDR endpoint ώστε να μπορεί μπλοκαρετε αυτοματα και απο τη λύση EDR	ΝΑΙ		

7.2.2.17 Λύση εκπαίδευσης για 250 χρήστες σε phishing campaigns και cyber attacks

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Γενικά Χαρακτηριστικά			
1.	Να αναφερθεί Τύπος – Κατασκευαστής.	ΝΑΙ		
2.	Να προσφερθούν 250 άδειες χρήσης.	ΝΑΙ		
3.	Να προσφερθεί λύση SaaS και συνδρομή για 36 μήνες	ΝΑΙ		
	Προσομοίωση phishing			

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
4.	Δυνατότητα για εύκολα τροποποιήσιμα πρότυπα για μηνύματα ηλεκτρονικού ταχυδρομείου προσομοίωσης phishing, σελίδες προορισμού και σελίδες σχολίων. Πρέπει επίσης να περιλαμβάνει μια εκτενή βιβλιοθήκη υπαρχόντων προτύπων και ένα διαισθητικό πρόγραμμα επεξεργασίας προτύπων.	NAI		
5.	Δυνατότητα για εκχώρηση διαφορετικών προσομοιώσεων σε διαφορετικά είδη κοινού για να μεγιστοποιήσετε τη συνάφεια της προσομοίωσης. Πρέπει επίσης να μπορεί να δημιουργεί και να χρησιμοποιεί δυναμικά φίλτρα, όπως τμήμα ή χώρα, για ανάθεση προσομοίωσης.	NAI		
6.	Δυνατότητα να παρέχει προσομοιώσεις phishing σε πολλές γλώσσες σύμφωνα με τον πίνακα παρακάτω.	NAI		
7.	Δυνατότητα ρύθμισης προσομοιώσεων για να εκτελούνται αυτόματα και συνεχώς αξιοποιώντας πολλαπλά σενάρια.	NAI		
8.	Δυνατότητα τυχαίων σεναρίων phishing για να αυξήσετε τη δυσκολία εντοπισμού	NAI		
9.	Δυνατότητα εύκολης διαμόρφωσης των καθυστερήσεων μεταξύ σεναρίων με βάση την προηγούμενη απόδοση χρήστη	NAI		
10.	Αναλύσεις και αναφορές: ο Δυνατότητα οπτικοποίησης των αποτελεσμάτων της καμπάνιας και προσδιορισμού του ποσοστού των χρηστών που ανέφεραν, άνοιξαν email προσομοίωσης, είδαν εικόνες, έκαναν κλικ σε συνδέσμους, άνοιξαν συνημμένα. ο Δυνατότητα δημιουργίας προκαθορισμένων αναφορών με λεπτομερή δεδομένα για τα αποτελέσματα προσομοίωσης, επαναλαμβανόμενα κλικ, χρήστες που δεν κάνουν κλικ στους συνδέσμους και συγκρίσεις προσομοίωσης. ο Δυνατότητα διαμόρφωσης και φιλτραρίσματος των αναφορών κατά χαρακτηριστικά όπως χώρα ή τμήμα.	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
11.	Να παρέχει μια προσθήκη του Outlook η οποία θα επιτρέπει στους χρήστες να αναφέρουν phishing. Το πρόσθετο να είναι διαμορφώσιμο και να ενσωματώνεται εύκολα με τη διαχείριση συστημάτων για ανάπτυξη.	ΝΑΙ		
12.	Η προτεινόμενη πλατφόρμα θα πρέπει να μπορεί να ενσωματωθεί στο μέλλον με λύση ασφάλειας ηλεκτρονικού ταχυδρομείου. Η ενοποίηση θα επιτρέψει στην προτεινόμενη λύση ασφάλειας ηλεκτρονικού ταχυδρομείου να λαμβάνει μια δυναμική λίστα χρηστών και να εφαρμόζει αυστηρές πολιτικές σε αυτούς τους χρήστες προκειμένου να τους προστατεύει καλύτερα. Οι άδειες για την λύση emailsecurityδεν απαιτείται να προσφερθούν στο παρον εργο	ΝΑΙ		
13.	Δυνατότητα συνδυασμού των δυνατοτήτων εκμάθησης του phishing με την εκπαίδευση ακριβώς στην ώρα (J.I.T.). Ανακατευθύνετε άμεσα τους χρήστες σε μια σελίδα εκμάθησης με κατάλληλο εκπαιδευτικό υλικό που σχετίζεται με τη συμπεριφορά που απαιτείται για βελτίωση.	ΝΑΙ		
	Πλατφόρμα ευαισθητοποίησης/κατάρτισης:			
14.	Δυνατότητα διαχείρισης εκστρατειών με τη χρήση ενός έξυπνου περιβάλλοντος εργασίας και λογικών ρών εργασίας	ΝΑΙ		
15.	Να παρέχει έναν υπεύθυνο δημιουργίας μαθημάτων για τη συγκέντρωση μαθημάτων σε λίγα λεπτά για να αντιμετωπίσει τη μοναδική και μεταβαλλόμενη εκπαίδευση που απαιτείται για μια διαφορετική κοινότητα χρηστών.	ΝΑΙ		
16.	Να παρέχει μια ευέλικτη βιβλιοθήκη για την παροχή περιεχομένου καθώς εξελίσσονται οι ανάγκες	ΝΑΙ		
17.	Να παρέχει μια βιβλιοθήκη κουίζ για την αξιολόγηση των γνώσεων του τελικού χρήστη, η οποία θα επιτρέπει τον καθορισμό	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	μιας γραμμής βάσης και τη μέτρηση της προόδου με την πάροδο του χρόνου. Δυνατότητα ελέγχου διατήρησης γνώσης του τελικού χρήστη από τα μαθήματα ευαισθητοποίησης ασφαλείας με κουίζ που χρησιμοποιούν διαφορετικές μορφές ερωτημάτων. Δυνατότητα επιλογής από μια τράπεζα προδιαμορφωμένων ερωτήσεων κουίζ ή δημιουργίας των δικών σας για να διασφαλίσετε ότι οι χρήστες σας λαμβάνουν το πιο σχετικό υλικό δοκιμών και απαντήσεων .			
18.	Να παρέχει δυνατότητες Gamification για να προτρέψει τους μαθητές και να επιτρέψει το φιλικό ανταγωνισμό μεταξύ των ομάδων χρηστών. Δυνατότητα ενδυνάμωσης των ατόμων, συμμετοχή, και ενθάρρυνση της μάθησης, προκαλώντας δυνατότητες παιχνιδιού. Με την ενεργοποίηση του χαρακτηριστικού gamification στα μαθήματα, οι χρήστες να μπορούν να έχουν επίσης μια κατάταξη, σε σύγκριση με άλλους χρήστες στην ομάδα τους, που έχουν ολοκληρώσει την ίδια εκπαίδευση.	ΝΑΙ		
19.	Να παρέχει προηγμένες δυνατότητες, όπως ένα μηχανισμό κανόνων, κλιμάκωση διαχειριστή και διεπαφές που βασίζονται σε SCIM για τη δημιουργία διαδρομών εκμάθησης βασισμένων σε συμπεριφορές χρήστη	ΝΑΙ		
20.	Δυνατότητα λεπτομερής παρακολούθησης, δυνατότητες αναφοράς και ευκολία χρήσης	ΝΑΙ		
	Επιπλέον Δυνατότητες			
21.	Δυνατότητα ελέγχου πρόσβασης βάσει ρόλων. Θα πρέπει να καθορίζονται αρκετοί ρόλοι, ο καθένας με διαφορετικά επίπεδα πρόσβασης στα προφίλ χρήστη και στις δυνατότητες διαχείρισης. Θα πρέπει να είναι δυνατή η διευθέτηση πολλών ρόλων/δικαιωμάτων για χρήστες. Σε κάθε ρόλο να χορηγείται η άδεια που απαιτείται από τη λειτουργία του:	ΝΑΙ		



A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	<p>a. Οι προκαθορισμένοι ρόλοι θα πρέπει να περιλαμβάνουν τουλάχιστον: Καθολικούς διαχειριστές: να μπορούν να δημιουργήσουν μαθήματα, κουίζ, να διαχειριστούν όλους τους χρήστες, να εκχωρήσουν δικαιώματα πρόσβασης σε άλλους χρήστες, γενικές καθολικές αναφορές, να ορίσουν ρυθμίσεις πλατφόρμας, να εφαρμόσουν έλεγχο ταυτότητας δύο παραγόντων.</p> <p>b. Διαχειριστές χρηστών: να μπορούν να διαχειριστούν μια καθορισμένη ομάδα χρηστών, αλλά να μην μπορούν να επηρεάσουν ή να δουν δεδομένα από άλλες ομάδες χρηστών</p> <p>c. Διαχειριστές ηλεκτρονικού "ψαρέματος": να μπορούν να σχεδιάζουν και να εκκινούν προσομοιώσεις ηλεκτρονικού "ψαρέματος", αλλά να μην έχουν πρόσβαση στην εκπαίδευση</p>			
22.	Πίνακες εργαλείων: Να παρέχει κεντρική ανάλυση, πίνακες εργαλείων και να μπορεί να προσαρμοστεί	ΝΑΙ		
23.	MobileResponse: η λύση θα πρέπει να είναι φιλική προς το κινητό, έτσι ώστε οι χρήστες να έχουν πρόσβαση σε εκπαιδευτικό περιεχόμενο από το smartphone, το tablet, το φορητό υπολογιστή ή τον επιτραπέζιο υπολογιστή τους, που θα τους δίνει την ευκαιρία να μάθουν σε μια συσκευή και σε μια στιγμή που λειτουργεί καλύτερα για το πρόγραμμά τους.	ΝΑΙ		
24.	Προσβασιμότητα: σε επίπεδα Α και ΑΑ σύμφωνα με το WCAG 2.1	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
25.	Καθολική σύνδεση: Δυνατότητα ενοποίησης με το MicrosoftActiveDirectory και υποστήριξη SAML 2.0	NAI		
26.	Εργαλεία επικοινωνίας: Η λύση θα πρέπει να περιλαμβάνει βιβλιοθήκη έτοιμων προς χρήση ενημερωτικών δελτίων κυβερνοασφάλειας, αφίσες και infographics για την ενίσχυση της εκστρατείας μέσω μιας ποικιλίας σημείων επαφής	NAI		
27.	Τα πρότυπα στις προσομοιώσεις ηλεκτρονικού "ψαρέματος" να μπορούν να δημιουργηθούν στα Ελληνικά.	NAI		
	Θέματα Χρηστών Ευαισθητοποίησης και Εκπαίδευσης για την Ασφάλεια			
28.	<p>Η πλατφόρμα θα πρέπει να παρέχει τουλάχιστον τις ακόλουθες εκπαιδευτικές ενότητες και τύπους μάθησης:</p> <ul style="list-style-type: none"> ▪ Introduction to Information Security ▪ Passwords ▪ Email ▪ Malware ▪ Phishing ▪ Identity Theft ▪ Social Engineering ▪ Social Networks ▪ Confidentiality on the Web ▪ Protecting Your Home Computer ▪ Smartphones ▪ Working Remotely (Mobile Users) ▪ Mobile Devices ▪ Traveling Securely ▪ Cloud Computing ▪ The Clean Desk Principle ▪ Physical Security ▪ Access Control ▪ Responsible Use of the Internet ▪ Bring Your Own Device (BYOD) ▪ Privacy ▪ Information Classification ▪ Information Lifecycle ▪ Intellectual Property ▪ Protecting Payment Card Data ▪ Ransomware 	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	<ul style="list-style-type: none"> Data Leakage Incident Reporting Business Email Compromise (BEC) Unintentional Insider Threat			
29.	Να περιλαμβάνονται δισδιάστατα κινούμενα βίντεο που επιτρέπουν στους χρήστες να κάνουν τις δικές τους επιλογές	NAI		
30.	Να περιλαμβάνονται μονάδες κλικ για ανακάλυψη μιας σελίδας, για την ενίσχυση της σωστής συμπεριφοράς, ειδικά αφού ένας χρήστης έχει κάνει κλικ σε έναν σύνδεσμο με ένα email προσομοίωσης phishing.	NAI		
31.	Να περιλαμβάνονται σύντομα, αφηγηματικά βίντεο που παρέχουν στους χρήστες μια σαφή, συνοπτική υπενθύμιση για τις συνέπειες μιας επίθεσης phishing και τις βέλτιστες πρακτικές που πρέπει να ακολουθήσουν για να διατηρούν τα δεδομένα τους ασφαλή.	NAI		
	Διαθέσιμες εκπαιδευτικές ενότητες στην ελληνική γλώσσα			
32.	Οι ενότητες e-learning, διάρκειας 4-7 λεπτών η καθεμία, να ξεκινούν με ένα βίντεο τουλάχιστον 90 δευτερολέπτων που θα έχει υπότιτλους στα ελληνικά και στη συνέχεια το υπόλοιπο μάθημα και η αξιολόγηση να γράφονται και να αφηγούνται στα ελληνικά	NAI		
33.	Οι ενότητες Micro-Learning, διάρκειας 2-3 λεπτών η καθεμία να είναι σε μορφή βίντεο, να έχουν υπότιτλους στα ελληνικά και οι ερωτήσεις να είναι στα ελληνικά	NAI		
34.	Οι ενότητες Nano-Learning, διάρκειας 1-2 λεπτών η καθεμία να είναι γραμμένες και να αφηγούνται στα ελληνικά.	NAI		
35.	Η κονσόλα διαχειριστή της πλατφόρμας μπορεί να είναι στα Αγγλικά, Γαλλικά και Ισπανικά	NAI		
36.	Η κονσόλα χρήστη ή η ζώνη εκμάθησης να είναι στα ελληνικά	NAI		



A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
37.	Τα πρότυπα στις προσομοιώσεις phishing να μπορούν να δημιουργηθούν στα ελληνικά	ΝΑΙ		
	Γλωσσική υποστήριξη			
38.	<p>Η πλατφόρμα ηλεκτρονικού ψαρέματος και το περιεχόμενο μαθημάτων θα πρέπει να είναι διαθέσιμα σε τουλάχιστον 40 γλώσσες:</p> <ul style="list-style-type: none"> ▪ Arabic ▪ Burmese ▪ Croatian ▪ Czech ▪ Danish ▪ Dutch ▪ English ▪ English - U.K. ▪ Finnish ▪ French – Canada ▪ French - France ▪ German ▪ Greek ▪ Hebrew ▪ Hindi ▪ Hungarian ▪ Indonesian ▪ Italian ▪ Japanese ▪ Korean ▪ Malay ▪ Norwegian ▪ Persian ▪ Polish ▪ Portuguese - Brazil ▪ Portuguese - Portugal ▪ Romanian ▪ Russian ▪ Serbian ▪ Simplified Chinese - Cantonese (P.R.C.) and Mandarin (P.R.C.) ▪ Slovak ▪ Spanish - LATAM ▪ Spanish - Spain ▪ Swedish ▪ Thai ▪ Traditional Chinese (Hong Kong) 	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	<ul style="list-style-type: none"> Traditional Chinese (Taiwan) Turkish Ukrainian Vietnamese 			

7.2.2.18 Λύση Ασφαλούς Προσβασης χρηστών στο εταιρικό δίκτυο

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
1.	Η προσφερόμενη λύση θα πρέπει να είναι appliance ή software-based και να υποστηρίζει τη δυνατότητα εγκατάστασης σε εικονική υποδομή Vmware, HyperV, KVM private cloud and AWS, Azure and OCI public cloud platforms. Να προσφερθούν δύο appliances (φυσικές ή εικονικές) για εφεδρεία	NAI		
2.	Η προσφερόμενη λύση θα πρέπει να παρέχει υπηρεσίες πιστοποίησης, εξουσιοδότησης και Λογιστικής (AAA) με βάση την ταυτότητα των χρηστών τους , συμμόρφωση με την πολιτική του οργανισμού και τον τύπο της συσκευής.	NAI		
3.	Η εφαρμογή θα προσφέρεται με άδεια κάλυψης τουλάχιστον 500 ταυτόχρονα συνδεδεμένων συσκευών στην τρέχουσα φάση του έργου, αλλά με δυνατότητα περαιτέρω αναβάθμισης χωρίς καμία αλλαγή στην ανάπτυξη της εικονικής μηχανής.	NAI		
4.	το λογισμικό θα πρέπει να χρησιμοποιεί ανοιχτά πρότυπα και να βασίζεται στα πρωτόκολλα IEEE 802.1x, RADIUS, RADIUSCoA και TACACS+ και να υποστηρίζει σημαντικούς τύπους EAP, συμπεριλαμβανομένων των EAP-TEAP και EAP.	NAI		
5.	Δυνατότητα passive authentication, Easy Connect και 802.1x	NAI		
6.	Το λογισμικό πρέπει να υποστηρίζει SAML για τον έλεγχο ταυτότητας της πύλης Guest, EndpointProvisioning, BYOD διαχείρισης και παροχής πιστοποιητικών.	NAI		
7.	Το λογισμικό θα πρέπει υποστηρίζει TACACS+ server, TACACS+ proxy	AI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
8.	Το λογισμικό θα πρέπει υποστηρίζει SecureSyslogRemoteLogging	ΝΑΙ		
9.	Το λογισμικό θα πρέπει να αναγνωρίζει αυτόματα όλα τα είδη των δικτυακών συσκευών όπως desktops, laptops, smartphones, tablets, printers, ip phones, ip cameras κλπ.	ΝΑΙ		
10	Προκειμένου η SW να αναγνωρίζει αυτόματα όλες τις συσκευές, οι ακόλουθοι ανιχνευτές θα πρέπει να δημιουργούν δεδομένα προφίλ: netflow, DHCP, DNS, HTTP, Radius, NMAP, SNMP, AD	ΝΑΙ		
11	Η πιστοποίηση και πρόσβαση του τελικού χρήστη θα πρέπει να γίνεται ανεξάρτητα από λειτουργικά συστήματα ή τύπο IP δικτυακής συσκευής.	ΝΑΙ		
12	Να υπάρχει κεντρική διαχείριση της λύσης	ΝΑΙ		
13	Το σύστημα πρέπει να αξιολογεί πληροφορίες posture τελικού σημείου μέσω agent ή/και μέσω εξωτερικών συστημάτων MDM ή MSSCCM. Με βάση την αξιολογούμενη στάση του τελικού σημείου και την ταυτότητα του πελάτη καθώς και άλλα δεδομένα συμφραζομένων, όπως τοποθεσία, ώρα, κ.λπ., το σύστημα πρέπει να μπορεί να περιορίζει τα δικαιώματα πρόσβασης στο δίκτυο με διάφορους τρόπους, συμπεριλαμβανομένης της εκχώρησης μιας ετικέτας ομάδας ασφαλείας, ότι το προτεινόμενο δίκτυο και το HW /εικονικές συσκευές FW μπορούν να τιμήσουν. Να προσφερθούν άδειες για 500 συσκευές ώστε να παρέχεται αυτή η λειτουργία	ΝΑΙ		
14	Θα πρέπει να υπάρχει μια διαδικασία ενσωμάτωσης και αυτόματης διαμόρφωσης μιας νέας συσκευής. Αναφέρετε τις δυνατότητες της πύλης και τις λεπτομερείς ενέργειες σύνδεσης μιας νέας συσκευής	ΝΑΙ		
15	Αυτόματη απεικόνιση και κεντρική εποπτεία της κατάστασης του δικτύου σχετικά με το	ΝΑΙ		

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	ποιο σύστημα και τι είδους, αλλά και ποιος χρήστης είναι συνδεδεμένος			
16	Αυτόματη απεικόνιση και κεντρική εποπτεία της συμμόρφωσης των συστημάτων που συνδέονται στο δίκτυο παρέχοντας πληροφορίες όπως αν το σύστημα είναι εξουσιοδοτημένο και συμβατό με τις πολιτικές ασφαλείας	ΝΑΙ		
17	Υποστήριξη μεγάλου εύρους επιλογών εξουσιοδότησης από προεπιλογή, συμπεριλαμβανομένων ενδεικτικά: ανακατεύθυνση HTTP(S), ACL με δυνατότητα λήψης, εκχώρηση VLAN και κατανομή ετικετών ομάδας ασφαλείας. Επιπλέον, πρέπει να υποστηρίζει συγκεκριμένα χαρακτηριστικά και προσαρμοσμένα χαρακτηριστικά RADIUS τρίτων κατασκευαστών στα μηνύματα RADIUSAccessResponse και CoA.	ΝΑΙ		
18	Το σύστημα θα πρέπει να αποφασίζει για την συμμόρφωση ή όχι των συστημάτων ελέγχοντας για την ύπαρξη και λειτουργία συγκεκριμένων ρυθμίσεων και προγραμμάτων βάσει της πολιτικής ασφαλείας	ΝΑΙ		
19	Το σύστημα να υποστηρίζει την ικανότητα αναγνώρισης των συνδεδεμένων με USB αφαιρούμενων συσκευών αποθήκευσης που λειτουργούν παράθυρα και ο μηχανισμός καραντίνας θα πρέπει να απομονώνει αποτελεσματικά το μη συμμορφούμενο σύστημα όταν είναι συνδεδεμένο ένα USBstick			
20	Η ενσωματωμένη λύση δημιουργίας προφίλ συσκευής πρέπει μεταξύ άλλων να υποστηρίζει ανιχνευτές βάσει ανάλυσης ονόματος DNS.			
21	"Η ενσωματωμένη λύση συμμόρφωσης στάσης πρέπει να υποστηρίζει τις ακόλουθες ενέργειες αποκατάστασης σε λειτουργικά συστήματα laptop: - Μήνυμα χρήστη. - Διανομή URL στους χρήστες. - Ενεργοποίηση ενημερώσεων συστήματος AV/Anti-malware. - Διανομή αρχείων στα τελικά σημεία των			

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Windows. - Αυτοματοποιημένη εκκίνηση προγράμματος στα τελικά σημεία των Windows. - Ενημέρωση των Windows και διαχείριση ενημερώσεων κώδικα. - Προσαρμοσμένα σενάρια αποκατάστασης σε όλες τις υποστηριζόμενες πλατφόρμες τελικού σημείου."			
22	Υποστήριξη αυτοματοποιημένης, εξωτερικά ενεργοποιημένης ή εκκινούμενης από τον διαχειριστή περιορισμού τελικών σημείων. Η εξωτερική σκανδάλη πρέπει να χρησιμοποιεί ένα API ανοιχτής προδιαγραφής και να υποστηρίζει τέτοιες ενέργειες αποκατάστασης που ενεργοποιούνται από το προτεινόμενο τείχος προστασίας και το σύστημα SOARoutofthebox.	ΝΑΙ		
23	υποστήριξη Ενσωμάτωσης – συνεργασία με υποδομές MSActiveDirectory. Δυνατότητα σύνδεσης με πολλούς τομείς της υπηρεσίας καταλόγου ActiveDirectory που έχουν μηδενική εμπιστοσύνη μεταξύ τους ενώ χρησιμοποιούνται στην ίδια ροή ελέγχου ταυτότητας ακόμη και σε επικαλυπτόμενα σενάρια ονομάτων χρήση.	ΝΑΙ		
24	"Τα υποστηριζόμενα καταστήματα εξωτερικών ταυτοτήτων πρέπει να περιλαμβάνουν ενδεικτικά: - MSActiveDirectory. - MSAzureADROPC; - SAML - ODBC; - RADIUSOTRκαιγενικούςδιακομιστέςRADIUS. - ΤυπικόLDAP."	ΝΑΙ		
25	Καθορισμός πολιτικών ασφάλειας βάση των οποίων θα επιτρέπεται ή όχι η πρόσβαση σε συγκεκριμένα συστήματα. Να αναφερθούν αναλυτικά οι δυνατότητες πολιτικών Οι πολιτικές ασφάλειας θα πρέπει να παραμετροποιούνται βάσει του χρήστη/ομάδας ή ρόλου αλλά και Άλλων συνθηκών όπως είδος συσκευής, μέρα και	ΝΑΙ		

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	ώρα, συμμόρφωση της συσκευής, τοποθεσία και τρόπο σύνδεσης στο δίκτυο			
26	Υποστηρίξτε τη δυνατότητα ενσωμάτωσης με λύσεις MobileDeviceManagement (MDM) και συγκεκριμένα Airwatch, Citrix, Good, MobileIron, SAP, intune. Η επιλεκτική εξουσιοδότηση συσκευής πρέπει να είναι δυνατή ανάλογα με την κατάσταση συμμόρφωσης της στάσης MDM	NAI		
27	Η προτεινόμενη λύση πρέπει να μπορεί να λειτουργεί ως διακομιστής Αρχής έκδοσης πιστοποιητικών (CA) ή διακομιστής μεσολάβησης CA. Αναλύστε τις δυνατότητες και τις περιπτώσεις χρήσης που υποστηρίζονται.	NAI		
28	Το λογισμικό θα πρέπει να υποστηρίζει offlineCertificateProvisioning	NAI		
29	Το λογισμικό θα πρέπει να υποστηρίζει CertificateProvisioning για VPNclients	NAI		
30	Δυνατότητα integration με λύσεις Security Information and Event Management (SIEM) και ειδικότερα Qradar, Arcsight, RSA, Splunk	NAI		
31	"Το σύστημα πρέπει να ενσωματωθεί με το προτεινόμενο υλικό και τα εικονικά συστήματα NGFW με τους ακόλουθους τρόπους: - Το σύστημα NGFW πρέπει να μπορεί να περιέχει αυτόματα τελικό σημείο στο επίπεδο πρόσβασης μέσω της προτεινόμενης λύσης NAC. Η συγκράτηση πρέπει να είναι ευέλικτη και να επιτρέπει τη χρήση τεχνικών εκ νέου ανάθεσης VLAN, dACL και SGT. - Η προτεινόμενη λύση NAC πρέπει να μπορεί να τροφοδοτεί την ταυτότητα του χρήστη στην αντιστοίχιση διευθύνσεων IP, τον τύπο τελικού σημείου-τοποθεσία- και πληροφορίες εκχώρησης SGT με τη λύση NGFWoutofthebox."	NAI		
32	Το σύστημα πρέπει να μπορεί να αξιολογεί τη στάση τρωτότητας του τελικού σημείου από τα ακόλουθα συστήματα σάρωσης ευπάθειας και να εξουσιοδοτεί τελικά σημεία με βάση τις βαθμολογίες ευπάθειας των πιο σοβαρών τρωτών σημείων που έχουν εντοπιστεί: -	NAI		

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Ποιότητες - Rapid7 Nexpose - Επαληθεύσιμο Κέντρο Ασφαλείας Nessus."			
33	Το σύστημα πρέπει να μπορεί να λαμβάνει πληροφορίες κατάστασης IoC από τον ίδιο agent τηλεμετρίας τελικού σημείου που χρησιμοποιεί η προτεινόμενη λύση NGFW.	ΝΑΙ		
34	Το λογισμικό θα πρέπει να θέτει πολιτικές ανεξάρτητα με τον τρόπο σύνδεσης στο δίκτυο είτε είναι η σύνδεση είναι ενσύρματη, ασύρματη ή με τη χρήση VPN. Θα πρέπει να μπορούν να οριστούν πολιτικές ανάλογα με τον τρόπο σύνδεσης ενός χρήστη.	ΝΑΙ		
35	ο έλεγχος συμμορφωσης της συσκευής και του τυπου της συσκευής πρεπει να ελέγχονται τόσο κατά τη στιγμή της σύνδεσης όσο και περιοδικά κατά τη διάρκεια της σύνδεσης και θα πρέπει να γίνονται ενέργειες ανάλογες με τα αποτελέσματα. Αναφέρετε λεπτομερώς τους ελέγχους και τις ενέργειες.	ΝΑΙ		
36	Το λογισμικό θα πρέπει να υποστηρίζει τμηματοποίηση που ορίζεται από λογισμικό. Εξηγήστε ποια υφάσματα SDN υποστηρίζονται και πώς			
37	"Ο προμηθευτής πρέπει να μπορεί να παρέχει τις ακόλουθες ροές δεδομένων: - Υπογραφές προφίλ τελικού σημείου. - Έλεγχος αξιολόγησης στάσης και απαιτήσεις (συνδυασμός πολλαπλών ελέγχων). Ταυτόχρονα, το σύστημα πρέπει να επιτρέπει τη δημιουργία προσαρμοσμένων απαιτήσεων στάσης και τη δημιουργία προφίλ «δακτυλικών αποτυπωμάτων». (profiling 'fingerprints'.)	ΝΑΙ		
38	Η προτεινόμενη λύση θα πρέπει να είναι εύκολα εφαρμόσιμη σε όλους τους χρήστες είτε είναι εσωτερικοί χρήστες είτε επισκέπτες. Να αναφερθεί η διαδικασία ένταξης νέων συστημάτων/χρηστών στο σύστημα	ΝΑΙ		
39	Καταγραφή γεγονότων και δημιουργία αναφορών. Να αναφερθούν οι δυνατότητες δημιουργίας αναφορών	ΝΑΙ		
40	Άμεση ενημέρωση του διαχειριστή για κάθε επιτυχημένη ή αποτυχημένη προσπάθεια	ΝΑΙ		

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	καθώς και οι ενέργειες που πάρθηκαν ως αποτέλεσμα. Να αναφερθούν οι τρόποι ενημέρωση των χρηστών.			
41	Υποστήριξη υψηλής διαθεσιμότητας	ΝΑΙ		
42	"Το σύστημα πρέπει να μπορεί να παρέχει δυνατότητες ελέγχου και διαχείρισης πρόσβασης χρήστη επισκέπτη, συμπεριλαμβανομένων, ενδεικτικά, των εξής: - Δυναμική πύλη ελέγχου ταυτότητας και εγγραφής επισκέπτη που υποστηρίζει πολλές γλώσσες και προσαρμόσιμες ροές διαδικασίας εγγραφής και ελέγχου ταυτότητας επισκέπτη. - Έλεγχος ταυτότητας επισκέπτη χρήστη βάσει λογαριασμού Facebook. - Δημιουργία χορηγού ή εγκεκριμένη από χορηγό εγγραφή επισκέπτη, συμπεριλαμβανομένων των δυνατοτήτων μαζικής δημιουργίας λογαριασμού επισκεπτών και εισαγωγής. - Υποστήριξη αυτοεγγραφής επισκεπτών. - Απλές ροές hot-spot με επιλογές κωδικού πρόσβασης AUP και μη συγκεκριμένου χρήστη. - Πολλαπλές ομάδες χρηστών χορηγών με διαφοροποιημένες άδειες χρηστών χορηγών. - Χορηγός ελέγχου ταυτότητας και εξουσιοδότησης χρήστη έναντι του MSAD. - Διαφορετικές ομάδες χρηστών επισκεπτών με συγκεκριμένα δικαιώματα πρόσβασης στο δίκτυο και προφίλ χρόνου (εγκυρότητας).	ΝΑΙ		
43	ολλαπλές επιλογές προσαρμογής πύλης επισκεπτών, συμπεριλαμβανομένων, ενδεικτικά, των εξής: - Απλό γραφικό στοιχείο, μορφοποίηση κειμένου και κειμένου πάνω από το διαχειριστικό περιβάλλον χρήστη. - Χρήση προσαρμοσμένων αρχείων CSS. - Πλήρως προσαρμοσμένος κώδικας HTML που περιλαμβάνει υποχρεωτικά στοιχεία, αλλά διαφορετικά μπορεί να περιλαμβάνει προσαρμοσμένο περιεχόμενο, σενάρια και μορφοποίηση."	ΝΑΙ		
44				
45	Δυνατότητα εφαρμογής πολιτικών πρόσβασης των επισκεπτών καθώς και	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	χρονικός περιορισμός στην πρόσβαση. Να αναφερθούν οι μηχανισμοί			
46	Δυνατότητα αναφορών ιστορικών και σε πραγματικό χρόνο για όλους τους χρήστες.	ΝΑΙ		
47	Έλεγχος πρόσβασης βάσει ρόλου (RBAC) για διαχειριστές. Τα δικαιώματα πρέπει να καλύπτουν τη διαμόρφωση χαρακτηριστικών καθώς και τους περιορισμούς πρόσβασης στα δεδομένα βάσει διαφόρων κριτηρίων. Το RBAC πρέπει να υποστηρίζει βάσεις δεδομένων MSAD και τοπικών χρηστών.	ΝΑΙ		
48	Συμμόρφωση με FIPS	ΝΑΙ		
49	Να προσφερθούν άδειες για 3 χρόνια	ΝΑΙ		
50	Να περιγραφεί η προτεινόμενη ενοποίηση NAC και MFA (ή οι επιλεον επιλογές ενσωμάτωσης εάν υπάρχουν) για το σενάριο ελέγχου πρόσβασης χρηστών απομακρυσμένης πρόσβασης	ΝΑΙ		

7.2.2.19 Λύση Πλατφόρμας Ενορχήστρωσης Ασφαλείας, Αυτοματοποίησης

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
1.	Η προσφερόμενη λύση να είναι cloudbased	ΝΑΙ		
2.	Το κέντρο δεδομένων, που φιλοξενεί την προτεινόμενη λύση cloud, πρέπει να βρίσκεται σε χώρα που ανήκει στην Ευρωπαϊκή Ένωση	ΝΑΙ		
3.	Υποστήριξη λήψης συμβάντων ασφαλείας από τη κεντρική πλατφόρμα διαχείρισης των συστημάτων ασφαλείας	ΝΑΙ		
4.	Η ενσωμάτωση της πλατφόρμας SOAR με την προτεινόμενη λύση ασφάλειας να είναι άμεση χωρίς ιδιαίτερες προσαρμογές και να συμπεριλαμβάνεται στην προσφορά.	ΝΑΙ		
5.	Η προσφερόμενη λύση SOAR να συνδυάζει τα συμβάντα ασφάλειας με το ThreatIntelligence του κατασκευαστή των συστημάτων ασφαλείας καθώς και με άλλες	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	πηγές προκειμένου να εντοπίζονται περισσότερες απειλές.			
6.	Δυνατότητα ενοποίησης του μηχανισμού ειδοποίησης (alerting) με email και πλατφόρμες ανταλλαγής μηνυμάτων και επικοινωνίας, όπως οι CiscoWebexTeams, και MicrosoftTeams, με άμεσα διαθέσιμα workflows	NAI		
7.	Δυνατότητα αυτοματοποίησης δημιουργίας ticket μέσω του εργαλείου SOAR σε συστήματα ticketing, όπως το ServiceNow με άμεσα διαθέσιμα Workflows.	NAI		
8.	Δυνατότητα threat hunting επιτρέποντας τη συλλογή παρατηρήσιμων (observables) όπως IPs, domain, hash αρχείων) από τη πλατφόρμα διαχείρισης των NGFWs και διερεύνηση ενάντια σε πληροφορίες από το Threat Intelligence του προμηθευτή ή άλλες πηγές threat intelligence	NAI		
9.	Τα συστήματα ασφαλείας (NGFWs) θα πρέπει να μπορούν να στέλνουν συμβάντα απευθείας στην πλατφόρμα από όπου μπορούν να προωθηθούν αυτόματα ή μη αυτόματα σε περιστατικά	NAI		
10.	Μέσω της ενορχήστρωσης να επιτρέπεται η αυτοματοποίηση επαναλαμβανόμενων και κρίσιμων εργασιών ασφαλείας, όπως η έρευνα απειλών και οι περιπτώσεις αποκατάστασης. Η πλατφόρμα να παρέχει προκατασκευασμένες ροές εργασίας και δυνατότητες απόκρισης ή δημιουργίας νέων από τον διαχειριστή μέσω απλού κώδικα ή λειτουργιών τύπου Drag-and-Drop.	NAI		
11.	Να υποστηρίζεται διαλειτουργικότητα με τη λύση Λύση Ασφαλείας και προστασίας των χρηστών από απειλές του διαδικτύου (Webproxy), ώστε να είναι εφικτά τα εξής: <ul style="list-style-type: none"> να μπλοκάρεται malicious web κίνηση από το SOAR σύστημα και να εφαρμόζεται η πολιτική στον proxy και στο firewall. 			

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	<ul style="list-style-type: none"> να επιλύονται γρήγορα οι εντοπισμένες απειλές και να παρέχονται άμεσες ενέργειες κατά των εντοπισμένων απειλών. να αποκλειστούν κακόβουλα domain, παρακολούθηση ύποπτων observable, έναρξη ενός workflow έγκρισης ή δημιουργία εισιτηρίου IT για την ενημέρωση της πολιτικής του Web proxy με αυτοματοποιημένο τρόπο. 			
12.	Να επιτρέπει ενσωματώσεις με εργαλεία ασφαλείας τρίτων κατασκευαστών μέσω ανοιχτού API	ΝΑΙ		
13.	Η προσφερόμενη λύση θα πρέπει να είναι του ιδίου κατασκευαστή με την προσφερόμενη λύση των NGFW, Ασφαλείας και προστασίας των χρηστών από απειλές του διαδικτύου (Webproxy), και microsegmentation με χρήση agent, για καλύτερη διαλειτουργικότητα	ΝΑΙ		

7.2.2.20 Πλατφόρμα Κυβερνοασφάλειας – Εκτεταμένης Ανίχνευσης & Απόκρισης (Cyber Security)

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
1.	Η πλατφόρμα πρέπει να έχει τη δυνατότητα συλλογής και επεξεργασίας από πολλαπλών τύπων πηγές δεδομένων και όχι μόνο αρχείων καταγραφής, κινούμενη στη φιλοσοφία του bigdatasecurityanalytics.	ΝΑΙ		
2.	Με την εκμετάλλευση αυτοματοποιημένης επεξεργασίας και μηχανικής μάθησης, το σύστημα θα πρέπει να μπορεί να λειτουργεί αποτελεσματικά ως ένα ολοκληρωμένο κέντρο αναφοράς και αυτόματης πρότασης και λήψης αντιμέτρων	ΝΑΙ		
3.	Το σύστημα θα πρέπει κατ' ελάχιστον να συνοδεύεται από τεχνολογίες SIEM, Sandbox, NTA, ThreatIntelligence και IDS και να μην απαιτείται η ξεχωριστή προμήθεια λογισμικού.	ΝΑΙ		
4.	Το προσφερόμενο σύστημα θα πρέπει να έχει τη δυνατότητα να υποστηρίζει και το μοντέλο MDR	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	<p>(ManagedDetection&Response) και θα πρέπει να υποστηρίζει το σύνολο του κύκλου ζωής αναγνώρισης και αντιμετώπισης απειλών, που αναλύεται στα στάδια:</p> <ul style="list-style-type: none"> • Συλλογή (Collect) • Εντοπισμός (Detect) • Έρευνα (Investigate) • Απόκριση (Respond) 			
5.	Το υπο προμήθεια σύστημα θα πρέπει να περιλαμβάνει την προμήθεια, εγκατάσταση και παραμετροποίηση αισθητήρων ασφαλείας (φυσικών ή εικονικών), οι οποίοι θα εφαρμόζουν λειτουργίες ML-IDS, antivirus, sandboxing και NTA.	ΝΑΙ		
	Χαρακτηριστικά NextGenSoc			
6.	Μοντέρνο περιβάλλον χρήσης (GUI) που ενσωματώνει απαραίτητες λειτουργίες παρακολούθησης και διαχείρισης.	ΝΑΙ		
7.	Πρόσβαση με χρήση ρόλων χρηστών (RBAC – RoleBasedAccess) για την διαχείριση δικαιωμάτων (userprivilegemanagement)	ΝΑΙ		
8.	Υποστήριξη πολλαπλών ενοίκων (multi-tenant) για την ξεχωριστή διαχείριση οντοτήτων, φυσικών δικτύων κτλ	ΝΑΙ		
9.	Εφαρμογή ξεχωριστού μοντέλου μηχανικής μάθησης ανά tenant για τη βελτίωση ακρίβειας των αποτελεσμάτων και τη μείωση των εσφαλμένων θετικών συμβάντων (falsepositives), εφαρμόζοντας ξεχωριστά συμπεριφορικά μοντέλα.	ΝΑΙ		
10.	Εξελιγμένες δυνατότητες μηχανικής μάθησης που να συμπεριλαμβάνουν τόσο supervised όσο και unsupervised διαδικασίες, τεχνολογίες graphML και να συνδυάζονται μεταξύ τους για την παραγωγή βέλτιστων αποτελεσμάτων	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
11.	Δυνατότητες ενσωμάτωσης με εργαλεία και τεχνολογίες ασφαλείας Firewalls, WAF, SWG, EDR, SOAR κτλ	NAI		
12.	Υποστήριξη API για ενσωμάτωση με τεχνολογίες HoneyPots, εργαλεία OSINT κτλ.	NAI		
13.	Μία ενοποιημένη, υψηλής απόδοσης, αποθήκη δεδομένων ("BigData" HighSpeedLake)	NAI		
14.	Δυνατότητα εγκατάστασης τόσο σε φυσικό εξοπλισμό, όσο και σε εικονικό ή περιβάλλον cloud	NAI		
15.	Κατανεμημένη και επεκτάσιμη αρχιτεκτονική που να υποστηρίζει ωστόσο και "AllInOne" σενάρια.	NAI		
16.	Υψηλή διαθεσιμότητα με τη χρήση clusters και ευέλικτη τήρηση και αποθήκευση δεδομένων.	NAI		
17.	Μηχανισμοί Συλλογής που να μπορούν να εγκατασταθούν τόσο σε φυσικό όσο και σε εικονικό περιβάλλον	NAI		
18.	Το σύστημα θα πρέπει να ακολουθεί ανοιχτή αρχιτεκτονική που να επιτρέπει την εισαγωγή δεδομένων από οποιαδήποτε συσκευή με τη χρήση IntegrationAPIs.	NAI		
19.	Κεντριοποιημένη διαχείριση	NAI		
20.	Απλό ενοποιημένο μοντέλο αδειών χωρίς επιπλέον κόστη	NAI		
	Next-GenerationSIEM			
21.	Η πλατφόρμα θα πρέπει να βασίζεται σε μια ενοποιημένη αποθήκη δεδομένων βασισμένη στην αρχιτεκτονική του bigdatalake και τα δεδομένα θα πρέπει κατ'ελάχιστον να μπορούν να εισαχθούν μέσω syslog.	NAI		
22.	Απλός όσο και εξεζητημένος μηχανισμός αναζήτησης που να βασίζεται σε λογικούς τελεστές (Booleanmodifiers)	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
23.	Οι αναζητήσεις να μπορούν να εφαρμοστούν ως μόνιμα φίλτρα σε όλο το περιβάλλον για ταχύτερη διερεύνηση και ανάλυση περιστατικών.	ΝΑΙ		
24.	Υψηλής απόδοσης και άμεσες ανταποκρίσεις στην αναζήτηση και το φιλτράρισμα στο bigdata	ΝΑΙ		
25.	Πρόσβαση σε πηγές δεδομένων και όχι μόνο σε syslog δεδομένα	ΝΑΙ		
26.	Συλλογή δεδομένων από δικτυακή κίνηση (μέσω TAP ή MirrorTraffic). Τα πακέτα θα πρέπει να γίνονται reduce, να κανονικοποιούνται και να μετατρέπονται σε αξιοποιήσιμα μετα-δεδομένα για την ενσωμάτωση στο bigdatalake.	ΝΑΙ		
27.	Συλλογή δεδομένων από user sources όπως το Microsoft AD μέσω API Connector	ΝΑΙ		
28.	Συλλογή δεδομένων από πηγές νέφους (cloud) Office365 μέσω Connectors	ΝΑΙ		
29.	Τα δεδομένα από πηγές πρέπει να κανονικοποιούνται, να εμπλουτίζονται και να συσχετίζονται αυτόματα από το σύστημα	ΝΑΙ		
30.	Πηγές εμπλουτισμού πρέπει να περιλαμβάνονται γεωγραφικού προσδιορισμού (Geo-Awareness), IPReputation, ThreatIntelligence και DPIApplicationawareness.	ΝΑΙ		
31.	Μοντέρνο περιβάλλον χρήστη με λειτουργίες SIEM που περιλαμβάνουν ερωτήματα και δημιουργίες κανόνων.	ΝΑΙ		
32.	Πρόσθετο για παραδοσιακή απεικόνιση SIEM (π.χ. Kibana)	ΝΑΙ		
	Εντοπισμός KillChain (KillChainDetections)			
33.	Το σύστημα πρέπει να έχει ενσωματωμένους μηχανισμούς εντοπισμών σε κάθε φάση του CyberSecurityKillChain, συμπεριλαμβάνοντας Reconnaissance, Delivery, Exploitation, Installation,	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Command&Control, andActions&Exfiltrations			
34.	Το σύστημα πρέπει να περιλαμβάνει ενσωματωμένη βάση υπογραφών IDS, ενισχυμένη από ανάλυση μηχανικής μάθησης (ML-IDS)	NAI		
35.	Η πλατφόρμα πρέπει να υποστηρίζει πολλαπλά ThreatIntelligenceFeeds, συμπεριλαμβάνοντας εμπορικές πηγές, open-source, anti-phishing κ.α.	NAI		
36.	Η πλατφόρμα πρέπει να επιτρέπει ενσωμάτωση με 3 rd partyfeeds μέσω STIX/TAXII και/ή MISP	NAI		
37.	Η πλατφόρμα πρέπει να έχει ενσωματωμένες δυνατότητες APTsandboxing για να αναγνωρίζει και να περιορίζει άγνωστα αρχεία, και για εντοπισμό ransomware, spyware.	NAI		
	ΑνάλυσηΔικτύου (Network Traffic Analysis)			
38.	Η πλατφόρμα πρέπει να ενσωματώνει λειτουργικότητα DeepPacketInspection (DPI) για την αναγνώριση τουλάχιστον 4000 εφαρμογών και να δομεί σχετικά συμπεριφορικά μοντέλα.	NAI		
39.	Τα δεδομένα κίνησης δικτύου πρέπει να μετασχηματίζονται σε κατάλληλα μετα-δεδομένα που περιλαμβάνουν και το payload, για την αντίστοιχη προαιρετική μείωση ανάγκης αποθηκευτικών χώρων.	NAI		
40.	Η πλατφόρμα πρέπει να ενσωματώνει λειτουργικότητα NTADetections, συμπεριλαμβάνοντας ApplicationUsageAnomalies, LongAppSessionAnomalies, και UnapprovedAssetActivity	NAI		
41.	Το σύστημα θα πρέπει να εντοπίζει ανωμαλίες στη συμπεριφορά των Firewalls, denialanomalies ή ruleusageanomalies	NAI		
	UserBehaviorAnalytics (UBA)			

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
42.	Το σύστημα πρέπει να πραγματοποιεί ανάλυση και εντοπισμό ανωμαλιών στη συμπεριφορά του χρήστη (userbehavior)	ΝΑΙ		
43.	Το σύστημα πρέπει να ενσωματώνει μοντέλα εντοπισμού ανωμαλιών αδύνατου ταξιδιού (ImpossibleTravelAnomaly) ή ώρες αυθεντικοποίησης (LogInTimeAnomaly)	ΝΑΙ		
44.	Εντοπισμούς NTA, έτσι κι εδώ όλα τα detections και τα σχετικά events στα logs και σε πηγές πρέπει να συσχετίζονται αυτόματα.	ΝΑΙ		
	EndpointBehaviorAnalytics (EBA)			
45.	Το σύστημα θα πρέπει να μπορεί να εισάγει δεδομένα από τρίτα συστήματα εντοπισμού ευπαθειών (vulnerabilityscanners) Nessus, Tenable, Rapid7 και να συσχετίζει τα ευρήματα με σχετικά γεγονότα ασφαλείας.	ΝΑΙ		
46.	Το σύστημα θα πρέπει να μπορεί να ανακαλύψει όλα τα assets σε ένα περιβάλλον και να τα κατηγοριοποιεί με βάση τη διεύθυνση MAC και IP.	ΝΑΙ		
47.	Η λίστα των ανακαλυφθέντων/εντοπισθέντων assets θα πρέπει να μπορεί να επαυξάνεται και να παραμετροποιείται με τη χρήση αρχείων csv με λίστες assets και περιγραφές.	ΝΑΙ		
48.	Το σύστημα πρέπει να μπορεί να καταγράφει όλους συσχετισμούς με ένα asset με IP διευθύνσεις, ιστορικά στοιχεία για τη χρήση εφαρμογών κτλ.	ΝΑΙ		
	Ορατότητα Δικτύου και Υπηρεσιών (Network&ServiceVisibility)			
49.	Το σύστημα θα πρέπει να περιλαμβάνει δυνατά εργαλεία απεικόνισης δικτύων και υπηρεσιών, μαζί με analytics, με στόχο να προσφέρει ορατότητα επιδόσεις δικτύου (networkperformance), applicationusage κτλ.	ΝΑΙ		
	ΚυνήγιΑπειλώνκαιΔιερεύνηση (Threat Hunting & Investigation)			

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
50.	Το σύστημα πρέπει να έχει ενσωματωμένα σχετικά εργαλεία, προκαθορισμένες αναζητήσεις και ερωτήματα, και οπτικοποιήσεις (visualizations).	ΝΑΙ		
51.	Τα visualizations πρέπει να είναι παραμετροποιήσιμα	ΝΑΙ		
52.	Το σύστημα πρέπει να προσφέρει εξελιγμένες δυνατότητες συσχετισμένες αναζητήσεις, που επιτρέπουν αναλυτές να συνδέσουν πολλαπλά ανεξάρτητα ερωτήματα με κοινά κριτήρια προκειμένου να δομήσουν πληροφορίες από attacksequences ή να απομονώσουν κοινές πληροφορίες.	ΝΑΙ		
53.	Όλα τα ερωτήματα θα πρέπει να μπορούν να αποθηκευθούν, επεξεργαστούν, κλωνοποιηθούν κτλ από χρήστες.	ΝΑΙ		
54.	Τα visualizations πρέπει να μπορούν να αποθηκευθούν σαν customdashboards.	ΝΑΙ		
55.	Τα ερωτήματα θα πρέπει να μπορούν να συνδυαστούν με ενέργειες/αποκρίσεις για PlayBooks	ΝΑΙ		
	Playbooks / Integrated Orchestration & Response (SOAR)			
56.	Το σύστημα πρέπει να συμπεριλαμβάνει μια βιβλιοθήκη με έτοιμα ενσωματωμέναplaybooks, που είναι αυτό-εκτελέσιμα ερωτήματα με ενσωματωμένες ενέργειες.	ΝΑΙ		
57.	Οι ενσωματωμένες ενέργειες/αποκρίσεις θα πρέπει να συμπεριλαμβάνουν: <ul style="list-style-type: none"> Alerts – Αποστολή e-mail/slack message κτλ Actions – Άνοιγμα case, εκτέλεσημιαεντολής API, δημιουργία security event κτλ Responses – Μπλοκάρισμα μιας IP στο Firewall, απενεργοποίηση 	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	χρήστη στο AD, εκτέλεση δέσμης ενεργειών κτλ			
58.	Παράλληλα με αυτοματοποιημένες ενέργειες, εξωτερικές ενέργειες το μπλοκάρισμα μια IP ή χρήστη θα πρέπει να είναι διαθέσιμες στο χρήστη μέσω του UI ώστε να μπορούν παράλληλα να υλοποιηθούν ως μέρος διερεύνησης/αντιμετώπισης ή ανάλυσης.	NAI		
59.	Δυνατότητα ενσωμάτωσης με εμπορικά εργαλεία SOAR	NAI		
	Ειδοποιήσεις (Alarming)			
60.	Το σύστημα θα πρέπει να προσφέρει έναν έξυπνο, μοντέρνο και παραμετροποιήσιμο μηχανισμό ειδοποιήσεων που να δύναται να οριστεί με βάση παραλήπτες και άλλα κριτήρια (scoreseverity, killchaincategory, etc.)	NAI		
61.	Οι ειδοποιήσεις πρέπει να μπορούν να αποσταλούν με email ή slack μηνύματα και τα μηνύματα πρέπει να είναι παραμετροποιήσιμα ως το περιεχόμενο και τα σχετικά δεδομένα.	NAI		
	Αναφορές (Reporting)			
62.	Το σύστημα πρέπει να περιέχει ένα σύγχρονο εξελιγμένο μηχανισμό αναφορών που θα επιτρέπει παράλληλα εύκολη δημιουργία νέων αναφορών με draganddrop και αποθήκευσή για χρήση σε οποιοδήποτε σημείο.	NAI		
63.	Οι αναφορές θα πρέπει να παράγονται με χρονοπρογραμματισμό και να αποστέλλονται σε διαφορετικούς χρήστες.	NAI		
64.	Οι αναφορές πρέπει να είναι δυνατόν να αποστέλλονται με email σαν pdf ή csv ή να γράφονται σε αρχείο.	NAI		
65.	Το σύστημα θα πρέπει να περιλαμβάνει πληθώρα έτοιμων αναφορών και templates.	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Portal			
66.	Πρόσβαση των χρηστών βάση ρόλου (UserRBACaccess) στο Portal με συνολική ή περιορισμένη πρόσβαση πληροφορίες.	ΝΑΙ		
67.	Custom Dashboards ανά ρόλο χρήστη.	ΝΑΙ		
68.	Χρονοπρογραμματισμένες αναφορές για κάθε tenant, tenantgroup και RBACusers.	ΝΑΙ		
69.	Η πρόσβαση των χρηστών πρέπει να μπορεί να περιορίζεται σε Read-Only, limitedview, μέχρι fullvisibilityandaccess.	ΝΑΙ		

7.2.2.21 Λύση Προστασίας Βάσεων Δεδομένων

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
1.	Να αναφερθεί ο κατασκευαστής, η έκδοση και η ημερομηνία διάθεσης.	ΝΑΙ		
2.	Να προσφερθεί η απαραίτητη αδειοδότηση για την κάλυψη εξυπηρετητών βάσεων δεδομένων. Η προσφερόμενη αδειοδότηση δε θα πρέπει να θέτει περιορισμούς στη διακίνηση των δεδομένων.	≥20		
3.	Υλοποίηση σε διάταξη υψηλής διαθεσιμότητας active- passive	ΝΑΙ		
4.	Διαχείριση μέσω κεντρικής κονσόλας διαχείρισης (GUI).	ΝΑΙ		
5.	Σύνδεση «παθητικά» στο δίκτυο σε promiscuousmode κυρίως για τον εντοπισμό απειλών (alert).	ΝΑΙ		
6.	Σύνδεση με πλήρη διαφάνεια στο δίκτυο «σε σειρά» (inlinebridge) με πλήρεις δυνατότητες ανίχνευσης και καταστολής απειλών.	ΝΑΙ		
7.	Ανίχνευση και καταστολή γνωστών επιθέσεων και απειλών σε επίπεδο υπηρεσίας (DBService) και εφαρμογής	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Βάσης Δεδομένων (π.χ. MSSQL, Oracle, κτλ).			
8.	Υποστήριξη της ανάλυσης της δομής ενός SQLtransaction για τον προσδιορισμό όλης της πληροφορίας που σχετίζεται με ένα query. Επίσης θα πρέπει να παρέχει δυνατότητα περαιτέρω συσχετισμού χαρακτηριστικών (attributes) για τον ακριβή προσδιορισμό των στοιχείων πρόσβασης.	ΝΑΙ		
9.	Διάθεση εργαλείου ανάλυσης SQL γραμματικής για την κατανόηση σύνθετων SQLstatements.	ΝΑΙ		
10.	Εκμάθηση της κανονικής και νόμιμης λειτουργίας της βάσης δεδομένων και δημιουργία «προφίλ» ασφαλούς λειτουργίας αυτής, με αυτόματη διαδικασία, αποτρέποντας κάθε είδους δικτυακή κίνηση – πρόσβαση προς την βάση, η οποία αντιτίθεται στο «προφίλ» ασφαλούς λειτουργίας της βάσης δεδομένων, μέσω ανάλυσης της δικτυακής κίνησης και εντός εύλογου χρονικού διαστήματος. Να τεκμηριωθεί αναλυτικά.	ΝΑΙ		
11.	Αποτροπή της επιστροφής ευαίσθητων πληροφοριών προς τον client ως αποτέλεσμα κάποιου μη εξουσιοδοτημένου SQLquery αναλύοντας το περιεχόμενο των SQLqueryresponses. Να τεκμηριωθεί αναλυτικά.	ΝΑΙ		
12.	Η προτεινόμενη λύση πρέπει να υποστηρίζει κατ' ελάχιστον την προστασία των συγκεκριμένων τύπων βάσεων δεδομένων, καθώς και κάθε νεότερη έκδοση αυτών	<ul style="list-style-type: none"> • MS-SQL • Oracle • S4/HANA 		
13.	Πλήρη παρακολούθηση και καταγραφή της πρόσβασης και των ενεργειών των διαχειριστών στη βάση. Αυτό θα πρέπει να γίνεται είτε η πρόσβαση πραγματοποιείται φυσικά στην λύση (locallogon) είτε μέσω κονσόλας διαχείρισης π.χ. remotedesktop, ssh,	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Xwindows κ.ά. Η λειτουργία αυτή δεν θα πρέπει να εισάγει φόρτο στη βάση δεδομένων και δεν θα πρέπει να βασίζεται στην ενεργοποίηση των εγγενών μηχανισμών audit του λειτουργικού συστήματος ή της βάσης.			
14.	Ο μηχανισμός καταγραφής της λύσης ασφάλειας θα πρέπει να επιτρέπει την πλήρη καταγραφή προσβάσεων στη βάση δεδομένων τουλάχιστον για τα παρακάτω: <ul style="list-style-type: none"> ▪ Database and Schema ▪ User or User groups (any/ all or only specific users all users, including sys dba) ▪ Source Application (any/ all or only specific items) ▪ Source IP Address ▪ Stored Procedures (any/ all or only specific items) ▪ Tables or tables groups (any/ all or only specific items) ▪ Column ▪ Operations ▪ User operation ▪ OS User name ▪ OS Computer name ▪ Query response size ▪ Query response time ▪ SQL exceptions ▪ Login/ logout ▪ Privilege operations Query executed	NAI		
15.	Πλήρη παρακολούθηση και καταγραφή της πρόσβασης και των ενεργειών των χρηστών στις βάσεις οι οποίες πραγματοποιούνται μέσω κονσόλας διαχείρισης π.χ. remotedesktop, ssh, Xwindows κ.ά. Να τεκμηριωθεί αναλυτικά.	NAI		
16.	Ο μηχανισμός καταγραφής των προσβάσεων και ενεργειών των χρηστών δεν θα πρέπει να εισάγει φόρτο στη βάση δεδομένων και δεν θα πρέπει να βασίζεται στην ενεργοποίηση των εγγενών	NAI		



A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	μηχανισμών καταγραφής του λειτουργικού συστήματος ή της βάσης (nativeOS/ DBaudit). Να τεκμηριωθεί αναλυτικά.			
17.	Ο μηχανισμός καταγραφής της λύσης ασφάλειας να επιτρέπει την λεπτομερή καταγραφή των ενεργειών των χρηστών στη βάση δεδομένων σε επίπεδο: <ul style="list-style-type: none"> • Local OS user • Database user Source OS user	ΝΑΙ		
18.	Η κονσόλα διαχείρισης να παρέχει τη δημιουργία διαφορετικών ρόλων πρόσβασης και διαχείρισης (π.χ. viewonly, περιορισμένη διαχείριση, πλήρης πρόσβαση κτλ.) .	ΝΑΙ		
19.	Η κονσόλα διαχείρισης θα πρέπει να επιτρέπει τη δημιουργία κανόνων συσχέτισης (correlationrules) ανάμεσα στα γεγονότα ασφάλειας που ανιχνεύονται. Να τεκμηριωθεί αναλυτικά.	ΝΑΙ		
20.	Η λύση θα πρέπει να υποστηρίζει masking.	ΝΑΙ		
21.	Η κονσόλα διαχείρισης θα πρέπει να επιτρέπει την δημιουργία και παραγωγή αναλυτικών αναφορών με βάση κατ' ελάχιστον τα συγκεκριμένα κριτήρια. <ul style="list-style-type: none"> • Ημερομηνία/ Ώρα • Διεύθυνση προέλευσης (sourceIPaddress) • Hostname προέλευσης • DB user name (login) • Διεύθυνση προορισμού (Destination IP address) • Server name προορισμού (DB name) • Client application Τύπος απειλής/ επίθεσης	ΝΑΙ		
22.	Η κονσόλα διαχείρισης θα πρέπει να παρέχει εργαλείο προτυποποιημένων αναφορών με έτοιμες αναφορές για την τεκμηρίωση της καταγραφής των γεγονότων του συστήματος.	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Να τεκμηριωθεί αναλυτικά.			
23.	Χρήση εικονικής μηχανής τύπου VMWareγια την υλοποίηση της λύσης	ΝΑΙ		
24.	Ενοποίηση με το υπάρχον σύστημα εφεδρείας netbackup (για λήψη των απαιτούμενων αντιγράφων ασφαλείας).	ΝΑΙ		
25.	Η λύση θα πρέπει να μπορεί να υποστηρίξει λειτουργικά συστήματα (βάσεων δεδομένων) τουλάχιστον τύπων Unix/ Linux, AIX, Windows.	ΝΑΙ		
26.	Δυνατότητα παρακολούθησης χωρίς τη SPAN πόρτα ή άλλη πόρτα από τα switches του δικτύου της για την παρακολούθηση (mirroring) της δικτυακής κίνησης. Εάν απαιτείται παρακολούθηση της δικτυακής κίνησης, ο Ανάδοχος πρέπει να παρέχει την απαραίτητη networktapping υποδομή και τις απαραίτητες υπηρεσίες υλοποίησης.	ΝΑΙ		
27.	Να αναφερθεί με λεπτομέρεια η αρχιτεκτονική της προτεινόμενης λύσης και τα υποσυστήματα που θα απαιτηθεί να υλοποιηθούν.	ΝΑΙ		
28.	Να αναφερθούν επιπλέον χαρακτηριστικά.	ΝΑΙ		
29.	Δεν θα επιφέρει επιβάρυνση στην λειτουργικότητα της εφαρμογής και της βάσης δεδομένων.	ΝΑΙ		
30.	Τα γεγονότα ασφαλείας θα πρέπει να προωθούνται για περαιτέρω ανάλυση και συσχέτισμό στην προσφερόμενη λύση SIEM.	ΝΑΙ		

7.2.2.22 Λογισμικό κυβερνοασφάλειας ΑΙ, συμπεριλαμβανομένης εγκατάστασης, εκπαίδευσης και υποστήριξης 24/7. 1000 Άδειες

Α/ Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗ ΣΗ	ΑΠΑΝΤΗ ΣΗ	ΠΑΡΑΠΟΜ ΠΗ
	Να αναφερθούν το όνομα και η έκδοση του προσφερόμενου λογισμικού και η χρονολογία διάθεσης της προσφερόμενης έκδοσης	ΝΑΙ		
	Η άδεια χρήσης μπορεί να διατίθεται με την μορφή Λογισμικού ως Υπηρεσία και θα παρέχεται για ελάχιστο χρονικό διάστημα τριάντα (30) μηνών. Να αναφερθεί η συνολική χρονική διάρκεια.	ΝΑΙ		
	Αυτόματη ανακάλυψη (discovery) και ταξινόμηση (classification) όλων των στοιχείων (assets)	ΝΑΙ		
	Δυνατότητα αυτόματης αναγνώρισης της λειτουργίας, των μοτίβων κυκλοφορίας και των πρωτοκόλλων εκτέλεσης για κάθε κεντρικό υπολογιστή ή ομάδα κεντρικών υπολογιστών και τον τύπο συσκευής κάθε κεντρικού υπολογιστή.	ΝΑΙ		
	Δυνατότητα αυτόματης αναγνώρισης χρηστών, πελατών (clients), όλων των φυσικών και εικονικών συσκευών και σχέσεων μεταξύ τους.	ΝΑΙ		
	Δημιουργία αυτόματων χαρτών που δείχνουν σχέσεις και εξαρτήσεις μεταξύ συστημάτων, διακομιστών και εφαρμογών.	ΝΑΙ		
	Αυτόματη αναγνώριση και ανάλυση διαφόρων πρωτοκόλλων AD (LDAP, Kerberos, DNS, DHCP).	ΝΑΙ		
	Συσχέτιση αναγνωρισμένων πληροφοριών μέσω άντλησης - διασύνδεσης από AD	ΝΑΙ		
	Αυτόματη αναγνώριση και ανάλυση πρωτοκόλλων επικοινωνίας (FTP, RDP, Telnet, SSH, syslog, SNMP, SMTP, POP3, NTP, SMPP κ.λπ.),	ΝΑΙ		
	Αυτόματη αναγνώριση και ανάλυση πρωτοκόλλων βάσεων δεδομένων (να υποστηρίζεται κατ' ελάχιστον η βάση MSSQL, με επιθυμητή πλέον την PostgreSQL, MySQL)	ΝΑΙ		
	Ανάλυση κίνησης δικτύου και πρωτοκόλλων από L2 έως L7	ΝΑΙ		
	Παρακολούθηση συσκευών IoT	ΝΑΙ		
	Να αναλύει την πρωτότυπη κυκλοφορία πακέτων δικτύου ή τις ροές επισκεψιμότητας σε πραγματικό χρόνο.			
	Παρακολούθηση της απόδοσης του δικτύου και των εφαρμογών. Παρακολούθηση της συμπεριφοράς, δημιουργία προφίλ και ανάλυση της φυσιολογικής	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	συμπεριφοράς του δικτύου και αναγνώριση / ειδοποίηση για μη φυσιολογική συμπεριφορά			
	Χρήση πολλών αλγορίθμων τεχνητής νοημοσύνης και αρκετών τεχνικών μηχανικής μάθησης, όπως η βαθιά μάθηση, η εποπτευόμενη μηχανική μάθηση και η μη εποπτευόμενη μηχανική μάθηση.	ΝΑΙ		
	Παρακολούθηση της κίνησης στο δίκτυο για τον εντοπισμό απειλών εσωτερικού	ΝΑΙ		
	Κρυπτογραφημένη Ανάλυση Κυκλοφορίας (ETA) στη λύση για τον εντοπισμό ύποπτης κίνησης στο δίκτυο και τον εντοπισμό κακόβουλου περιεχομένου στην κρυπτογραφημένη κίνηση.	ΝΑΙ		
	Ανίχνευση απειλών			
	Προσδιορισμός τυχόν ύποπτης συμπεριφοράς στο δίκτυο και επισήμανση αυτών των συμπεριφορών σε πραγματικό χρόνο. Μηχανισμοί και μέθοδοι για την ανίχνευση απειλών σε πραγματικό χρόνο	ΝΑΙ		
	Δυνατότητα εντοπισμού βάσει ψηφιακής υπογραφής	ΝΑΙ		
	Προσδιορισμός νέων και άγνωστων συμπεριφορών επίθεσης χωρίς χρήση ψηφιακών υπογραφών ή κανόνων,	ΝΑΙ		
	Ανίχνευση διαφορετικών τύπων συμβάντων ασφαλείας (ICMP flood, Beaconing, remote Powershell, Brute force login κ.λπ.),	ΝΑΙ		
	Εντοπισμός κρυπτογραφημένης κίνησης κακόβουλου λογισμικού.	ΝΑΙ		
	Ανίχνευση της μη συμμόρφωσης και της παραβίασης των οδηγιών ασφαλείας πληροφοριών, όπως παραβίαση πολιτικής, μη ασφαλή πρωτόκολλα, παρωχημένα πρωτόκολλα κρυπτογράφησης και κρυπτογραφήματα (ciphers), νέες συσκευές ή συσκευές rogue, κοινή χρήση αρχείων, αποθήκευση cloud κ.λπ.	ΝΑΙ		
	Εντοπισμός μη εξουσιοδοτημένης πρόσβασης αρχείων και άρνησης πρόσβασης σε αρχεία.	ΝΑΙ		
	Οι εντοπισμοί να αναφέρονται στο CVEDB για την ευπάθεια ή το πλαίσιο MITERATT&CK.	ΝΑΙ		
	Κλιμάκωση συμβάντων ασφαλείας σε διαφορετικά μοντέλα εidoποιήσεων / παραβίασης (Anomalies, Data exfiltration,	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	dDoS, Exploitation, Lateral movement, Reconnaissance, Botnet (Command&Control) traffic, Remote execution, malware propagation, Man in the Middle (MitM) attack).			
	Δυνατότητα αυτόματης διαφοροποίησης μεταξύ των κανονικών συμπεριφορών και εκείνων που είναι πιο πιθανό να στοχεύονται ως απειλές botnet	ΝΑΙ		
	Οι ειδοποιήσεις και οι ανωμαλίες συγκεντρώνονται και συσχετίζονται για τη δημιουργία συμβάντων και μπορούν να φιλτραριστούν κατά συσκευή, χρήστη και τύπο παραβίασης.	ΝΑΙ		
	Οι ειδοποιήσεις και οι δυσλειτουργίες συγκεντρώνονται και συσχετίζονται για τη δημιουργία συμβάντων και εμφανίζουν αυτόματα τη βαθμολογία κινδύνου και τη φάση επίθεσης της ανίχνευσης.	ΝΑΙ		
	Αυτοματοποίηση διερεύνησης, χρησιμοποιώντας μηχανική εκμάθηση, για ανίχνευση και ιεράρχηση συμβάντων με διαφορετικά επίπεδα σοβαρότητας σε πραγματικό χρόνο	ΝΑΙ		
	Τροφοδότηση πληροφοριών απειλών (threatintelligencefeed),	ΝΑΙ		
	Πλήρης fullpacketcapture (PCAP) αποθήκευση & ανάλυση για ανίχνευση απειλών	ΝΑΙ		
	Απόκριση Περιστατικών			
	Μηχανισμός απόκρισης που μπορεί να ενεργοποιηθεί με τη δράση του χειριστή ή αυτόνομα ανάλογα με το επίπεδο ορατότητας, σοβαρότητας / κινδύνου και βεβαιότητας που απαιτείται από την ομάδα ασφαλείας για την αυτόματη απόκριση.	ΝΑΙ		
	Αυτόνομη ανταπόκριση σε πραγματικό χρόνο σε περιστατικά υψηλού κινδύνου ή για περιορισμό απειλών σε εξέλιξη	ΝΑΙ		
	Λειτουργικότητα απόκρισης σε συντονισμό με λύσεις τελικού σημείου (EndpointresponseEDR).	ΝΑΙ		
	Λειτουργικότητα απόκρισης σε συντονισμό με εργαλεία ελέγχου πρόσβασης δικτύου (NetworkAccessControlNAC).	ΝΑΙ		
	Εκτέλεση αναδρομικής αναζήτησης απειλών χρησιμοποιώντας μεταδεδομένα δικτύου.	ΝΑΙ		

Α/ Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗ ΣΗ	ΑΠΑΝΤΗ ΣΗ	ΠΑΡΑΠΟΜ ΠΗ
	Η πλήρης διατήρηση πακέτων να υποστηρίζει τουλάχιστον 30 ημερες	ΝΑΙ		
	Η διατήρηση μεταδεδομένων να υποστηρίζει τουλάχιστον 90 ημερες	ΝΑΙ		
	Διαχείριση			
	Πρόσβαση βάσει ρόλου για πολλούς χρήστες σε λειτουργίες δικτύου και ομάδες ασφαλείας.	ΝΑΙ		
	Προσαρμόσιμες προβολές με διάφορες πληροφορίες διαθέσιμες μέσω ξεχωριστών ταμπλό, ανάλογα με το ρόλο του χρήστη.	ΝΑΙ		
	Προσαρμόσιμες προβολές με διάφορους τύπους πληροφοριών σύμφωνα με διαφορετικές περιπτώσεις χρήσης.	ΝΑΙ		
	Εσωτερική ορατότητα δικτύου, που απαιτείται για γρήγορο εντοπισμό και αντιμετώπιση πολλών προβλημάτων δικτύου.	ΝΑΙ		
	Ενσωμάτωση πληροφοριών χρήστη με στατιστικά στοιχεία κίνησης δικτύου για την παροχή λεπτομερών πληροφοριών στη δραστηριότητα των χρηστών οπουδήποτε στο δίκτυο.	ΝΑΙ		
	Δυνατότητα του αναλυτή να διερευνήσει τα δεδομένα (drilldown) σε ένα επιλεγμένο συμβάν.	ΝΑΙ		
	Δυνατότητα αναλυτικής προβολής (drilldown) σε κοινόχρηστα αρχεία στο δίκτυο.	ΝΑΙ		
	Δυνατότητα αναζήτησης συμβάντων σε αναλυμένα δεδομένα χρησιμοποιώντας ερωτήματα.	ΝΑΙ		
	Ανάλυση συσχετισμένων συμβάντων σε ένα γραφικό χρονοδιάγραμμα	ΝΑΙ		
	Κεντρική διαχείριση για διαμόρφωση συστήματος όπως ενημερώσεις (patches) O/S για όλες τις συσκευές,	ΝΑΙ		
	Το κεντρικό σύστημα διαχείρισης θα ενσωματώνει τις απόψεις (views) από όλους τους ιστότοπους που παρακολουθούνται και τα αντίστοιχα δεδομένα / πληροφορίες	ΝΑΙ		
	Κεντρικό σύστημα διαχείρισης για διαμόρφωση και λειτουργία λήψης δεδομένων	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Λοιπές Απαιτήσεις			
	Η λύση να προσφέρεται για εικονικά περιβάλλοντα όπως το ESXi και HyperV	ΝΑΙ		
	Παρακολούθηση σε ιδιωτικά/ δημόσια/ υβριδικά περιβάλλοντα cloud όπως το Azure κλπ.	ΝΑΙ		
	Παρακολούθηση της κυκλοφορίας μέσω SPAN / TAP / Mirror	ΝΑΙ		
	Ενσωμάτωση με λύση SIEM για χειρισμό και συσχέτιση ειδοποιήσεων.	ΝΑΙ		
	Τα μεταδεδομένα να μπορούν να προωθηθούν σε μια λύση SIEM.	ΝΑΙ		
	Ενσωμάτωση με τυπικά συστήματα υποστήριξης για τη διαχείριση συμβάντων.	ΝΑΙ		
	Ενσωμάτων με πλατφόρμες SOAR	ΝΑΙ		
	Υποστήριξη ειδοποιήσεων μέσω email σε συγκεκριμένη ομάδα χρηστών	ΝΑΙ		
	Ειδικές (ad hoc) και προγραμματισμένες αναφορές που παρουσιάζουν στατιστικές πληροφορίες για θέματα ασφάλειας και δικτύου για μια συγκεκριμένη χρονική περίοδο	ΝΑΙ		
	Εφαρμογή για κινητά για ειδοποίηση και διαχείριση συμβάντων.	ΝΑΙ		
	Ο ανάδοχος θα πρέπει να παρέχει διαρκώς επικαιροποιημένο υλικό εκπαίδευσης επί της λύσης του στο οποίο θα συμπεριλαμβάνεται και η χειροκίνητη ανίχνευση τεχνικών και τακτικών περιστατικών κυβερνοασφάλειας.	ΝΑΙ		

7.2.3 Πίνακες Συμμόρφωσης Τμήματος 3 «Εξειδικευμένες λύσεις και υπηρεσίες ασφάλειας για το Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο»»

7.2.3.1 Παροχή υπηρεσίας SOC

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
1.	Τα Data Centers να βρίσκονται εντός της Ελληνικής Επικράτειας και σε κάθε περίπτωση εντός της ΕΕ. Να παρατεθούν λεπτομέρειες για τα DataCenters καθώς και για τους μηχανισμούς ασφαλείας που τα προστατεύουν.	ΝΑΙ		
2.	Αρχιτεκτονική με βάση βέλτιστες πρακτικές η οποία διέπει τις υπηρεσίες	ΝΑΙ		
3.	Δυνατότητα συσχέτισης περιστατικών μεταξύ διαφορετικών πηγών δεδομένων και ανάλυσης ετερογενών δεδομένων για τον εντοπισμό πραγματικών περιστατικών ασφάλειας. Να ληφθεί υπόψη ότι θα συλλέγονται logs και περιστατικά που προέρχονται από διαφορετικά συστήματα και συσκευές του περιβάλλοντος όπως συσκευές παρακολούθησης και διαχείρισης δικτύου, συσκευές ασφαλείας, διακομιστές δικτύου, διακομιστές εφαρμογών, βάσεις δεδομένων, λειτουργικά συστήματα κ.λπ.	ΝΑΙ		
4.	Διαλειτουργικότητα της υπηρεσίας με όλα τα υφιστάμενα αλλά και τα μελλοντικά συστήματα του Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο». Εφόσον απαιτηθεί επιπρόσθετο κόστος ανάπτυξης για την εγκαθίδρυση της διαλειτουργικότητας με τα συστήματα του Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο» αυτό επιβαρύνει αποκλειστικά τον Ανάδοχο.	ΝΑΙ		
5.	Δυνατότητα ενσωμάτωσης απεριόριστου ορίου όγκου δεδομένων αρχείων καταγραφής που παράγονται από τα συστήματα του Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο» στην υπηρεσία. Επιπρόσθετα απαιτείται να μην υφίσταται όριο	Assets 300		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Peakeventpersecond (EPS) rates με σκοπό την αντιμετώπιση πιθανών επιθέσεων στην υποδομή του Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο».			
6.	Μη ύπαρξη αντικτύπου στην υπηρεσία (π.χ. απώλεια ορατότητας, απώλεια αρχείων καταγραφής ή περιστατικών κ.λπ.) σε περίπτωση που για συγκεκριμένο χρονικό διάστημα η υπηρεσία ξεπεράσει τα όρια που έχουν τεθεί στην απαίτηση 5του παρόντος πίνακα συμμόρφωσης.	ΝΑΙ		
7.	Δυνατότητα αναζήτησης και περιήγησης στα πρωτότυπα δεδομένα καταγραφής (rawdata). Απαιτείται η παράθεση των απαραίτητων προδιαγραφών από τον Ανάδοχο ώστε να μην υφίστανται περιορισμοί στην παραπάνω δυνατότητα σύμφωνα με τις Απαιτήσεις του Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο» που αφορούν την περίοδο διακράτησης των δεδομένων καταγραφής, όπως αυτές περιγράφονται στην απαίτηση 13 του παρόντος πίνακα συμμόρφωσης.	ΝΑΙ		
8.	Χρήση εξωτερικών πηγών δεδομένων για την ανάλυση πιθανών απειλών για το περιβάλλον του Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο». Απαιτείται να ενημερώνεται το Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο» για τις πιθανές απειλές και η υπηρεσία να προσαρμόζεται ανάλογα με την ανάλυση των απειλών.	ΝΑΙ		
9.	Δυνατότητα συλλογής και ανάλυσης δεδομένων ευπαθειών από τρίτες πηγές/εργαλεία καθώς και η δυνατότητα συλλογής και ανάλυσης δεδομένων ευπαθειών τα οποία έχουν εντοπισθεί από τρίτους με χειροκίνητες μεθόδους (π.χ. στο	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	πλαίσιο εκτέλεσης PenetrationTest). Να παρασχεθούν λεπτομέρειες σχετικά με τη μεθοδολογία από τον Ανάδοχο για τη συλλογή και ανάλυση δεδομένων ευπαθειών και παραβιάσεων από όλες τις πηγές και τις δυνατότητες ενσωμάτωσης μεταξύ των προσφερόμενων υπηρεσιών.			
10	Δυνατότητα εντοπισμού προσαρμοσμένων ή στοχευμένων επιθέσεων που απευθύνονται στους χρήστες ή τα συστήματά του Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο».	ΝΑΙ		
11	<p>Διαδικτυακή πλατφόρμα/ κονσόλα που σχετίζεται με τις υπηρεσίες του Αναδόχου. Η συγκεκριμένη πλατφόρμα θα αποτελεί τη διεπαφή του Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο» με την υπηρεσία και θα περιλαμβάνει όλες τις απαραίτητες πληροφορίες για την υπηρεσία και θα προσδίδει και δυνατότητες αλληλεπίδρασης του Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο» με την υπηρεσία (π.χ. ticketing σύστημα, σύστημα διαχείρισης συμβάντων, αναφορές υπηρεσίας σε μορφή Dashboards κλπ.).</p> <p>Η πλατφόρμα θα περιλαμβάνει υπηρεσίες οι οποίες θα περιλαμβάνουν χωρίς να περιορίζονται στην περιορισμένη πρόσβαση βάσει ρόλου, στην προσαρμογή οθονών και παρουσίασης δεδομένων, στη ροή εργασιών / έκδοση tickets, προκαθορισμένους κανόνες συσχέτισης και προκαθορισμένες αναφορές. Προσδιορίστε εάν όλες οι υπηρεσίες, συμπεριλαμβανομένων εκείνων που παρέχονται από τους συνεργάτες (εάν υπάρχουν), θα είναι διαθέσιμες μέσω μίας πλατφόρμας.</p>	ΝΑΙ		



Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
12	Δυνατότητα ενσωμάτωσης δεδομένων εκτίμησης ευπαθειών, συμπεριλαμβανομένου του τρόπου με τον οποίο χρησιμοποιούνται τα δεδομένα ευπαθειών για την υποστήριξη των δυνατοτήτων ειδοποίησης και αναφοράς.	ΝΑΙ		
13	Διατήρηση των πρωτογενών και των αναλυμένων δεδομένων του Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο» καθώς και τη δυνατότητα για εφαρμογή διαφορετικών πολιτικών διατήρησης δεδομένων σε διαφορετικούς τύπους συστημάτων/συσκευών εφόσον απαιτηθεί ώστε να πληρούνται οι απαιτήσεις του Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο».	Διάρκεια διατήρησης >12 μήνες		
14	Διαθεσιμότητα επιπέδου υπηρεσίας 99,9%, εξαιρουμένων τυχόν προκαθορισμένων περιόδων συντήρησης οι οποίες θα δηλώνονται ρητά στο SLA.	Διαθεσιμότητα >99,9%		
15	Σαφής καθορισμός εντός του SLA της υπηρεσίας, των χρόνων απόκρισης κατά τον εντοπισμό/ απόκριση σε περιστατικών ασφάλειας, για τις παρακάτω ενέργειες: <ul style="list-style-type: none">• Παραγωγή ειδοποίησης από το σύστημα• Επισκόπηση συμβάντος από εξειδικευμένο μηχανικό• Αποκλεισμός συμβάντων "falsepositive" και "falsenegative"• Καταγραφή διορθωτικών ενεργειών για την αντιμετώπιση του συμβάντος• Επικοινωνία του συμβάντος και των διορθωτικών ενεργειών στο Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο»	ΝΑΙ		

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	<ul style="list-style-type: none"> Απόκριση από την πλευρά του αναδόχου ως προς τις ενέργειες που θα εκτελέσει το Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο» Παρακολούθηση κατά και μετά το κλείσιμο του συμβάντος <p>Προσδιορίστε τα πιο πάνω διαστήματα.</p>			
16	Ανάληψη της ευθύνης για την ασφαλιστική κάλυψη του Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο» σε περίπτωση παραβίασης των ορών της συμφωνίας. Καταχωρίστε τους ακριβείς όρους.	NAI		
17	Για όλη τη διάρκεια της σύμβασης τα συστήματα τα οποία θα χρησιμοποιηθούν/προσφερθούν για την παροχή της υπηρεσίας συνεχίζουν να πληρούν τις απαιτήσεις του διαγωνισμού και να φέρουν υποστήριξη από τον κατασκευαστή. Σε οποιοδήποτε ενδεχόμενο κατάργησης συστημάτων ή τερματισμού υποστήριξης τους από τον κατασκευαστή ο Ανάδοχος οφείλει να τα αντικαταστήσει με συστήματα ίδιων ή ανώτερων προδιαγραφών κατόπιν συνεννόησης και συμφωνίας με του Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο».	NAI		
18	Σε ό,τι αφορά τα περιστατικά αναγνώρισης να υπάρχει δυνατότητα κατηγοριοποίησής τους. Να αναφερθούν οι δυνατότητες.	NAI		
19	Ενσωμάτωση στην SOCυπηρεσίας της επιτήρησης των χρηστών με αυξημένα δικαιώματα. Να περιγραφεί λεπτομερώς πώς θα παρέχεται στο Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο» τη δυνατότητα αναγνώρισης από μια κονσόλα / αναφορά των χρηστών με αυξημένα	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	δικαιώματα που πραγματοποιήσαν συνδέσεις, τυχόν αυξήσεις δικαιωμάτων			
20	Στα πλαίσια της υπηρεσίας SOCaaSχρήση από ττο Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο» προχωρημένης ανάλυσης δεδομένων. Να περιγραφούν λεπτομερώς τις περιπτώσεις χρήσης Analytics (Analytics Use Cases) που θα είναι διαθέσιμες στο Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο» από την εκκίνησης της υπηρεσίας.	NAI		
21	Επαρκής μεθοδολογία από τον ανάδοχο για τη μείωση ψευδών θετικών και ψευδών αρνητικών ειδοποιήσεων. Να περιγράφει η μεθοδολογία του Αναδόχου για τη μείωση ψευδών θετικών και ψευδών αρνητικών ειδοποιήσεων και για την διαβάθμιση των περιστατικών ασφαλείας.	NAI		
22	Υποστήριξη διαφορετικών τύπων δυνατοτήτων συσχέτισης. Να περιγραφούν λεπτομερώς οι διαφορετικοί τύποι δυνατοτήτων συσχέτισης που υποστηρίζει η προτεινόμενη μηχανή συσχετισμού.	NAI		
23	Λύση ticketing που να συμπεριλαμβάνεται στην υπηρεσία. Να περιγραφεί λεπτομερώς η προσφερόμενη λύση ticketing / ροής εργασίας για την κλιμάκωση των περιστατικών.	NAI		
24	Αυτοματοποιημένη λύση ροών εργασίας (workflow) η οποία να είναι ενσωματωμένη στην προσφερόμενη υπηρεσία.	NAI		
25	Καταγεγραμμένες ροές εργασίας για την λύση ticketing. Περιγράψτε πώς θα χρησιμοποιηθεί η προσφερόμενη λύση ticketing / ροής εργασίας από την ομάδα SOCτου Αναδόχου και	NAI		

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	την ομάδα του Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο» για τον συντονισμό και την αποτελεσματική απόκριση κατά τη διάρκεια περιστατικών ασφαλείας.			
26	Η προσφερόμενη λύση ticketing / ροής εργασίας υποστηρίζει την ενσωμάτωση raw Logs και συσχετιζόμενων περιστατικών (Correlated Events) σε ένα ticket περιστατικού.	ΝΑΙ		
27	Η ομάδα παρακολούθησης του Αναδόχου αναλαμβάνει πλήρως την ευθύνη της ενημέρωσης κάθε ticket περιστατικών με rawlogs και συσχετιζόμενα Περιστατικά (Correlated Events) καθ' όλη την περίοδο κατά την οποία το συμβάν βρίσκεται σε εξέλιξη. Να περιγραφεί αναλυτικά η σχετική προσέγγισή.	ΝΑΙ		
28	Λεπτομερής τεκμηρίωση της μεθοδολογίας και η προσέγγισή του Αναδόχου για την Υλοποίηση, Τεκμηρίωση, Διαχείριση Έργου.	ΝΑΙ		
29	Εκπαίδευση των στελεχών του Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο» αναφορικά με την λειτουργία της υπηρεσίας.	ΝΑΙ		
30	Υποβολή τακτικής έκθεσης προς το Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο» στην οποία θα συνοψίζονται τα περιστατικά ασφαλείας και η συνολική κατάσταση του περιβάλλοντος του Οργανισμού κατά την περίοδο αναφοράς.	ΝΑΙ		
31	Κατάρτιση εβδομαδιαίας τεχνικής έκθεσης η οποία θα είναι διαθέσιμη στις τεχνικές ομάδες του Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο». Ο ανάδοχος θα πρέπει να παρέχει ένα δείγμα αναφοράς όπως παρέχεται σε άλλον πελάτη με παρόμοιες απαιτήσεις.	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
32	Να παρασχεθούν παραδείγματα λειτουργικών, κανονιστικών και εκτελεστικών αναφορών.	NAI		
33	Προσαρμοσμένες, ad hoc αναζητήσεις (queries) και αναφορές. Να συμπεριληφθούν τυχόν περιορισμοί στις ad hoc αναζητήσεις ή στη δημιουργία αναφορών, συμπεριλαμβανομένων των πηγών δεδομένων, της παλαιότητας των δεδομένων, της συχνότητας των αναζητήσεων κτλ.	NAI		
34	Δημιουργία αναφορών: Διεπαφή αναφορών που μπορεί να αξιοποιήσει πολλαπλές υφιστάμενες αναφορές. Αναφέρατε το παρεχόμενο πλήθος, καθώς και τη δημιουργία νέων αναφορών που δεν απαιτούν περίπλοκες τεχνικές αναζητήσεις.	NAI		
35	Η λειτουργικότητα παραγωγής αναφορών δεν επηρεάζεται αν μια συγκεκριμένη τεχνολογία, όπως ένα firewall, αντικατασταθεί με ένα νεότερο προϊόν ή προμηθευτή. Οι αναφορές θα πρέπει να συνεχίσουν να εκτελούνται και να περιλαμβάνουν τη νέα τεχνολογία στα κριτήρια αναφοράς αυτόματα.	NAI		
36	Προγραμματισμός αναφορών: Η λύση παρέχει τη δυνατότητα προγραμματισμού των αναφορών ώστε να εκτελούνται σε προκαθορισμένα διαστήματα (ωριαία, καθημερινά, εβδομαδιαία ή μηνιαία). Υφίστανται πολλές μορφές εξαγωγών και επιλογές παράδοσης για προγραμματισμένες αναφορές.	NAI		
37	Αναφορές συμμόρφωσης: Η λύση παρέχει τη δυνατότητα αναφοράς ως προς τη συμμόρφωση με κοινώς αποδεκτά πρότυπα στο χώρο της ασφάλειας (ISO 27002, NIST), τα	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	οποία αντιστοιχίζονται απευθείας σε οποιοδήποτε κανονιστικό πρότυπο ή πολιτική ασφάλειας			
38	Προσαρμοσμένα Dashboards: Η λύση παρέχει το πλαίσιο για τη δημιουργία προσαρμοσμένων dashboards για όλες τις επιχειρηματικές ομάδες.	NAI		
39	Σε περίπτωση διαρροής προσωπικών δεδομένων ή επιχειρησιακών δεδομένων ο ανάδοχος θα προετοιμάζει τις ζητούμενες αναφορές προς την ΑΠΔΠΧ και την Εθνική Αρχή Κυβερνοασφάλειας.	NAI		
40	Επαρκή μέτρα ασφάλειας τα οποία λαμβάνονται από τον Ανάδοχο για την προστασία των δικών του συστημάτων ώστε να μην είναι εφικτή πιθανή επέκταση ενός περιστατικού ασφάλειας στο Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο» ή διαρροή πληροφοριών ή δεδομένων του Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο».	NAI		
41	Lessons Learned, καθώς και Advisories από τον ανάδοχο.	NAI		
42	Περιορισμός Bandwidth: Η λύση πρέπει να παρέχει τη δυνατότητα περιορισμού του Internet bandwidth που χρησιμοποιείται για τη μετάδοση δεδομένων περιστατικών.	NAI		
43	Διασφάλιση συναλλαγών: Η λύση παρέχει μηχανισμό που εγγυάται την αποστολή περιστατικών στο σύστημα διαχείρισης αρχείων καταγραφής και δεν παραλείπονται περιστατικά εάν το σύστημα διαχείρισης καταγραφής δεν είναι διαθέσιμο.	NAI		
44	Υψηλή διαθεσιμότητα συλλογής: Η λύση παρέχει επιλογές για υψηλή	NAI		

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	διαθεσιμότητα αναφορικά με τη συλλογή αρχείων καταγραφής χωρίς την ανάγκη πρόσθετου υλικού.			
45	Επεκτασιμότητα στη διαχείριση αρχείων καταγραφής: Η λύση πρέπει να παρέχει τη δυνατότητα επέκτασης σε μεγαλύτερα περιβάλλοντα και την ένταξη πρόσθετων πηγών περιστατικών χωρίς να απαιτείται επιπλέον εξοπλισμός.	ΝΑΙ		
46	Η λύση δεν απαιτεί εγκατάσταση agent στα συστήματα υπό παρακολούθηση για τη συλλογή των αρχείων καταγραφής (logs). Εφόσον η προσφερόμενη λύση απαιτεί agent να αναφερθούν οι πιθανές επιπτώσεις σε υπολογιστικούς πόρους, ανά τύπο συστήματος μέσω αναφορών σε επίσημα τεχνικά εγχειρίδια του κατασκευαστή. Να αναφερθεί το επίπεδο πρόσβασης/δικαιώματα που θα απαιτείται στα διάφορα συστήματα του Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο» (π.χ. Administrator) για την εγκατάσταση, παραμετροποίηση, αναβάθμιση και συντήρηση των agents εφόσον απαιτηθούν. Επίσης, να αναφερθούν τυχόν απαιτήσεις σε συστήματα και σε συμμετοχή προσωπικού του Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο» για την εγκατάσταση και λειτουργία της λύσης.	ΝΑΙ		
47	Επεξεργασία κατανεμημένων (distributed) περιστατικών: Η λύση πρέπει να συλλέγει αρχεία καταγραφής με κατανεμημένο (distributed) τρόπο, κατανέμοντας τις απαιτήσεις επεξεργασίας του συστήματος διαχείρισης αρχείων	ΝΑΙ		

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	καταγραφής για εργασίες όπως φιλτράρισμα, συγκέντρωση, συμπίεση και κρυπτογράφηση			
48	Η προσφερόμενη λύση θα παρέχει τη δυνατότητα διασύνδεσης και συλλογής αρχείων καταγραφής από όλα τα συστήματα και συσκευές συμπεριλαμβανομένων customized συστήματα και εφαρμογές. Οι οποίες υπηρεσίες απαιτούνται για την υλοποίηση υποστήριξης πρέπει να περιλαμβάνονται στην προσφερόμενη λύση.	ΝΑΙ		
49	Κατηγοριοποίηση δεδομένων περιστατικών: Η λύση κατηγοριοποιεί τα δεδομένα καταγραφής σε μια μορφή αναγνώσιμη για να εξαλείψει την ανάγκη γνώσης αναγνωριστικών περιστατικών συγκεκριμένων προμηθευτών.	ΝΑΙ		
50	Μείωση περιστατικών: Η λύση παρέχει τη δυνατότητα μείωσης των δεδομένων περιστατικών.	ΝΑΙ		
51	Ασφαλής μεταφορά: Η λύση παρέχει κρυπτογραφημένη μετάδοση δεδομένων καταγραφής για όλων των ειδών της επικοινωνίας.	ΝΑΙ		
52	Παρακολούθηση Κατάστασης Συλλογής: Οποιαδήποτε αστοχία της υποδομής συλλογής περιστατικών εντοπίζεται άμεσα και να ενημερώνονται τα εμπλεκόμενα μέρη. Η παρακολούθηση της κατάστασης περιλαμβάνει τη δυνατότητα επιβεβαίωσης ότι οι αρχικές πηγές εξακολουθούν να αποστέλλουν περιστατικά	ΝΑΙ		
53	Εύκολη και γρήγορη αναζήτηση ανάμεσα στα αποθηκευμένα δεδομένα καταγραφής και	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	παραγωγή σχετικών αναφορών με εφαρμογή ειδικών φίλτρων.			
54	Ο προσφερόμενος αριθμός έτοιμων διαθέσιμων κανόνων συσχέτισης είναι επαρκής για την άμεση ανάδειξη σημαντικών θεμάτων ασφάλειας της υποδομής και καλύπτει όλες τις κατηγορίες των κατηγοριών πλαισίων ασφαλείας.	ΝΑΙ		
55	Δημιουργία κανόνων συσχέτισης χρησιμοποιώντας ως βάση τους έτοιμους κανόνες που παρέχει η λύση. Περιγράψτε την προσφερόμενη προσέγγιση.	ΝΑΙ		
56	Λεπτομερής εξέταση των γεγονότων καταγραφής που προκαλούν την ενεργοποίηση ενός κανόνα, με επιλογή γραφικής αναπαράστασης της σειράς των γεγονότων. Περιγράψτε την προσφερόμενη λύση.	ΝΑΙ		
57	Η προσφερόμενη υπηρεσία θα προσφέρει δυνατότητα δημιουργίας και αποστολής ειδοποιήσεων (alerts) σε καθορισμένους χρήστες, μέσω εξειδικευμένης κονσόλας.	ΝΑΙ		
58	Η παραγωγή alerts γίνεται με βάση τη συχνότητα και τον χρόνο εμφάνισης κάποιου γεγονότος, καθώς επίσης και όταν κάποιος κανόνας (time, term) πληρείται.	ΝΑΙ		
59	Η προσφερόμενη υπηρεσία προσφέρει εγγενής (native) δυνατότητα ενσωμάτωσης στην υπηρεσία των cloud υποδομών και τεχνολογιών ασφαλείας του οικοσυστήματος της Microsoft, τις οποίες διαθέτει το Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο». Διευκρινίστε αν για το πιο πάνω θα απαιτείται επιπλέον οικονομική επιβάρυνση για του Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο».	ΝΑΙ		

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
60	Ανάλυση Αρχείων Καταγραφής σε όλο το Περιβάλλον	ΝΑΙ		
61	Η προσφερόμενη πλατφόρμα θα πρέπει να προσφέρει δυνατότητες καταγραφής και ανάλυσης πληροφοριών που προέρχονται τόσο από τη δικτυακή κίνηση όσο και από καταγραφές σε αρχεία logs σε εφαρμογές on premise και στο cloud σε μία ενιαία πλατφόρμα.	ΝΑΙ		
62	Αριθμός ελεγχόμενων συσκευών και συστημάτων σε τακτά χρονικά διαστήματα τόσο εσωτερικά στο περιβάλλον όσο και από το εξωτερικό περιβάλλον (περιμετρικά).	>300 συσκευές		
63	Η λύση θα πρέπει να ανιχνεύει αδυναμίες σε επίπεδο λειτουργικών συστημάτων, υπηρεσιών, δικτύου, τερματικών, Web Εφαρμογών, και Cloud συστημάτων.	ΝΑΙ		
64	Ως μέρος της λύσης θα πρέπει να είναι και η παραγωγή διαφορετικών τύπων αναφορών για διαφορετικού τύπου παραλήπτες προς τους διαχειριστές της υποδομής, καθώς και συνοπτικές αναφορές υψηλού επιπέδου προς τη διοίκηση (highlevelexecutivereports).	ΝΑΙ		
65	Ο ανάδοχος θα πρέπει να παρέχει ως υπηρεσία την διαχείριση αδυναμιών με αυτοματοποιημένο εργαλείο λογισμικού και χρήση ροών εργασιών (workflows) το οποίο θα προσφέρει τη δυνατότητα κεντροποιημένης διαχείρισης. Η συγκεκριμένη υπηρεσία θα χρησιμοποιείται με σκοπό τη διαχείριση όλων των αδυναμιών οι οποίες έχουν εντοπιστεί οριζόντια σε όλη την Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο». Η διαχείριση θα καλύπτει όλο τον κύκλο ζωής των αδυναμιών, από τη στιγμή της	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	αναγνώρισης μέχρι και τη διαχείριση των κινδύνων που απορρέουν από αυτές.			
66	Η προσφερόμενη υπηρεσία μέσω κατάλληλης πλατφόρμας θα πρέπει να περιλαμβάνει μηχανισμό ροής εργασιών με καθορισμένους ρόλους το οποίο διαχειρίζεται αδυναμίες και θα τις αναθέτει ως δραστηριότητες στους κατάλληλους Υπεύθυνους Συστημάτων για τις απαραίτητες ενέργειες διαχείρισης των σχετικών κινδύνων.	NAI		
67	Η προσφερόμενη υπηρεσία μέσω κατάλληλης πλατφόρμας θα πρέπει να παρέχει τη δυνατότητα να ομαδοποιεί τις αδυναμίες κατά προτεραιότητα, σύμφωνα με σαφώς ορισμένα χαρακτηριστικά και θα παρέχει τη δυνατότητα της εξαγωγής των δεδομένων που σχετίζονται με τις αδυναμίες σε διάφορες μορφές.	NAI		
68	Η προσφερόμενη υπηρεσία μέσω κατάλληλης πλατφόρμας θα πρέπει να υποστηρίζει τη δημιουργία αναφορών με δυνατότητα οπτικοποίησης των συσχετίσεων αλλά και περαιτέρω λεπτομερούς ανάλυσης των δεδομένων των αδυναμιών.	NAI		
69	Η προσφερόμενη υπηρεσία μέσω κατάλληλης πλατφόρμας θα πρέπει υποστηρίζει μηχανισμούς/ διαδικασίες όπως υπενθυμίσεις/ ενημερώσεις σε μορφή e-mail των δραστηριοτήτων που έχουν ανατεθεί στους Υπεύθυνους. Ακόμη, θα υποστηρίζει μηχανισμό ελέγχου/ καταγραφής καθώς και τις σχετικές λειτουργικές διαδικασίες.	NAI		
70	Η πλατφόρμα θα πρέπει να παρέχει τη δυνατότητα εισαγωγής δεδομένων υφισταμένων ελέγχων	NAI		

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	τρωτότητας και παρείσδυσης. Επίσης, απαιτείται η υποστήριξη μηχανισμού αυθεντικοποίησης τεχνολογίας Single Sign-on, ο οποίος θα μπορεί να συνδέεται με την λίστα χρηστών του Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο» (LDAP, Active Directory).			
71	Το 24x7 SLA διάρκειας 36 μηνών είναι μέρος της σύμβασης και θα παρακολουθείται. Το SLA θα πρέπει να περιλαμβάνει πλήρη υπηρεσίες υποστήριξης της προσφερόμενης λύσης.	ΝΑΙ		
72	Η προσφερόμενη λύση θα πρέπει να παρέχει την αξιολόγηση όλων των περιστατικών από έμπειρους αναλυτές και κλιμάκωση μόνο των πραγματικών περιστατικών στα προκαθορισμένα όρια παροχής επιπέδου υπηρεσιών (SLA)	ΝΑΙ		
73	Η κλιμάκωση των περιστατικών θα πρέπει πάντα να συνοδεύεται με περιγραφή συμβάντος, τα συστήματα που επηρεάζονται, τους δυνητικούς κινδύνους για το Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο» και προτάσεις για την διαχείριση του κινδύνου	ΝΑΙ		
74	Η προσφερόμενη λύση θα πρέπει να παρέχει την ανάλυση για τον εντοπισμό της προέλευσης των απειλών, τον μετριασμό τους, την έναρξη μέτρων για την πρόληψη της επανεμφάνισης.	ΝΑΙ		
75	Η προσφερόμενη λύση θα πρέπει να παρέχει την συνεχή βελτιστοποίηση των περιπτώσεων χρήσης (usecases), ανάπτυξη νέων usecases, διαχείρισης απόδοσης και προτάσεις για την συνεχή βελτίωση της υπηρεσίας	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
76	Η προσφερόμενη λύση θα πρέπει να ενσωματώνει ένα εγγενές εργαλείο διαχείρισης συμβάντων/ έκδοσης αναφορών (Tickets). Η προσφερόμενη λύση θα πρέπει επίσης να ενσωματωθεί στο εργαλείο διαχείρισης συμβάντων/ εισιτηρίων του Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο».	ΝΑΙ		
77	Η προσφερόμενη λύση θα πρέπει να περιλαμβάνει σχετικές υπηρεσίες εκπαίδευσης (να αναφερθούν οι προσφερόμενες ώρες εκπαίδευσης και το περιεχόμενο αυτής).	ΝΑΙ		
78	Η προσφερόμενη λύση θα πρέπει να είναι σε θέση να συλλέγει αρχεία καταγραφής από οποιονδήποτε αριθμό φυσικών τοποθεσιών, όπως αυτό θα υπαγορεύεται από το Ν.Π.Δ.Δ. «Ελληνικό Κτηματολόγιο», χωρίς καμία επίπτωση στο κόστος της άδειας.	ΝΑΙ		
79	Οι άδειες της προσφερόμενης πλατφόρμας που θα χρησιμοποιηθούν στην υπηρεσία SOCaaS θα ανήκουν στον Φορέα.	ΝΑΙ		

7.2.3.2 Λύση DDOS

A.A	Προδιαγραφή	Απαίτηση	Απάντηση	Παραπομπή
1.	Να περιγραφεί η γενική προσέγγιση της προτεινόμενης on premise και Cloud-based λύσης προστασίας από κατανεμημένες επιθέσεις άρνησης υπηρεσίας (DDoS) και με ποιο τρόπο προστατεύει την επιχειρησιακή συνέχεια (business continuity) και τη διαθεσιμότητα των υπηρεσιών (Δικτυακή δομή -Website - Portal) τους από τις επιθέσεις DDoS	ΝΑΙ		
2.	Αποφυγή Inbound (Εντός εσωτερικού δικτύου) και Outbound απειλές (Από εξωτερικά δίκτυα). Ελάχιστο network traffic το οποίο μπορεί να προστατευτεί από την cloud DDoS λύση ≥ 200 Mbps. Να περιγραφεί αναλυτικά.	ΝΑΙ		

3.	Αποφυγή των γνωστών (μέχρι σήμερα) τύπων DDoS επιθέσεων (DNS, NTP, Chargen, SSDP, SNMP, Portmap, MSSQL, SYN, Slow Rate Attacks, SIP, Volumetric, RFC) amplification attacks, TCP, UDP State exhaustion. Να περιγραφούν άλλοι τύποι επιθέσεων που μπορούν να αποτραπούν και παρατεθούν στοιχεία (π.χ. από ENISA ή άλλο διεθνή οργανισμό).	NAI		
4.	Ελάχιστο inspected throughput	200 Mbps		
5.	Η συσκευή προστασίας DDoS που θα εγκατασταθεί θα πρέπει να παρέχει τη δυνατότητα μετριασμού (mitigation) 6 Gbps, ανεξάρτητα από την άδεια χρήσης.	NAI		
6.	Η συσκευή προστασίας DDoS θα πρέπει να παρέχει τη δυνατότητα αναβάθμισης της άδειας χρήσης για προστασία έως και 5 Gbps καθαρής κίνησης χωρίς την ανάγκη αντικατάστασης υλικού. Αρχικά να προσφερθεί με άδεια για 2Gbp aggregate καθαρή κίνηση	NAI		
7.	Η προσφερόμενη λύση θα πρέπει να παρέχει τη δυνατότητα application layer και state exhausting attacks, εκτός από τις προαναφερόμενες.	NAI		
8.	Η προσφερόμενη λύση θα πρέπει να παρέχει τη δυνατότητα IPV4/IPV6 Header checks, fragmentation checks, layer 4 checks. Να περιγραφούν οι δυνατότητες οι οποίες περιλαμβάνονται.	NAI		
9.	Η DDoS συσκευή που θα προσφερθεί θα πρέπει να εγκατασταθεί στο Data center της ΗΔΙΚΑ	NAI		
10.	Η προτεινόμενη συσκευή θα πρέπει να υποστηρίζει 6 copper Ethernet θύρες και 2xSFP+	NAI		
11.	Η προτεινόμενη συσκευή θα πρέπει να μπορεί με υποστηρίξει λειτουργία IP mode και transparent λειτουργία	NAI		
12.	Η προτεινόμενη DDoS συσκευή θα πρέπει να είναι εξειδικευμένη συσκευή για DDoS Και όχι firewall ή load balancer	NAI		
13.	Η προτεινόμενη συσκευή θα πρέπει να υποστηρίζει τη αντιμετώπιση 0day Burst Attacks με υπογραφή η οποία δημιουργείται αυτόματα.	nAI		
14.	<ul style="list-style-type: none"> Η προτεινόμενη συσκευή θα πρέπει να υποστηρίζει μηδενικό χρόνο για τον μετριασμό των επιθέσεων Burst, ξεκινώντας από το πρώτο χτύπημα burst. 	NAI		
15.	Η προτεινόμενη συσκευή θα πρέπει να παρέχει προστασίας behavioral-DoS χρησιμοποιώντας υπογραφές πραγματικού χρόνου που δημιουργούνται με βάση πολλαπλές παραμέτρους σε κεφαλίδες πακέτων L3 έως L7, αντί για αποκλεισμό διεύθυνσης IP προέλευσης ή περιορισμό ρυθμού	NAI		
16.	Η προτεινόμενη συσκευή θα πρέπει να υποστηρίζει behavioral DDoS προστασία για DNS τόσο σε TCP και UDP.	NAI		
17.	Η προτεινόμενη συσκευή θα πρέπει να υποστηρίζει bahavioral based application layer HTTP DDoS προστασία	NAI		

18.	Η προτεινόμενη συσκευή θα πρέπει να υποστηρίζει προστασία από zero day επιθέσεις	NAI		
19.	Η προτεινόμενη συσκευή θα πρέπει να υποστηρίζει mitigation SLA 18 sec από τον εντοπισμό	NAI		
20.	Η προτεινόμενη συσκευή θα πρέπει να υποστηρίζει IPS.	NAI		
21.	Η προτεινόμενη συσκευή θα πρέπει να υποστηρίζει εβδομαδιαίες ενημερώσεις για signatures feeds για προστασία από νέες επιθέσεις	NAI		
22.	<ul style="list-style-type: none"> Η προτεινόμενη συσκευή θα πρέπει να υποστηρίζει χιλιάδες υπογραφές ταυτόχρονα 	NAI		
23.	Η προτεινόμενη συσκευή θα πρέπει να υποστηρίζει προστασία σε επίπεδο SSL/TLS	NAI		
24.	Η προσφερόμενη λύση θα πρέπει να έχει τη δυνατότητα δημιουργίας Protection Groups. Κάθε PG να μπορεί να αντιστοιχεί σε διαφορετική υποδομή του δικτύου ή server.	NAI		
25.	Η on-premise συσκευή θα πρέπει να έχει τη δυνατότητα εκμάθησης κανονικών επιπέδων κυκλοφορίας και να προτείνει κατάλληλα όρια προστασίας για κάθε υπό παρακολούθηση στοιχείο.	NAI		
26.	<p>Να δοθεί αναλυτική περιγραφή της αρχιτεκτονικής και της λειτουργικότητας της προσφερόμενης λύσης με τη λογική ότι υφίσταται ήδη firewall.</p> <p>Να αναλυθεί το γεγονός ότι η προσφερόμενη λύση DDoS προστατεύει από άλλου τύπου επιθέσεις σε περίπτωση που το υφιστάμενο firewall παρέχει βασικές IPS/IDS λειτουργίες.</p>	NAI		
27.	<p>Η προτεινόμενη συσκευή θα πρέπει να παρέχει SSL προστασία με τους παρακάτω τρόπους</p> <ul style="list-style-type: none"> Keyless SSL Protection (χωρίς certificate και χωρίς decryption) First Request SSL Protection (με decryption Μόνο του πρώτου https request και μόνο κατά τη διάρκεια επίθεσης που εντοπίστηκε μέσω IP reputation) Selective Full SSL Protection (με πλήρη decryption κατά τη διάρκεια επίθεσης και για τις ύποπτες συνδέσεις) Full SSL Protection 	NAI		
28.	Θα πρέπει να υποστηρίζονται οι ακόλουθοι τρόποι λειτουργίας (Modes), κατ' ελάχιστον: inline, SPAN.	NAI		
29.	Η on-premise συσκευή θα πρέπει να υποστηρίζει τις ενσωματωμένες επιλογές παράκαμψης για αστοχία ανοίγματος και αποτυχία κλεισίματος.	NAI		
30.	Η προσφερόμενη λύση θα πρέπει να παρουσιάζει τις πληροφορίες σε ένα φιλικό προς το χρήστη περιβάλλον (GUI).	NAI		

31.	Η προσφερόμενη λύση θα πρέπει παρέχει τη δυνατότητα whitelisting και blacklisting IP διευθύνσεων (Δυνατότητα IPV4 και IPV6.	NAI		
32.	Η προσφερόμενη λύση θα πρέπει να συνοδεύεται από τις απαραίτητες άδειες λειτουργίας οι οποίες θα πρέπει να αφορούν τόσο το λειτουργικό σύστημα, εάν αυτό απαιτεί ξεχωριστή άδεια χρήσης όσο και το λογισμικό. Όλες οι άδειες θα βαρύνουν τον ανάδοχο	NAI		
33.	Η Υποστήριξη του λογισμικού και οι αναβαθμίσεις σε νεότερες εκδόσεις του θα πρέπει παρέχονται από τον ανάδοχο στο πλαίσιο του έργου.	NAI		
34.	Υποστήριξη IPv4 και IPv6 και prefix matching.	NAI		
35.	Υποστήριξη τουλάχιστον SNMP v2 & v3.	NAI		
36.	Η προσφερόμενη λύση θα πρέπει να υποστηρίζει το RESTful API για τη διαμόρφωση του στοιχείου εσωτερικής εγκατάστασης και την παρακολούθηση του στοιχείου cloud.	NAI		
37.	Δυνατότητα για SSL. Να αναφερθούν οι SSL decryption επιλογές	NAI		
38.	Να αναφερθούν τα πρωτόκολλα που χρησιμοποιούνται την προστασία από DDOS επιθέσεις.	NAI		
39.	Η on-premise συσκευή θα πρέπει να υποστηρίζει από τον κατασκευαστή ενημερώσεις για DDos και botnet intelligence.	NAI		
40.	Η On premise συσκευή θα πρέπει να υποστηρίζει εισαγωγή threat feeds (pm IP reputation, active attackers) του κατασκευαστή.	NAI		
41.	Γραφικό περιβάλλον για παρακολούθηση και παραμετροποίηση.	NAI		
42.	Η προσφερόμενη λύση θα πρέπει να έχει τη δυνατότητα για notifications SNMP trap, syslog, email.	NAI		
43.	Να αναφερθούν οι υποστηριζόμενοι φυλλομετρητές (browsers).	NAI		
44.	Η προσφερόμενη λύση θα πρέπει να παρέχει δυνατότητα αναγγελίας συμβάντος μέσω ηλεκτρονικού ταχυδρομείου (email) για σοβαρά συμβάντα, συστημικά συμβάντα ή άλλα θέματα κίνησης.	NAI		
45.	Η προσφερόμενη λύση θα πρέπει να παράγει μηνύματα συμβάντων εξαιτίας λάθους του συστήματος/ κατάσταση υπερφόρτωσης (πχ. Λάθος επεξεργασίας, φόρτωση CPU, υψηλή κατανάλωση μνήμης.)	NAI		
46.	Η προσφερόμενη λύση θα πρέπει να παρέχει αναφορές real-time για πληροφορίες IPV4 και IPV6, total traffic, passed/ blocked traffic, top URL, domain, κλπ.	NAI		
47.	Η προσφερόμενη λύση θα πρέπει να εξαγει δεδομένα σε πολλαπλές μορφές συμπεριλαμβανομένου των παρακάτω δημοφιλών τύπων αρχείων: CSV, XML, PDF, etc.	NAI		

48.	VLAN Tagging support (IEEE 802.1q)	NAI		
49.	Η προσφερόμενη λύση θα πρέπει να δημιουργεί αναγγελίες συμβάντων (alerts) όταν μία τιμή έχει ξεπεράσει το κατώφλι, δείχνοντας: συνολικό traffic, το ποσοστό αποκλεισμένου και το botnet traffic	NAI		
50.	Η προσφερόμενη λύση θα πρέπει να παρέχει μετριάσμο προστασίας OnDemand / AlwaysON έναντι ογκομετρικών (volumetric) επιθέσεων σε πραγματικό χρόνο.	NAI		
51.	Η προσφερόμενη λύση θα πρέπει να μπορεί να ανιχνεύσει και να μετριάσει DDoS επιθέσεις από επίπεδο 3 στο επίπεδο7 του OSI μοντέλου. Στην περίπτωση της Cloud υπηρεσίας η συνολική χωρητικότητα των mitigation κέντρων να είναι 10Tbps.	NAI		
52.	Να περιγράφει ο τρόπος με τον οποίο θα ελαχιστοποιηθεί ο κίνδυνος τοπικής συμφόρησης κάθε Mitigation κέντρο της cloud υπηρεσίας να υποστηρίζει τουλάχιστον 200gbps.	NAI		
53.	Η υπηρεσία cloud θα πρέπει να υποστηρίζει περιοδικές δοκιμές από άκρη σε άκρη της υπηρεσίας, χωρίς επιπλέον κόστος.	NAI		
54.	Η προσφερόμενη cloud λύση θα πρέπει να προστατεύει από volumetric και application DDoS επιθέσεις.	NAI		
55.	Η προσφερόμενη λύση θα πρέπει να βασίζεται στο cloud και σε υβριδικό μοντέλο (λύση που ενσωματώνει εντοπισμό και μετριάσμο on premise εγκατάστασης με volumetric καθαρισμό επιθέσεων βάσει cloud)	NAI		
56.	Η προσφερόμενη cloud DDOS λύση θα πρέπει να ενσωματώνεται με παρόχους Public Cloud για αυτόματη ανίχνευση και εκτροπή στο Cloud Scrubbing Center	NAI		
57.	Η προσφερόμενη λύση cloud DDoS θα πρέπει να αξιοποιεί προσφερόμενη On premise λύση του ίδιου κατασκευαστή	NAI		
58.	Η προσφερόμενη cloud DDoS λύση θα πρέπει να υποστηρίζει SSL encrypted επιθέσεις.	NAI		
59.	Η προσφερόμενη cloud DDoS λύση θα πρέπει να παρέχει προστασία χωρίς να κάνει decrypt πλήρως όλη την κίνηση	NAI		
60.	Η προσφερόμενη cloud DDOS λύση θα πρέπει να είναι πιστοποιημένη σύμφωνα με τα παρακάτω πρότυπα: <ul style="list-style-type: none"> ○ ISO/IEC 27017:2015 (Information Security for Cloud Services) ○ ISO/ IEC 27018:2014 (Information Security Protection of Personally Identifiable Information (PII) in Public Clouds). ○ PCI-DSS v3.1 (Payment Card Industry Data Security Standard) ○ ISO/IEC 27001:2013 (Information Security Management Systems) ○ ISO/IEC 27032:2012 (Security Techniques -- Guidelines for Cybersecurity) ○ ISO 28000:2007 (Supply Chain Security Management System) ○ ISO 9001:2015 (Quality Management System) 	NAI		

	ISO 14001:2015 (Environment Management System)			
61.	Η προσφερόμενη λύση θα πρέπει να είναι ανεξάρτητη του υφιστάμενου παρόχου τηλεπικοινωνιών.	NAI		
62.	Να περιγραφεί ο τρόπος με τον οποίο η προσφερόμενη λύση θα προκαλέσει μετριάσεις On premise και με ποιον τρόπο θα αναδρομολογεί κίνηση στο cloud.	NAI		
63.	Η λύση θα πρέπει να υποστηρίζει εκτροπή κίνησης βάση BGP και DNS	NAI		
64.	Η προσφερόμενη λύση θα πρέπει να υποστηρίζει πολυεπίπεδη προστασία DDoS με σηματοδότηση από μηχανή σε μηχανή από εσωτερική συσκευή μετριάσεων DDoS στο cloud όταν απαιτείται μετριάσεις. Ο χρήστης να μπορεί να διαμορφώσει τη σηματοδότηση χειροκίνητα ή αυτόματα, όπως επιθυμεί.	NAI		
65.	Η υπηρεσία θα πρέπει να μπορεί να παρακολουθεί την εσωτερική συσκευή μετριάσεων DDoS μέσω heartbeat και να ανιχνεύει εάν αυτή η συσκευή δεν είναι πλέον προσβάσιμη.	NAI		
66.	Να περιγραφεί ο τρόπος με τον οποίο η προσφερόμενη λύση θα εκτρέψει την κίνηση.	NAI		
67.	Να περιγραφεί ο τρόπος με τον οποίο η προσφερόμενη λύση θα επαναφέρει την κυκλοφορία	NAI		
68.	Η λύση θα πρέπει να υποστηρίζει asymmetric traffic και symmetric traffic for DDOS τεχνικές μετριάσεων ανάλογα με το μοντέλο ανάπτυξης.	NAI		
69.	Η προσφερόμενη λύση να προστατεύει από DNS flood επιθέσεις			
70.	Η προσφερόμενη λύση θα πρέπει να εντοπίζει και προστατεύει από όλα τα zero-day DNS floods	NAI		
71.	Η λύση πρέπει να μπορεί να προστατεύει από οριζόντιες (all IP and same IP scan) και κατακόρυφες (σε καταστάσεις "σάρωσης".	NAI		
72.	Η λύση πρέπει να μπορεί να προστατεύει από τις ακόλουθες καταστάσεις flood: <ul style="list-style-type: none"> • UDP • TCP ICMP	NAI		
73.	Η λύση θα πρέπει να υποστηρίζει την ανίχνευση της συμπεριφοράς και τον μετριάσμό με μεγάλη ακρίβεια κατά τυχαίων sub-domain flood (για παράδειγμα: Mirai DNS Water Torisation)	NAI		
74.	Η προσφερόμενη λύση θα πρέπει να παρέχει τη δυνατότητα αποκλεισμού της κυκλοφορίας βάσει συγκεκριμένων υπογραφών botnet / επιθέσεων και / ή δακτυλικών αποτυπωμάτων και / ή στην ανάλυση συμπεριφοράς και τη μηχανική μάθηση	NAI		
75.	Η προσφερόμενη λύση θα πρέπει να επιτρέπει την προ-διαμόρφωση προτύπων μετριάσεων για τους πελάτες κατά την αρχική παροχή βάσει	NAI		

	των λεπτομερειών των υπηρεσιών που προστατεύονται και άλλων συγκεκριμένων πληροφοριών για τους πελάτες. Οι χρήστες να έχουν τη δυνατότητα να ενημερώνουν αυτά τα πρότυπα περιοδικά. Αυτά τα πρότυπα πρέπει να εφαρμόζονται σε μετριάσμούς όταν ξεκινά ένας μετριάσμός.			
76.	Η προσφερόμενη λύση θα πρέπει να παρέχει πληροφορίες σχετικά με τον αριθμό των κέντρων μετριάσμού που περιλαμβάνονται στη λύση και τη γεωγραφική θέση των κέντρων μετριάσμού.	ΝΑΙ		
77.	Η προσφερόμενη λύση θα πρέπει να παρέχει μια ειδική πύλη (portal) η οποία να περιλαμβάνει πληροφορίες σε πραγματικό χρόνο σχετικά με την κυκλοφορία που πέρασε, την κυκλοφορία η οποία μειώθηκε κατά τη διάρκεια συμβάντων μετριάσμού, και να επιτρέπει στο χρήστη να επιλέξει τη χρονική περίοδο και τα δεδομένα τα οποία τον αφορούν.	ΝΑΙ		
78.	Η υπηρεσία μετριάσμού cloud θα πρέπει να μην απαιτεί χρέωση ρύθμισης.	ΝΑΙ		
79.	Η λύση cloud θα πρέπει περιλαμβάνει 24/7 SOC πρόσβαση χωρίς επιπλέον κόστος.	ΝΑΙ		
80.	Ο Ανάδοχος ν θα πρέπει α παρέχει τα κάτωθι: vi. Σεμινάρια κατασκευαστή. vii. Οδηγίες χρήσης και γνώση των προϊόντων. viii. Τεκμηρίωση της προσφοράς. ix. Γνωσιακή βάση με γνωστά προβλήματα λογισμικού / υλικού και τρόπους αντιμετώπισής τους. x. Ενημέρωση για επερχόμενες αλλαγές (σφάλματα, επιδιορθώσεις).	ΝΑΙ		
81.	Η προσφερόμενη λύση θα πρέπει να επιτρέπει παραμετροποίηση των δικαιωμάτων των ομάδων Χρηστών (User Account Groups).	ΝΑΙ		
82.	Η προσφερόμενη λύση θα πρέπει να διαθέτει Menu κεντρικής διαχείρισης συμβάντων και σφαλμάτων και δυνατότητα αποστολής ειδοποιήσεων μέσω SNMP, Email, syslog.	ΝΑΙ		
83.	Η διαχείριση της λύσης θα πρέπει να γίνεται μέσω ενός αποκλειστικού συστήματος διαχείρισης που ανήκει στον ίδιο προμηθευτή της ίδιας της συσκευής.	ΝΑΙ		
84.	Η ολοκληρωμένη λύση διαχείρισης πρέπει να υποστηρίζει συγκεκριμένα τα ακόλουθα: • κεντρική διαχείριση των διαμορφώσεων συστήματος των συσκευών Hw (Διαχείριση Διαμόρφωσης). • Συγκεντρωτικό καθορισμό και διανομή των Πολιτικών Ασφαλείας σε διαχειριζόμενες συσκευές. • κεντρική συλλογή και συσχέτιση πληροφοριών (καταγραφής) διαχειριζόμενων συσκευών. • εκτέλεση της εγκληματολογικής ανάλυσης των πληροφοριών που συλλέγονται (ημερολόγιο). • Μηχανισμό εξουσιοδότησης διαφορετικών προφίλ διαχείρισης που βασίζονται σε ρόλους (RBAC - Role Based Access Control).	ΝΑΙ		

	δημιουργία προκαθορισμένων ή προσαρμοσμένων αναφορών που σχετίζονται με τον διαχειριζόμενο εξοπλισμό. Οι αναφορές που δημιουργούνται πρέπει να εξαχθούν σε μορφές "CSV", "PDF" ή "XML".			
85.	Σε περίπτωση σφάλματος (bug) στο λογισμικό, η πλήρης αποκατάσταση του σφάλματος με κατάλληλη διορθωτική έκδοση (patch/fix) θα πρέπει να ολοκληρώνεται εντός μιας (1) ημερολογιακής εβδομάδας. Να περιγραφεί η διαδικασία που θα πρέπει ακολουθείται για την αποκατάσταση των προβλημάτων και να αναφερθεί το μέσο και μέγιστο χρόνο αποκατάστασης.	NAI		
86.	Η προσφερόμενη λύση θα πρέπει να προσφερθεί με subscription και υποστηρίζει για 36 μήνες.	NAI		
87.	Η προσφερόμενη λύση θα πρέπει να διαθέτει κεντρικό μενού με εύκολη πλοήγηση προς όλες τις πληροφορίες και τις αναφορές.	NAI		
88.	Η προσφερόμενη λύση θα πρέπει να έχει τη δυνατότητα προγραμματισμού για ημερήσιες, εβδομαδιαίες ή μηνιαίες αναφορές και δυνατότητα είτε παρακολούθησης από αντίστοιχη ιστοσελίδα είτε εξαγωγής τους σε αρχείο XML, PDF, CSV.	NAI		

7.2.3.3 Υπηρεσίες ανάκαμψης από καταστροφή και λήψης αντιγράφων ασφαλείας

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Το τμήμα Δημοσίου Υπολογιστικού Νέφους (PublicCloud) της προσφερόμενης λύσης θα πρέπει να παρέχει υπηρεσίες φιλοξενίας τύπου Cloud/Hosting, με υπηρεσίες υποδομής ως υπηρεσία (IaaS) και πλατφόρμας ως υπηρεσία (PaaS) από έναν πάροχο Δημοσίου Υπολογιστικού Νέφους.	NAI		
	Η Αναθέτουσα Αρχή θα μπορεί να επιλέξει σε ποια γεωγραφική περιοχή (region) θα φιλοξενηθούν οι επιλεγόμενες υπηρεσίες.	NAI		
	Ο πάροχος θα πρέπει να μπορεί να διαθέτει τις υπηρεσίες του από δύο τουλάχιστον γεωγραφικές περιοχές (regions), εντός Ευρωπαϊκής Ένωσης, με ελάχιστη απόσταση 500 χιλιομέτρων μεταξύ τους, τα οποία θα μπορούν να χρησιμοποιηθούν για την υλοποίηση υπηρεσιών που απαιτούν τον ύψιστο βαθμό υψηλής διαθεσιμότητας με χαρακτηριστικά ανάνηψης από καταστροφή (DisasterRecovery). Να αναφερθούν οι χώρες φιλοξενίας.	NAI		
	Το τμήμα του δημοσίου υπολογιστικού νέφους (PublicCloud) της προσφερόμενης λύσης θα επιτρέπει τη διαμόρφωση υπηρεσιών υψηλής διαθεσιμότητας (highavailability) και ανάκαμψης από καταστροφή (DisasterRecovery).	NAI		
	Απαιτείται η ύπαρξη μηχανισμού παρακολούθησης και ελέγχου της κατάστασης (health) των χρησιμοποιούμενων πόρων σε συνάρτηση με την κατάσταση της υποδομής του παρόχου. Ο μηχανισμός να διαθέτει δυνατότητα μηχανισμού αποστολής ειδοποιήσεων κατά μόναν ή σε ομάδες, email, webhook βάσει κανόνων που τίθενται από το διαχειριστή.	NAI		

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Οι όροι SLA των υπηρεσιών να είναι δημοσιευμένοι στην επίσημη ιστοσελίδα του παρόχου. Να αναφερθεί η σχετική ιστοσελίδα.	ΝΑΙ		
	Για λόγους διαφάνειας και ελέγχου συμμόρφωσης με τα παρεχόμενα επίπεδα SLA η τρέχουσα κατάσταση λειτουργίας του συνόλου των υπηρεσιών θα πρέπει να είναι δημόσια διαθέσιμη στο επίσημο ιστότοπο του παρόχου. Να αναφερθεί η σχετική ιστοσελίδα.	ΝΑΙ		
	<p>Ο πάροχος να διαθέτει δωρεάν υπηρεσίες για τη συνολική διακυβέρνηση – governance των πόρων που θα αξιοποιηθούν από τον φορέα λειτουργίας. Κατ'ελάχιστο απαιτούνται:</p> <ul style="list-style-type: none"> • δυνατότητα οργάνωσης και ελέγχου πρόσβασης στο σύνολο πολλαπλών λογαριασμών και συνδρομών • δυνατότητα διαμόρφωσης και εφαρμογής πολιτικών χρήσης των υπολογιστικών πόρων που περιλαμβάνονται σε λογαριασμούς και στις συνδρομές • καθορισμός πολλαπλών προϋπολογισμών με καθορισμό ορίων στο επιθυμητό επίπεδο εφαρμογής (scope) πόρων και δυνατότητα ενημέρωσης διαχειριστών μέσω email <p>εποπτεία και ανάλυση τρεχουσών χρεώσεων, ιστορικών χρεώσεων και πρόβλεψη της εξέλιξης τους</p>	ΝΑΙ		
	Ο πάροχος να διαθέτει εγγενή μηχανισμό παροχής προτάσεων χωρίς επιπλέον κόστος, για βελτιστοποίηση της χρήσης των χρησιμοποιούμενων πόρων, στους τοείς της ασφάλειας, της διαθεσιμότητας, των επιδόσεων καθώς και του κόστους αυτών, κατά τις βέλτιστες πρακτικές του παρόχου υπολογιστικού νέφους.	ΝΑΙ		
	Να παρέχεται από τον πάροχο του δημοσίου υπολογιστικού νέφους ελεύθερα προσπελάσιμος επίσημος ιστότοπος με πληροφορίες, οδηγούς και εγχειρίδια χρήσης, ρυθμίσεις, συχνές ερωτήσεις και παραδείγματα κώδικα για το σύνολο των υπηρεσιών του. Να αναφερθεί η σχετική ιστοσελίδα.	ΝΑΙ		
	Να παρέχεται δωρεάν εκπαιδευτικό υλικό μέσω ηλεκτρονικής μάθησης σε επίσημο ιστότοπο του παρόχου με ενότητες στους εκάστοτε τομείς των υπηρεσιών υπολογιστικού νέφους. Να αναφερθεί η σχετική ιστοσελίδα.	ΝΑΙ		
	Πιστοποίηση σε ισχύ που να αποδεικνύει τη συμμόρφωση της λειτουργίας του παρόχου με το πρότυπο διασφάλισης ποιότητας ISO/IEC 9001:2015. Να κατατεθεί αντίγραφο της πιστοποίησης.	ΝΑΙ		
	Πιστοποίηση σε ισχύ που να αποδεικνύει τη συμμόρφωση της λειτουργίας του παρόχου με το πρότυπο ασφάλειας ISO/IEC 27001:2013. Να κατατεθεί αντίγραφο της πιστοποίησης.	ΝΑΙ		
	Πιστοποίηση σε ισχύ που να αποδεικνύει τη συμμόρφωση της λειτουργίας του παρόχου με το πρότυπο ασφαλείας πληροφοριακών ελέγχων ISO/IEC 27017:2015. Να κατατεθεί αντίγραφο της πιστοποίησης.	ΝΑΙ		
	Πιστοποίηση σε ισχύ που να αποδεικνύει τη συμμόρφωση της λειτουργίας του παρόχου με το πρότυπο διασφάλισης της προστασίας προσωπικών	ΝΑΙ		

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	δεδομένων ISO/IEC27018:2019. Να κατατεθεί αντίγραφο της πιστοποίησης.			
	Πιστοποίηση σε ισχύ που να αποδεικνύει τη συμμόρφωση της λειτουργίας του παρόχου με το πρότυπο ιδιωτικότητας πληροφοριών ISO/IEC 27701:2019. Να κατατεθεί αντίγραφο της πιστοποίησης.	NAI		
	Πιστοποίηση σε ισχύ που να αποδεικνύει τη συμμόρφωση της λειτουργίας του παρόχου με το πρότυπο διασφάλισης της επιχειρησιακής συνέχειας ISO/IEC 22301:2019. Να κατατεθεί αντίγραφο της πιστοποίησης.	NAI		
	Πιστοποίηση σε ισχύ που να αποδεικνύει τη συμμόρφωση της λειτουργίας του παρόχου με το πρότυπο διαχείρισης υπηρεσιών πληροφοριακού συστήματος ISO/IEC 20000-1:2018	NAI		
	Συμμόρφωση της υποδομής του παρόχου κατά ServiceOrganizationControls (SOC) 1,2 και 3. Να κατατεθούν τα τρία σχετικά reports.	NAI		
	Συμμόρφωση της υποδομής του παρόχου κατά Payment Card Industry (PCI) Data Security Standards (DSS) έκδοση 3.2.1 - Level 1 . Να κατατεθεί η σχετική βεβαίωση.	NAI		
	Η υποδομή του παρόχου δημοσίου υπολογιστικού νέφους να διαθέτει benchmark με πρακτικές και προτάσεις καθοδήγησης, από το CenterforInternetSecurity (CIS) για την προστασία συστημάτων πληροφορικής ανεπτυγμένα στο δημόσιο υπολογιστικό νέφος έναντι κυβερνο-απειλών. Να κατατεθεί το σχετικό benchmark.	NAI		
	Το marketplace του παρόχου δημοσίου υπολογιστικού νέφους να διαθέτει ενισχυμένα -hardened- templates εικονικών μηχανών από το CenterforInternetSecurity (CIS).	NAI		
	Συμμόρφωση της λειτουργίας του παρόχου με το Cloud Control Matrix (CCM) του Cloud Security Alliance (CSA), με τη μορφή του Consensus Assessments Initiative Questionnaire (CAIQ) στην έκδοση 3.1 ή μεταγενέστερη. Να κατατεθεί το σχετικό αποδεικτικό αυτοαξιολόγησης (self assessment).	NAI		
	Πιστοποίηση σε ισχύ που να αποδεικνύει τη συμμόρφωση της λειτουργίας του παρόχου με το πρότυπο CSA-STAR του CloudSecurityAlliance (CSA). Να κατατεθεί αντίγραφο της πιστοποίησης.	NAI		
	Συμμόρφωση της υποδομής του παρόχου κατά EN 301 549. Να κατατεθεί το σχετικό αποδεικτικό.	NAI		
	Οι υπηρεσίες του παρόχου θα πρέπει να είναι συμβατές με τον Κανονισμό (ΕΕ) 2016/679 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα (GDPR Regulation).	NAI		
	Ο Πάροχος του Δημόσιου Υπολογιστικού Νέφους θα πρέπει να είναι μέλος του EUDataCentresEnergyEfficiencyCoC σύμφωνα με την λίστα που δημοσιεύεται στον παρακάτω σύνδεσμο: https://e3p.jrc.ec.europa.eu/node/575	NAI		

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Να αναφερθούν άλλα στοιχεία και μέτρα που αναλαμβάνει ο πάροχος ως προς την ασφάλεια και την κανονιστική συμμόρφωση.	ΝΑΙ		
	Υπηρεσία εξυπηρέτησης εγγενών φορτίων τεχνολογίας VMware με υποστήριξη τεχνολογιών vCenterServer, vSAN, vSphere και NSX-T, στην υποδομή του παρόχου υπολογιστικού νέφους. Ο Πάροχος να αποτελεί εγκεκριμένο προμηθευτή VMwareCloud τεχνολογιών.	ΝΑΙ		
	Παροχή μηνιαίου SLA για την υπηρεσία εξυπηρέτησης εγγενών φορτίων τεχνολογίας VMware, τουλάχιστον 99.9%.	ΝΑΙ		
	Η υπηρεσία εξυπηρέτησης εγγενών φορτίων τεχνολογίας VMware να προσφέρει υψηλό επίπεδο ασφάλειας και προστασίας δεδομένων των χρηστών, με δυνατότητες Role-BasedAccessControlκαι αυθεντικοποίησης μέσω SingleSignOn, αλλά και κρυπτογράφησης των καταχωρούμενων δεδομένων.	ΝΑΙ		
	Να προσφέρεται η δυνατότητα δικτύωσης στο περιβάλλον της υπηρεσίας εξυπηρέτησης εγγενών φορτίων τεχνολογίας VMware, τόσο από την τοπική υποδομή όσο και από το περιβάλλον υπολογιστικού νέφους.	ΝΑΙ		
	Να προσφέρεται η δυνατότητα ανάκαμψης από καταστροφή υφιστάμενης υποδομής VMwareμε χρήση VMwareSiteRecoveryManager (SRM) στην υπηρεσία εξυπηρέτησης εγγενών φορτίων τεχνολογίας VMwareστο περιβάλλον υπολογιστικού νέφους μέσω αποκλειστικού κυκλώματος διασύνδεσης.	ΝΑΙ		
	Να προσφέρεται υπηρεσία αποκατάστασης φορτίων as-a-serviceαπό τον Πάροχο του Δημοσίου Υπολογιστικού Νέφους.	ΝΑΙ		
	Ο πάροχος της προσφερόμενης λύσης να αναφέρεται στηλίστα Leaders του φορέα αξιολόγησης Gartner στην κατηγορία DisasterRecoveryasaService (DRaaS).	ΝΑΙ		
	Μέσωτηςπροσφερόμενηςλύσης, ναπροσφέρεταιπροστασίαυπολογιστικώνσυστημάτωναπόκαταστροφήμέσω συνεχούς replication,διαδικασία μετάπτωσης μετά καταστροφή καθώς και επανάκαμψης και επαναλειτουργίας.	ΝΑΙ		
	Ναπροσφέρεταιη δυνατότητα αποκατάστασης καταστροφών για τις εικονικές μηχανές που λειτουργούν σε περιβάλλον εικονικοποίησης VMware, vSphere/vCenterέκδοσης τουλάχιστον 6.0, μέσω της αναπαραγωγής τους σε περιβάλλον δημοσίου υπολογιστικού νέφους του κατασκευαστή της προσφερόμενης λύσης.	ΝΑΙ		
	Να προσφέρεται η δυνατότητα αποκατάστασης καταστροφών για τις εικονικές μηχανές που λειτουργούν σε περιβάλλον εικονικοποίησης Hyper-V έκδοσης τουλάχιστον 2012 R2, μέσω της αναπαραγωγής τους σε περιβάλλον δημοσίου υπολογιστικού νέφους του κατασκευαστή της προσφερόμενης λύσης.	ΝΑΙ		
	Να προσφέρεται η δυνατότητα αποκατάστασης καταστροφών για τους φυσικούς διακομιστές LinuxκαιWindows, που λειτουργούν σε περιβάλλον τοπικής υποδομής μέσω της αναπαραγωγής τους, είτε σε μια δευτερεύουσα	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	τοπική υποδομή είτε σε περιβάλλον δημοσίου υπολογιστικού νέφους του κατασκευαστή της προσφερόμενης λύσης.			
	Να προσφέρεται δυνατότητα αποκατάστασης καταστροφών για τις εικονικές μηχανές που λειτουργούν στο περιβάλλον δημοσίου νέφους του κατασκευαστή της προσφερόμενης λύσης μέσω της αναπαραγωγής τους σε μια δευτερεύουσα περιοχή του δημοσίου υπολογιστικού νέφους.	NAI		
	Παροχή μηνιαίου SLA για την υπηρεσία αποκατάστασης φορτίων από τοπική υποδομή στο περιβάλλον δημοσίου υπολογιστικού νέφους, εντός 2 ωρών.	NAI		
	Κατά την προστασία των εικονικών, η διαδικασία του replication να μην επηρεάζει τα πρωτότυπα δεδομένα.	NAI		
	Να προσφέρεται η δυνατότητα πραγματοποίησης δοκιμαστικής αποκατάστασης καταστροφών, χωρίς να προκαλούνται ανεπιθύμητες επιπτώσεις στις εφαρμογές και τα δεδομένα του Οργανισμού.	NAI		
	Να προσφέρεται η δυνατότητα πραγματοποίησης δοκιμαστικής αποκατάστασης καταστροφών, τόσο σε κάποια προγραμματισμένη χρονική στιγμή, όσο και σε κάποια η οποία δεν έχει προκαθοριστεί.	NAI		
	Να προσφέρεται η δυνατότητα σχεδιασμού και παραμετροποίησης των σχεδίων αποκατάστασης από καταστροφή από τον Οργανισμό, καθώς και ομαδοποίησης και προτεραιοποίησης της αποκατάστασης των εφαρμογών στα σχέδια αυτά. Επιπλέον, να είναι δυνατή η ενσωμάτωση της προσφερόμενης λύσης με εξειδικευμένα για την εκάστοτε εφαρμογή σενάρια αποκατάστασης καταστροφών.	NAI		
	Κατά την προστασία των εικονικών μηχανών να προσφέρεται η δυνατότητα applicationconsistent σημείων ανάκαμψης.	NAI		
	Να προσφέρεται η δυνατότητα replication κατ'ελάχιστον για τις παρακάτω εφαρμογές τοπικής υποδομής: <ul style="list-style-type: none"> • MicrosoftActiveDirectory • IIS • SQL • SharePoint υποστηρίζοντας τους εγγενείς μηχανισμούς υψηλής διαθεσιμότητας.	NAI		
	Η προσφερόμενη λύση να διαθέτει παραμετροποίηση δικτυακών ρυθμίσεων των προστατευόμενων εικονικών μηχανών, καθώς και συνεργασία με δικτυακές υπηρεσίες του παρόχου υπολογιστικού νέφους.	NAI		
	Ο πάροχος δημοσίου υπολογιστικού νέφους να προσφέρει κανάλι πρόσθετων επιλογών τύπου Marketplace, μέσω του οποίου να προσφέρονται εξειδικευμένες λύσεις αποκατάστασης καταστροφών από αντίστοιχους επίσημους συνεργάτες και κατασκευαστές λογισμικού.	NAI		

7.2.3.4 Λύση Προστασίας Βάσεων Δεδομένων

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
1.	Να αναφερθεί ο κατασκευαστής, η έκδοση και η ημερομηνία διάθεσης.	ΝΑΙ		
2.	Να προσφερθεί η απαραίτητη αδειοδότηση για την κάλυψη εξυπηρετητών βάσεων δεδομένων. Η προσφερόμενη αδειοδότηση δε θα πρέπει να θέτει περιορισμούς στη διακίνηση των δεδομένων.	≥20		
3.	Υλοποίηση σε διάταξη υψηλής διαθεσιμότητας active- passive	ΝΑΙ		
4.	Διαχείριση μέσω κεντρικής κονσόλας διαχείρισης (GUI).	ΝΑΙ		
5.	Σύνδεση «παθητικά» στο δίκτυο σε promiscuousmode κυρίως για τον εντοπισμό απειλών (alert).	ΝΑΙ		
6.	Σύνδεση με πλήρη διαφάνεια στο δίκτυο «σε σειρά» (inlinebridge) με πλήρεις δυνατότητες ανίχνευσης και καταστολής απειλών.	ΝΑΙ		
7.	Ανίχνευση και καταστολή γνωστών επιθέσεων και απειλών σε επίπεδο υπηρεσίας (DBService) και εφαρμογής Βάσης Δεδομένων (π.χ. MSSQL, Oracle, κτλ).	ΝΑΙ		
8.	Υποστήριξη της ανάλυσης της δομής ενός SQLtransaction για τον προσδιορισμό όλης της πληροφορίας που σχετίζεται με ένα query. Επίσης θα πρέπει να παρέχει δυνατότητα περαιτέρω συσχετισμού χαρακτηριστικών (attributes) για τον ακριβή προσδιορισμό των στοιχείων πρόσβασης.	ΝΑΙ		
9.	Διάθεση εργαλείου ανάλυσης SQL γραμματικής για την κατανόηση σύνθετων SQLstatements.	ΝΑΙ		
10.	Εκμάθηση της κανονικής και νόμιμης λειτουργίας της βάσης δεδομένων και δημιουργία «προφίλ» ασφαλούς λειτουργίας αυτής, με αυτόματη διαδικασία, αποτρέποντας κάθε είδους	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	δικτυακή κίνηση – πρόσβαση προς την βάση, η οποία αντιτίθεται στο «προφίλ» ασφαλούς λειτουργίας της βάσης δεδομένων, μέσω ανάλυσης της δικτυακής κίνησης και εντός εύλογου χρονικού διαστήματος. Να τεκμηριωθεί αναλυτικά.			
11.	Αποτροπή της επιστροφής ευαίσθητων πληροφοριών προς τον client ως αποτέλεσμα κάποιου μη εξουσιοδοτημένου SQLquery αναλύοντας το περιεχόμενο των SQLqueryresponses. Να τεκμηριωθεί αναλυτικά.	NAI		
12.	Η προτεινόμενη λύση πρέπει να υποστηρίζει κατ' ελάχιστον την προστασία των συγκεκριμένων τύπων βάσεων δεδομένων, καθώς και κάθε νεότερη έκδοση αυτών	<ul style="list-style-type: none"> • MS-SQL • Oracle • S4/HANA 		
13.	Πλήρη παρακολούθηση και καταγραφή της πρόσβασης και των ενεργειών των διαχειριστών στη βάση. Αυτό θα πρέπει να γίνεται είτε η πρόσβαση πραγματοποιείται φυσικά στην λύση (locallogon) είτε μέσω κονσόλας διαχείρισης π.χ. remotedesktop, ssh, Xwindows κ.ά. Η λειτουργία αυτή δεν θα πρέπει να εισάγει φόρτο στη βάση δεδομένων και δεν θα πρέπει να βασίζεται στην ενεργοποίηση των εγγενών μηχανισμών audit του λειτουργικού συστήματος ή της βάσης.	NAI		
14.	Ο μηχανισμός καταγραφής της λύσης ασφάλειας θα πρέπει να επιτρέπει την πλήρη καταγραφή προσβάσεων στη βάση δεδομένων τουλάχιστον για τα παρακάτω: <ul style="list-style-type: none"> ▪ Database and Schema ▪ User or User groups (any/ all or only specific users all users, including sys dba) ▪ Source Application (any/ all or only specific items) ▪ Source IP Address ▪ Stored Procedures (any/ all or only specific items) 	NAI		



A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	<ul style="list-style-type: none"> ▪ Tables or tables groups (any/ all or only specific items) ▪ Column ▪ Operations ▪ User operation ▪ OS User name ▪ OS Computer name ▪ Query response size ▪ Query response time ▪ SQL exceptions ▪ Login/ logout ▪ Privilege operations Query executed			
15.	Πλήρη παρακολούθηση και καταγραφή της πρόσβασης και των ενεργειών των χρηστών στις βάσεις οι οποίες πραγματοποιούνται μέσω κονσόλας διαχείρισης π.χ. remotedesktop, ssh, Xwindows κ.ά. Να τεκμηριωθεί αναλυτικά.	ΝΑΙ		
16.	Ο μηχανισμός καταγραφής των προσβάσεων και ενεργειών των χρηστών δεν θα πρέπει να εισάγει φόρτο στη βάση δεδομένων και δεν θα πρέπει να βασίζεται στην ενεργοποίηση των εγγενών μηχανισμών καταγραφής του λειτουργικού συστήματος ή της βάσης (nativeOS/ DBaudit). Να τεκμηριωθεί αναλυτικά.	ΝΑΙ		
17.	Ο μηχανισμός καταγραφής της λύσης ασφάλειας να επιτρέπει την λεπτομερή καταγραφή των ενεργειών των χρηστών στη βάση δεδομένων σε επίπεδο: <ul style="list-style-type: none"> • Local OS user • Database user Source OS user	ΝΑΙ		
18.	Η κονσόλα διαχείρισης να παρέχει τη δημιουργία διαφορετικών ρόλων πρόσβασης και διαχείρισης (π.χ. viewonly, περιορισμένη διαχείριση, πλήρης πρόσβαση κτλ.) .	ΝΑΙ		
19.	Η κονσόλα διαχείρισης θα πρέπει να επιτρέπει τη δημιουργία κανόνων συσχέτισης (correlationrules) ανάμεσα	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	στα γεγονότα ασφάλειας που ανιχνεύονται. Να τεκμηριωθεί αναλυτικά.			
20.	Η λύση θα πρέπει να υποστηρίζει masking.	NAI		
21.	Η κονσόλα διαχείρισης θα πρέπει να επιτρέπει την δημιουργία και παραγωγή αναλυτικών αναφορών με βάση κατ' ελάχιστον τα συγκεκριμένα κριτήρια. <ul style="list-style-type: none"> • Ημερομηνία/ Ώρα • Διεύθυνση προέλευσης (sourceIPaddress) • Hostname προέλευσης • DB user name (login) • Διεύθυνση προορισμού (Destination IP address) • Server name προορισμού (DB name) • Client application Τύπος απειλής/ επίθεσης	NAI		
22.	Η κονσόλα διαχείρισης θα πρέπει να παρέχει εργαλείο προτυποποιημένων αναφορών με έτοιμες αναφορές για την τεκμηρίωση της καταγραφής των γεγονότων του συστήματος. Να τεκμηριωθεί αναλυτικά.	NAI		
23.	Χρήση εικονικής μηχανής τύπου VMWare για την υλοποίηση της λύσης	NAI		
24.	Ενοποίηση με το υπάρχον σύστημα εφεδρείας netbackup (για λήψη των απαιτούμενων αντιγράφων ασφάλειας).	NAI		
25.	Η λύση θα πρέπει να μπορεί να υποστηρίξει λειτουργικά συστήματα (βάσεων δεδομένων) τουλάχιστον τύπων Unix/ Linux, AIX, Windows.	NAI		
26.	Δυνατότητα παρακολούθησης χωρίς τη SPAN πόρτα ή άλλη πόρτα από τα switches του δικτύου της για την παρακολούθηση (mirroring) της δικτυακής κίνησης. Εάν απαιτείται παρακολούθηση της δικτυακής κίνησης, ο Ανάδοχος πρέπει να παρέχει την	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	απαραίτητη networktapping υποδομή και τις απαραίτητες υπηρεσίες υλοποίησης.			
27.	Να αναφερθεί με λεπτομέρεια η αρχιτεκτονική της προτεινόμενης λύσης και τα υποσυστήματα που θα απαιτηθεί να υλοποιηθούν.	ΝΑΙ		
28.	Να αναφερθούν επιπλέον χαρακτηριστικά.	ΝΑΙ		
29.	Δεν θα επιφέρει επιβάρυνση στην λειτουργικότητα της εφαρμογής και της βάσης δεδομένων.	ΝΑΙ		
30.	Τα γεγονότα ασφαλείας θα πρέπει να προωθούνται για περαιτέρω ανάλυση και συσχέτισμό στην προσφερόμενη λύση SIEM.	ΝΑΙ		

7.2.3.5 Πλατφόρμα Κυβερνοασφάλειας – Εκτεταμένης Ανίχνευσης & Απόκρισης (Cyber Security)

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
1.	Η πλατφόρμα πρέπει να έχει τη δυνατότητα συλλογής και επεξεργασίας από πολλαπλών τύπων πηγές δεδομένων και όχι μόνο αρχείων καταγραφής, κινούμενη στη φιλοσοφία του bigdatasecurityanalytics.	ΝΑΙ		
2.	Με την εκμετάλλευση αυτοματοποιημένης επεξεργασίας και μηχανικής μάθησης, το σύστημα θα πρέπει να μπορεί να λειτουργεί αποτελεσματικά ως ένα ολοκληρωμένο κέντρο αναφοράς και αυτόματης πρότασης και λήψης αντιμέτρων	ΝΑΙ		
3.	Το σύστημα θα πρέπει κατ' ελάχιστον να συνοδεύεται από τεχνολογίες SIEM, Sandbox,NTA, ThreatIntelligence και IDSκαι να μην απαιτείται η ξεχωριστή προμήθεια λογισμικού.	ΝΑΙ		
4.	Το προσφερόμενο σύστημα θα πρέπει να έχει τη δυνατότητα να υποστηρίζει και το μοντέλο MDR (ManagedDetection&Response) και θα	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	<p>πρέπει να υποστηρίζει το σύνολο του κύκλου ζωής αναγνώρισης και αντιμετώπισης απειλών, που αναλύεται στα στάδια:</p> <ul style="list-style-type: none"> • Συλλογή (Collect) • Εντοπισμός (Detect) • Έρευνα (Investigate) • Απόκριση (Respond) 			
5.	Το υπο προμήθεια σύστημα θα πρέπει να περιλαμβάνει την προμήθεια, εγκατάσταση και παραμετροποίηση αισθητήρων ασφαλείας (φυσικών ή εικονικών), οι οποίοι θα εφαρμόζουν λειτουργίες ML-IDS, antivirus, sandboxing και NTA.	NAI		
	Χαρακτηριστικά NextGenSoc			
6.	Μοντέρνο περιβάλλον χρήσης (GUI) που ενσωματώνει απαραίτητες λειτουργίες παρακολούθησης και διαχείρισης.	NAI		
7.	Πρόσβαση με χρήση ρόλων χρηστών (RBAC – RoleBasedAccess) για την διαχείριση δικαιωμάτων (userprivilegemanagement)	NAI		
8.	Υποστήριξη πολλαπλών ενοίκων (multi-tenant) για την ξεχωριστή διαχείριση οντοτήτων, φυσικών δικτύων κτλ	NAI		
9.	Εφαρμογή ξεχωριστού μοντέλου μηχανικής μάθησης ανά tenant για τη βελτίωση ακρίβειας των αποτελεσμάτων και τη μείωση των εσφαλμένων θετικών συμβάντων (falsepositives), εφαρμόζοντας ξεχωριστά συμπεριφορικά μοντέλα.	NAI		
10.	Εξελιγμένες δυνατότητες μηχανικής μάθησης που να συμπεριλαμβάνουν τόσο supervised όσο και unsupervised διαδικασίες, τεχνολογίες graphML και να συνδυάζονται μεταξύ τους για την παραγωγή βέλτιστων αποτελεσμάτων	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
11.	Δυνατότητες ενσωμάτωσης με εργαλεία και τεχνολογίες ασφαλείας Firewalls, WAF, SWG,EDR, SOAR κτλ	NAI		
12.	Υποστήριξη API για ενσωμάτωση με τεχνολογίες HoneyPots, εργαλεία OSINT κτλ.	NAI		
13.	Μία ενοποιημένη, υψηλής απόδοσης, αποθήκη δεδομένων ("BigData" HighSpeedLake)	NAI		
14.	Δυνατότητα εγκατάστασης τόσο σε φυσικό εξοπλισμό, όσο και σε εικονικό ή περιβάλλον cloud	NAI		
15.	Κατανεμημένη και επεκτάσιμη αρχιτεκτονική που να υποστηρίζει ωστόσο και "AllInOne" σενάρια.	NAI		
16.	Υψηλή διαθεσιμότητας με τη χρήση clusters και ευέλικτη τήρηση και αποθήκευση δεδομένων.	NAI		
17.	Μηχανισμοί Συλλογής που να μπορούν να εγκατασταθούν τόσο σε φυσικό όσο και σε εικονικό περιβάλλον	NAI		
18.	Το σύστημα θα πρέπει να ακολουθεί ανοιχτή αρχιτεκτονική που να επιτρέπει την εισαγωγή δεδομένων από οποιαδήποτε συσκευή με τη χρήση IntegrationAPIs.	NAI		
19.	Κεντριοποιημένη διαχείριση	NAI		
20.	Απλό ενοποιημένο μοντέλο αδειών χωρίς επιπλέον κόστη	NAI		
	Next-GenerationSIEM			
21.	Η πλατφόρμα θα πρέπει να βασίζεται σε μια ενοποιημένη αποθήκη δεδομένων βασισμένη στην αρχιτεκτονική του bigdatalake και τα δεδομένα θα πρέπει κατ' ελάχιστον να μπορούν να εισαχθούν μέσω syslog.	NAI		
22.	Απλός όσο και εξεζητημένος μηχανισμός αναζήτησης που να βασίζεται σε λογικούς τελεστές (Booleanmodifiers)	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
23.	Οι αναζητήσεις να μπορούν να εφαρμοστούν ως μόνιμα φίλτρα σε όλο το περιβάλλον για ταχύτερη διερεύνηση και ανάλυση περιστατικών.	NAI		
24.	Υψηλής απόδοσης και άμεσες ανταποκρίσεις στην αναζήτηση και το φιλτράρισμα στο bigdata	NAI		
25.	Πρόσβαση σε πηγές δεδομένων και όχι μόνο σε syslog δεδομένα	NAI		
26.	Συλλογή δεδομένων από δικτυακή κίνηση (μέσω TAP ή MirrorTraffic). Τα πακέτα θα πρέπει να γίνονται reduce, να κανονικοποιούνται και να μετατρέπονται σε αξιοποιήσιμα μετα-δεδομένα για την ενσωμάτωση στο bigdatalake.	NAI		
27.	Συλλογή δεδομένων από user sources όπως το Microsoft AD μέσω API Connector	NAI		
28.	Συλλογή δεδομένων από πηγές νέφους (cloud) Office365 μέσω Connectors	NAI		
29.	Τα δεδομένα από πηγές πρέπει να κανονικοποιούνται, να εμπλουτίζονται και να συσχετίζονται αυτόματα από το σύστημα	NAI		
30.	Πηγές εμπλουτισμού πρέπει να περιλαμβάνονται γεωγραφικού προσδιορισμού (Geo-Awareness), IPReputation, ThreatIntelligence και DPIApplicationawareness.	NAI		
31.	Μοντέρνο περιβάλλον χρήστη με λειτουργίες SIEM που περιλαμβάνουν ερωτήματα και δημιουργίες κανόνων.	NAI		
32.	Πρόσθετο για παραδοσιακή απεικόνιση SIEM (π.χ. Kibana)	NAI		
	Εντοπισμός KillChain (KillChainDetections)			
33.	Το σύστημα πρέπει να έχει ενσωματωμένους μηχανισμούς εντοπισμών σε κάθε φάση του CyberSecurityKillChain, συμπεριλαμβάνοντας Reconnaissance, Delivery, Exploitation, Installation,	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Command&Control, andActions&Exfiltrations			
34.	Το σύστημα πρέπει να περιλαμβάνει ενσωματωμένη βάση υπογραφών IDS, ενισχυμένη από ανάλυση μηχανικής μάθησης (ML-IDS)	NAI		
35.	Η πλατφόρμα πρέπει να υποστηρίζει πολλαπλά ThreatIntelligenceFeeds, συμπεριλαμβάνοντας εμπορικές πηγές, open-source, anti-phishing κ.α.	NAI		
36.	Η πλατφόρμα πρέπει να επιτρέπει ενσωμάτωση με 3 rd partyfeeds μέσω STIX/TAXII και/η MISP	NAI		
37.	Η πλατφόρμα πρέπει να έχει ενσωματωμένες δυνατότητες APTsandboxing για να αναγνωρίζει και να περιορίζει άγνωστα αρχεία, και για εντοπισμό ransomware, spyware.	NAI		
	ΑνάλυσηΔικτύου (Network Traffic Analysis)			
38.	Η πλατφόρμα πρέπει να ενσωματώνει λειτουργικότητα DeepPacketInspection (DPI) για την αναγνώριση τουλάχιστον 4000 εφαρμογών και να δομεί σχετικά συμπεριφορικά μοντέλα.	NAI		
39.	Τα δεδομένα κίνησης δικτύου πρέπει να μετασχηματίζονται σε κατάλληλα μετα-δεδομένα που περιλαμβάνουν και το payload, για την αντίστοιχη προαιρετική μείωση ανάγκης αποθηκευτικών χώρων.	NAI		
40.	Η πλατφόρμα πρέπει να ενσωματώνει λειτουργικότητα NTADetections, συμπεριλαμβάνοντας ApplicationUsageAnomalies, LongAppSessionAnomalies, καιUnapprovedAssetActivity	NAI		
41.	Το σύστημα θα πρέπει να εντοπίζει ανωμαλίες στη συμπεριφορά των Firewalls, denialanomalies ή ruleusageanomalies	NAI		
	UserBehaviorAnalytics (UBA)			

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
42.	Το σύστημα πρέπει να πραγματοποιεί ανάλυση και εντοπισμό ανωμαλιών στη συμπεριφορά του χρήστη (userbehavior)	ΝΑΙ		
43.	Το σύστημα πρέπει να ενσωματώνει μοντέλα εντοπισμού ανωμαλιών αδύνατου ταξιδιού (ImpossibleTravelAnomaly) ή ώρες αυθεντικοποίησης (LogInTimeAnomaly)	ΝΑΙ		
44.	Εντοπισμούς NTA, έτσι κι εδώ όλα τα detections και τα σχετικά events στα logs και σε πηγές πρέπει να συσχετίζονται αυτόματα.	ΝΑΙ		
	EndpointBehaviorAnalytics (EBA)			
45.	Το σύστημα θα πρέπει να μπορεί να εισάγει δεδομένα από τρίτα συστήματα εντοπισμού ευπαθειών (vulnerabilityscanners) Nessus, Tenable, Rapid7 και να συσχετίζει τα ευρήματα με σχετικά γεγονότα ασφαλείας.	ΝΑΙ		
46.	Το σύστημα θα πρέπει να μπορεί να ανακαλύψει όλα τα assets σε ένα περιβάλλον και να τα κατηγοριοποιεί με βάση τη διεύθυνση MAC και IP.	ΝΑΙ		
47.	Η λίστα των ανακαλυφθέντων/εντοπισθέντων assets θα πρέπει να μπορεί να επαυξάνεται και να παραμετροποιείται με τη χρήση αρχείων csv με λίστες assets και περιγραφές.	ΝΑΙ		
48.	Το σύστημα πρέπει να μπορεί να καταγράφει όλους συσχετισμούς με ένα asset με IP διευθύνσεις, ιστορικά στοιχεία για τη χρήση εφαρμογών κτλ.	ΝΑΙ		
	Ορατότητα Δικτύου και Υπηρεσιών (Network&ServiceVisibility)			
49.	Το σύστημα θα πρέπει να περιλαμβάνει δυνατά εργαλεία απεικόνισης δικτύων και υπηρεσιών, μαζί με analytics, με στόχο να προσφέρει ορατότητα επιδόσεις δικτύου (networkperformance), applicationusage κτλ.	ΝΑΙ		
	ΚυνήγιΑπειλώνκαιΔιερεύνηση (Threat Hunting & Investigation)			

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
50.	Το σύστημα πρέπει να έχει ενσωματωμένα σχετικά εργαλεία, προκαθορισμένες αναζητήσεις και ερωτήματα, και οπτικοποιήσεις (visualizations).	ΝΑΙ		
51.	Τα visualizations πρέπει να είναι παραμετροποιήσιμα	ΝΑΙ		
52.	Το σύστημα πρέπει να προσφέρει εξελιγμένες δυνατότητες συσχετισμένες αναζητήσεις, που επιτρέπουν αναλυτές να συνδέσουν πολλαπλά ανεξάρτητα ερωτήματα με κοινά κριτήρια προκειμένου να δομήσουν πληροφορίες από attacksequences ή να απομονώσουν κοινές πληροφορίες.	ΝΑΙ		
53.	Όλα τα ερωτήματα θα πρέπει να μπορούν να αποθηκευθούν, επεξεργαστούν, κλωνοποιηθούν κτλ από χρήστες.	ΝΑΙ		
54.	Τα visualizations πρέπει να μπορούν να αποθηκευθούν σαν customdashboards.	ΝΑΙ		
55.	Τα ερωτήματα θα πρέπει να μπορούν να συνδυαστούν με ενέργειες/αποκρίσεις για PlayBooks	ΝΑΙ		
	Playbooks / Integrated Orchestration & Response (SOAR)			
56.	Το σύστημα πρέπει να συμπεριλαμβάνει μια βιβλιοθήκη με έτοιμα ενσωματωμένα playbooks, που είναι αυτό-εκτελέσιμα ερωτήματα με ενσωματωμένες ενέργειες.	ΝΑΙ		
57.	Οι ενσωματωμένες ενέργειες/αποκρίσεις θα πρέπει να συμπεριλαμβάνουν: <ul style="list-style-type: none"> Alerts – Αποστολή e-mail/slack message κτλ Actions – Άνοιγμα case, εκτέλεσημιαεντολής API, δημιουργία security event κτλ Responses – Μπλοκάρισμα μιας IP στο Firewall, απενεργοποίηση χρήστη στο AD, εκτέλεση δέσμης ενεργειών κτλ 	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
58.	Παράλληλα με αυτοματοποιημένες ενέργειες, εξωτερικές ενέργειες το μπλοκάρισμα μια IP ή χρήστη θα πρέπει να είναι διαθέσιμες στο χρήστη μέσω του UI ώστε να μπορούν παράλληλα να υλοποιηθούν ως μέρος διερεύνησης/αντιμετώπισης ή ανάλυσης.	NAI		
59.	Δυνατότητα ενσωμάτωσης με εμπορικά εργαλεία SOAR	NAI		
	Ειδοποιήσεις (Alarming)			
60.	Το σύστημα θα πρέπει να προσφέρει έναν έξυπνο, μοντέρνο και παραμετροποιήσιμο μηχανισμό ειδοποιήσεων που να δύναται να οριστεί με βάση παραλήπτες και άλλα κριτήρια (scoreseverity, killchaincategory, etc.)	NAI		
61.	Οι ειδοποιήσεις πρέπει να μπορούν να αποσταλούν με email ή slack μηνύματα και τα μηνύματα πρέπει να είναι παραμετροποιήσιμα ως το περιεχόμενο και τα σχετικά δεδομένα.	NAI		
	Αναφορές (Reporting)			
62.	Το σύστημα πρέπει να περιέχει ένα σύγχρονο εξελιγμένο μηχανισμό αναφορών που θα επιτρέπει παράλληλα εύκολη δημιουργία νέων αναφορών με draganddropκαι αποθήκευσή για χρήση σε οποιοδήποτε σημείο.	NAI		
63.	Οι αναφορές θα πρέπει να παράγονται με χρονοπρογραμματισμό και να αποστέλλονται σε διαφορετικούς χρήστες.	NAI		
64.	Οι αναφορές πρέπει να είναι δυνατόν να αποστέλλονται με email σαν pdf ή csvή να γράφονται σε αρχείο.	NAI		
65.	Το σύστημα θα πρέπει να περιλαμβάνει πληθώρα έτοιμων αναφορών και templates.	NAI		
	Portal			

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
66.	Πρόσβαση των χρηστών βάση ρόλου (UserRBACaccess) στο Portal με συνολική ή περιορισμένη πρόσβαση πληροφορίες.	ΝΑΙ		
67.	Custom Dashboards ανάρόλοχρήστη.	ΝΑΙ		
68.	Χρονοπρογραμματισμένες αναφορές για κάθε tenant, tenantgroup και RBACusers.	ΝΑΙ		
69.	Η πρόσβαση των χρηστών πρέπει να μπορεί να περιορίζεται σε Read-Only, limitedview, μέχρι fullvisibilityandaccess.	ΝΑΙ		

7.2.3.6 Λογισμικό κυβερνοασφάλειας ΑΙ, συμπεριλαμβανομένης εγκατάστασης, εκπαίδευσης και υποστήριξης 24/7. 1000 Άδειες

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
1.	Να αναφερθούν το όνομα και η έκδοση του προσφερόμενου λογισμικού και η χρονολογία διάθεσης της προσφερόμενης έκδοσης	ΝΑΙ		
2.	Η άδεια χρήσης μπορεί να διατίθεται με την μορφή Λογισμικού ως Υπηρεσία και θα παρέχεται για ελάχιστο χρονικό διάστημα τριάντα (30) μηνών. Να αναφερθεί η συνολική χρονική διάρκεια.	ΝΑΙ		
3.	Αυτόματη ανακάλυψη (discovery) και ταξινόμηση (classification) όλων των στοιχείων (assets)	ΝΑΙ		
4.	Δυνατότητα αυτόματης αναγνώρισης της λειτουργίας, των μοτίβων κυκλοφορίας και των πρωτοκόλλων εκτέλεσης για κάθε κεντρικό υπολογιστή ή ομάδα κεντρικών υπολογιστών και τον τύπο συσκευής κάθε κεντρικού υπολογιστή.	ΝΑΙ		
5.	Δυνατότητα αυτόματης αναγνώρισης χρηστών, πελατών (clients), όλων των φυσικών και εικονικών συσκευών και σχέσεων μεταξύ τους.	ΝΑΙ		
6.	Δημιουργία αυτόματων χαρτών που δείχνουν σχέσεις και εξαρτήσεις μεταξύ συστημάτων, διακομιστών και εφαρμογών.	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠ ΟΜΠΗ
7.	Αυτόματη αναγνώριση και ανάλυση διαφόρων πρωτοκόλλων AD (LDAP, Kerberos, DNS, DHCP).	ΝΑΙ		
8.	Συσχέτιση αναγνωρισμένων πληροφοριών μέσω άντλησης - διασύνδεσης από AD	ΝΑΙ		
9.	Αυτόματη αναγνώριση και ανάλυση πρωτοκόλλων επικοινωνίας (FTP, RDP, Telnet, SSH, syslog, SNMP, SMTP, POP3, NTP, SMPP κ.λπ.),	ΝΑΙ		
10.	Αυτόματη αναγνώριση και ανάλυση πρωτοκόλλων βάσεων δεδομένων (να υποστηρίζεται κατ' ελάχιστον η βάση MSSQL, με επιθυμητή πλέον την PostgreSQL, MySQL)	ΝΑΙ		
11.	Ανάλυση κίνησης δικτύου και πρωτοκόλλων από L2 έως L7	ΝΑΙ		
12.	Παρακολούθηση συσκευών IoT	ΝΑΙ		
13.	Να αναλύει την πρωτότυπη κυκλοφορία πακέτων δικτύου ή τις ροές επισκεψιμότητας σε πραγματικό χρόνο.			
14.	Παρακολούθηση της απόδοσης του δικτύου και των εφαρμογών. Παρακολούθηση της συμπεριφοράς, δημιουργία προφίλ και ανάλυση της φυσιολογικής συμπεριφοράς του δικτύου και αναγνώριση / ειδοποίηση για μη φυσιολογική συμπεριφορά	ΝΑΙ		
15.	Χρήση πολλών αλγορίθμων τεχνητής νοημοσύνης και αρκετών τεχνικών μηχανικής μάθησης, όπως η βαθιά μάθηση, η εποπτευόμενη μηχανική μάθηση και η μη εποπτευόμενη μηχανική μάθηση.	ΝΑΙ		
16.	Παρακολούθηση της κίνησης στο δίκτυο για τον εντοπισμό απειλών εσωτερικού	ΝΑΙ		
17.	Κρυπτογραφημένη Ανάλυση Κυκλοφορίας (ETA) στη λύση για τον εντοπισμό ύποπτης κίνησης στο δίκτυο και τον εντοπισμό κακόβουλου περιεχομένου στην κρυπτογραφημένη κίνηση.	ΝΑΙ		
	Ανίχνευση απειλών			
18.	Προσδιορισμός τυχόν ύποπτης συμπεριφοράς στο δίκτυο και επισήμανση αυτών των συμπεριφορών σε πραγματικό χρόνο. Μηχανισμοί και μέθοδοι για την ανίχνευση απειλών σε πραγματικό χρόνο	ΝΑΙ		
19.	Δυνατότητα εντοπισμού βάσει ψηφιακής υπογραφής	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
20.	Προσδιορισμός νέων και άγνωστων συμπεριφορών επίθεσης χωρίς χρήση ψηφιακών υπογραφών ή κανόνων,	ΝΑΙ		
21.	Ανίχνευση διαφορετικών τύπων συμβάντων ασφαλείας (ICMP flood, Beaconing, remote Powershell, Brute force login κ.λπ.),	ΝΑΙ		
22.	Εντοπισμός κρυπτογραφημένης κίνησης κακόβουλου λογισμικού.	ΝΑΙ		
23.	Ανίχνευση της μη συμμόρφωσης και της παραβίασης των οδηγιών ασφαλείας πληροφοριών, όπως παραβίαση πολιτικής, μη ασφαλή πρωτόκολλα, παρωχημένα πρωτόκολλα κρυπτογράφησης και κρυπτογραφήματα (ciphers), νέες συσκευές ή συσκευές rogue, κοινή χρήση αρχείων, αποθήκευση cloud κ.λπ.	ΝΑΙ		
24.	Εντοπισμός μη εξουσιοδοτημένης πρόσβασης αρχείων και άρνησης πρόσβασης σε αρχεία.	ΝΑΙ		
25.	Οι εντοπισμοί να αναφέρονται στο CVEDB για την ευπάθεια ή το πλαίσιο MITERATT&CK.	ΝΑΙ		
26.	Κλιμάκωση συμβάντων ασφαλείας σε διαφορετικά μοντέλα διδασκαλίας / παραβίασης (Anomalies, Data exfiltration, dDoS, Exploitation, Lateral movement, Reconnaissance, Botnet (Command&Control) traffic, Remote execution, malware propagation, Man in the Middle (MitM) attack).	ΝΑΙ		
27.	Δυνατότητα αυτόματης διαφοροποίησης μεταξύ των κανονικών συμπεριφορών και εκείνων που είναι πιο πιθανό να στοχεύονται ως απειλές botnet	ΝΑΙ		
28.	Οι ειδοποιήσεις και οι ανωμαλίες συγκεντρώνονται και συσχετίζονται για τη δημιουργία συμβάντων και μπορούν να φιλτραριστούν κατά συσκευή, χρήστη και τύπο παραβίασης.	ΝΑΙ		
29.	Οι ειδοποιήσεις και οι δυσλειτουργίες συγκεντρώνονται και συσχετίζονται για τη δημιουργία συμβάντων και εμφανίζουν αυτόματα τη βαθμολογία κινδύνου και τη φάση επίθεσης της ανίχνευσης.	ΝΑΙ		
30.	Αυτοματοποίηση διερεύνησης, χρησιμοποιώντας μηχανική εκμάθηση, για ανίχνευση και ιεράρχηση συμβάντων με διαφορετικά επίπεδα σοβαρότητας σε πραγματικό χρόνο	ΝΑΙ		
31.	Τροφοδότηση πληροφοριών απειλών (threatintelligencefeed),	ΝΑΙ		

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
32.	Πλήρης fullpacketcapture (PCAP) αποθήκευση & ανάλυση για ανίχνευση απειλών	ΝΑΙ		
	Απόκριση Περιστατικών			
33.	Μηχανισμός απόκρισης που μπορεί να ενεργοποιηθεί με τη δράση του χειριστή ή αυτόνομα ανάλογα με το επίπεδο ορατότητας, σοβαρότητας / κινδύνου και βεβαιότητας που απαιτείται από την ομάδα ασφαλείας για την αυτόματη απόκριση.	ΝΑΙ		
34.	Αυτόνομη ανταπόκριση σε πραγματικό χρόνο σε περιστατικά υψηλού κινδύνου ή για περιορισμό απειλών σε εξέλιξη	ΝΑΙ		
35.	Λειτουργικότητα απόκρισης σε συντονισμό με λύσεις τελικού σημείου (EndpointresponseEDR).	ΝΑΙ		
36.	Λειτουργικότητα απόκρισης σε συντονισμό με εργαλεία ελέγχου πρόσβασης δικτύου (NetworkAccessControlNAC).	ΝΑΙ		
37.	Εκτέλεση αναδρομικής αναζήτησης απειλών χρησιμοποιώντας μεταδεδομένα δικτύου.	ΝΑΙ		
38.	Η πλήρης διατήρηση πακέτων να υποστηρίζει τουλάχιστον 30 ημερες	ΝΑΙ		
39.	Η διατήρηση μεταδεδομένων να υποστηρίζει τουλάχιστον 90 ημερες	ΝΑΙ		
	Διαχείριση			
40.	Πρόσβαση βάσει ρόλου για πολλούς χρήστες σε λειτουργίες δικτύου και ομάδες ασφαλείας.	ΝΑΙ		
41.	Προσαρμόσιμες προβολές με διάφορες πληροφορίες διαθέσιμες μέσω ξεχωριστών ταμπλό, ανάλογα με το ρόλο του χρήστη.	ΝΑΙ		
42.	Προσαρμόσιμες προβολές με διάφορους τύπους πληροφοριών σύμφωνα με διαφορετικές περιπτώσεις χρήσης.	ΝΑΙ		
43.	Εσωτερική ορατότητα δικτύου, που απαιτείται για γρήγορο εντοπισμό και αντιμετώπιση πολλών προβλημάτων δικτύου.	ΝΑΙ		
44.	Ενσωμάτωση πληροφοριών χρήστη με στατιστικά στοιχεία κίνησης δικτύου για την παροχή λεπτομερών	ΝΑΙ		

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	πληροφοριών στη δραστηριότητα των χρηστών οπουδήποτε στο δίκτυο.			
45.	Δυνατότητα του αναλυτή να διερευνήσει τα δεδομένα (drilldown) σε ένα επιλεγμένο συμβάν.	ΝΑΙ		
46.	Δυνατότητα αναλυτικής προβολής (drilldown) σε κοινόχρηστα αρχεία στο δίκτυο.	ΝΑΙ		
47.	Δυνατότητα αναζήτησης συμβάντων σε αναλυμένα δεδομένα χρησιμοποιώντας ερωτήματα.	ΝΑΙ		
48.	Ανάλυση συσχετισμένων συμβάντων σε ένα γραφικό χρονοδιάγραμμα	ΝΑΙ		
49.	Κεντρική διαχείριση για διαμόρφωση συστήματος όπως ενημερώσεις (patches) O/S για όλες τις συσκευές,	ΝΑΙ		
50.	Το κεντρικό σύστημα διαχείρισης θα ενσωματώνει τις απόψεις (views) από όλους τους ιστότοπους που παρακολουθούνται και τα αντίστοιχα δεδομένα / πληροφορίες	ΝΑΙ		
51.	Κεντρικό σύστημα διαχείρισης για διαμόρφωση και λειτουργία λήψης δεδομένων	ΝΑΙ		
	Λοιπές Απαιτήσεις			
52.	Η λύση να προσφέρεται για εικονικά περιβάλλοντα όπως το ESXi και HyperV	ΝΑΙ		
53.	Παρακολούθηση σε ιδιωτικά/ δημόσια/ υβριδικά περιβάλλοντα cloud όπως το Azure κλπ.	ΝΑΙ		
54.	Παρακολούθηση της κυκλοφορίας μέσω SPAN / TAP / Mirror	ΝΑΙ		
55.	Ενσωμάτωση με λύση SIEM για χειρισμό και συσχέτιση ειδοποιήσεων.	ΝΑΙ		
56.	Τα μεταδεδομένα να μπορούν να προωθηθούν σε μια λύση SIEM.	ΝΑΙ		
57.	Ενσωμάτωση με τυπικά συστήματα υποστήριξης για τη διαχείριση συμβάντων.	ΝΑΙ		
58.	Ενσωμάτων με πλατφόρμες SOAR	ΝΑΙ		
59.	Υποστήριξη ειδοποιήσεων μέσω email σε συγκεκριμένη ομάδα χρηστών	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
60.	Ειδικές (ad hoc) και προγραμματισμένες αναφορές που παρουσιάζουν στατιστικές πληροφορίες για θέματα ασφάλειας και δικτύου για μια συγκεκριμένη χρονική περίοδο	ΝΑΙ		
61.	Εφαρμογή για κινητά για ειδοποίηση και διαχείριση συμβάντων.	ΝΑΙ		
62.	Ο ανάδοχος θα πρέπει να παρέχει διαρκώς επικαιροποιημένο υλικό εκπαίδευσης επί της λύσης του στο οποίο θα συμπεριλαμβάνεται και η χειροκίνητη ανίχνευση τεχνικών και τακτικών περιστατικών κυβερνοασφάλειας.	ΝΑΙ		

7.2.3.7 Λύση προστασίας ηλεκτρονικού ταχυδρομείου Mail Security - 3.000 σταθμούς εργασίας

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
1.	Η λύση θα πρέπει να παρέχει μηχανισμό αποτροπής emails που περιέχουν κακόβουλα συνημμένα αρχεία είτε γνωστά είτε μηδενικού χρόνου (0-day).	ΝΑΙ		
2.	Η λύση θα πρέπει να ελέγχει emails τα οποία περιλαμβάνουν συνημμένα αρχεία και να τα παραδίδει σε πραγματικό χρόνο στο χρήστη σε καθαρή μορφή, από όπου έχει αφαιρεθεί οποιοδήποτε κακόβουλο περιεχόμενο (file scrubbing).	ΝΑΙ		
3.	Η λύση θα πρέπει να παρέχει μηχανισμό αποτροπής emails που έχουν σκοπό την παραπλάνηση του χρήστη μέσω ηλεκτρονικού "ψαρέματος" (anti-phishing).	ΝΑΙ		
4.	Η λύση θα πρέπει να παρέχει μηχανισμό ελέγχου και αποτροπής κακόβουλων emails που περιλαμβάνουν συνδέσμους (URLs) σε πραγματικό χρόνο.	ΝΑΙ		
5.	Η λύση θα πρέπει να τροποποιεί τους συνδέσμους (URLs) για την προστασία των χρηστών και να ελέγχει κατά πόσο είναι ασφαλείς κάθε φορά που κάποιος χρήστης τους ακολουθεί.	ΝΑΙ		
6.	Η λύση θα πρέπει να απαγορεύει στους χρήστες να ακολουθήσουν κάποιον κακόβουλο σύνδεσμο (URL) με δυνατότητα	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	παράκαμψης της λειτουργίας αν το ορίζει η πολιτική του οργανισμού.			
7.	Η λύση θα πρέπει να βάζει τα κακόβουλα emails σε καραντίνα με σκοπό να μην παραδίδονται στους χρήστες.	NAI		
8.	Σε περίπτωση που ένα email μπαίνει σε καραντίνα, θα πρέπει να υπάρχει δυνατότητα ενημέρωσης του χρήστη.	NAI		
9.	Η λύση θα πρέπει να ελέγχει τα εισερχόμενα emails καθώς και τα emails που αποστέλλονται εσωτερικά, μεταξύ των χρηστών του οργανισμού για την αποφυγή μετάδοσης κάποιας πιθανής μόλυνσης μεταξύ των χρηστών.	NAI		
10.	Η λύση θα πρέπει να ανιχνεύει και να αποτρέπει περιπτώσεις μίμησης τρίτων οργανισμών (brand impersonation) ή χρηστών του οργανισμού τον οποίο προστατεύει (user/nickname impersonation).	NAI		
11.	Η λύση θα πρέπει να παρέχει μηχανισμό ελέγχου και αποτροπής απώλειας ευαίσθητων δεδομένων (DLP).	NAI		
12.	Η λύση θα πρέπει να παρέχει δυνατότητα επιβολής διαφορετικής πολιτικής ασφαλείας σε διαφορετικά τμήματα ενός οργανισμού.	NAI		
13.	Η λύση θα πρέπει να παρέχει λεπτομερείς αναφορές και στατιστικά από όλες τις λειτουργίες για κάθε περιστατικό.	NAI		
14.	Η λύση θα πρέπει να παρέχει τη δυνατότητα εξαγωγής των logs για διαχείριση και συσχέτισμό από κεντρικό σύστημα διαχείρισης ασφάλειας.	NAI		
15.	Η λύση θα πρέπει να παρέχει γενικές αναφορές οι οποίες θα μπορούν να είναι συγκεντρωτικές και διαδραστικές, ώστε να παρέχουν χρήσιμες πληροφορίες στο διαχειριστή για όλες τις λειτουργίες ασφαλείας, χωρίς να χρειάζεται περεταίρω συσχέτισμός των γεγονότων και αναζήτηση σε raw logs.	NAI		
16.	Η λύση θα πρέπει να παράγει αυτόματα εβδομαδιαίες αναφορές οι οποίες θα αναπαριστούν τα κυριότερα περιστατικά ασφαλείας με γραφικό τρόπο και θα υπάρχει	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	η δυνατότητα να αποστέλλονται αυτόματα ως email στον/στους διαχειριστή/ες.			
17.	Η λύση θα πρέπει να παρέχει δυνατότητα αυτόματης ενεργοποίησης χωρίς την απαίτηση δημιουργίας κανόνων χειροκίνητα από το διαχειριστή στο domain.	ΝΑΙ		
18.	Η διαχείριση όλων των πολιτικών ασφαλείας θα πρέπει να γίνεται από το ίδιο διαχειριστικό περιβάλλον.	ΝΑΙ		

7.2.3.8 Λύση Endpoint Detection and Response - 3.000 σταθμούεργασίας

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
1.	Η ζητούμενη πλατφόρμα πρέπει να αποτελεί μια ολοκληρωμένη λύση η οποία να εξασφαλίζει την κεντρική παρακολούθηση και διαχείριση.	ΝΑΙ.		
2.	Το σύστημα να βασίζεται σε λογισμικό που να παρέχεται σαν SaaS	ΝΑΙ		
3.	Αριθμός υποστηριζόμενων τελικών σημείων	>=3.000		
4.	Η προσφερόμενη λύση θα μπορεί να λειτουργήσει σε απομονωμένο air-gapped περιβάλλον προσφέροντας το ίδιο επίπεδο ανίχνευσης και προστασίας	ΝΑΙ		
5.	Η προσφερόμενη λύση θα επιτρέπει την απεγκατάσταση του agent στο endpoint απομακρυσμένα.	ΝΑΙ		
6.	Ο agent θα υποστηρίζεται κατ' ελάχιστο στα παρακάτω λειτουργικά: Windows 7 (SP1), 8, 8.1, 10, 10-POS Windows server 2008R2 (SP2), 2012, 2016, 2019 Linux Ubuntu 16, 18-Centos, 7-Debian 8, 10-RedHat 7, Mint 18+ MacOS Sierra+ onwards Android 4.2+ onwards	Να αναφερθεί		
7.	Η προσφερόμενη λύση θα έχει τη δυνατότητα ανίχνευσης κακόβουλου λογισμικού	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	(malware) βάσει ανάλυσης συμπεριφοράς χωρίς τη χρήση υπογραφών.			
8.	Η προσφερόμενη λύση θα προσφέρει λειτουργία antivirus ή θα μπορεί να συνυπάρξει με υπάρχουσα λύση antivirus.	ΝΑΙ		
9.	Για την ανίχνευση απειλών θα υλοποιούνται στο endpoint πάνω από εβδομήντα (70) behavioral models.	ΝΑΙ		
10.	Η προσφερόμενη λύση θα έχει δυνατότητα ομαδοποίησης για να διαχωρίζει διαφορετικά τελικά σημεία και να εφαρμόζει πολιτικές βάσει ομάδων.	ΝΑΙ		
11.	Ο agent θα πρέπει να υποστηρίζει (για τα λειτουργικά συστήματα που επιτρέπεται) τη δυνατότητα παρακολούθησης του λειτουργικού σε επίπεδο hypervisor ώστε να μην είναι δυνατή ο εντοπισμός και η απενεργοποίηση του agent σε περίπτωση επίθεσης.	ΝΑΙ		
12.	Η προσφερόμενη λύση να έχει κατ'ελάχιστο δυνατότητα ανίχνευσης των κακόβουλων συμπεριφορών: Keylogging, Dynamic Impersonation, Credential Harvesting, Kernel Exploits, Screen captures.	Να αναφερθεί		
13.	Η λύση δεν θα κάνει full logging, παρά μόνο αν παρουσιαστεί μία απειλή.	ΝΑΙ		
14.	Οι ανακτηθείσες εγκληματολογικές πληροφορίες (forensic information) από το τελικό σημείο θα προστατεύονται με κωδικό πρόσβασης και ο κωδικός πρόσβασης καθορίζεται από τον αναλυτή.	ΝΑΙ		
15.	Θα μπορεί να εμφανίζει behavioral tree που αποτελείται από την αλυσίδα επίθεσης, επιλογές εξ αποστάσεως τερματισμού διαδικασίας, δημιουργία μαύρης λίστας και hunting για την ίδια διαδικασία εντός της υποδομής.	ΝΑΙ		
16.	Θα παρέχει αντιστοίχιση MITRE στα συμβάντα που καταγράφονται.	ΝΑΙ.		
17.	Θα προσφέρει τη δυνατότητα απομόνωσης του τελικού σημείου από την κονσόλα διαχείρισης.	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
18.	Δυνατότητα scripting για τη δημιουργία νέων κανόνων και πολιτικών.	ΝΑΙ		
19.	Η προσφερόμενη λύση να υποστηρίζει αυτοματοποιημένη τεχνητή νοημοσύνη για τον εντοπισμό απειλών.	ΝΑΙ.		

7.2.3.9 Λύση Διαβάθμισης και Σήμανσης Εγγράφων

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
1.	Οι endpointagents του Συστήματος Διαβάθμισης Δεδομένων, πρέπει να είναι συμβατοί με Λειτουργικά Συστήματα: Windows 10, WindowsServer 2008 R2, 2012, 2016, 2019 , , MacOS / X, AndroidEnterprise, IOS.	ΝΑΙ		
2.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να καλύπτει χίλια (1.000) τερματικά του οργανισμού	ΝΑΙ		
3.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να έχει δυνατότητα να θέτει σήμανση σε έγγραφα της ακόλουθης μορφής: 1. ΣουίταMS Office (π.χ. Word, Excel, Power Point, Visio, Microsoft Project, OneNote). 2. Outlook email (π.χ. msg, pst, ost) 3.Αρχεία PDF 4. Αρχείακειμένου (π.χ. TXT, ASC, ANS, ACL, HTML, XML, ODM, OTT, INFO, PAP, PAGES) 5. Συμπεσμένααρχεία (π.χ. ZIP, 7zip, RAR, WinRAR, BZip, Gzip, Tar, Bz2) 6. Αρχείαβίντεο (π.χ. mpg, mp4, amv, wmv, mov, avi, mkv) 7. Αρχείαήχου (π.χ. mp3, wma, wav, DVR-MS, WTV) 8. Αρχείαεικόνας (π.χ. JPEG, TIFF, GIF, BMP, PNG, AI, CDR, ADT, PSD, PUB) 9. Αρχείαβάσηςδεδομένων (π.χ. ACCDB, ADT, DB, MDB, MYD, MYI, ORA, SQL, SDF, sqlite, 10. Κρυπτογραφημένααρχεία (π.χ. ssh, pub, rpk, cert, crt, der, p7b, PEM, PFX, AXX, EEA, TC, BPW, KDB, KDBX) 11. Άλλοιτύποιαρχείων (π.χ. CMD, BAT, JSP, PL, PHP, ASP, PYO, VBS)	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
4.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να διαβαθμίζει τα έγγραφα με τρόπο, ώστε η πληροφορία για το επίπεδο διαβάθμισης (π.χ. πληροφορίες μεταδεδομένων) να μην μπορεί να διαγραφεί ή τροποποιηθεί από τον απλό χρήστη.	ΝΑΙ		
5.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να επιβάλλει πολιτικές σχετικά με το αρχικό επίπεδο διαβάθμισης που θα έχει κάθε νέο έγγραφο (π.χ. οποιοδήποτε νέο έγγραφο δημιουργείται πρέπει να διαβαθμίζεται αυτόματα ως Εσωτερικό).	ΝΑΙ		
6.	Η πληροφορία για το επίπεδο διαβάθμισης πρέπει να ακολουθεί ένα διαβαθμισμένο έγγραφο κατά τη διάρκεια κάθε είδους μεταφοράς (π.χ. μέσω email, μέσω διαδικτύου, εφαρμογών cloud, μέσω FTP / SFTP, αντιγραφή σε οποιονδήποτε τύπο αφαιρούμενου μέσου, εάν κρυπτογραφεί και αποκρυπτογραφεί, σε περίπτωση συμπίεσης)	ΝΑΙ		
7.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να είναι σε θέση να επιβάλλει τουλάχιστον 4 διαφορετικά επίπεδα ταξινόμησης (π.χ. Δημόσιο, Εσωτερικό, Εμπιστευτικό και αυστηρά Εμπιστευτικό) και να έχει δυνατότητα να υποστηρίζει έως και πρακτικά απεριόριστα επίπεδα διαβάθμισης	ΝΑΙ		
8.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει επίσης να μπορεί να διαφοροποιεί και να επιβάλλει διαφορετικές πολιτικές σε διαφορετικά επίπεδα διαβάθμισης εγγράφων (υποκατάταξη) με βάση τα τμήματα του οργανισμού, όπως αποτυπώνονται στο κέντρικό κατάλογο χρηστών του οργανισμού (ActiveDirectory). Για παράδειγμα, θα μπορούσε να έχει ένα διαβαθμισμένο έγγραφο ως Εμπιστευτικό / Τμήμα Οικονομικών και άλλο έγγραφο, ως Εμπιστευτικό / Τμήμα εξυπηρέτησης κοινού, κ.λπ.	ΝΑΙ		
9.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να μπορεί να καθορίζει την πολιτική	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	χρονικής διατήρησης ανάλογα με το επίπεδο διαβάθμισης και τον τύπο του εγγράφου			
10.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να έχει δυνατότητες σάρωσης των εγγράφων και εντοπισμού χαρακτηριστικών σημείων του περιεχομένου π.χ. λέξεις-κλειδιά, regular expressions, περιεχόμενα λεξικών κ.λπ.	ΝΑΙ		
11.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να μπορεί να υποστηρίξει και να επιβάλλει διαφορετικές τεχνικές διαβάθμισης, όπως οι ακόλουθες: 3. Χειροκίνητη Διαβάθμιση (π.χ. με ένα κλικ ενός κουμπιού, επιλέγοντας μεταξύ των 4 διαφορετικών επιπέδων και υπο-επιπέδων. 4. Ημιαυτόματη ταξινόμηση (π.χ. με βάση το περιεχόμενο του εγγράφου για να δώσει κάποιες ενδείξεις στον χρήστη για το τι επίπεδο διαβάθμισης πρέπει να θέσει) Μαζική ταξινόμηση (Το εργαλείο πρέπει να ταξινομήσει όλα τα αρχεία σε έναν συγκεκριμένο folder με βάση το απαιτούμενο επίπεδο διαβάθμισης ή με βάση τη σάρωση περιεχομένου, π.χ. σε περίπτωση που ανακαλύπτει προσωπικά δεδομένα σε αυτό κ.λπ.)	ΝΑΙ		
12.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να έχει δυνατότητα ρύθμισης για το αν επιτρέπεται ή όχι η αλλαγή του επιπέδου διαβάθμισης από τους χρήστες (π.χ. αναβάθμιση ή υποβάθμιση).	ΝΑΙ		
13.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να δίνει την δυνατότητα αυτόματης διαβάθμισης εγγράφων κατά την αποθήκευση των εγγράφων .	ΝΑΙ		
14.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να εκτελεί μαζική σάρωση εγγράφων που είναι αποθηκευμένα είτε σε τοπικούς servers είτε σε εφαρμογές αποθήκευσης εγγράφων στο νέφος και αυτόματης διαβάθμισης με βάση το περιεχόμενο τους.	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Η διαχείριση των σχετικών ενεργειών πρέπει να εκτελείται από την κεντρική κονσόλα του συστήματος.			
15.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να μπορεί να σαρώνει μεγάλο όγκο εγγράφων ώστε να διαβαθμιστούν έγγραφα που έχουν παραχθεί στο παρελθόν και διατηρούνται στα πληροφοριακά συστήματα του ΔΕΔΔΗΕ.	ΝΑΙ		
16.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να εκτελεί αυτόματο καθορισμό των επιπέδων διαβάθμισης με βάση τον εντοπισμό χαρακτηριστικών λέξεων και φράσεων στο περιεχόμενο των εγγράφων.	ΝΑΙ		
17.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να εκτελεί αυτόματο καθορισμό των επιπέδων διαβάθμισης με βάση τον εντοπισμό σειρών χαρακτήρων που ακολουθούν συγκεκριμένους κανόνες (regular expressions). Η διαχείριση των σχετικών ενεργειών πρέπει να εκτελείται από την κεντρική κονσόλα του συστήματος.	ΝΑΙ		
18.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να μπορεί να επιβάλει την αλλαγή του επιπέδου διαβάθμισης με βάση την ημερομηνία δημιουργίας ή τροποποίησης του εγγράφου (πχ αλλαγή επιπέδου διαβάθμισης από «εμπιστευτικό» σε «δημόσιο» μετά από καθορισμένο χρόνο από την ημερομηνία δημιουργίας ενός εγγράφου).	ΝΑΙ		
19.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να παρέχει στατιστικά για την εξέλιξη της αυτόματης διαβάθμισης των υφιστάμενων εγγράφων από την κεντρική κονσόλα της λύσης.	ΝΑΙ		
20.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να συντάσσει καταλόγο (inventory) με τα έγγραφα που έχουν εντοπιστεί με βάση κάποια πολιτική η οποία λαμβάνει υπ όψιν το περιεχόμενο τους ή/και τα επίπεδα διαβάθμισης τους. Η διαχείριση των	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	σχετικών ενεργειών πρέπει να εκτελείται από την κεντρική κονσόλα του συστήματος.			
21.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να είναι σε θέση να σαρώσει, να αναγνωρίσει και να διαβαθμίσει δεδομένα που είναι αποθηκευμένα σε συστήματα διαμοιρασμού εγγράφων: <ul style="list-style-type: none"> • Sharepoint • OneDrive • Dropbox • Box • Windows Filesharing 			
22.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να μπορεί να τοποθετεί οπτική σήμανση χαρακτηριστικής του επιπέδου διαβάθμισης εντός των εγγράφων της οικογένειας MsOffice (word, exec, powerpoint)	ΝΑΙ		
23.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να μπορεί να θέτει αυτόματα σήμανση εντός των εγγράφων με βάση το επίπεδο ταξινόμησής τους (π.χ. υδατογράφημα, υποσέλιδο, κεφαλίδα κ.λπ.)	ΝΑΙ		
24.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να μπορεί να προσαρμόζει τη σήμανση στις απαιτήσεις του ΔΕΔΔΗΕ (πχ χρώματα, λεκτικά, θέση, κλπ)	ΝΑΙ		
25.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να μπορεί να τοποθετεί σήμανση χαρακτηριστική του επιπέδου διαβάθμισης εντός μηνυμάτων ηλεκτρονικής αλληλογραφίας της εφαρμογής MsOutlook.	ΝΑΙ		
26.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να μπορεί να θέτει αυτόματα σήμανση στα εικονίδια εγγράφων (π.χ. τα εικονίδια επιφάνειας εργασίας κάθε εγγράφου) με βάση το επίπεδο διαβάθμισης τους (π.χ. κόκκινη ετικέτα για αυστηρά εμπιστευτικό, πορτοκαλί ετικέτα για εμπιστευτικό, κίτρινη ετικέτα Εσωτερικό και πράσινη ετικέτα για Δημόσιας χρήσης).	ΝΑΙ		
27.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να μπορεί να επισημάνει τα έγγραφα με μεταδεδομένα (metadata) στα οποία	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	περιλαμβάνονται όλες οι πληροφορίες για τα επίπεδα και υποεπίπεδα διαβάθμισης των εγγράφων			
28.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να μπορεί να προσθέσει στα μεταδεδομένα κάθε εγγράφου και πληροφορία για την πολιτική διατήρησης ανάλογα με το επίπεδο διαβάθμισης και τον τύπο του εγγράφου.	ΝΑΙ		
29.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να προστατεύει τα μεταδεδομένα από διαγραφή ή τροποποίηση από τον απλό χρήστη.	ΝΑΙ		
30.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να μπορεί να διατηρεί τα μεταδεδομένα επί του εγγράφου κατά τη διάρκεια κάθε είδους μεταφοράς (π.χ. μέσω email, μέσω διαδικτύου, εφαρμογών cloud, ftp/sftp, αντιγραφής, κρυπτογράφηση/αποκρυπτογράφησης, συμπίεσης, κλπ).	ΝΑΙ		
31.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να είναι απολύτως συμβατό με το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) (π.χ. τα μεταδεδομένα τα σχετικά με το επίπεδο διαβάθμισης πρέπει να αναγνωρίζονται από το εργαλείο DLP το οποίο θα εφαρμόζει κατάλληλες πολιτικές ελέγχου).	ΝΑΙ		
32.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να είναι πλήρως συμβατό με την λύση IRM του ΔΕΔΔΗΕ. Τα μεταδεδομένα σχετικά με το επίπεδο διαβάθμισης πρέπει να αναγνωρίζονται από την λύση IRM.	ΝΑΙ		
33.	Το Σύστημα Διαβάθμισης Δεδομένων θα πρέπει να συνεργάζεται με εργαλεία Εξωτερικής κρυπτογράφησης.	ΝΑΙ		
34.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να έχει χαρακτηριστικά ανοικτής αρχιτεκτονικής ώστε να εξασφαλίζεται η διαλειτουργικότητα του με τα υφιστάμενα πληροφοριακά συστήματα του ΔΕΔΔΗΕ.	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
35.	Μετά από μαζική σάρωση εγγράφων σε servers ή σε εφαρμογές αποθήκευσης εγγράφων (πχ sharepoint), το Σύστημα Διαβάθμισης Δεδομένων πρέπει να παράγει αναφορές και στατιστικά καθώς και τα αντίστοιχα γραφήματα τους .	ΝΑΙ		
36.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να μπορεί να εξάγει τις αναφορές υπό μορφή αρχείου.	ΝΑΙ		
37.	Η κονσόλα διαχείρισης του Συστήματος Διαβάθμισης Δεδομένων θα πρέπει να συλλέγει καταγραφές συμβάντων (logs) από τα τερματικά χρηστών, στις ακόλουθες περιπτώσεις: 1. Εάν ένας χρήστης αλλάξει το επίπεδο ταξινόμησης ενός εγγράφου (π.χ. μείωση του επιπέδου ταξινόμησης) 2. Εάν έχει σταλεί προειδοποίηση για κάποια ενέργεια (alert) ή έχει ζητηθεί αιτιολόγηση από τον χρήστη για κάποια ενέργεια.	ΝΑΙ		
38.	Το Σύστημα Διαβάθμισης Δεδομένων θα έχει την Δυνατότητα μεταφοράς των καταγραφών των ενεργειών χρηστών σε syslogserver.	ΝΑΙ		
39.	Το Σύστημα Διαβάθμισης Δεδομένων θα πρέπει να υποστηρίζει πλήρως την ελληνική γλώσσα, (π.χ. πληροφορίες αναδυόμενων παραθύρων, ενσωματωμένα κουμπιά σε εφαρμογές του Office κ.λπ.).	ΝΑΙ		
40.	Η αρχιτεκτονική του Συστήματος Διαβάθμισης Δεδομένων , θα πρέπει να περιλαμβάνει μια κεντρική κονσόλα διαχείρισης από την οποία δημιουργούνται και προωθούνται οι κατάλληλες πολιτικές στα τερματικά των χρηστών.	ΝΑΙ		
41.	Ο agent του Συστήματος Διαβάθμισης Δεδομένων δεν πρέπει να καταναλώνει περισσότερο από 5% των πόρων σταθμού εργασίας / διακομιστή, βάσει δεδομένων και έγκυρων μετρήσεων.	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
42.	Θα πρέπει να υπάρχει δυνατότητα ελέγχου και εντοπισμού κακόβουλης απενεργοποίησης του agent .	ΝΑΙ		
43.	Μετά από μαζική σάρωση εγγράφων σε servers ή σε εφαρμογές αποθήκευσης εγγράφων (πχ sharepoint), το Σύστημα Διαβάθμισης Δεδομένων πρέπει να μπορεί να αρχειοθετεί αυτόματα τα διαβαθμισμένα έγγραφα που φτάνουν στην ημερομηνία λήξης σύμφωνα με την πολιτική διατήρησης.	ΝΑΙ		
44.	Η σειρά εφαρμογής ή προτεραιότητα των πολιτικών διαβάθμισης, θα πρέπει να είναι σαφής και να καθορίζεται είτε από την σειρά της δήλωσής τους.	ΝΑΙ		
45.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να υποστηρίζει λειτουργίες διαχείρισης πολιτικής όπως, μεταξύ άλλων, προσθήκη πολιτικής, κατάργηση πολιτικής, ενεργοποίηση πολιτικής, απενεργοποίηση πολιτικής, προσθήκη, κατάργηση και αλλαγή κανόνων πολιτικής, αλλαγή παραμέτρων πολιτικής, σύνδεση πολιτικής με συγκεκριμένους agents, πολιτική δοκιμών κ.λπ.	ΝΑΙ		
46.	Ο ανάδοχος πρέπει να παρέχει διαγράμματα αρχιτεκτονικής για το πώς θα υλοποιηθεί το Σύστημα και τους υπολογιστικούς πόρους που απαιτούνται για τη φιλοξενία του Συστήματος και για την Πρόληψη απώλειας δεδομένων.	ΝΑΙ		
47.	Ο ανάδοχος θα είναι υπεύθυνος για την εγκατάσταση της πλήρους υποδομής που απαιτείται για την υλοποίηση του Συστήματος (π.χ. εγκατάσταση λογισμικού και λειτουργικού συστήματος, DB, εφαρμογής κ.λπ.).	ΝΑΙ		
48.	Ο ανάδοχος θα είναι υπεύθυνος να εγκαταστήσει τους απαιτούμενους agents στους τερματικούς σταθμούς εργασίας των χρηστών.	ΝΑΙ		
49.	Ο ανάδοχος θα είναι υπεύθυνος για τη δημιουργία όλων των συμφωνημένων	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	πολιτικών διαβάθμισης με βάση τις ανάγκες του αναθέτοντος οργανισμού και τις αντίστοιχες πολιτικές της εταιρείας αλλά και τα αποτελέσματα της μελέτης αξιολόγησης.			
50.	Ο ανάδοχος πρέπει να παρέχει την κατάλληλη εκπαίδευση σε υπεύθυνους πληροφορικής του αναθέτοντος οργανισμού σχετικά με την λειτουργία του Συστήματος, αλλά και στο σύνολο των χρηστών της εταιρείας ώστε όλοι οι χρήστες να γνωρίζουν πως μπορούν να χρησιμοποιήσουν το σύστημα, σύμφωνα με τις απαιτήσεις της παραγράφου Error! Reference source not found..	ΝΑΙ		

7.2.3.10 Λύση Προστασίας Δεδομένων από Διαρροή

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
1.	Οι agents του συστήματος αποτροπής διαρροής δεδομένων που εγκαθίστανται στα τερματικά (endpoints), πρέπει να είναι συμβατοί με Λειτουργικά Συστήματα: Windows 10, WindowsServer 2008 R2, 2012, 2016, 2019 , , MacOS / X,	ΝΑΙ		
2.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) πρέπει να έχει τέλεια συμβατότητα με το εργαλείο διαβάθμισης και σήμανσης εγγράφων και με την λύση IRM .	ΝΑΙ		
3.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να καλύπτει χίλια (1.000) τερματικά του οργανισμού	ΝΑΙ		
4.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να μπορεί να ανιχνεύει την ενέργεια και να λαμβάνει μέτρα (πχ αποτροπή / αιτιολόγηση / ενημέρωση) εάν ένας χρήστης αντιγράψει και επικολλήσει δεδομένα σε έναν μη έμπιστο προορισμό.	ΝΑΙ		
5.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) πρέπει να μπορεί να επιθεωρεί την κυκλοφορία SSL	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	(SSLinspection) εάν απαιτείται αλλά και να υποστηρίζει εξαιρέσεις (targetswhitelisting).			
6.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να μπορεί να παρέχει σε πραγματικό χρόνο καταγραφών της διακίνησης των δεδομένων στα πληροφοριακά συστήματα.	NAI		
7.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να μπορεί να καταγράφει τις κινήσεις που δεν είναι συμβατές με την αποδεκτή πολιτική διακίνησης δεδομένων,	NAI		
8.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να παρακολουθεί μέσω κεντρικής κονσόλα διαχείρισης την συνολική εικόνα διακίνησης των δεδομένων δηλ. ποια είδη δεδομένων χρησιμοποιούνται, ή διαβιβάζονται και από ποιους	NAI		
9.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να ανιχνεύει τις κινήσεις που αφορούν ενέργειες επί των δεδομένων στα τελικά σημεία όπως για παράδειγμα copy/paste σε εξωτερική μονάδα δίσκου ή USBstick, εκτυπώσεις αρχείων, λειτουργία printscreen.	NAI		
10.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να ανιχνεύει την διακίνηση δεδομένων από μέσα προς τα έξω, μέσω των κεντρικών δικτυακών υποδομών και μέσω των διαφόρων πρωτοκόλλων επικοινωνίας ftp, http, https, smtp, αλλά και στιγμιαίο μήνυμα (IM).	NAI		
11.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να δημιουργεί incidents τα οποία πρέπει να διαβαθμίζονται αυτόματα σε διάφορα επίπεδα διαβάθμισης (πχ low, high, serious), με βάση τις πολιτικές και την κατηγοριοποίηση των δεδομένων.	NAI		
12.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει αποστέλλει ενημερώσεις ασφαλείας με διάφορα μέσα	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	επικοινωνίας παραβίασης (πχ. Email, sms, κλπ)			
13.	<p>Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να είναι σε θέση να σαρώσει, να εντοπίσει και να αποτρέψει τη διαρροή (με βάση τις πολιτικές) που είναι αποθηκευμένα στις ακόλουθες μορφές:</p> <ol style="list-style-type: none"> 1. Αρχεία Excel 2. Αρχεία με οριοθετημένες στήλες (συγκεκριμένη γραμμογράφηση) 3. Δεδομένα που αποθηκεύονται σε γνωστές βάσεις δεδομένων όπως Oracle, MS-SQL, PostgreSQL, MongoDB, DB2 και χρησιμοποιεί η εταιρεία. 4. Δεδομένα που αποθηκεύονται σε συστήματα διαμοιρασμού εγγράφων: <ul style="list-style-type: none"> • Filenet • Sharepoint • OneDrive • OwnCloud • Windows Filesharing 	ΝΑΙ		
14.	<p>Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) πρέπει να περιέχει δυνατότητες αναγνώρισης δεδομένων σε όλα τα πληροφοριακά συστήματα του οργανισμού, βάσει πολιτικών περιεχομένου (π.χ. λέξεις-κλειδιά, regular expressions, περιεχόμενα λεξικών κ.λπ.). Ο εγκαταστάτης θα πρέπει να παρέχει υπηρεσίες ανάπτυξης Regular expressions οι οποίες να καλύπτουν την αναγνώριση των ακόλουθων δεδομένων:</p> <ol style="list-style-type: none"> 1. Αριθμοί Φορολογικού Μητρώου (ΑΦΜ) 2. Τηλεφωνικά νούμερα (Ελληνικά κινητά ή σταθερά τηλέφωνα) 3. Αριθμοί Ελληνικών Ταυτοτήτων. 4. Ελληνικά ονόματα (π.χ. πιθανώς με τεχνική λεξικού) 5. Διευθύνσεις (π.χ. πιθανώς με τεχνική λεξικού) 6. Αριθμοί πιστωτικών ή χρεωστικών καρτών 7. Αριθμοί λογαριασμών IBAN 8. Αριθμός Παροχής 	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	9. Αριθμός Μητρώου Μισθωτού			
15.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα ανακαλύπτει τα δεδομένα που αποθηκεύονται σε διάφορους τύπους πληροφοριακών συστημάτων ενός δικτύου (discovery), όπως σε Fileservers ή κεντρικά storage καθώς και πάνω σε σταθμούς εργασίας (endpoints).	ΝΑΙ		
16.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα παρέχει πληροφορίες για το περιεχόμενο των δεδομένων και για την διακίνηση τους, που θα δώσουν στους διαχειριστές ασφάλειας του ΔΕΔΔΗΕ πλήρη εποπτεία για το ποιος μπορεί να διακινήσει, ποιες πληροφορίες, από ποιο σημείο, και με ποιον τρόπο.	ΝΑΙ		
17.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα καθορίζει πολιτικές αναζήτησης με βάση τα χαρακτηριστικά ή το περιεχόμενο των αρχείων.	ΝΑΙ		
18.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα καθορίζει με βάση τις απαιτήσεις του οργανισμού ποιες αναζητήσεις μπορούν να γίνουν σε εργάσιμες ώρες, και ποιες λόγω όγκου και επιβάρυνσης του δικτύου, πρέπει να γίνονται σε προγραμματισμένες μη εργάσιμες ώρες.	ΝΑΙ		
19.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα καθορίζει τις περιοχές καθώς και των Τελικών Σημείων που θα εκτελείται η αναζήτηση δεδομένων.	ΝΑΙ		
20.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) πρέπει να αποτρέπει τη διαρροή εταιρικών πληροφοριών, που είναι: 1. Αποθηκευμένες σε Πληροφοριακά Συστήματα (in rest) 2. Σε διαμετακόμιση (in transit) 3. Σε χρήση (in use)	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
21.	<p>Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) πρέπει να καλύπτει τις ακόλουθες ανάγκες του οργανισμού:</p> <ol style="list-style-type: none"> 1. Πρόληψη απώλειας δεδομένων προς τον ιστό (forward Proxy) 2. Πρόληψη απώλειας δεδομένων στο email 3. Πρόληψη απώλειας δεδομένων στο OWA - Outlook Web Access (web mail reverse proxy) 4. Πρόληψη απώλειας δεδομένων στο δίκτυο / VPN 5. Πρόληψη απώλειας δεδομένων από τα τερματικά (π.χ. αποτροπή εξαγωγής δεδομένων σε αφαιρούμενες συσκευές) 	ΝΑΙ		
22.	<p>Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) πρέπει να έχει δυνατότητα να εφαρμόσει τους ακόλουθους κανόνες / τύπους ενεργειών επί των δεδομένων :</p> <ol style="list-style-type: none"> 1. Επιτρεπτή ενέργεια (allow) 2. Αποτροπή (block) 3. προειδοποίηση και αιτιολόγηση (π.χ. αίτημα προς τον τελικό χρήστη να περιγράψει τον λόγο για τον οποίο θέλει να κάνει την ενέργεια) 4. Καραντίνα 5. Κρυπτογράφηση <p>Ο Οργανισμός θα μπορεί να επιλέξει για ποιες από τις παραπάνω ενέργειες θα πρέπει να δημιουργούνται άμεσα alerts σε καθορισμένους ρόλους</p>	ΝΑΙ		
23.	<p>Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να μπορεί να ανιχνεύει και να αποτρέπει τη διαρροή δεδομένων (βάσει πολιτικών), μέσω οποιουδήποτε πιθανού καναλιού επικοινωνίας δεδομένων, και οπωσδήποτε από τα ακόλουθα:</p> <ol style="list-style-type: none"> 1. HTTP / HTTPS 2. FTP / FTPS 3. SMB (Κοινή χρήση αρχείων) 4. SSH / Telnet 5. VPN / OpenVPN (TLS / SSL / IPSEC / PPTP / PPTPS) 6. RDP 	ΝΑΙ		



A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	7. POP / POP3 / IMAP / IMAP4 / SMTP 8. IRC / SNMP 9. RPC / NFS 10. Rsync			
24.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να μπορεί να εντοπίζει και να αποτρέπει διαρροές δεδομένων ηλεκτρονικού ταχυδρομείου μέσω: 1. Microsoft Outlook 2. Outlook Web Anywhere (OWA) 3. Outlook Active Sync	ΝΑΙ		
25.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP), θα πρέπει να μπορεί να εντοπίζει και να αποτρέπει διαρροές δεδομένων από τους τερματικούς σταθμούς που επιχειρούνται μέσω των ακόλουθων καναλιών: 1. Wi-Fi 2. USB 3. Κάρτες Micro / Mini / Midi SD 4. CD / DCD 5. NFS / SMB	ΝΑΙ		
26.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να μπορεί να ανιχνεύει και να αποτρέπει διαρροές δεδομένων μέσω οποιουδήποτε τύπου εφαρμογών cloud, όπως: 1. Skype / Skype for business 2. DropBox 3. Evernote 4. OneDrive 5. iCloud 6. GoogleDrive 7. OneNote 8. Yammer 9. Jabber 10. Logmein 11. Citrix 12. TeamViewer	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	13. WebEx 14. Gmail 15. Facebook 16. Twitter 17. Instagram 18. Yammer 19. Wetransfer 20. Γιουσέντιπ 21. YouTransfer 22. Sendanywhere 23. FileDrop 24. BOX25. Filenet 26. Sharepoint 27. Teams 28. Etc.			
27.	<p>Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να μπορεί να αναγνωρίζει, να ταξινομεί και να αποτρέπει τη διαρροή (βάσει πολιτικών) εγγράφων της ακόλουθης μορφής:</p> <p>1. Σουίταγραφείου (π.χ. Word, Excel, Power Point, Visio, Microsoft Project, one-note κ.λπ.).</p> <p>2. Email Outlook (π.χ. msg, pst, ost, κλπ)</p> <p>3. Αρχεία PDF</p> <p>4. Αρχείακειμένου (π.χ. TXT, ASC, ANS, ACL, 0, HTML, XML, ODM, OTT, INFO, PAP, PAGES κ.λπ.)</p> <p>5. Συμπιεσμένα αρχεία (π.χ. ZIP, 7zip, RAR, WinRAR, BZip, Gzip, Tar, Bz2 κ.λπ.)</p> <p>6. Αρχείαβίντεο (π.χ. mpg, mp4, amv, wmv, mov, avi, mkv κ.λπ.)</p> <p>7. Αρχείαήχου (π.χ. mp3, wma, wav, DVR-MS, WTV κ.λπ.)</p> <p>8. Αρχείαεικόνας (π.χ. JPEG, TIFF, GIF, BMP, PNG, AI, CDR, ADT, PSD, PUB κ.λπ.)</p> <p>9. Αρχείαβάσηςδεδομένων (π.χ. ACCDB, ADT, DB, MDB, MYD, MYI, ORA, SQL, SDF, sqlite,</p>	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	10. Κρυπτογραφημένα αρχεία (π.χ. ssh, pub, rpkr, cert, crt, der, p7b, PEM, PFX, AXX, EEA, TC, BPW, KDB, KDBX κ.λπ.) 11. Άλλοι τύποι αρχείων (π.χ. CMD, BAT, JSP, PL, PHP, ASP, PYO, VBS κ.λπ.)			
28.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να μπορεί να ανιχνεύει την ενέργεια και να λαμβάνει μέτρα (πχ αποτροπή / αιτιολόγηση / ενημέρωση) εάν ένας χρήστης προσπαθήσει να εκτυπώσει ή να αντιγράψει την οθόνη (printscreen)	ΝΑΙ		
29.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να έχει ενσωματωμένη δυνατότητα να φιλτράρει την δικτυακή κίνηση, να ανιχνεύει την ενέργεια και να λαμβάνει μέτρα (πχ αποτροπή / αιτιολόγηση / ενημέρωση) εάν ένα έγγραφο με τύπο εικόνας περιέχει διαβαθμισμένες πληροφορίες (π.χ. δυνατότητες OCR)	ΝΑΙ		
30.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) προστατεύει τα δεδομένα, με συγκεκριμένες διαδικασίες και με προκαθορισμένες αυτοματοποιημένες πολιτικές βασισμένες πάνω στις πολιτικές ασφαλείας που ορίζει η εταιρεία αλλά και με εκτεταμένο εύρος ενσωματωμένων πολιτικών ανά γεωγραφική περιοχή και επιχειρηματική δραστηριότητα.	ΝΑΙ		
31.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα εκτελεί συγκεκριμένες κινήσεις όταν οι ενέργειες του χρήστη παραβαίνουν την πολιτική ασφαλείας του Οργανισμού.	ΝΑΙ		
32.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα καταγράφει την ενέργεια του χρήστη (Monitor)	ΝΑΙ		
33.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα προειδοποιεί τον χρήστη (Alert)	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
34.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα αποτρέπει αυτόματα μία ενέργεια του χρήστη (Block),	ΝΑΙ		
35.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα μπορεί να απαίτεί από τον χρήστη αιτιολόγησης μίας ενέργειας (Justify).	ΝΑΙ		
36.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα μπορεί να παραμετροποιεί τους κανόνες που καθορίζουν το είδος της ενέργειας που θα εκτελέσει το σύστημα DLP, ώστε να λαμβάνουν υπ όψιν την ταυτότητα του χρήστη που επιχειρεί την διακίνηση των δεδομένων, το είδος των δεδομένων, τον υπο διακίνηση δεδομένων, τον όγκο των υπο διακίνηση δεδομένων, την πηγή και τον αποδέκτη των δεδομένων, κλπ.	ΝΑΙ		
37.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να κατηγοριοποιεί δεδομένα των εφαρμογών συνολικά	ΝΑΙ		
38.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα μπορεί να δημιουργεί κανόνες ελέγχου για συγκεκριμένες κατηγορίες τελικών σημείων	ΝΑΙ		
39.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) δεν θα έχει περιορισμούς στον αριθμό των κανόνων ελέγχου και θα μπορεί να εφαρμόζει πολλαπλούς κανόνες	ΝΑΙ		
40.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα εφαρμόζει κανόνες με βάση το σύστημα/εφαρμογή που προέρχονται τα δεδομένα	ΝΑΙ		
41.	Η κονσόλα διαχείρισης του Συστήματος Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να συλλέγει δεδομένα από οποιονδήποτε αισθητήρα DLP (με βάση agents ή με βάση το δίκτυο) και θα πρέπει να παρέχει τις ακόλουθες αναφορές:	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	<p>1. Χρήστες οι οποίοι έχουν τον μεγαλύτερο αριθμό ενεργοποίησης κανόνων (triggered policies).</p> <p>2. Συμβάντα για τα οποία ενεργοποιήθηκε η πολιτική αποτροπής (Block)</p> <p>3. Συμβάντα για τα οποία ενεργοποιήθηκε αιτιολόγησης (Justify)</p> <p>6. Προσπάθειες (επιτυχείς ή ανεπιτυχείς) που έχουν γίνει για την απομάκρυνση εταιρικών δεδομένων όταν το τερματικό ήταν εκτός εταιρικού δικτύου ή όταν ήταν συνδεδεμένο στο εταιρικό δίκτυο.</p> <p>7. Περιστατικά για τα οποία ενεργοποιήθηκε Καραντίνα</p> <p>8. Αναφορές ανά κανόνα ή ανά πολιτική</p>			
42.	Οι αναφορές και τα στατιστικά στοιχεία θα πρέπει να είναι διαθέσιμα σε μορφή excel ή CSV και επιπλέον να περιλαμβάνουν γραφήματα.	ΝΑΙ		
43.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) πρέπει να παράγει αρχεία καταγραφής συμβάντων από τις ενέργειες των χρηστών (logs), τα οποία θα πρέπει να μεταφέρονται εύκολα σε πλατφόρμα SIEM (να περιγραφεί ο τρόπος διασύνδεσης). Επίσης, το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) πρέπει να έχει τη δυνατότητα αποστολής μόνο ανώνυμων δεδομένων (απόκρυψη του ονόματος χρήστη).	ΝΑΙ		
44.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα μπορεί να δημιουργεί αναφορές σε διάφορα επίπεδα συμπεριλαμβανομένου πλήρες ιστορικού ανά ένδειξη/περιστατικό	ΝΑΙ		
45.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα μπορεί να δημιουργεί αναφορές που καλύπτουν τις απαιτήσεις του Νομοθετικού/Κανονιστικού πλαισίου	ΝΑΙ		
46.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα μπορεί να δημιουργεί	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	αναφορές ανά χρήστη, τελικό σημείο, κατηγορία ένδειξης/περιστατικού, κλπ			
47.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα μπορεί να δημιουργεί αναφορές που δίνουν την αποτύπωση της συνολικής εικόνα των εγκαταστάσεων της εφαρμογής σε επίπεδο εταιρείας και στατιστικών στοιχείων των κανόνων	ΝΑΙ		
48.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα έχει την δυνατότητα να μεταφέρει αυτοματοποιημένα τις καταγραφές σε συστήματα SIEM.	ΝΑΙ		
49.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) πρέπει να έχει ενσωματωμένη δυνατότητα να εντοπίζει και να απεικονίζει στην κονσόλα πληροφορία βασισμένη σε αποδεκτά στατιστικά μοντέλα για ποιοι είναι οι πιο επικίνδυνοι χρήστες για διαρροή δεδομένων.			
50.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) να υποστηρίζει μέσω παραμετροποίησης την ελληνική γλώσσα (π.χ. πληροφορίες αναδυόμενων παραθύρων)	ΝΑΙ		
51.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να αναγνωρίζει εάν ένας σταθμός εργασίας είναι συνδεδεμένος στο εταιρικό δίκτυο ή εκτός σύνδεσης εταιρικού δικτύου και να λαμβάνει τα κατάλληλα μέτρα σε κάθε περίπτωση (βάσει των πολιτικών DLP)	ΝΑΙ		
52.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να είναι σε θέση να αναγνωρίζει οποιονδήποτε τύπο κρυπτογραφημένων αρχείων και να δίνει την δυνατότητα αποτροπής αποστολή τους εκτός της εταιρείας.	ΝΑΙ		
53.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) πρέπει να είναι σε θέση να κρυπτογραφεί (βάσει πολιτικών) έγγραφα που έχουν χαρακτηριστεί ως εμπιστευτικά (μέσω εφαρμογής διαβάθμισης εγγράφων),	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	όταν επιχειρείται η εξαγωγή τους από τον σταθμό εργασίας (endpoint) σε αποσπώμενα μέσα αποθήκευσης (USB).			
54.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) πρέπει να έχει δυνατότητα ψευδοανωνυμοποίησης σχετικά με τα λεπτομερή αποτελέσματα των ενεργειών των χρηστών. Τα αποτελέσματα της ανάλυσης θα πρέπει να προβάλλονται μόνο μετά από αίτημα παροχής στοιχείων σε περίπτωση συμβάντος και με την τεχνική splitknowledge (π.χ. διαπιστευτήρια του CISO και του διευθυντή IT).	NAI		
55.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να υποστηρίζει την ελληνική γλώσσα, σε αναδυόμενα παράθυρα (pop-up). Επιπλέον, θα πρέπει να αναγνωρίζει ελληνικούς χαρακτήρες που μπορεί να περιλαμβάνονται σε έγγραφα.	NAI		
56.	Ο agent του Συστήματος Αποτροπής Διαρροής Δεδομένων (DLP) δεν πρέπει να καταναλώνει περισσότερο από 5% των πόρων σταθμού εργασίας / διακομιστή, βάσει δεδομένων και έγκυρων μετρήσεων.	NAI		
57.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) πρέπει να είναι απολύτως συμβατό με το Σύστημα Διαβάθμισης Δεδομένων (π.χ. τα μεταδεδομένα τα σχετικά με το επίπεδο διαβάθμισης οποιουδήποτε αρχείου πρέπει να αναγνωρίζονται, από το εργαλείο DLP το οποίο θα εφαρμόζει κατάλληλες πολιτικές ελέγχου) και με τα υπόλοιπα συστήματα του Οργανισμού.	NAI		
58.	Ο agent που εγκαθιστάται στο τερματικό χρήστη πρέπει να προστατεύεται από περιπτώσεις κακόβουλης απενεργοποίησης. Θα πρέπει να υπάρχει άμεση ενημέρωση (alert) σε περίπτωση που εντοπιστεί περίπτωση μη εξουσιοδοτημένης απενεργοποίησης	NAI		
59.	Η σειρά εφαρμογής ή προτεραιότητα των κανόνων / πολιτικών θα πρέπει να είναι	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	σαφής και να καθορίζεται είτε από την σειρά της δήλωσής τους ή ρητά με αριθμό προτεραιότητας ή σπουδαιότητας.			
60.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) πρέπει να υποστηρίζει λειτουργίες διαχείρισης πολιτικής όπως, μεταξύ άλλων, προσθήκη πολιτικής, κατάργηση πολιτικής, ενεργοποίηση πολιτικής, απενεργοποίηση πολιτικής, προσθήκη, κατάργηση και αλλαγή κανόνων πολιτικής, αλλαγή παραμέτρων πολιτικής, σύνδεση πολιτικής με συγκεκριμένους agents, πολιτική δοκιμών κ.λπ.	NAI		
61.	Το "UserInterface" του συστήματος πρέπει να καθορίζεται με βάση τους ρόλους του συστήματος. Πρέπει να διακρίνονται κατ'ελάχιστον οι ρόλοι (α) διαχειριστής, (β) υπεύθυνος ασφαλείας, (γ) κοινός χρήστης	NAI		
62.	Ο agent του συστήματος Αποτροπής Διαρροής Δεδομένων (DLP) θα μπορεί να εγκαθίσταται εξ αποστάσεως και θα είναι συμβατός με άλλα εργαλεία που λειτουργούν στα τελικά σημεία (antivirus κλπ)	NAI		
63.	Οι agents του Συστήματος Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να είναι δυνατόν να εγκατασταθούν στα τελικά σημεία (endpoint) εξ αποστάσεως	NAI		
64.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα έχει την δυνατότητα εγκατάστασης δικτυακών στοιχείων για την παρακολούθηση της διακίνησης δεδομένων μέσω του κεντρικού δικτύου,	NAI		
65.	Οι κανόνες θα εφαρμόζονται τόσο σε online όσο και offline κατάσταση του τελικού σημείου	NAI		
66.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα δίνει την δυνατότητα Ενεργοποίησης/Απενεργοποίησης κανόνων εξ αποστάσεως μόνο από συγκεκριμένους εξουσιοδοτημένους χρήστες	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
67.	Οι άμεσες ενημερώσεις θα διαχειρίζονται Εύκολα και κεντρικοποιημένα	ΝΑΙ		
68.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να μπορεί να διακρίνει ρόλους χρηστών στην κεντρική κονσόλα διαχείρισης	ΝΑΙ		
69.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) δεν θα πρέπει να δίνει την δυνατότητα απενεργοποίησης της εφαρμογής από τον τελικό χρήστη	ΝΑΙ		
70.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να υποστηρίζει διεπαφές (RESTAPI) ώστε να εξασφαλίζεται η διαλειτουργικότητα του με τα υφιστάμενα πληροφοριακά συστήματα του ΔΕΔΔΗΕ.	ΝΑΙ		
71.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να μπορεί να διαχειρίζεται μεγάλο όγκου δεδομένων	ΝΑΙ		
72.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να είναι επεκτάσιμο	ΝΑΙ		
73.	Ο ανάδοχος πρέπει να παρέχει διαγράμματα αρχιτεκτονικής για το πώς θα υλοποιηθεί το Σύστημα και τους υπολογιστικούς πόρους που απαιτούνται για τη φιλοξενία του Συστήματος και για την Πρόληψη απώλειας δεδομένων.	ΝΑΙ		
74.	Ο ανάδοχος θα είναι υπεύθυνος για την εγκατάσταση της πλήρους υποδομής που απαιτείται για την υλοποίηση του Συστήματος (π.χ. εγκατάσταση λογισμικού και λειτουργικού συστήματος, DB, εφαρμογής κ.λπ.).	ΝΑΙ		
75.	Ο ανάδοχος θα είναι υπεύθυνος να εγκαταστήσει τους απαιτούμενους agents στους τερματικούς σταθμούς εργασίας των χρηστών.	ΝΑΙ		
76.	Ο ανάδοχος θα είναι υπεύθυνος για τη δημιουργία όλων των συμφωνημένων	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	πολιτικών διαβάθμισης με βάση τις ανάγκες του φορέα.			
77.	Ο ανάδοχος πρέπει να παρέχει την κατάλληλη εκπαίδευση σχετικά με τη λειτουργία του Συστήματος ώστε όλοι οι χρήστες να γνωρίζουν πως μπορούν να χρησιμοποιήσουν το σύστημα	ΝΑΙ		

7.2.3.11 Λύση Διαχείρισης Δικαιωμάτων Εγγράφων

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
1.	Η λύση πρέπει να επιτρέπει τον καθορισμό του είδους των δικαιωμάτων που έχει κάθε χρήστης επί του εγγράφου (πχ μόνο ανάγνωση, επεξεργασία, ορισμός δικαιούχων, κλπ)	ΝΑΙ		
2.	Η λύση πρέπει να επιτρέπει στους διαχειριστές να παρακολουθούν τις ενέργειες πρόσβασης (επιτυχείς ή αποτυχημένες) από τελικούς χρήστες.			
3.	Η λύση πρέπει να επιτρέπει σε επιλεγμένους χρήστες να παρακολουθούν τις ενέργειες πρόσβασης (επιτυχείς ή αποτυχημένες) από τελικούς χρήστες.			
4.	Η λύση πρέπει να δίνει τη δυνατότητα εξ αποστάσεως αναίρεσης των δικαιωμάτων που έχουν παραχωρηθεί σε χρήστες ή διαγραφής ενός εγγράφου	ΝΑΙ		
5.	Η λύση πρέπει να δίνει τη δυνατότητα ορισμού ημερομηνιών λήξης της ισχύος των δικαιωμάτων πρόσβασης.	ΝΑΙ		
6.	Η λύση πρέπει να δίνει τη δυνατότητα σε διαχειριστές να καθορίζουν πολιτικές πρόσβασης και σε χρήστες να εφαρμόζουν αυτές τις πολιτικές πρόσβασης σε έγγραφα.	ΝΑΙ		
7.	Η λύση Λύση Διαχείρισης Δικαιωμάτων Εγγράφων θα πρέπει να προσφερθεί για καλύπτει χίλιους (1000) χρήστες	ΝΑΙ		
8.	Η λύση πρέπει να έχει την δυνατότητα να αποδίδει συγκεκριμένα δικαιώματα	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	πρόσβασης είτε σε μεμονωμένους χρήστες είτε σε ομάδες χρηστών.			
9.	Η λύση πρέπει να έχει την δυνατότητα να εφαρμόζει πολιτικές απόδοσης δικαιωμάτων πρόσβασης τόσο σε επίπεδο εταιρείας όσο και σε συγκεκριμένους χρήστες.			
10.	Η λύση πρέπει να επιτρέπει σε επιλεγμένους χρήστες (όχι μόνο διαχειριστές) να διαχειρίζονται πολιτικές απόδοσης δικαιωμάτων πρόσβασης.			
11.	Η λύση πρέπει να δίνει την δυνατότητα καθορισμού των διαδικτυακών διευθύνσεων από τις οποίες επιτρέπεται η πρόσβαση στα έγγραφα.	ΝΑΙ		
12.	Η λύση πρέπει να αναγνωρίζει και να αυθεντικοποιεί τους χρήστες που ανήκουν στον οργανισμό μέσω πλήρους λειτουργικής διασύνδεσης με το AD του οργανισμού.	ΝΑΙ		
13.	Η λύση πρέπει να έχει την δυνατότητα απόδοσης συγκεκριμένων δικαιωμάτων πρόσβασης σε χρήστες που ανήκουν σε συγκεκριμένες ομάδες του οργανισμού (ActiveDirectorygroups).	ΝΑΙ		
14.	Η λύση πρέπει να δίνει την δυνατότητα να καθορίζονται ονομαστικά οι χρήστες (εσωτερικοί ή εξωτερικοί) στους οποίους επιτρέπεται η πρόσβαση σε έγγραφα του οργανισμού καθώς και το είδος της πρόσβασης που παρέχεται.	ΝΑΙ		
15.	Η λύση πρέπει να δίνει την δυνατότητα να καθορίζονται ομάδες χρηστών στις οποίες επιτρέπεται η πρόσβαση σε έγγραφα του οργανισμού.			
16.	Η λύση πρέπει να έχει την δυνατότητα αποστολής ειδοποιήσεων/προσλήξεων (invitations) σε εξωτερικούς χρήστες στους οποίους παραχωρείται πρόσβαση σε ένα έγγραφο.	ΝΑΙ		
17.	Οι χρήστες στους οποίους αποδίδεται δικαίωμα πρόσβασης σε ένα έγγραφο	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	πρέπει να μπορούν να διαχειρίζονται το έγγραφο χωρίς την χρήση ειδικών προγραμμάτων (transparency).			
18.	Η λύση πρέπει να δίνει την δυνατότητα καθορισμού δικαιωμάτων πρόσβασης σε οποιονδήποτε τύπο αρχείου			
19.	Η λύση πρέπει να δίνει την δυνατότητα καθορισμού δικαιωμάτων πρόσβασης είτε σε διακριτά έγγραφα είτε σε όλα τα έγγραφα που διατηρούνται σε συγκεκριμένα διακριτά σημεία διατήρησης (φακέλους ή μέσα αποθήκευσης).	ΝΑΙ		
20.	Η λύση πρέπει να δίνει δυνατότητα καθορισμού δικαιωμάτων πρόσβασης σε αρχεία που διατηρούνται σε τοπικούς σταθμούς εργασίας, servers, σε εφαρμογές νέφους (Office365, Sharepoint, OneDrive, κλπ).	ΝΑΙ		
21.	Ο τρόπος διαχείρισης των δικαιωμάτων πρόσβασης των εγγράφων θα πρέπει να είναι ίδιος ανεξάρτητα από το μέσο διατήρησης των αρχείων.	ΝΑΙ		
22.	Η λύση πρέπει να έχει πλήρη συμβατότητα με τις εφαρμογές του Office 365 και να δίνει δυνατότητα στους χρήστες των εφαρμογών να καθορίζουν τα δικαιώματα επί των δεδομένων μέσα από το περιβάλλον των ιδίων των εφαρμογών ή μέσω της εφαρμογής.	ΝΑΙ		
23.	Η λύση πρέπει να έχει πλήρη συμβατότητα με τις εφαρμογές Outlook και Exchange.	ΝΑΙ		
24.	Η λύση πρέπει να έχει δυνατότητα καθορισμού δικαιωμάτων πρόσβασης σε αρχεία pdf.	ΝΑΙ		
25.	Η λύση πρέπει να έχει την δυνατότητα λειτουργικής διασύνδεσης με την λύση DLP του Οργανισμού (DataLossPrevention) και τη λύση Διαβάθμισης Εγγράφων καθώς και τις υπόλοιπες εφαρμογές του Οργανισμού.	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
26.	Δυνατότητα Διασύνδεσης με το SIEM του οργανισμού	ΝΑΙ		
27.	Ο ανάδοχος πρέπει να παρέχει την κατάλληλη εκπαίδευση σχετικά με τη λειτουργία του Συστήματος ώστε όλοι οι χρήστες να γνωρίζουν πως μπορούν να χρησιμοποιήσουν το σύστημα	ΝΑΙ		

7.2.3.12 Λύση Διαχείρισης Λογαριασμών και Δικαιωμάτων Πρόσβασης Χρηστών

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Να αναφερθεί το όνομα, η έκδοση, η ημερομηνία ανακοίνωσης και ο κατασκευαστής της προσφερόμενης πλατφόρμας.	ΝΑΙ		
	Ο κατασκευαστής της προσφερόμενης πλατφόρμας λογισμικού Identity&AccessRightsManagement IAM θα πρέπει να διαθέτει τοπική παρουσία με τοπικό γραφείο εκπροσώπησης / θυγατρική στην Ελλάδα	ΝΑΙ		
	ΗπροσφερόμενηΛύσηIdentity&AccessRightsManagementIAM θακαλύπτειχίλιους (1.000) λογαριασμούς.	ΝΑΙ		
	Η προτεινόμενη αρχιτεκτονική υλοποίησης της πλατφόρμας θα πρέπει να περιλαμβάνει λειτουργία σε διάταξη υψηλής διαθεσιμότητας.	ΝΑΙ		
	Η προτεινόμενη αρχιτεκτονική υλοποίησης της πλατφόρμας θα πρέπει να υποστηρίζει λειτουργία 24x7.	ΝΑΙ		
	Χρήση μιας κεντρικής ενιαίας σχεσιακής βάσης δεδομένων για την διαχείριση του συνόλου των δεδομένων της προτεινόμενης πλατφόρμας.	ΝΑΙ		
	Η προτεινόμενη αρχιτεκτονική υλοποίησης της πλατφόρμας θα πρέπει να προσφέρει τη δυνατότητα οριζόντιας και κάθετης κλιμάκωσης.	ΝΑΙ		
	Η δυνατότητα οριζόντιας κλιμάκωσης θα προβλέπει δυναμική προσθήκη επιπλέον κόμβων στη βάση δεδομένων και στους εξυπηρετητές εφαρμογών της πλατφόρμας χωρίς καμιά διακοπή της υπηρεσίας. Κάθε νέος κόμβος που θα προστίθεται θα γίνεται άμεσα ενεργός και θα αναλαμβάνει μέρος του φόρτου εργασίας και των συνδέσεων των εφαρμογών.	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Οι προσφερόμενες άδειες χρήσης λογισμικού της πλατφόρμας IAM θα επιτρέπουν στον φορέα εάν το επιθυμεί να μεταφέρει και να λειτουργήσει την πλατφόρμα IAM σε υποδομές PublicCloud. Η προσφερόμενη λύση θα πρέπει να μπορεί να μεταφερθεί και να λειτουργήσει κατ'ελάχιστων στις ακόλουθες υποδομές Δημόσιου Νέφους (PublicCloudInfrastructure): α) Microsoft Azure, β) Amazon Web Services.			
	Όλα τα δομικά συστατικά της προτεινόμενης πλατφόρμας λογισμικού θα πρέπει να λειτουργούν σε διάταξη υψηλής διαθεσιμότητας και ισοκατανομής φόρτου εργασίας	ΝΑΙ		
	Υποστήριξη κεντροκοποιημένης πολιτικής με χρήση των ακόλουθων στοιχείων: <ul style="list-style-type: none"> • Χρήστες (users) • Ρόλοι χρηστών (roles) • Δικαιώματα (permissions) • Εφαρμογές (applications) • Εξαιρέσεις (exclusions) • Κίνδυνοι (risks) Οργανισμοί (organizations)	ΝΑΙ		
	Υποστήριξη εκχώρησης της δυνατότητας εκτέλεσης των διαθέσιμων διαχειριστικών ενεργειών στο σύστημα είτε απευθείας σε χρήστες, είτε σε ομάδες χρηστών (delegatedadministration).	ΝΑΙ		
	Εργαλείο αναζήτησης βάση πολλαπλών κριτηρίων.	ΝΑΙ		
	Δυνατότητα επαναφοράς του συνθηματικού χρήστη στις εφαρμογές από τον χρήστη, χωρίς τη διαμεσολάβηση διαχειριστή (self-servicepasswordreset).	ΝΑΙ		
	Η πλατφόρμα θα πρέπει να υποστηρίζει πολλαπλά πρωτόκολλα για αυθεντικοποίηση και εξουσιοδότηση (Active Directory/ADFS, LDAP, OpenID, OAuth, Identity Management Systems etc).	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Να περιγραφεί η διαδικασία εξουσιοδότησης και συγκεκριμένα η διαδικασία δημιουργίας ρόλων και ανάθεσης δικαιωμάτων εξουσιοδότησης.	ΝΑΙ		
	Η πλατφόρμα θα πρέπει να παρέχει δυνατότητες προσαρμογής της διεπαφής χρήσης καθώς και των connectors και των διαδικασιών.	ΝΑΙ		
	Η πλατφόρμα θα πρέπει να υποστηρίζει την παραμετροποίηση τήρησης των αποθηκευμένων διαπιστευτηρίων (saved/cachedcredentials).	ΝΑΙ		
	Η πλατφόρμα θα πρέπει να διασφαλίζει την εξουσιοδοτημένη πρόσβαση σε υπηρεσίες και δεδομένα.	ΝΑΙ		
	Η πλατφόρμα θα πρέπει να παρέχει τη δυνατότητα ανάθεσης μόνο των τελειώς απαραίτητων δικαιωμάτων σε κάθε χρήστη ανάλογα με τον ρόλο του και εφαρμόζοντας την αρχή του LeastPrivilege.	ΝΑΙ		
	Η πλατφόρμα θα πρέπει να υποστηρίζει το RESTAPIs για εισερχόμενες διεπαφές με τρίτα συστήματα.	ΝΑΙ		
	Να διατεθούν και να υλοποιηθούν adapters με τον ActiveDirectory και με μία βάση (Oracle ή MSSQL) του Φορέα	ΝΑΙ		
	Η προτεινόμενη πλατφόρμα θα πρέπει να έχει τη δυνατότητα διασύνδεσης με ActiveDirectory για την παραμετροποίηση των ρόλων των χρηστών.	ΝΑΙ		
	Η πλατφόρμα θα πρέπει να υποστηρίζει το RoleBasedAccessControl (RBAC) μοντέλο. Θα πρέπει να ανατεθούν σε χρήστες επιχειρησιακοί ρόλοι που θα μεταφράζονται σε δικαιώματα εφαρμογών και θα ανταποκρίνονται στη θέση τους στον οργανισμό.	ΝΑΙ		
	Η πλατφόρμα θα πρέπει να υποστηρίζει MultiFactorAuthentication.	ΝΑΙ		
	Δυνατότητα δημιουργίας ρόλων αιτημάτων χρήσης μέσω γραφικού περιβάλλοντος, με τα παρακάτω χαρακτηριστικά: <ul style="list-style-type: none"> Υποστήριξη παράλληλων και σειριακών διεργασιών με αιτήματα έγκρισης από ευέλικτα καθοριζόμενους χρήστες (approvaltasks). Δυνατότητα προώθησης συγκεκριμένων αιτημάτων έγκρισης σε άλλους χρήστες. Δυνατότητα προσωρινής εκχώρησης των δικαιωμάτων έγκρισης σε άλλο χρήστη (και με ημερομηνία λήξης). 	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	<ul style="list-style-type: none"> Δυνατότητα παρακολούθησης της κατάστασης ενός αιτήματος (και για χρήστες μη εγγεγραμμένους στο σύστημα). Δυνατότητα έγκρισης/απόρριψης ενός αιτήματος από το e-mail του χρήστη. <p>Δυνατότητα έναρξης αιτημάτων για δημιουργία λογαριασμού χωρίς την ανάγκη κατοχής λογαριασμού χρήσης στο σύστημα.</p>			
	Δυνατότητα υποστήριξης αυτόματων μεταβολών στις προσβάσεις ενός χρήστη ανάλογα με τις κινήσεις που γίνονται στο trustedsource (HRMS) σύστημα (πρόσληψη, μετακίνηση, αλλαγή θέσης, τερματισμός).	ΝΑΙ		
	Αυτοματοποιημένη μεταβολή των δικαιωμάτων πρόσβασης στα συνδεδεμένα (connected) συστήματα.	ΝΑΙ		
	Δυνατότητα αποδοχής ή άρνησης των αιτήσεων πρόσβασης στις εφαρμογές.	ΝΑΙ		
	Δυνατότητα προσωρινής εκχώρησης των δικαιωμάτων έγκρισης σε άλλο χρήστη (και με ημερομηνία λήξης).	ΝΑΙ		
	Δυνατότητα παρακολούθησης της κατάστασης ενός αιτήματος (και για χρήστες μη εγγεγραμμένους στο σύστημα).	ΝΑΙ		
	Να παρέχεται έτοιμο λογισμικό, χωρίς την ανάγκη ανάπτυξης κώδικα, για τη σύνδεση με συστήματα αποθήκευσης χρηστών (userrepositories). Να αναφερθούν τα υποστηριζόμενα συστήματα	ΝΑΙ		
	Να παρέχονται εύκολα παραμετροποιήσιμοι οδηγοί (wizards) για την σύνδεση και διαχείριση χρηστών σε συστήματα ευρέως χρησιμοποιούμενων τεχνολογιών (π.χ CSV αρχεία, συστήματα, συστήματα με webservices διεπαφές, πίνακες σε βάσεις δεδομένων με ειδική μορφή).	ΝΑΙ		
	Δυνατότητα διασύνδεσης εφαρμογών ως disconnected, με την αποστολή εργασίας (task) στον διαχειριστή ενός συστήματος, ώστε να μπορούν να συνδεθούν δυναμικά όλες οι εφαρμογές του οργανισμού.	ΝΑΙ		
	Η πλατφόρμα θα πρέπει να διαθέτει connectors τα οποία θα πρέπει να υποστηρίζουν εργασίες για το provisioning (δημιουργία, ενημέρωση, κατάργηση) των χρηστών στα διασυνδεδεμένα συστήματα καθώς και το reconciliation αυτών (ανάκτηση χρήστη και των δικαιωμάτων του). Οι προσβάσεις που έχουν αποδοθεί εκτός των διαδικασιών της λύσης, θα πρέπει να έχουν την αντίστοιχη ένδειξη για να	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	μπορούν να ληφθούν αποφάσεις είτε χειροκίνητα (κατάργηση τους από τον διαχειριστή του συστήματος) είτε αυτόματα (κατάργηση τους μέσω διεργασίας).			
	Ορισμός πολιτικών εξαιρέσεων και διαχωρισμού των προσβάσεων ανάλογα με τον ρόλο του χρήστη (Segregation of Duties). Θα πρέπει να εφαρμόζονται οι πολιτικές κατά το αίτημα ενός χρήστη για πρόσβαση καθώς και να μπορεί να προγραμματιστεί περιοδικός έλεγχος που θα αναθέτει μια εργασία αποκατάστασης (remediation task) σε εξουσιοδοτημένους χρήστες.	ΝΑΙ		
	Καταγραφή του συνόλου των γεγονότων του συστήματος και παραγωγή έτοιμων αναφορών (out of the box reports) κατ'ελάχιστον για τα ακόλουθα: <ul style="list-style-type: none"> • Πολιτικές πρόσβασης ανά ρόλο χρηστών και συνδεδεμένο σύστημα • Κατάσταση αιτημάτων έγκρισης και εγκριτικών ροών εργασίας • Κατάσταση χρηστών ανά σύστημα και ρόλο χρηστών Δικαιώματα πρόσβασης ανά χρήστη, ρόλο, οργανισμό, και συνδεδεμένο σύστημα	ΝΑΙ		
	Το σύστημα θα πρέπει να υποστηρίζει τον σχεδιασμό νέων αναφορών μέσω wizards.	ΝΑΙ		
	Η πλατφόρμα θα πρέπει να προσφέρει δυνατότητες καταγραφής.	ΝΑΙ		
	Θα πρέπει να διαλειτουργεί με κεντρική logging ή SIEM υποδομή.	ΝΑΙ		
	Υποστήριξη κατηγοριοποίησης γεγονότων βασιζόμενοι σε τύπο (π.χ. error, warning, information, debug etc.) και σημαντικότητα (π.χ. critical, major, normal etc.) με τρόπο που να είναι εύκολο το φιλτράρισμα σε αναφορές.	ΝΑΙ		
	Το επίπεδο καταγραφής θα πρέπει να είναι προσαρμόσιμο.	ΝΑΙ		
	Να περιγράφουν οι δυνατότητες καταγραφής της πλατφόρμας αναφέροντας: <ul style="list-style-type: none"> • ενέργειες και γεγονότα που καταγράφονται • τεχνολογίες που χρησιμοποιούνται εκτυπωτικές δυνατότητες	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Η πλατφόρμα θα πρέπει να διατηρεί ιστορικά αρχεία (logs) με ασφαλή τρόπο που να αποτρέπει οποιαδήποτε απόπειρα τροποποίησης.	ΝΑΙ		
	Η γραφική διεπαφή της προσφερόμενης πλατφόρμας θα πρέπει να είναι διαθέσιμη σε πολλαπλά είδη συσκευών (desktop, tablet, mobile).	ΝΑΙ		
	Η γραφική διεπαφή της προσφερόμενης πλατφόρμας θα πρέπει να διατίθεται μέσω webbrowser.	ΝΑΙ		
	Υποστήριξη πολιτικών πρόσβασης με βάση τα παρακάτω κριτήρια: <ul style="list-style-type: none"> Εφαρμογή για την οποία ζητείται η πρόσβαση Ταυτότητα χρήστη Ομάδα χρήστη IP διεύθυνση Ωρα εισόδου	ΝΑΙ		
	Δυνατότητα υποστήριξης πολλαπλών μηχανισμών αυθεντικοποίησης όπως: <ul style="list-style-type: none"> Αναγνωριστικό Χρήστη/Κωδικός Πρόσβασης One Time Password Passwordless Authentication	ΝΑΙ		
	Δυνατότητα καθορισμού χρόνου λήξης ανενεργού συνόδου χρήσης (idlelogout).	ΝΑΙ		
	Καταγραφή και αναφορά της IP διεύθυνσης των συνδεδεμένων χρηστών.	ΝΑΙ		
	Παροχή API για την δημιουργία κατά παραγγελία μεθόδων αυθεντικοποίησης (customauthenticationmodules).	ΝΑΙ		
	Υψηλή διαθεσιμότητα αξιοποιώντας εγγενώς τεχνολογίες caching, διαμοιρασμού φορτίου, failover.	ΝΑΙ		
	Δυνατότητα ορισμού επιπέδων αυθεντικοποίησης μεταξύ των διαφόρων μεθόδων αυθεντικοποίησης (multi-levelauthentication) και αντιστοίχιση των επιπέδων με τις προσφερόμενες υπηρεσίες. Στην περίπτωση απόπειρας πρόσβασης σε υπηρεσία υψηλότερου επιπέδου από το τρέχον επίπεδο αυθεντικοποίησης του χρήστη, ο χρήστης θα πρέπει να προτρέπει για επιπρόσθετη αυθεντικοποίηση, (step-upauthentication).	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Υποστήριξη δυνατοτήτων κληρονόμησης δικαιωμάτων από χρήστες ή ομάδες.	ΝΑΙ		
	Υποστήριξη του πρωτοκόλλου SAML 2.0.	ΝΑΙ		
	Υποστήριξη OAuth 2.0/OpenIDConnect	ΝΑΙ		
	Υποστήριξη αυτόματης αντιστοίχισης της ταυτότητας μεταξύ ενός απομακρυσμένου και ενός τοπικού χρήστη (accountmapping).	ΝΑΙ		
	Δυνατότητα προτροπής της συγκατάβασης από τον χρήστη, για την σύνδεση ή όχι μεταξύ της τοπικής και απομακρυσμένης ταυτότητας (opt-in, opt-outsso)	ΝΑΙ		
	Να αναφερθούν λεπτομερώς οι δυνατότητες ολοκλήρωσης με υποδομή LDAP καταλόγου.	ΝΑΙ		
	Η πλατφόρμα πρέπει να προσφέρει ένα RoleMining εργαλείο για την ανάλυση των useraccounts και των entitlements σε εφαρμογές και να προτείνει υποψήφιους επιχειρησιακούς ρόλους.	ΝΑΙ		
	Το RoleMining εργαλείο θα πρέπει να διαλειτουργεί με την πλατφόρμα για να: <ul style="list-style-type: none"> Φορτώνει δεδομένα από IDM πλατφόρμα που είναι απαραίτητα για ανάλυση Δημοσιεύει τον υποψήφιο ρόλο σε IDM πλατφόρμα για να γίνει διαθέσιμη σε αιτήσεις χρηστών	ΝΑΙ		
	Το RoleMining εργαλείο θα πρέπει να επιτρέπει κλιμακωτή φόρτωση υποψήφιων ρόλων σε IDM πλατφόρμα για να ενημερωθούν αλλαγές σε ρόλους αλλά και να φορτωθούν νέοι ρόλοι που δημιουργήθηκαν μετά το αρχικό load.	ΝΑΙ		
	Το RoleMining εργαλείο θα πρέπει προσφέρει τη δυνατότητα σύγκρισης υποψήφιων ρόλων με τους υφιστάμενους ρόλους για τον εντοπισμό πιθανών διπλών ρόλων.	ΝΑΙ		
	Το RoleMining εργαλείο θα πρέπει προσφέρει τη δυνατότητα συγκέντρωσης δεδομένων από διαφορετικές πηγές (IDM και CSV αρχεία).	ΝΑΙ		
	Το RoleMining εργαλείο θα πρέπει προσφέρει δυνατότητες what-ifanalysis πριν δημοσιεύσει τους ρόλους σε IDM πλατφόρμα.	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Να αναφερθεί το όνομα, η έκδοση του προσφερόμενου Συστήματος Διαχείρισης Βάσεων Δεδομένων (Σ.Δ.Β.Δ.) και η χρονολογία διάθεσης της προσφερόμενης έκδοσης	ΝΑΙ		
	Υποστηριζόμενες πλατφόρμες υλικού και λογισμικού: - Unix και Linux - Windows	ΝΑΙ		
	Συνοπτική περιγραφή της αρχιτεκτονικής του προσφερόμενου Σ.Δ.Β.Δ., του τρόπου συνεργασίας με το Λ.Σ. και του τρόπου αξιοποίησης της φυσικής αρχιτεκτονικής του συστήματος	ΝΑΙ		
	Ο ανάδοχος πρέπει να παρέχει την κατάλληλη εκπαίδευση, ώστε όλοι οι χρήστες να γνωρίζουν πως μπορούν να χρησιμοποιήσουν το σύστημα	ΝΑΙ		

7.2.3.13 Λύση Διαχείρισης Προνομιούχων Λογαριασμών Πρόσβασης

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
1.	Να αναφερθεί το λογισμικό και ο κατασκευαστής.	ΝΑΙ		
2.	Αριθμός Υποστηριζόμενων Διαχειριστών	≥ 100		
3.	Αριθμός υποστηριζόμενων συνεργατών (namedusers)	≥ 50		
4.	Η προσφερόμενη λύση θα πρέπει να υποστηρίζει μηχανισμούς υψηλής διαθεσιμότητας.	ΝΑΙ		
5.	Η προσφερόμενη λύση θα πρέπει να υποστηρίζει διατάξεις Active/ Active και Active/ Passive.	ΝΑΙ		
6.	Η προσφερόμενη λύση θα πρέπει να υποστηρίζει την δυνατότητα οριζόντιας κλιμάκωσης σε περιπτώσεις υψηλού φόρτου.	ΝΑΙ		
7.	Η προσφερόμενη λύση θα πρέπει να υποστηρίζει την κλιμακούμενη αύξηση του αριθμού των χρηστών και των υποστηριζόμενων συστημάτων.	ΝΑΙ		
8.	Η προσφερόμενη λύση δεν θα πρέπει να χρειάζεται ενδιάμεσους "jumpservers" για			

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	την διαχείριση των συνδέσεων με τα υπό διαχείριση συστήματα.			
9.	Η πρόσβαση στην προσφερόμενη λύση θα πρέπει να υλοποιείται με χρήση διεθνών αναγνωρισμένων μηχανισμών κρυπτογράφησης .	ΝΑΙ		
10.	Η προσφερόμενη λύση θα πρέπει να υποστηρίζει, κατ' ελάχιστα, την διασύνδεση με τα ακόλουθα συστήματα: <ul style="list-style-type: none"> • Windows • (Windows 10, Windowsserver 2012, 2016 και 2019 και μεταγενέστερες). • Unix / Linux (Oracle Enterprise Linux, RHEL, AIX, Ubuntu). • Databases (DB2, Oracle, MSSQL, MongoDB, PostgreSQL). • Network devices (Checkpoint, Fortigate firewalls, HP και Cisco switches, routers, Cisco balancers, κτλ.) • Εικονικά Συστήματα. • Εφαρμογές Web. 	ΝΑΙ		
11.	Η προσφερόμενη λύση θα πρέπει να υποστηρίζει την εφαρμογή διαφορετικών πολιτικών συνθηματικών καθώς και εναλλαγής/ διαχείρισης περιόδων σύνδεσης.	ΝΑΙ		
12.	Η προσφερόμενη λύση θα πρέπει να υποστηρίζει την εφαρμογή ελέγχου ταυτότητας πολλαπλών παραγόντων (MFA) για τους διαχειριστές καθώς και μηχανισμούς ελέγχου ενός παράγοντα για όλες τις εταιρικές εφαρμογές ιστού και κινητών.	ΝΑΙ		
13.	Η προσφερόμενη λύση θα πρέπει να υποστηρίζει μηχανισμούς ελέγχου ταυτότητας βασισμένους στον βαθμό επικινδυνότητας του χρήστη.	ΝΑΙ		
14.	Η προσφερόμενη λύση θα πρέπει να διαθέτει μηχανισμό προ-ελέγχου ταυτότητας για τις εφαρμογές που ανακτούν κωδικούς από ασφαλή αποθετήριο (securestore).	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
15.	Η προσφερόμενη λύση θα πρέπει να διαθέτει μηχανισμό ελέγχου πρόσβασης σε οποιοδήποτε σύστημα, υπηρεσία ή/ και εφαρμογή, που συνδέονται χρήστες με αυξημένα δικαιώματα καθώς και να παρέχει την δυνατότητα περιορισμού των δικαιωμάτων "superuser".	NAI		
16.	Η προσφερόμενη λύση θα πρέπει να παρέχει την δυνατότητα σύνδεσης με αυξημένα δικαιώματα σε συστήματα, υπηρεσίες και εφαρμογές όταν αυτό απαιτείται.	NAI		
17.	Η προσφερόμενη λύση θα πρέπει παρέχει την δυνατότητα εκχώρησης ρόλων στους λογαριασμούς χρηστών με σκοπό την διασφάλιση της αρχής του ελάχιστου δικαιώματος (leastprivilege) και αποφυγή παραχώρησης αυξημένων δικαιωμάτων πρόσβασης όταν δεν απαιτείται.	NAI		
18.	Η προσφερόμενη λύση θα πρέπει να παρέχει την δυνατότητα τερματισμού ή αποκλεισμού μιας συνόδου (session) η οποία έχει υλοποιηθεί με λογαριασμό με αυξημένα δικαιώματα είτε λόγω αδράνειας είτε μετά από αίτημα του διαχειριστή.	NAI		
19.	Η προσφερόμενη λύση θα πρέπει να παρέχει την δυνατότητα περιορισμού απομακρυσμένης πρόσβασης και ενεργειών σε συστήματα, υπηρεσίες ή/και εφαρμογές του οργανισμού.	NAI		
20.	Η προσφερόμενη λύση θα πρέπει να παρέχει ένα ενοποιημένο περιβάλλον για τη διαχείριση πολλαπλών απομακρυσμένων συνδέσεων RemoteDesktop και SSH από την ίδια κονσόλα.	NAI		
21.	Η προσφερόμενη λύση θα πρέπει να υποστηρίζει την δημιουργία συνεδρίας αυξημένων δικαιωμάτων για σύνδεση των διαχειριστών σε συστήματα Linux και συσκευές δικτύου μέσω SSH.	NAI		
22.	Η προσφερόμενη λύση θα πρέπει να υποστηρίζει την δημιουργία συνεδρίας αυξημένων δικαιωμάτων για σύνδεση των	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	διαχειριστών σε συστήματα Windows μέσω RDP.			
23.	Τα δεδομένα της προσφερόμενης λύσης θα πρέπει να διατηρούν τα ίδια επίπεδα ασφάλειας και κρυπτογράφησης κατά την διαδικασία λήψης αντίγραφου ασφαλείας	NAI		
24.	Η προσφερόμενη λύση θα πρέπει να διαθέτει διαδικτυακή πύλη μέσω της οποίας οι χρήστες (εξωτερικοί και εσωτερικοί) θα αποκτούν πρόσβαση στα εξουσιοδοτημένα συστήματα.	NAI		
25.	Η προσφερόμενη λύση θα πρέπει να διαθέτει υποσύστημα για κινητές συσκευές μέσω της οποίας θα είναι διαθέσιμη η αποδοχή ή απόρριψη ρών έγκρισης.	NAI		
26.	Η προσφερόμενη λύση θα πρέπει να διαθέτει εφαρμογή για κινητές συσκευές η οποία θα λειτουργεί σαν εναλλακτική μέθοδος σύνδεσης κάνοντας χρήση λογαριασμού με αυξημένα δικαιώματα.	NAI		
27.	Η προσφερόμενη λύση θα πρέπει να παρέχει την δυνατότητα ανάκτησης κωδικού πρόσβασης μέσω SDK. Τα διαπιστευτήρια που σχετίζονται με την εφαρμογή θα πρέπει να αποθηκεύονται σε ένα ασφαλές αποθηκευτικό χώρο.	NAI		
28.	Η βάση δεδομένων της προσφερόμενης λύσης θα πρέπει να χρησιμοποιεί κρυπτογράφηση με κλειδί AES256 (AdvancedEncryptionStandards).	NAI		
29.	Η προσφερόμενη λύση θα πρέπει να παρέχει δυνατότητα αναβάθμισης.	NAI		
30.	Η προσφερόμενη λύση θα πρέπει να διασυνδέεται με κεντρικό κατάλογο χρηστών (ActiveDirectory). Να αναφερθούν οι δυνατότητες	NAI		
31.	Η προσφερόμενη λύση θα πρέπει να παρέχει δυνατότητα αυθεντικοποίησης διαχειριστών που δεν ανήκουν στον Φορέα (εξωτερικοί συνεργάτες)	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
32.	Η πρόσβαση στην προσφερόμενη λύση θα πρέπει να επιτυγχάνεται με την χρήση των τρεχόντων διαπιστευτηρίων των χρηστών και χωρίς την ύπαρξη λογισμικού (agentless) στους σταθμούς εργασίας τους.	NAI		
33.	Η προσφερόμενη λύση θα πρέπει να υποστηρίζει την δημιουργία κατά απαίτηση (adhoc) σύνδεσης με συγκεκριμένο τύπου τερματικού στην περίπτωση έλλειψης προεπιλεγμένης διασύνδεσης.	NAI		
34.	Η προσφερόμενη λύση θα πρέπει να διαχειρίζεται διαπιστευτήρια βασισμένα στις πολιτικές που ορίζονται στα τελικά συστήματα καθώς και να επιτρέπει την διαχείριση των κλειδιών SSH και API για περιβάλλοντα νέφους.	NAI		
35.	Η προσφερόμενη λύση θα πρέπει να εντοπίζει, να εισάγει και να διαχειρίζεται λογαριασμούς σε όλο το περιβάλλον του οργανισμού.	NAI		
36.	Κατά τη δημιουργία νέου λογαριασμού με αυξημένα δικαιώματα, η προσφερόμενη λύση θα πρέπει να εντοπίζει και να ενημερώνει για την ύπαρξη προηγούμενου λογαριασμού με το ίδιο αναγνωριστικό σε οποιοδήποτε σύστημα, εφαρμογή και/ ή υπηρεσία, για την αποφυγή επαναχρησιμοποίησης του.	NAI		
37.	Η προσφερόμενη λύση θα πρέπει να προστατεύει τις πληροφορίες που είναι απαραίτητες για την αυθεντικοποίηση των χρηστών με αυξημένα δικαιώματα για την αποφυγή μια πιθανής εκμετάλλευσης από μη εξουσιοδοτημένους χρήστες.	NAI		
38.	Η προσφερόμενη λύση θα πρέπει να μπορεί να περιορίζει τις αποτυχημένες προσπάθειες σύνδεσης για την αποφυγή επιθέσεων τύπου bruteforce/ dictionaryattack και να ενημερώνει αυτόματα συγκεκριμένους χρήστες εντός της εταιρείας.	NAI		
39.	Να αναφερθούν οι μηχανισμοί ασφαλείας.	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
40.	Η προσφερόμενη λύση θα πρέπει να υποστηρίζει την κρυπτογράφηση των αποθηκευμένων διαπιστευτηρίων χρησιμοποιώντας διεθνώς αναγνωρισμένους αλγόριθμους κρυπτογράφησης όπως AES-256, RSA-2048 κ.λπ.	NAI		
41.	Η προσφερόμενη λύση θα πρέπει να χρησιμοποιεί κρυπτογραφημένο κανάλι επικοινωνίας για την μεταφορά των δεδομένων από/ προς το αποθετήριο.			
42.	Η προσφερόμενη λύση θα πρέπει να μπορεί να αλλάζει αυτόματα, τα συνθηματικά που εισάγονται στο αποθετήριο.			
43.	Η προσφερόμενη λύση θα πρέπει να διασφαλίζει την εναλλαγή των συνθηματικών των λογαριασμών των χρηστών με υψηλά προνόμια.	NAI		
44.	Η προσφερόμενη λύση θα πρέπει να διασφαλίζει την εναλλαγή των συνθηματικών, όπου η ύπαρξη των λογαριασμών με αυξημένα δικαιώματα είναι απαραίτητη π.χ. κώδικας σε αρχεία παραμετροποίησης, συνδέσεις με βάσεις δεδομένων κ.λπ.			
45.	Η προσφερόμενη λύση θα πρέπει να παρέχει δυνατότητα αποθήκευσης στο αποθετήριο, διαπιστευτήρια που δεν πρέπει να γίνουν αλλαγή (π.χ. λογαριασμοί έκτακτης ανάγκης).			
46.	Η προσφερόμενη λύση θα πρέπει να παρέχει τη δυνατότητα αλλαγής των συνθηματικών που ανήκουν σε συστήματα καταλόγου, όπως και σε εκείνα που ανήκουν σε συστήματα Windows και Linux.	NAI		
47.	Η προσφερόμενη λύση θα πρέπει να μπορεί να περιορίσει το χρόνο ισχύος των συνθηματικών που χρησιμοποιούνται από λογαριασμούς με αυξημένα προνόμια επιτρέποντας την δημιουργία εξαιρέσεων στην γενική πολιτική.	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
48.	Η προσφερόμενη λύση θα πρέπει να επιτρέπει την δημιουργία συνθηματικών μίας χρήσης και να διατηρεί ιστορικό των διαπιστευτηρίων για την αποφυγή επαναχρησιμοποίησης τους σύμφωνα με τους περιορισμούς χρόνου που έχει θέσει ο οργανισμός.	ΝΑΙ		
49.	Για περιστασιακές περιπτώσεις, η προσφερόμενη λύση θα πρέπει να διαθέτει μηχανισμό αυτόματης αλλαγής συνθηματικών.	ΝΑΙ		
50.	Η προσφερόμενη λύση θα πρέπει να δυνατότητα επιβολής της πολιτικής ασφάλειας του ΔΕΔΔΗΕ σχετικά με τους κωδικούς πρόσβασης και δυνατότητα να υποστηρίζει τις σχετικές κανονιστικές απαιτήσεις και τις βέλτιστες πρακτικές.			
51.	Η προσφερόμενη λύση θα πρέπει να επιβάλει κανόνες για την συνθετότητα των κωδικών, που περιλαμβάνουν μήκος κωδικών, μίξη αλφανουμερικών και ειδικών χαρακτήρων, διάκριση μεταξύ κεφαλαίων και μικρών (upper και lower).			
52.	Η προσφερόμενη λύση θα πρέπει να δίνει την δυνατότητα στους administrators για αλλαγή των κωδικών <ul style="list-style-type: none"> • σε συγκεκριμένα διαστήματα με βάση την πολιτική του οργανισμού. • σε περιοδική βάση, • μετά από κάθε πρόσβαση εφόσον κριθεί αναγκαίο • κωδικών κατ' εντολή. 	ΝΑΙ		
53.	Η προσφερόμενη λύση θα πρέπει να παρέχει τους απαραίτητους μηχανισμούς παρακολούθησης, καταγραφής και ελέγχου της χρήσης των λογαριασμών με αυξημένα δικαιώματα σε οποιοδήποτε σύστημα, εφαρμογή και/ ή υπηρεσία.	ΝΑΙ		
54.	Η προσφερόμενη λύση θα πρέπει υποστηρίζει την προώθηση όλων των	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	ενεργειών των χρηστών στο SIEM της εταιρείας .			
55.	Η προσφερόμενη λύση θα πρέπει να παρέχει τους απαραίτητους μηχανισμούς προστασίας από διαγραφή ή/ και τροποποίηση των συμβάντων ασφαλείας.	ΝΑΙ		
56.	Η προσφερόμενη λύση θα πρέπει να παρέχει την δυνατότητα παρακολούθησης των συνοδών SSH που πραγματοποιούνται από τον τελικό χρήστη σε διακομιστή Linux ή άλλη δικτυακή συσκευή, με δυο διαφορετικούς τρόπους: <ul style="list-style-type: none"> • καταγραφή της περιόδου λειτουργίας σε δευτερόλεπτα για όσο διάστημα είναι ενεργή η σύνδεση • καταγραφή όλων των εντολών και ενεργειών που εκτελούνται κατά τη διάρκεια της συνόδου 	ΝΑΙ		
57.	Η προσφερόμενη λύση θα πρέπει να παρέχει την δυνατότητα εύρεσης των εντολών που εκτέλεσε ο χρήστης μέσω των καταγραφών της συνόδου SSH	ΝΑΙ		
58.	Η προσφερόμενη λύση θα πρέπει να παρέχει την δυνατότητα παρακολούθησης των συνοδών RDP που πραγματοποιούνται από τον τελικό χρήστη σε διακομιστή Windows με δυο διαφορετικούς τρόπους: <ul style="list-style-type: none"> • καταγραφή της συνόδου σε δευτερόλεπτα για όσο διάστημα είναι ενεργή • καταγραφή όλων των εντολών και ενεργειών που εκτελούνται κατά τη διάρκεια της συνόδου 	ΝΑΙ		
59.	Δυνατότητα καταγραφής (videorecording) των ενεργειών των χρηστών και για νομικές/κανονιστικές απαιτήσεις			
60.	Όλες οι ενέργειες του διαχειριστή της εφαρμογής θα πρέπει να υπάρχει η δυνατότητα να αποστέλλονται στο SIEM			
61.	Η προσφερόμενη λύση θα πρέπει να παρέχει στους διαχειριστές της λύσης την δυνατότητα	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	<ul style="list-style-type: none"> • δυναμικής παροχής πρόσβασης - πχ. χρονικού περιορισμού της πρόσβασης (πχ. Πρόσβαση για τις επόμενες Χ ώρες) • διακοπής πρόσβασης μέσω του Συστήματος εφόσον κριθεί αναγκαίο • έγκρισης της πρόσβασης από τρίτον χρήστη • πολλαπλών τρόπων έγκρισης για άμεση ενεργοποίηση 			
62.	Η προσφερόμενη λύση θα μπορεί να επιβάλει επιπλέον κανόνων ελέγχου πρόσβασης που δεν καθορίζονται μόνο από το ρόλο του χρήστη όπως ο χρόνος της πρόσβασης (ημέρα, βράδυ, εργάσιμες ημέρες αργίες).	NAI		
63.	Η προσφερόμενη λύση θα μπορεί να περιορίζει την πρόσβαση από συγκεκριμένα δικτυακά σημεία.	NAI		
64.	Η προσφερόμενη λύση θα μπορεί να μεσολαβεί μεταξύ του διαχειριστή και του υπό διαχείριση συστήματος προωθώντας εντολές του διαχειριστή χωρίς ο ίδιος να γνωρίζει τον κωδικό πρόσβασης στο υπό διαχείριση σύστημα (sessionproxy).	NAI		
65.	Δυνατότητα πλήρους καταγραφής των ενεργειών του διαχειριστή ώστε να αποδεικνύεται η συμμόρφωση με Νομικές/Κανονιστικές απαιτήσεις.	NAI		
66.	Η προσφερόμενη λύση θα πρέπει διαθέτει μηχανισμούς ανάλυσης της συμπεριφοράς των χρηστών, με σκοπό τον εντοπισμό των ανωμαλιών ή των περιπτώσεων απόκλισης από την συνηθισμένη ασυνήθιστη δραστηριότητα ή ανωμαλιών σε πραγματικό χρόνο. Και να ενημερώνει αυτόματα συγκεκριμένους ρόλους και θέσεις εντός της εταιρείας.	NAI		
67.	Η προσφερόμενη λύση θα πρέπει να υποστηρίζει την δημιουργία προτύπου αναφοράς (baseline) σύμφωνα με την συμπεριφορά των χρηστών. Το ως άνω πρότυπο θα βασίζεται σε αλγόριθμους μηχανικής εκμάθησης που αναλύουν την	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	συμπεριφορά σε βάθος χρόνου, τη συμπεριφορά πρόσβασης, την σπουδαιότητα των διαπιστευτηρίων και την συμπεριφορά των απλών χρηστών. Μόλις ένας χρήστης παρεκκλίνει από το ως άνω πρότυπο, θα βαθμολογείται η επικινδυνότητα σε πραγματικό χρόνο.			
68.	Η προσφερόμενη λύση θα πρέπει να βαθμολογεί την συμπεριφορά των χρηστών βάσει της επικινδυνότητας.	ΝΑΙ		
69.	Η προσφερόμενη λύση θα πρέπει να μπορεί να καταγράψει τους λογαριασμούς με αυξημένα δικαιώματα και τους χρήστες που έχουν πρόσβαση σε αυτούς. Επιπλέον οι χρήστες ή/ και τα διαπιστευτήρια θα πρέπει να μπορούν να ομαδοποιηθούν ώστε να μπορεί να διαπιστωθεί εάν ένα διαπιστευτήριο περιέχεται σε μια ομάδα ή εάν οι χρήστες έχουν πρόσβαση σε διαπιστευτήρια ή στοιχεία που ανήκουν σε άλλα τμήματα.	ΝΑΙ		
70.	Η Λύση Διαχείρισης Προνομιούχων Λογαριασμών Πρόσβασης θα μπορεί να ανακαλύπτει λογαριασμούς με αυξημένα δικαιώματα ώστε να αποφεύγεται το ενδεχόμενο ύπαρξης κάποιου λογαριασμού ο οποίος δεν έχει πέσει στην αντίληψη της ομάδας πληροφορικής και οποίος ενδεχομένως χρησιμοποιείται κακόβουλα ώστε να παρακάμψει τα εφαρμοζόμενα μέτρα προστασίας και λογοδοσίας (auditing).	ΝΑΙ		
71.	Η Λύση Διαχείρισης Προνομιούχων Λογαριασμών Πρόσβασης θα μπορεί να διαχειρίζεται κεντρικά και αυτοματοποιημένα τους λογαριασμούς με αυξημένα δικαιώματα σε όλα τα συστήματα με τα οποία θα διασυνδεθεί.	ΝΑΙ		
72.	Η Λύση Διαχείρισης Προνομιούχων Λογαριασμών Πρόσβασης θα μπορεί να εντοπίζει εύκολα τα διαπιστευτήρια των διαχειριστών που δεν ελέγχονται μέσω του Συστήματος	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
73.	Η Λύση Διαχείρισης Προνομιούχων Λογαριασμών Πρόσβασης θα μπορεί να εντοπίζει εύκολα τα διαπιστευτήρια εντός εφαρμογών (hard-coded/embedded application credentials) και περιορισμό αυτών.	NAI		
74.	Η Λύση Διαχείρισης Προνομιούχων Λογαριασμών Πρόσβασης θα μπορεί να εκδίδει ειδοποιήσεις (alerts) σε κάθε περίπτωση που θα διαπιστωθεί η ύπαρξη κάποιου μη αναμενόμενου λογαριασμού.	NAI		
75.	Η προσφερόμενη λύση θα διατηρεί λεπτομερείς αναφορές σχετικά με την χρήση των κωδικών πρόσβασης από τους διαχειριστές των συστημάτων (logging).	NAI		
76.	Η προσφερόμενη λύση θα διατηρεί λεπτομερείς αναφορές με το ποια πολιτική διαχείρισης κωδικών εφαρμόζεται σε κάθε σύστημα και ποιες εξαιρέσεις ισχύουν.	NAI		
77.	Η προσφερόμενη λύση θα διατηρεί λεπτομερείς αναφορές σε διάφορα επίπεδα συμπεριλαμβανομένου πλήρους ιστορικού ενεργειών ανά διαχειριστή/σύστημα.	NAI		
78.	Η προσφερόμενη λύση θα διατηρεί λεπτομερείς αναφορές για το ποιος απόκτησε πρόσβαση με αυξημένα δικαιώματα, τότε και για ποιον λόγο.	NAI		
79.	Η προσφερόμενη λύση θα παρέχει Δυνατότητα αποστολής των καταγραφών σε σύστημα SIEM	NAI		
80.	Ο ανάδοχος πρέπει να παρέχει την κατάλληλη εκπαίδευση ώστε όλοι οι χρήστες να γνωρίζουν πως μπορούν να χρησιμοποιήσουν το σύστημα	NAI		

7.2.4 Πίνακες Συμμόρφωσης Τμήματος 4 «Εξειδικευμένες λύσεις και υπηρεσίες ασφάλειας για την Ε.Δ.Υ.Τ.Ε. Α.Ε.»

7.2.4.1 Παροχή υπηρεσίας SOC

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
1.	Τα Data Centers βρίσκονται εντός της Ελληνικής Επικράτειας και σε κάθε περίπτωση εντός της ΕΕ. Να παρατεθούν λεπτομέρειες για τα DataCenters καθώς και για τους μηχανισμούς ασφαλείας που τα προστατεύουν.	ΝΑΙ		
2.	Αρχιτεκτονική με βάση βέλτιστες πρακτικές η οποία διέπει τις υπηρεσίεςSOC	ΝΑΙ		
3.	Δυνατότητα συσχέτισης περιστατικών μεταξύ διαφορετικών πηγών δεδομένωνκαι ανάλυσης ετερογενών δεδομένων για τον εντοπισμό πραγματικών περιστατικών ασφάλειας. Να ληφθεί υπόψη ότι θα συλλέγονται logs και περιστατικά που προέρχονται από διαφορετικά συστήματα και συσκευές του περιβάλλοντος όπως συσκευές παρακολούθησης και διαχείρισης δικτύου, συσκευές ασφάλειας, διακομιστές δικτύου, διακομιστές εφαρμογών, βάσεις δεδομένων, λειτουργικά συστήματα κ.λπ.	ΝΑΙ		
4.	Διαλειτουργικότητα της υπηρεσίας με όλα τα υφιστάμενα αλλά και τα μελλοντικά συστήματα της ΕΔΥΤΕ ΑΕ. Εφόσον απαιτηθεί επιπρόσθετο κόστος ανάπτυξης για την εγκαθίδρυση της διαλειτουργικότητας με τα συστήματα της ΕΔΥΤΕ ΑΕ αυτό επιβαρύνει αποκλειστικά τον Ανάδοχο.	ΝΑΙ		
5.	Δυνατότητα ενσωμάτωσης απεριόριστου ορίου όγκου δεδομένων αρχείων καταγραφής που παράγονται από τα συστήματα της ΕΔΥΤΕ ΑΕ στην υπηρεσία. Επιπρόσθετα απαιτείται να μην	Αριθμός Assets >= 300		



A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	υφίσταται όριο Peak event per second (EPS) rates με σκοπό την αντιμετώπιση πιθανών επιθέσεων στην υποδομή της ΕΔΥΤΕ ΑΕ.			
6.	Μη ύπαρξη αντικτύπου στην υπηρεσία (π.χ. απώλεια ορατότητας, απώλεια αρχείων καταγραφής ή περιστατικών κ.λπ.) σε περίπτωση που για συγκεκριμένο χρονικό διάστημα η υπηρεσία ξεπεράσει τα όρια που έχουν τεθεί στην απαίτηση 5του παρόντος πίνακα συμμόρφωσης.	ΝΑΙ		
7.	Δυνατότητα αναζήτησης και περιήγησης στα πρωτότυπα δεδομένα καταγραφής (rawdata). Απαιτείται η παράθεση των απαραίτητων προδιαγραφών από τον Ανάδοχο ώστε να μην υφίστανται περιορισμοί στην παραπάνω δυνατότητα σύμφωνα με τις Απαιτήσεις της ΕΔΥΤΕ ΑΕ που αφορούν την περίοδο διακράτησης των δεδομένων καταγραφής, όπως αυτές περιγράφονται στην απαίτηση 13του παρόντος πίνακα συμμόρφωσης.	ΝΑΙ		
8.	Χρήση εξωτερικών πηγών δεδομένων για την ανάλυση πιθανών απειλών για το περιβάλλον της ΕΔΥΤΕ ΑΕ. Απαιτείται να ενημερώνεται η ΕΔΥΤΕ ΑΕ για τις πιθανές απειλές και η υπηρεσία να προσαρμόζεται ανάλογα με την ανάλυση των απειλών.	ΝΑΙ		
9.	Δυνατότητα συλλογής και ανάλυσης δεδομένων ευπαθειών από τρίτες πηγές/εργαλεία καθώς και η δυνατότητα συλλογής και ανάλυσης δεδομένων ευπαθειών τα οποία έχουν εντοπισθεί από τρίτους με χειροκίνητες μεθόδους (π.χ. στο πλαίσιο εκτέλεσης PenetrationTest). Να παρασχεθούν λεπτομέρειες σχετικά με τη μεθοδολογία από τον	ΝΑΙ		

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Ανάδοχο για τη συλλογή και ανάλυση δεδομένων ευπαθειών και παραβιάσεων από όλες τις πηγές και τις δυνατότητες ενσωμάτωσης μεταξύ των προσφερόμενων υπηρεσιών.			
10	Δυνατότητα εντοπισμού προσαρμοσμένων ή στοχευμένων επιθέσεων που απευθύνονται στους χρήστες ή τα συστήματά της ΕΔΥΤΕ ΑΕ.	ΝΑΙ		
11	<p>Διαδικτυακή πλατφόρμα/ κονσόλα που σχετίζεται με τις υπηρεσίες του Αναδόχου. Η συγκεκριμένη πλατφόρμα θα αποτελεί τη διεπαφή της ΕΔΥΤΕ ΑΕ με την υπηρεσία και θα περιλαμβάνει όλες τις απαραίτητες πληροφορίες για την υπηρεσία και θα προσδίδει και δυνατότητες αλληλεπίδρασης της ΕΔΥΤΕ ΑΕ με την υπηρεσία (π.χ. ticketing σύστημα, σύστημα διαχείρισης συμβάντων, αναφορές υπηρεσίας σε μορφή Dashboards κλπ.).</p> <p>Η πλατφόρμα θα περιλαμβάνει υπηρεσίες οι οποίες θα περιλαμβάνουν χωρίς να περιορίζονται στην περιορισμένη πρόσβαση βάσει ρόλου, στην προσαρμογή οθονών και παρουσίασης δεδομένων, στη ροή εργασιών / έκδοση tickets, προκαθορισμένους κανόνες συσχέτισης και προκαθορισμένες αναφορές. Προσδιορίστε εάν όλες οι υπηρεσίες, συμπεριλαμβανομένων εκείνων που παρέχονται από τους συνεργάτες (εάν υπάρχουν), θα είναι διαθέσιμες μέσω μίας πλατφόρμας.</p>	ΝΑΙ		
12	Δυνατότητα ενσωμάτωσης δεδομένων εκτίμησης ευπαθειών, συμπεριλαμβανομένου του τρόπου με τον οποίο χρησιμοποιούνται τα	ΝΑΙ		



A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	δεδομένα ευπαθειών για την υποστήριξη των δυνατοτήτων ειδοποίησης και αναφοράς.			
13	Διατήρηση των πρωτογενών και των αναλυμένων δεδομένων της ΕΔΥΤΕ ΑΕ καθώς και τη δυνατότητα για εφαρμογή διαφορετικών πολιτικών διατήρησης δεδομένων σε διαφορετικούς τύπους συστημάτων/συσκευών εφόσον απαιτηθεί ώστε να πληρούνται οι απαιτήσεις της ΕΔΥΤΕ ΑΕ.	Διάρκεια διατήρησης >12 μήνες		
14	Διαθεσιμότητα επιπέδου υπηρεσίας 99,9%, εξαιρουμένων τυχόν προκαθορισμένων περιόδων συντήρησης οι οποίες θα δηλώνονται ρητά στο SLA.	Διαθεσιμότητα >99,9%		
15	Σαφής καθορισμός εντός του SLA της υπηρεσίας, των χρόνων απόκρισης κατά τον εντοπισμό/ απόκριση σε περιστατικών ασφάλειας, για τις παρακάτω ενέργειες: <ul style="list-style-type: none"> • Παραγωγή ειδοποίησης από το σύστημα • Επισκόπηση συμβάντος από εξειδικευμένο μηχανικό • Αποκλεισμός συμβάντων "falsepositive" και "falsenegative" • Καταγραφή διορθωτικών ενεργειών για την αντιμετώπιση του συμβάντος • Επικοινωνία του συμβάντος και των διορθωτικών ενεργειών στην ΕΔΥΤΕ ΑΕ • Απόκριση από την πλευρά του αναδόχου ως προς τις ενέργειες που θα εκτελέσει η ΕΔΥΤΕ ΑΕ • Παρακολούθηση κατά και μετά το κλείσιμο του συμβάντος 	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Προσδιορίστε τα πιο πάνω διαστήματα.			
16	Ανάληψη της ευθύνης για την ασφαλιστική κάλυψη της ΕΔΥΤΕ ΑΕ σε περίπτωση παραβίασης των ορών της συμφωνίας. Καταχωρίστε τους ακριβείς όρους.	ΝΑΙ		
17	Για όλη τη διάρκεια της σύμβασης τα συστήματα τα οποία θα χρησιμοποιηθούν/προσφερθούν για την παροχή της υπηρεσίας συνεχίζουν να πληρούν τις απαιτήσεις του διαγωνισμού και να φέρουν υποστήριξη από τον κατασκευαστή. Σε οποιοδήποτε ενδεχόμενο κατάργησης συστημάτων ή τερματισμού υποστήριξης τους από τον κατασκευαστή ο Ανάδοχος οφείλει να τα αντικαταστήσει με συστήματα ίδιων ή ανώτερων προδιαγραφών κατόπιν συνεννόησης και συμφωνίας με της ΕΔΥΤΕ ΑΕ.	ΝΑΙ		
18	Σε ό,τι αφορά τα περιστατικά αναγνώρισης να υπάρχει δυνατότητα κατηγοριοποίησής τους. Να ανφερθούν οι δυνατότητες.	ΝΑΙ		
19	Ενσωμάτωση στην SOCυπηρεσίας της επιτήρησης των χρηστών με αυξημένα δικαιώματα. Να περιγραφεί λεπτομερώς πώς θα παρέχεται στην ΕΔΥΤΕ ΑΕ τη δυνατότητα αναγνώρισης από μια κονσόλα / αναφορά των χρηστών με αυξημένα δικαιώματα που πραγματοποίησαν συνδέσεις, τυχόν αυξήσεις δικαιωμάτων	ΝΑΙ		
20	Στα πλαίσια της υπηρεσίας SOCχρήση από την ΕΔΥΤΕ ΑΕ προχωρημένης ανάλυσης δεδομένων. Να περιγραφούν	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	λεπτομερώς τις περιπτώσεις χρήσης Analytics (Analytics Use Cases) που θα είναι διαθέσιμες στην ΕΔΥΤΕ ΑΕ από την εκκίνησης της υπηρεσίας.			
2.	Επαρκής μεθοδολογία από τον ανάδοχο για τη μείωση ψευδών θετικών και ψευδών αρνητικών ειδοποιήσεων. Να περιγράφει η μεθοδολογία του Αναδόχου για τη μείωση ψευδών θετικών και ψευδών αρνητικών ειδοποιήσεων και για την διαβάθμιση των περιστατικών ασφαλείας.	NAI		
2.	Υποστήριξη διαφορετικών τύπων δυνατοτήτων συσχέτισης. Να περιγραφούν λεπτομερώς οι διαφορετικοί τύποι δυνατοτήτων συσχέτισης που υποστηρίζει η προτεινόμενη μηχανή συσχετισμού.	NAI		
2.	Λύση ticketing που να συμπεριλαμβάνεται στην υπηρεσία. Να περιγραφεί λεπτομερώς η προσφερόμενη λύση ticketing / ροής εργασίας για την κλιμάκωση των περιστατικών.	NAI		
2.	Αυτοματοποιημένη λύση ροών εργασίας (workflow) η οποία να είναι ενσωματωμένη στην προσφερόμενη υπηρεσία.	NAI		
2.	Καταγεγραμμένες ροές εργασίας για την λύση ticketing. Περιγράψτε πώς θα χρησιμοποιηθεί η προσφερόμενη λύση ticketing / ροής εργασίας από την ομάδα SOC του Αναδόχου και την ομάδα της ΕΔΥΤΕ ΑΕ για τον συντονισμό και την αποτελεσματική απόκριση κατά τη διάρκεια περιστατικών ασφαλείας.	NAI		
2.	Η προσφερόμενη λύση ticketing / ροής εργασίας υποστηρίζει την ενσωμάτωση raw Logs και συσχετιζόμενων περιστατικών	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	(Correlated Events) σε ένα ticket περιστατικού.			
28	Η ομάδα παρακολούθησης του Αναδόχου αναλαμβάνει πλήρως την ευθύνη της ενημέρωσης κάθε ticket περιστατικών με rawlogs και Συσχετιζόμενα Περιστατικά (Correlated Events) καθ' όλη την περίοδο κατά την οποία το συμβάν βρίσκεται σε εξέλιξη. Να περιγραφεί αναλυτικά η σχετική προσέγγισή.	NAI		
28	Λεπτομερής τεκμηρίωση της μεθοδολογίας και η προσέγγισή του Αναδόχου για την Υλοποίηση, Τεκμηρίωση, Διαχείριση Έργου.	NAI		
29	Εκπαίδευση των στελεχών της ΕΔΥΤΕ ΑΕ αναφορικά με την λειτουργία της υπηρεσίας.	NAI		
30	Υποβολή τακτικής έκθεσης προς την ΕΔΥΤΕ ΑΕ στην οποία θα συνοψίζονται τα περιστατικά ασφάλειας και η συνολική κατάσταση του περιβάλλοντος του Οργανισμού κατά την περίοδο αναφοράς.	NAI		
31	Κατάρτιση εβδομαδιαίας τεχνικής έκθεσης η οποία θα είναι διαθέσιμη στις τεχνικές ομάδες της ΕΔΥΤΕ ΑΕ. Ο ανάδοχος θα πρέπει να παρέχει ένα δείγμα αναφοράς όπως παρέχεται σε άλλον πελάτη με παρόμοιες απαιτήσεις.	NAI		
32	Να παρασχεθούν παραδείγματα λειτουργικών, κανονιστικών και εκτελεστικών αναφορών.	NAI		
33	Προσαρμοσμένες, ad hoc αναζητήσεις (queries) και αναφορές. Να συμπεριληφθούν τυχόν περιορισμοί στις ad hoc αναζητήσεις ή στη δημιουργία αναφορών, συμπεριλαμβανομένων των πηγών δεδομένων, της παλαιότητας των	NAI		

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	δεδομένων, της συχνότητας των αναζητήσεων κτλ.			
34	Δημιουργία αναφορών: Διεπαφή αναφορών που μπορεί να αξιοποιήσει πολλαπλές υφιστάμενες αναφορές. Αναφέρατε το παρεχόμενο πλήθος, καθώς και τη δημιουργία νέων αναφορών που δεν απαιτούν περίπλοκες τεχνικές αναζητήσεις.	ΝΑΙ		
35	Η λειτουργικότητα παραγωγής αναφορών δεν επηρεάζεται αν μια συγκεκριμένη τεχνολογία, όπως ένα firewall, αντικατασταθεί με ένα νεότερο προϊόν ή προμηθευτή. Οι αναφορές θα πρέπει να συνεχίσουν να εκτελούνται και να περιλαμβάνουν τη νέα τεχνολογία στα κριτήρια αναφοράς αυτόματα.	ΝΑΙ		
36	Προγραμματισμός αναφορών: Η λύση παρέχει τη δυνατότητα προγραμματισμού των αναφορών ώστε να εκτελούνται σε προκαθορισμένα διαστήματα (ωριαία, καθημερινά, εβδομαδιαία ή μηνιαία). Υφίστανται πολλές μορφές εξαγωγών και επιλογές παράδοσης για προγραμματισμένες αναφορές.	ΝΑΙ		
37	Αναφορές συμμόρφωσης: Η λύση παρέχει τη δυνατότητα αναφοράς ως προς τη συμμόρφωση με κοινώς αποδεκτά πρότυπα στο χώρο της ασφάλειας (ISO 27002, NIST), τα οποία αντιστοιχίζονται απευθείας σε οποιοδήποτε κανονιστικό πρότυπο ή πολιτική ασφάλειας	ΝΑΙ		
38	Προσαρμοσμένα Dashboards: Η λύση παρέχει το πλαίσιο για τη δημιουργία προσαρμοσμένων dashboards για όλες τις επιχειρηματικές ομάδες.	ΝΑΙ		
39	Σε περίπτωση διαρροής προσωπικών δεδομένων ή επιχειρησιακών	ΝΑΙ		

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	δεδομένων ο ανάδοχος θα προετοιμάζει τις ζητούμενες αναφορές προς την ΑΠΔΠΧ και την Εθνική Αρχή Κυβερνοασφάλειας.			
40	Επαρκή μέτρα ασφάλειας τα οποία λαμβάνονται από τον Ανάδοχο για την προστασία των δικών του συστημάτων ώστε να μην είναι εφικτή πιθανή επέκταση ενός περιστατικού ασφάλειας στην ΕΔΥΤΕ ΑΕ η διαρροή πληροφοριών ή δεδομένων της ΕΔΥΤΕ ΑΕ.	ΝΑΙ		
41	Lessons Learned, καθώς και Advisories από τον ανάδοχο.	ΝΑΙ		
42	Περιορισμός Bandwidth: Η λύση πρέπει να παρέχει τη δυνατότητα περιορισμού του Internet bandwidth που χρησιμοποιείται για τη μετάδοση δεδομένων περιστατικών.	ΝΑΙ		
43	Διασφάλιση συναλλαγών: Η λύση παρέχει μηχανισμό που εγγυάται την αποστολή περιστατικών στο σύστημα διαχείρισης αρχείων καταγραφής και δεν παραλείπονται περιστατικά εάν το σύστημα διαχείρισης καταγραφής δεν είναι διαθέσιμο.	ΝΑΙ		
44	Υψηλή διαθεσιμότητα συλλογής: Η λύση παρέχει επιλογές για υψηλή διαθεσιμότητα αναφορικά με τη συλλογή αρχείων καταγραφής χωρίς την ανάγκη πρόσθετου υλικού.	ΝΑΙ		
45	Επεκτασιμότητα στη διαχείριση αρχείων καταγραφής: Η λύση πρέπει να παρέχει τη δυνατότητα επέκτασης σε μεγαλύτερα περιβάλλοντα και την ένταξη πρόσθετων πηγών περιστατικών χωρίς να απαιτείται επιπλέον εξοπλισμός.	ΝΑΙ		
46	Η λύση δεν απαιτεί εγκατάσταση agent στα συστήματα υπό	ΝΑΙ		

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	<p>παρακολούθηση για τη συλλογή των αρχείων καταγραφής (logs).</p> <p>Εφόσον η προσφερόμενη λύση απαιτεί agent να αναφερθούν οι πιθανές επιπτώσεις σε υπολογιστικούς πόρους, ανά τύπο συστήματος μέσω αναφορών σε επίσημα τεχνικά εγχειρίδια του κατασκευαστή. Να αναφερθεί το επίπεδο πρόσβασης/δικαιώματα που θα απαιτείται στα διάφορα συστήματα της ΕΔΥΤΕ ΑΕ (π.χ. Administrator) για την εγκατάσταση, παραμετροποίηση, αναβάθμιση και συντήρηση των agents εφόσον απαιτηθούν. Επίσης, να αναφερθούν τυχόν απαιτήσεις σε συστήματα και σε συμμετοχή προσωπικού της ΕΔΥΤΕ ΑΕ για την εγκατάσταση και λειτουργία της λύσης.</p>			
47	Επεξεργασία κατανεμημένων (distributed) περιστατικών: Η λύση πρέπει να συλλέγει αρχεία καταγραφής με κατανεμημένο (distributed) τρόπο, κατανέμοντας τις απαιτήσεις επεξεργασίας του συστήματος διαχείρισης αρχείων καταγραφής για εργασίες όπως φιλτράρισμα, συγκέντρωση, συμπίεση και κρυπτογράφηση	ΝΑΙ		
48	Η προσφερόμενη λύση θα παρέχει τη δυνατότητα διασύνδεσης και συλλογής αρχείων καταγραφής από όλα τα συστήματα και συσκευές συμπεριλαμβανομένων customized συστήματα και εφαρμογές. Οι οποίες υπηρεσίες απαιτούνται για την υλοποίηση υποστήριξης πρέπει να περιλαμβάνονται στην προσφερόμενη λύση.	ΝΑΙ		
49	Κατηγοριοποίηση δεδομένων περιστατικών: Η λύση κατηγοριοποιεί τα δεδομένα καταγραφής σε μια μορφή	ΝΑΙ		

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	αναγνώσιμη για να εξαλείψει την ανάγκη γνώσης αναγνωριστικών περιστατικών συγκεκριμένων προμηθευτών.			
50	Μείωση περιστατικών: Η λύση παρέχει τη δυνατότητα μείωσης των δεδομένων περιστατικών	ΝΑΙ		
51	Ασφαλής μεταφορά: Η λύση παρέχει κρυπτογραφημένη μετάδοση δεδομένων καταγραφής για όλων των ειδών της επικοινωνίας.	ΝΑΙ		
52	Παρακολούθηση Κατάστασης Συλλογής: Οποιαδήποτε αστοχία της υποδομής συλλογής περιστατικών εντοπίζεται άμεσα και να ενημερώνονται τα εμπλεκόμενα μέρη. Η παρακολούθηση της κατάστασης περιλαμβάνει τη δυνατότητα επιβεβαίωσης ότι οι αρχικές πηγές εξακολουθούν να αποστέλλουν περιστατικά	ΝΑΙ		
53	Εύκολη και γρήγορη αναζήτηση ανάμεσα στα αποθηκευμένα δεδομένα καταγραφής και παραγωγή σχετικών αναφορών με εφαρμογή ειδικών φίλτρων.	ΝΑΙ		
54	Ο προσφερόμενος αριθμός έτοιμων διαθέσιμων κανόνων συσχέτισης είναι επαρκής για την άμεση ανάδειξη σημαντικών θεμάτων ασφάλειας της υποδομής και καλύπτει όλες τις κατηγορίες των κατηγοριών πλαισίων ασφαλείας.	ΝΑΙ		
55	Δημιουργία κανόνων συσχέτισης χρησιμοποιώντας ως βάση τους έτοιμους κανόνες που παρέχει η λύση. Περιγράψτε την προσφερόμενη προσέγγιση.	ΝΑΙ		
56	Λεπτομερής εξέταση των γεγονότων καταγραφής που προκαλούν την ενεργοποίηση ενός κανόνα, με επιλογή γραφικής αναπαράστασης της σειράς των γεγονότων.	ΝΑΙ		

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Περιγράψτε την προσφερόμενη λύση.			
57	Η προσφερόμενη υπηρεσία θα προσφέρει δυνατότητα δημιουργίας και αποστολής ειδοποιήσεων (alerts) σε καθορισμένους χρήστες, μέσω εξειδικευμένης κονσόλας.	ΝΑΙ		
58	Η παραγωγή alerts γίνεται με βάση τη συχνότητα και τον χρόνο εμφάνισης κάποιου γεγονότος, καθώς επίσης και όταν κάποιος κανόνας (time, term) πληρείται.	ΝΑΙ		
59	Η προσφερόμενη υπηρεσία προσφέρει εγγενής (native) δυνατότητα ενσωμάτωσης στην υπηρεσία των cloud υποδομών και τεχνολογιών ασφάλειας του οικοσυστήματος της Microsoft, τις οποίες διαθέτει η ΕΔΥΤΕ ΑΕ. Διευκρινίστε αν για το πιο πάνω θα απαιτείται επιπλέον οικονομική επιβάρυνση για της ΕΔΥΤΕ ΑΕ.	ΝΑΙ		
60	Ανάλυση Αρχείων Καταγραφής σε όλο το Περιβάλλον:	ΝΑΙ		
61	Η προσφερόμενη πλατφόρμα θα πρέπει να προσφέρει δυνατότητες καταγραφής και ανάλυσης πληροφοριών που προέρχονται τόσο από τη δικτυακή κίνηση όσο και από καταγραφές σε αρχεία logs σε εφαρμογές on premise και στο cloud σε μία ενιαία πλατφόρμα.	ΝΑΙ		
62	Αριθμός ελεγχόμενων συσκευών και συστημάτων σε τακτά χρονικά διαστήματα τόσο εσωτερικά στο περιβάλλον όσο και από το εξωτερικό περιβάλλον (περιμετρικά).	>300 συσκευές		
63	Η λύση θα πρέπει να ανιχνεύει αδυναμίες σε επίπεδο λειτουργικών συστημάτων, υπηρεσιών, δικτύου,	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	τερματικών, Web Εφαρμογών, και Cloud συστημάτων.			
64	Ως μέρος της λύσης θα πρέπει να είναι και η παραγωγή διαφορετικών τύπων αναφορών για διαφορετικού τύπου παραλήπτες προς τους διαχειριστές της υποδομής, καθώς και συνοπτικές αναφορές υψηλού επιπέδου προς τη διοίκηση (highlevelexecutive reports).	ΝΑΙ		
65	Ο ανάδοχος θα πρέπει να παρέχει ως υπηρεσία την διαχείριση αδυναμιών με αυτοματοποιημένο εργαλείο λογισμικού και χρήση ροών εργασιών (workflows) το οποίο θα προσφέρει τη δυνατότητα κεντροποιημένης διαχείρισης. Η συγκεκριμένη υπηρεσία θα χρησιμοποιείται με σκοπό τη διαχείριση όλων των αδυναμιών οι οποίες έχουν εντοπιστεί οριζόντια σε όλη την ΕΔΥΤΕ ΑΕ. Η διαχείριση θα καλύπτει όλο τον κύκλο ζωής των αδυναμιών, από τη στιγμή της αναγνώρισης μέχρι και τη διαχείριση των κινδύνων που απορρέουν από αυτές.	ΝΑΙ		
66	Η προσφερόμενη υπηρεσία μέσω κατάλληλης πλατφόρμας θα πρέπει να περιλαμβάνει μηχανισμό ροής εργασιών με καθορισμένους ρόλους το οποίο διαχειρίζεται αδυναμίες και θα τις αναθέτει ως δραστηριότητες στους κατάλληλους Υπεύθυνους Συστημάτων για τις απαραίτητες ενέργειες διαχείρισης των σχετικών κινδύνων.	ΝΑΙ		
67	Η προσφερόμενη υπηρεσία μέσω κατάλληλης πλατφόρμας θα πρέπει να παρέχει τη δυνατότητα να ομαδοποιεί τις αδυναμίες κατά προτεραιότητα, σύμφωνα με σαφώς ορισμένα χαρακτηριστικά και θα παρέχει τη δυνατότητα της εξαγωγής των δεδομένων που	ΝΑΙ		

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	σχετίζονται με τις αδυναμίες σε διάφορες μορφές.			
68	Η προσφερόμενη υπηρεσία μέσω κατάλληλης πλατφόρμας θα πρέπει να υποστηρίζει τη δημιουργία αναφορών με δυνατότητα οπτικοποίησης των συσχετίσεων αλλά και περαιτέρω λεπτομερούς ανάλυσης των δεδομένων των αδυναμιών.	ΝΑΙ		
69	Η προσφερόμενη υπηρεσία μέσω κατάλληλης πλατφόρμας θα πρέπει υποστηρίζει μηχανισμούς/ διαδικασίες όπως υπενθυμίσεις/ ενημερώσεις σε μορφή e-mail των δραστηριοτήτων που έχουν ανατεθεί στους Υπεύθυνους. Ακόμη, θα υποστηρίζει μηχανισμό ελέγχου/ καταγραφής καθώς και τις σχετικές λειτουργικές διαδικασίες.	ΝΑΙ		
70	Η πλατφόρμα θα πρέπει να παρέχει τη δυνατότητα εισαγωγής δεδομένων υφισταμένων ελέγχων τρωτότητας και παρείσδυσης. Επίσης, απαιτείται η υποστήριξη μηχανισμού αυθεντικοποίησης τεχνολογίας Single Sign-on, ο οποίος θα μπορεί να συνδέεται με την λίστα χρηστών της ΕΔΥΤΕ ΑΕ (LDAP, Active Directory).	ΝΑΙ		
71	Το 24x7 SLA διάρκειας 36 μηνών είναι μέρος της σύμβασης και θα παρακολουθείται. Το SLA θα πρέπει να περιλαμβάνει πλήρη υπηρεσίες υποστήριξης της προσφερόμενης λύσης.	ΝΑΙ		
72	Η προσφερόμενη λύση θα πρέπει να παρέχει την αξιολόγηση όλων των περιστατικών από έμπειρους αναλυτές και κλιμάκωση μόνο των πραγματικών περιστατικών στα προκαθορισμένα όρια παροχής επιπέδου υπηρεσιών (SLA)	ΝΑΙ		

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
73	Η κλιμάκωση των περιστατικών θα πρέπει πάντα να συνοδεύεται με περιγραφή συμβάντος, τα συστήματα που επηρεάζονται, τους δυνητικούς κινδύνους για την ΕΔΥΤΕ ΑΕ και προτάσεις για την διαχείριση του κινδύνου	NAI		
74	Η προσφερόμενη λύση θα πρέπει να παρέχει την ανάλυση για τον εντοπισμό της προέλευσης των απειλών, τον μετριασμό τους, την έναρξη μέτρων για την πρόληψη της επανεμφάνισης.	NAI		
75	Η προσφερόμενη λύση θα πρέπει να παρέχει την συνεχή βελτιστοποίηση των περιπτώσεων χρήσης (usecases), ανάπτυξη νέων usecases, διαχείρισης απόδοσης και προτάσεις για την συνεχή βελτίωση της υπηρεσίας	NAI		
76	Η προσφερόμενη λύση θα πρέπει να ενσωματώνει ένα εγγενές εργαλείο διαχείρισης συμβάντων/ έκδοσης αναφορών (Tickets) . Η προσφερόμενη λύση θα πρέπει επίσης να ενσωματωθεί στο εργαλείο διαχείρισης συμβάντων/ εισιτηρίων της ΕΔΥΤΕ ΑΕ.	NAI		
77	Η προσφερόμενη λύση θα πρέπει να περιλαμβάνει σχετικές υπηρεσίες εκπαίδευσης (να αναφερθούν οι προσφερόμενες ώρες εκπαίδευσης και το περιεχόμενο αυτής).	NAI		
78	Η προσφερόμενη λύση θα πρέπει να είναι σε θέση να συλλέγει αρχεία καταγραφής από οποιονδήποτε αριθμό φυσικών τοποθεσιών, όπως αυτό θα υπαγορεύεται από την ΕΔΥΤΕ ΑΕ, χωρίς καμία επίπτωση στο κόστος της άδειας.	NAI		
79	Η προσφερόμενη λύση θα πρέπει να είναι σε θέση να διασυνδεθεί με το ΝΟCτης ΕΔΥΤΕ ΑΕ και τα	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	συστήματα του με σκοπό τη συσχέτιση γεγονότων και τον εντοπισμό περιστατικών ασφάλειας.			
80	Οι άδειες της προσφερόμενης πλατφόρμας που θα χρησιμοποιηθούν στην υπηρεσία SOCaaS θα ανήκουν στον Φορέα	ΝΑΙ		

7.2.4.2 Λύση DDOS

A.A	Προδιαγραφή	Απαίτηση	Απάντηση	Παραπομπή
1.	Να περιγραφεί η γενική προσέγγιση της προτεινόμενης on premise και Cloud-based λύσης προστασίας από κατανεμημένες επιθέσεις άρνησης υπηρεσίας (DDoS) και με ποιο τρόπο προστατεύει την επιχειρησιακή συνέχεια (business continuity) και τη διαθεσιμότητα των υπηρεσιών (Δικτυακή δομή -Website - Portal) τους από τις επιθέσεις DDoS	ΝΑΙ		
2.	Αποφυγή Inbound (Εντός εσωτερικού δικτύου) και Outbound απειλές (Από εξωτερικά δίκτυα). Ελάχιστο network traffic το οποίο μπορεί να προστατευτεί από την cloud DDoS λύση ≥ 200 Mbps. Να περιγραφεί αναλυτικά.	ΝΑΙ		
3.	Αποφυγή των γνωστών (μέχρι σήμερα) τύπων DDoS επιθέσεων (DNS, NTP, Chargen, SSDP, SNMP, Portmap, MSSQL, SYN, Slow Rate Attacks, SIP, Volumetric, RFC) amplification attacks, TCP, UDP State exhaustion. Να περιγραφούν άλλοι τύποι επιθέσεων που μπορούν να αποτραπούν και παρατεθούν στοιχεία (π.χ. από ENISA ή άλλο διεθνή οργανισμό).	ΝΑΙ		

4.	Ελάχιστο inspected throughput	<u>200</u> Mbps		
5.	Η συσκευή προστασίας DDoS που θα εγκατασταθεί θα πρέπει να παρέχει τη δυνατότητα μετριασμού (mitigation) 6 Gbps, ανεξάρτητα από την άδεια χρήσης.	NAI		
6.	Η συσκευή προστασίας DDoS θα πρέπει να παρέχει τη δυνατότητα αναβάθμισης της άδειας χρήσης για προστασία έως και 5 Gbps καθαρής κίνησης χωρίς την ανάγκη αντικατάστασης υλικού. Αρχικά να προσφερθεί με άδεια για 2Gbps aggregate καθαρή κίνηση	NAI		
7.	Η προσφερόμενη λύση θα πρέπει να παρέχει τη δυνατότητα application layer και state exhausting attacks, εκτός από τις προαναφερόμενες.	NAI		
8.	Η προσφερόμενη λύση θα πρέπει να παρέχει τη δυνατότητα IPV4/IPV6 Header checks, fragmentation checks, layer 4 checks. Να περιγραφούν οι δυνατότητες οι οποίες περιλαμβάνονται.	NAI		
9.	Η DDoS συσκευή που θα προσφερθεί θα πρέπει να εγκατασταθεί στο Data center της ΗΔΙΚΑ	NAI		
10.	Η προτεινόμενη συσκευή θα πρέπει να υποστηρίζει 6 copper Ethernet θύρες και 2xSFP+	NAI		
11.	Η προτεινόμενη συσκευή θα πρέπει να μπορεί με υποστηρίζει λειτουργία IP mode και transparent λειτουργία	NAI		
12.	Η προτεινόμενη DDoS συσκευή θα πρέπει να είναι εξειδικευμένη συσκευή για DDoS Και όχι firewall ή load balancer	NAI		
13.	Η προτεινόμενη συσκευή θα πρέπει να υποστηρίζει τη αντιμετώπιση Day Burst Attacks με υπογραφή η οποία δημιουργείται αυτόματα.	nAI		
14.	<ul style="list-style-type: none"> Η προτεινόμενη συσκευή θα πρέπει να υποστηρίζει μηδενικό χρόνο για τον μετριασμό των 	NAI		

	επιθέσεων Burst, ξεκινώντας από το πρώτο χτύπημα burst.			
15.	Η προτεινόμενη συσκευή θα πρέπει να παρέχει προστασίας behavioral-DoS χρησιμοποιώντας υπογραφές πραγματικού χρόνου που δημιουργούνται με βάση πολλαπλές παραμέτρους σε κεφαλίδες πακέτων L3 έως L7, αντί για αποκλεισμό διεύθυνσης IP προέλευσης ή περιορισμό ρυθμού	NAI		
16.	Η προτεινόμενη συσκευή θα πρέπει να υποστηρίζει behavioral DDoS προστασία για DNS τόσο σε TCP και UDP.	NAI		
17.	Η προτεινόμενη συσκευή θα πρέπει να υποστηρίζει bahavioral based application layer HTTP DDoS προστασία	NAI		
18.	Η προτεινόμενη συσκευή θα πρέπει να υποστηρίζει προστασία από zero day επιθέσεις	NAI		
19.	Η προτεινόμενη συσκευή θα πρέπει να υποστηρίζει mitigation SLA 18 sec από τον εντοπισμό	NAI		
20.	Η προτεινόμενη συσκευή θα πρέπει να υποστηρίζει IPS.	NAI		
21.	Η προτεινόμενη συσκευή θα πρέπει να υποστηρίζει εβδομαδιαίες ενημερώσεις για signatures feeds για προστασία από νέες επιθέσεις	NAI		
22.	<ul style="list-style-type: none"> Η προτεινόμενη συσκευή θα πρέπει να υποστηρίζει χιλιάδες υπογραφές ταυτόχρονα 	NAI		
23.	Η προτεινόμενη συσκευή θα πρέπει να υποστηρίζει προστασία σε επίπεδο SSL/TLS	NAI		
24.	Η προσφερόμενη λύση θα πρέπει να έχει τη δυνατότητα δημιουργίας Protection Groups. Κάθε PG να μπορεί να αντιστοιχεί σε διαφορετική υποδομή του δικτύου ή server.	NAI		
25.	Η on-premise συσκευή θα πρέπει να έχει τη δυνατότητα εκμάθησης κανονικών επιπέδων κυκλοφορίας και να προτείνει κατάλληλα όρια	NAI		

	προστασίας για κάθε υπό παρακολούθηση στοιχείο.			
26.	<p>Να δοθεί αναλυτική περιγραφή της αρχιτεκτονικής και της λειτουργικότητας της προσφερόμενης λύσης με τη λογική ότι υφίσταται ήδη firewall.</p> <p>Να αναλυθεί το γεγονός ότι η προσφερόμενη λύση DDoS προστατεύει από άλλου τύπου επιθέσεις σε περίπτωση που το υφιστάμενο firewall παρέχει βασικές IPS/IDS λειτουργίες.</p>	NAI		
27.	<p>Η προτεινομένη συσκευή θα πρέπει να παρέχει SSL προστασία με τους παρακάτω τρόπους</p> <ul style="list-style-type: none"> • Keyless SSL Protection (χωρίς certificate και χωρίς decryption) • First Request SSL Protection (με decryption Μόνο του πρώτου https request και μόνο κατά τη διάρκεια επίθεσης που εντοπίστηκε μέσω IP reputation) • Selective Full SSL Protection (με πλήρη decryption κατά τη διάρκεια επίθεσης και για τις ύποπτες συνδέσεις) • Full SSL Protection 	NAI		
28.	Θα πρέπει να υποστηρίζονται οι ακόλουθοι τρόποι λειτουργίας (Modes), κατ' ελάχιστον: inline, SPAN.	NAI		
29.	Η on-premise συσκευή θα πρέπει να υποστηρίζει τις ενσωματωμένες επιλογές παράκαμψης για αστοχία ανοίγματος και αποτυχία κλεισίματος.	NAI		
30.	Η προσφερόμενη λύση θα πρέπει να παρουσιάζει τις πληροφορίες σε ένα φιλικό προς το χρήστη περιβάλλον (GUI).	NAI		

31.	Η προσφερόμενη λύση θα πρέπει παρέχει τη δυνατότητα whitelisting και blacklisting IP διευθύνσεων (Δυνατότητα IPV4 και IPV6.	ΝΑΙ		
32.	Η προσφερόμενη λύση θα πρέπει να συνοδεύεται από τις απαραίτητες άδειες λειτουργίας οι οποίες θα πρέπει να αφορούν τόσο το λειτουργικό σύστημα, εάν αυτό απαιτεί ξεχωριστή άδεια χρήσης όσο και το λογισμικό. Όλες οι άδειες θα βαρύνουν τον ανάδοχο	ΝΑΙ		
33.	Η Υποστήριξη του λογισμικού και οι αναβαθμίσεις σε νεότερες εκδόσεις του θα πρέπει παρέχονται από τον ανάδοχο στο πλαίσιο του έργου.	ΝΑΙ		
34.	Υποστήριξη IPv4 και IPv6 και prefix matching.	ΝΑΙ		
35.	Υποστήριξη τουλάχιστον SNMP v2 & v3.	ΝΑΙ		
36.	Η προσφερόμενη λύση θα πρέπει να υποστηρίζει το RESTful API για τη διαμόρφωση του στοιχείου εσωτερικής εγκατάστασης και την παρακολούθηση του στοιχείου cloud.	ΝΑΙ		
37.	Δυνατότητα για SSL. Να αναφερθούν οι SSL decryption επιλογές	ΝΑΙ		
38.	Να αναφερθούν τα πρωτόκολλα που χρησιμοποιούνται την προστασία από DDOS επιθέσεις.	ΝΑΙ		

39.	Η on-premise συσκευή θα πρέπει να υποστηρίζει από τον κατασκευαστή ενημερώσεις για DDos και botnet intelligence.	NAI		
40.	Η On premise συσκευή θα πρέπει να υποστηρίζει εισαγωγή threat feeds (pm IP reputation, active attackers) του κατασκευαστή.	NAI		
41.	Γραφικό περιβάλλον για παρακολούθηση και παραμετροποίηση.	NAI		
42.	Η προσφερόμενη λύση θα πρέπει να έχει τη δυνατότητα για notifications SNMP trap, syslog, email.	NAI		
43.	Να αναφερθούν οι υποστηριζόμενοι φυλλομετρητές (browsers).	NAI		
44.	Η προσφερόμενη λύση θα πρέπει να παρέχει δυνατότητα αναγγελίας συμβάντος μέσω ηλεκτρονικού ταχυδρομείου (email) για σοβαρά συμβάντα, συστημικά συμβάντα ή άλλα θέματα κίνησης.	NAI		
45.	Η προσφερόμενη λύση θα πρέπει να παράγει μηνύματα συμβάντων εξαιτίας λάθους του συστήματος/ κατάσταση υπερφόρτωσης (πχ. Λάθος επεξεργασίας, φόρτωση CPU, υψηλή κατανάλωση μνήμης.)	NAI		
46.	Η προσφερόμενη λύση θα πρέπει να παρέχει αναφορές real-time για πληροφορίες IPV4 και IPV6, total traffic, passed/ blocked traffic, top URL, domain, κλπ.	NAI		
47.	Η προσφερόμενη λύση θα πρέπει να εξαγάγει δεδομένα σε πολλαπλές μορφές συμπεριλαμβανομένου των παρακάτω δημοφιλών τύπων αρχείων: CSV, XML, PDF, etc.	NAI		
48.	VLAN Tagging support (IEEE 802.1q)	NAI		
49.	Η προσφερόμενη λύση θα πρέπει να δημιουργεί αναγγελίες συμβάντων (alerts) όταν μία τιμή έχει ξεπεράσει το κατώφλι, δείχνοντας: συνολικό traffic, το ποσοστό αποκλεισμένου και το botnet traffic	NAI		
50.	Η προσφερόμενη λύση θα πρέπει να παρέχει μετριάσμο προστασίας	NAI		

	OnDemand / AlwaysON έναντι ογκομετρικών (volumetric) επιθέσεων σε πραγματικό χρόνο.			
51.	Η προσφερόμενη λύση θα πρέπει να μπορεί να ανιχνεύσει και να μετριάσει DDoS επιθέσεις από επίπεδο 3 στο επίπεδο 7 του OSI μοντέλου. Στην περίπτωση της Cloud υπηρεσίας η συνολική χωρητικότητα των mitigation κέντρων να είναι 10Tbps.	NAI		
52.	Να περιγράφει ο τρόπος με τον οποίο θα ελαχιστοποιηθεί ο κίνδυνος τοπικής συμφόρησης κάθε Mitigation κέντρο της cloud υπηρεσίας να υποστηρίζει τουλάχιστον 200gbps.	NAI		
53.	Η υπηρεσία cloud θα πρέπει να υποστηρίζει περιοδικές δοκιμές από άκρη σε άκρη της υπηρεσίας, χωρίς επιπλέον κόστος.	NAI		
54.	Η προσφερόμενη cloud λύση θα πρέπει να προστατεύει από volumetric και application DDoS επιθέσεις.	NAI		
55.	Η προσφερόμενη λύση θα πρέπει να βασίζεται στο cloud και σε υβριδικό μοντέλο (λύση που ενσωματώνει εντοπισμό και μετριασμό on premise εγκατάστασης με volumetric καθαρισμό επιθέσεων βάσει cloud)	NAI		
56.	Η προσφερόμενη cloud DDOS λύση θα πρέπει να ενσωματώνεται με παρόχους Public Cloud για αυτόματη ανίχνευση και εκτροπή στο Cloud Scrubbing Center	NAI		
57.	Η προσφερόμενη λύση cloud DDoS θα πρέπει να αξιοποιεί προσφερόμενη On premise λύση του ίδιου κατασκευαστή	NAI		
58.	Η προσφερόμενη cloud DDoS λύση θα πρέπει να υποστηρίζει SSL encrypted επιθέσεις.	NAI		
59.	Η προσφερόμενη cloud DDoS λύση θα πρέπει να παρέχει προστασία χωρίς να κάνει decrypt πλήρως όλη την κίνηση	NAI		
60.	Η προσφερόμενη cloud DDoS λύση θα πρέπει να είναι πιστοποιημένη σύμφωνα με τα παρακάτω πρότυπα:	NAI		

	<ul style="list-style-type: none"> ○ ISO/IEC 27017:2015 (Information Security for Cloud Services) ○ ISO/ IEC 27018:2014 (Information Security Protection of Personally Identifiable Information (PII) in Public Clouds). ○ PCI-DSS v3.1 (Payment Card Industry Data Security Standard) ○ ISO/IEC 27001:2013 (Information Security Management Systems) ○ ISO/IEC 27032:2012 (Security Techniques -- Guidelines for Cybersecurity) ○ ISO 28000:2007 (Supply Chain Security Management System) ○ ISO 9001:2015 (Quality Management System) ISO 14001:2015 (Environment Management System) 			
61.	Η προσφερόμενη λύση θα πρέπει να είναι ανεξάρτητη του υφιστάμενου παρόχου τηλεπικοινωνιών.	NAI		
62.	Να περιγραφεί ο τρόπος με τον οποίο η προσφερόμενη λύση θα προκαλέσει μετριάσεις On premise και με ποιον τρόπο θα αναδρομολογεί κίνηση στο cloud.	NAI		
63.	Η λύση θα πρέπει να υποστηρίζει εκτροπή κίνησης βάση BGP Και DNS	NAI		
64.	Η προσφερόμενη λύση θα πρέπει να υποστηρίζει πολυεπίπεδη προστασία DDoS με σηματοδότηση από μηχανή σε μηχανή από εσωτερική συσκευή μετριάσεων DDoS στο cloud όταν απαιτείται μετριάσεις. Ο χρήστης να μπορεί να διαμορφώσει τη σηματοδότηση χειροκίνητα ή αυτόματα, όπως επιθυμεί.	NAI		
65.	Η υπηρεσία θα πρέπει να μπορεί να παρακολουθεί την εσωτερική συσκευή μετριάσεων DDoS μέσω heartbeat και να ανιχνεύει εάν αυτή η συσκευή δεν είναι πλέον προσβάσιμη.	NAI		

66.	Να περιγραφεί ο τρόπος με τον οποίο η προσφερόμενη λύση θα εκτρέπει την κίνηση.	NAI		
67.	Να περιγραφεί ο τρόπος με τον οποίο η προσφερόμενη λύση θα επαναφέρει την κυκλοφορία	NAI		
68.	Η λύση θα πρέπει να υποστηρίζει asymmetric traffic και symmetric traffic for DDOS τεχνικές μετριάσμού ανάλογα με το μοντέλο ανάπτυξης.	NAI		
69.	Η προσφερόμενη λύση να προστατεύει από DNS flood επιθέσεις			
70.	Η προσφερόμενη λύση θα πρέπει να εντοπίζει και προστατεύει από όλα τα zero-day DNS floods	NAI		
71.	Η λύση πρέπει να μπορεί να προστατεύει από οριζόντιες (all IP and same IP scan) και κατακόρυφες (σα καταστάσεις "σάρωσης".	NAI		
72.	Η λύση πρέπει να μπορεί να προστατεύει από τις ακόλουθες καταστάσεις flood: <ul style="list-style-type: none"> • UDP • TCP ICMP	NAI		
73.	Η λύση θα πρέπει να υποστηρίζει την ανίχνευση της συμπεριφοράς και τον μετριάσμό με μεγάλη ακρίβεια κατά τυχαίων sub-domain flood (για παράδειγμα: Mirai DNS Water Torisation)	NAI		
74.	Η προσφερόμενη λύση θα πρέπει να παρέχει τη δυνατότητα αποκλεισμού της κυκλοφορίας βάσει συγκεκριμένων υπογραφών botnet / επιθέσεων και / ή δακτυλικών αποτυπωμάτων και / ή στην ανάλυση συμπεριφοράς και τη μηχανική μάθηση	NAI		
75.	Η προσφερόμενη λύση θα πρέπει να επιτρέπει την προ-διαμόρφωση προτύπων μετριάσμού για τους πελάτες κατά την αρχική παροχή βάσει των λεπτομερειών των υπηρεσιών που προστατεύονται και άλλων συγκεκριμένων πληροφοριών για τους πελάτες.	NAI		

	Οι χρήστες να έχουν τη δυνατότητα να ενημερώνουν αυτά τα πρότυπα περιοδικά. Αυτά τα πρότυπα πρέπει να εφαρμόζονται σε μετριάσμούς όταν ξεκινά ένας μετριάσμός.			
76.	Η προσφερόμενη λύση θα πρέπει να παρέχει πληροφορίες σχετικά με τον αριθμό των κέντρων μετριάσμού που περιλαμβάνονται στη λύση και τη γεωγραφική θέση των κέντρων μετριάσμού.	ΝΑΙ		
77.	Η προσφερόμενη λύση θα πρέπει να παρέχει μια ειδική πύλη (portal) η οποία να περιλαμβάνει πληροφορίες σε πραγματικό χρόνο σχετικά με την κυκλοφορία που πέρασε, την κυκλοφορία η οποία μειώθηκε κατά τη διάρκεια συμβάντων μετριάσμού, και να επιτρέπει στο χρήστη να επιλέξει τη χρονική περίοδο και τα δεδομένα τα οποία τον αφορούν.	ΝΑΙ		
78.	Η υπηρεσία μετριάσμού cloud θα πρέπει να μην απαιτεί χρέωση ρύθμισης.	ΝΑΙ		
79.	Η λύση cloud θα πρέπει περιλαμβάνει 24/7 SOC πρόσβαση χωρίς επιπλέον κόστος.	ΝΑΙ		
80.	Ο Ανάδοχος ν θα πρέπει α παρέχει τα κάτωθι: xi. Σεμινάρια κατασκευαστή. xii. Οδηγίες χρήσης και γνώση των προϊόντων. xiii. Τεκμηρίωση της προσφοράς. xiv. Γνωσιακή βάση με γνωστά προβλήματα λογισμικού / υλικού και τρόπους αντιμετώπισής τους. xv. Ενημέρωση για επερχόμενες αλλαγές (σφάλματα, επιδιορθώσεις).	ΝΑΙ		
81.	Η προσφερόμενη λύση θα πρέπει να επιτρέπει παραμετροποίηση των δικαιωμάτων των ομάδων Χρηστών (User Account Groups).	ΝΑΙ		
82.	Η προσφερόμενη λύση θα πρέπει να διαθέτει Menu κεντρικής διαχείρισης	ΝΑΙ		



	συμβάντων και σφαλμάτων και δυνατότητα αποστολής ειδοποιήσεων μέσω SNMP, Email, syslog.			
83.	Η διαχείριση της λύσης θα πρέπει να γίνεται μέσω ενός αποκλειστικού συστήματος διαχείρισης που ανήκει στον ίδιο προμηθευτή της ίδιας της συσκευής.	ΝΑΙ		
84.	<p>Η ολοκληρωμένη λύση διαχείρισης πρέπει να υποστηρίζει συγκεκριμένα τα ακόλουθα:</p> <ul style="list-style-type: none">• κεντρική διαχείριση των διαμορφώσεων συστήματος των συσκευών Hw (Διαχείριση Διαμόρφωσης).• Συγκεντρωτικό καθορισμό και διανομή των Πολιτικών Ασφαλείας σε διαχειριζόμενες συσκευές.• κεντρική συλλογή και συσχέτιση πληροφοριών (καταγραφής) διαχειριζόμενων συσκευών.• εκτέλεση της εγκληματολογικής ανάλυσης των πληροφοριών που συλλέγονται (ημερολόγιο).• Μηχανισμό εξουσιοδότησης διαφορετικών προφίλ διαχείρισης που βασίζονται σε ρόλους (RBAC - Role Based Access Control). <p>δημιουργία προκαθορισμένων ή προσαρμοσμένων αναφορών που σχετίζονται με τον διαχειριζόμενο εξοπλισμό. Οι αναφορές που δημιουργούνται πρέπει να εξαχθούν σε μορφές "CSV", "PDF" ή "XML".</p>	ΝΑΙ		
85.	<p>Σε περίπτωση σφάλματος (bug) στο λογισμικό, η πλήρης αποκατάσταση του σφάλματος με κατάλληλη διορθωτική έκδοση (patch/fix) θα πρέπει να ολοκληρώνεται εντός μιας (1) ημερολογιακής εβδομάδας.</p> <p>Να περιγραφεί η διαδικασία που θα πρέπει ακολουθείται για την αποκατάσταση των προβλημάτων και να αναφερθεί το μέσο και μέγιστο χρόνο αποκατάστασης.</p>	ΝΑΙ		

86.	Η προσφερωμενη λύση θα πρέπει να προσφερθεί με subscription και υποστηρίζει για 36 μήνες.	NAI		
87.	Η προσφερόμενη λύση θα πρέπει να διαθέτει κεντρικό μενού με εύκολη πλοήγηση προς όλες τις πληροφορίες και τις αναφορές.	NAI		
88.	Η προσφερόμενη λύση θα πρέπει να έχει τη δυνατότητα προγραμματισμού για ημερήσιες, εβδομαδιαίες ή μηνιαίες αναφορές και δυνατότητα είτε παρακολούθησης από αντίστοιχη ιστοσελίδα είτε εξαγωγής τους σε αρχείο XML, PDF, CSV.	NAI		

7.2.4.3 Υπηρεσίες ανάκαμψης από καταστροφή και λήψης αντιγράφων ασφαλείας

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Το τμήμα Δημοσίου Υπολογιστικού Νέφους (PublicCloud) της προσφερόμενης λύσης θα πρέπει να παρέχει υπηρεσίες φιλοξενίας τύπου Cloud/Hosting, με υπηρεσίες υποδομής ως υπηρεσία (IaaS) και πλατφόρμας ως υπηρεσία (PaaS) από έναν πάροχο Δημοσίου Υπολογιστικού Νέφους.	NAI		
	Η Αναθέτουσα Αρχή θα μπορεί να επιλέξει σε ποια γεωγραφική περιοχή (region) θα φιλοξενηθούν οι επιλεγόμενες υπηρεσίες.	NAI		
	Ο πάροχος θα πρέπει να μπορεί να διαθέτει τις υπηρεσίες του από δύο τουλάχιστον γεωγραφικές περιοχές (regions), εντός Ευρωπαϊκής Ένωσης, με ελάχιστη απόσταση 500 χιλιομέτρων μεταξύ τους, τα οποία θα μπορούν να χρησιμοποιηθούν για την υλοποίηση υπηρεσιών που απαιτούν τον ύψιστο βαθμό υψηλής διαθεσιμότητας με χαρακτηριστικά ανάνηψης από καταστροφή (DisasterRecovery). Να αναφερθούν οι χώρες φιλοξενίας.	NAI		
	Το τμήμα του δημοσίου υπολογιστικού νέφους (PublicCloud) της προσφερόμενης λύσης θα επιτρέπει τη διαμόρφωση υπηρεσιών υψηλής διαθεσιμότητας (highavailability) και ανάκαμψης από καταστροφή (DisasterRecovery).	NAI		
	Απαιτείται η ύπαρξη μηχανισμού παρακολούθησης και ελέγχου της κατάστασης (health) των χρησιμοποιούμενων πόρων σε συνάρτηση με την κατάσταση της υποδομής του παρόχου. Ο μηχανισμός να διαθέτει δυνατότητα μηχανισμού αποστολής ειδοποιήσεων κατά μόνος ή σε ομάδες, email, webhook βάσει κανόνων που τίθενται από το διαχειριστή.	NAI		
	Οι όροι SLA των υπηρεσιών να είναι δημοσιευμένοι στην επίσημη ιστοσελίδα του παρόχου. Να αναφερθεί η σχετική ιστοσελίδα.	NAI		

Α/ Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣ Η	ΑΠΑΝΤΗ ΣΗ	ΠΑΡΑΠΟΜ ΠΗ
	Για λόγους διαφάνειας και ελέγχου συμμόρφωσης με τα παρεχόμενα επίπεδα SLA η τρέχουσα κατάσταση λειτουργίας του συνόλου των υπηρεσιών θα πρέπει να είναι δημόσια διαθέσιμη στο επίσημο ιστότοπο του παρόχου. Να αναφερθεί η σχετική ιστοσελίδα.	ΝΑΙ		
	Ο πάροχος να διαθέτει δωρεάν υπηρεσίες για τη συνολική διακυβέρνηση – governancetων πόρων που θα αξιοποιηθούν από τον φορέα λειτουργίας. Κατ'ελάχιστο απαιτούνται: <ul style="list-style-type: none"> • δυνατότητα οργάνωσης και ελέγχου πρόσβασης στο σύνολο πολλαπλών λογαριασμών και συνδρομών • δυνατότητα διαμόρφωσης και εφαρμογής πολιτικών χρήσης των υπολογιστικών πόρων που περιλαμβάνονται σε λογαριασμούς και στις συνδρομές • καθορισμός πολλαπλών προϋπολογισμών με καθορισμό ορίων στο επιθυμητό επίπεδο εφαρμογής (score) πόρων και δυνατότητα ενημέρωσης διαχειριστών μέσω email εποπτεία και ανάλυση τρεχουσών χρεώσεων, ιστορικών χρεώσεων και πρόβλεψη της εξέλιξης τους	ΝΑΙ		
	Ο πάροχος να διαθέτει εγγενή μηχανισμό παροχής προτάσεων χωρίς επιπλέον κόστος, για βελτιστοποίηση της χρήσης των χρησιμοποιούμενων πόρων, στους τοείς της ασφάλειας, της διαθεσιμότητας, των επιδόσεων καθώς και του κόστους αυτών, κατά τις βέλτιστες πρακτικές του παρόχου υπολογιστικού νέφους.	ΝΑΙ		
	Να παρέχεται από τον πάροχο του δημοσίου υπολογιστικού νέφους ελεύθερα προσπελάσιμος επίσημος ιστότοπος με πληροφορίες, οδηγούς και εγχειρίδια χρήσης, ρυθμίσεις, συχνές ερωτήσεις και παραδείγματα κώδικα για το σύνολο των υπηρεσιών του. Να αναφερθεί η σχετική ιστοσελίδα.	ΝΑΙ		
	Να παρέχεται δωρεάν εκπαιδευτικό υλικό μέσω ηλεκτρονικής μάθησης σε επίσημο ιστότοπο του παρόχου με ενότητες στους εκάστοτε τομείς των υπηρεσιών υπολογιστικού νέφους. Να αναφερθεί η σχετική ιστοσελίδα.	ΝΑΙ		
	Πιστοποίηση σε ισχύ που να αποδεικνύει τη συμμόρφωση της λειτουργίας του παρόχου με το πρότυπο διασφάλισης ποιότητας ISO/IEC9001:2015. Να κατατεθεί αντίγραφο της πιστοποίησης.	ΝΑΙ		
	Πιστοποίηση σε ισχύ που να αποδεικνύει τη συμμόρφωση της λειτουργίας του παρόχου με το πρότυπο ασφάλειας ISO/IEC 27001:2013. Να κατατεθεί αντίγραφο της πιστοποίησης.	ΝΑΙ		
	Πιστοποίηση σε ισχύ που να αποδεικνύει τη συμμόρφωση της λειτουργίας του παρόχου με το πρότυπο ασφάλειας πληροφοριακών ελέγχων ISO/IEC 27017:2015. Να κατατεθεί αντίγραφο της πιστοποίησης.	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Πιστοποίηση σε ισχύ που να αποδεικνύει τη συμμόρφωση της λειτουργίας του παρόχου με το πρότυπο διασφάλισης της προστασίας προσωπικών δεδομένων ISO/IEC 27018:2019. Να κατατεθεί αντίγραφο της πιστοποίησης.	NAI		
	Πιστοποίηση σε ισχύ που να αποδεικνύει τη συμμόρφωση της λειτουργίας του παρόχου με το πρότυπο ιδιωτικότητας πληροφοριών ISO/IEC 27701:2019. Να κατατεθεί αντίγραφο της πιστοποίησης.	NAI		
	Πιστοποίηση σε ισχύ που να αποδεικνύει τη συμμόρφωση της λειτουργίας του παρόχου με το πρότυπο διασφάλισης της επιχειρησιακής συνέχειας ISO/IEC 22301:2019. Να κατατεθεί αντίγραφο της πιστοποίησης.	NAI		
	Πιστοποίηση σε ισχύ που να αποδεικνύει τη συμμόρφωση της λειτουργίας του παρόχου με το πρότυπο διαχείρισης υπηρεσιών πληροφοριακού συστήματος ISO/IEC 20000-1:2018	NAI		
	Συμμόρφωση της υποδομής του παρόχου κατά ServiceOrganizationControls (SOC) 1,2 και 3. Να κατατεθούν τα τρία σχετικά reports.	NAI		
	Συμμόρφωση της υποδομής του παρόχου κατά Payment Card Industry (PCI) Data Security Standards (DSS) έκδοση 3.2.1 - Level 1 . Να κατατεθεί η σχετική βεβαίωση.	NAI		
	Η υποδομή του παρόχου δημοσίου υπολογιστικού νέφους να διαθέτει benchmark με πρακτικές και προτάσεις καθοδήγησης, από το CenterforInternetSecurity (CIS) για την προστασία συστημάτων πληροφορικής ανεπτυγμένα στο δημόσιο υπολογιστικό νέφος έναντι κυβερνο-απειλών. Να κατατεθεί το σχετικό benchmark.	NAI		
	Το marketplace του παρόχου δημοσίου υπολογιστικού νέφους να διαθέτει ενισχυμένα -hardened- templates εικονικών μηχανών από το CenterforInternetSecurity (CIS).	NAI		
	Συμμόρφωση της λειτουργίας του παρόχου με το Cloud Control Matrix (CCM) του Cloud Security Alliance (CSA), με τη μορφή του Consensus Assessments Initiative Questionnaire (CAIQ) στην έκδοση 3.1 ή μεταγενέστερη. Να κατατεθεί το σχετικό αποδεικτικό αυτοαξιολόγησης (self assessment).	NAI		
	Πιστοποίηση σε ισχύ που να αποδεικνύει τη συμμόρφωση της λειτουργίας του παρόχου με το πρότυπο CSA-STAR του CloudSecurityAlliance (CSA). Να κατατεθεί αντίγραφο της πιστοποίησης.	NAI		
	Συμμόρφωση της υποδομής του παρόχου κατά EN 301 549. Να κατατεθεί το σχετικό αποδεικτικό.	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Οι υπηρεσίες του παρόχου θα πρέπει να είναι συμβατές με τον Κανονισμό (ΕΕ) 2016/679 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα (GDPR Regulation).	ΝΑΙ		
	Ο Πάροχος του Δημόσιου Υπολογιστικού Νέφους θα πρέπει να είναι μέλος του EU Data Centres Energy Efficiency CoC σύμφωνα με την λίστα που δημοσιεύεται στον παρακάτω σύνδεσμο: https://e3p.jrc.ec.europa.eu/node/575	ΝΑΙ		
	Να αναφερθούν άλλα στοιχεία και μέτρα που αναλαμβάνει ο πάροχος ως προς την ασφάλεια και την κανονιστική συμμόρφωση.	ΝΑΙ		
	Υπηρεσία εξυπηρέτησης εγγενών φορτίων τεχνολογίας VMware με υποστήριξη τεχνολογιών vCenter Server, vSAN, vSphere και NSX-T, στην υποδομή του παρόχου υπολογιστικού νέφους. Ο Πάροχος να αποτελεί εγκεκριμένο προμηθευτή VMware Cloud τεχνολογιών.	ΝΑΙ		
	Παροχή μηνιαίου SLA για την υπηρεσία εξυπηρέτησης εγγενών φορτίων τεχνολογίας VMware, τουλάχιστον 99.9%.	ΝΑΙ		
	Η υπηρεσία εξυπηρέτησης εγγενών φορτίων τεχνολογίας VMware να προσφέρει υψηλό επίπεδο ασφάλειας και προστασίας δεδομένων των χρηστών, με δυνατότητες Role-Based Access Control και αυθεντικοποίησης μέσω Single Sign On, αλλά και κρυπτογράφησης των καταχωρούμενων δεδομένων.	ΝΑΙ		
	Να προσφέρεται η δυνατότητα δικτύωσης στο περιβάλλον της υπηρεσίας εξυπηρέτησης εγγενών φορτίων τεχνολογίας VMware, τόσο από την τοπική υποδομή όσο και από το περιβάλλον υπολογιστικού νέφους.	ΝΑΙ		
	Να προσφέρεται η δυνατότητα ανάκαμψης από καταστροφή υφιστάμενης υποδομής VMware με χρήση VMware Site Recovery Manager (SRM) στην υπηρεσία εξυπηρέτησης εγγενών φορτίων τεχνολογίας VMware στο περιβάλλον υπολογιστικού νέφους μέσω αποκλειστικού κυκλώματος διασύνδεσης.	ΝΑΙ		
	Να προσφέρεται υπηρεσία αποκατάστασης φορτίων as-a-service από τον Πάροχο του Δημοσίου Υπολογιστικού Νέφους.	ΝΑΙ		
	Ο πάροχος της προσφερόμενης λύσης να αναφέρεται στη λίστα Leaders του φορέα αξιολόγησης Gartner στην κατηγορία Disaster Recovery as a Service (DRaaS).	ΝΑΙ		
	Μέσω της προσφερόμενης λύσης, να προσφέρεται προστασία υπολογιστικών συστημάτων από καταστροφή μέσω συνεχούς replication, διαδικασία μετάπτωσης μετά καταστροφή καθώς και επανάκαμψης και επαναλειτουργίας.	ΝΑΙ		

Α/ Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣ Η	ΑΠΑΝΤΗ ΣΗ	ΠΑΡΑΠΟΜ ΠΗ
	Να προσφέρεται η δυνατότητα αποκατάστασης καταστροφών για τις εικονικές μηχανές που λειτουργούν σε περιβάλλον εικονικοποίησης VMware, vSphere/vCenter έκδοσης τουλάχιστον 6.0, μέσω της αναπαραγωγής τους σε περιβάλλον δημοσίου υπολογιστικού νέφους του κατασκευαστή της προσφερόμενης λύσης.	ΝΑΙ		
	Να προσφέρεται η δυνατότητα αποκατάστασης καταστροφών για τις εικονικές μηχανές που λειτουργούν σε περιβάλλον εικονικοποίησης Hyper-V έκδοσης τουλάχιστον 2012 R2, μέσω της αναπαραγωγής τους σε περιβάλλον δημοσίου υπολογιστικού νέφους του κατασκευαστή της προσφερόμενης λύσης.	ΝΑΙ		
	Να προσφέρεται η δυνατότητα αποκατάστασης καταστροφών για τους φυσικούς διακομιστές Linux και Windows, που λειτουργούν σε περιβάλλον τοπικής υποδομής μέσω της αναπαραγωγής τους, είτε σε μια δευτερεύουσα τοπική υποδομή είτε σε περιβάλλον δημοσίου υπολογιστικού νέφους του κατασκευαστή της προσφερόμενης λύσης.	ΝΑΙ		
	Να προσφέρεται η δυνατότητα αποκατάστασης καταστροφών για τις εικονικές μηχανές που λειτουργούν στο περιβάλλον δημοσίου νέφους του κατασκευαστή της προσφερόμενης λύσης μέσω της αναπαραγωγής τους σε μια δευτερεύουσα περιοχή του δημοσίου υπολογιστικού νέφους.	ΝΑΙ		
	Παροχή μηνιαίου SLA για την υπηρεσία αποκατάστασης φορτίων από τοπική υποδομή στο περιβάλλον δημοσίου υπολογιστικού νέφους, εντός 2 ωρών.	ΝΑΙ		
	Κατά την προστασία των εικονικών, η διαδικασία του replication να μην επηρεάζει τα πρωτότυπα δεδομένα.	ΝΑΙ		
	Να προσφέρεται η δυνατότητα πραγματοποίησης δοκιμαστικής αποκατάστασης καταστροφών, χωρίς να προκαλούνται ανεπιθύμητες επιπτώσεις στις εφαρμογές και τα δεδομένα του Οργανισμού.	ΝΑΙ		
	Να προσφέρεται η δυνατότητα πραγματοποίησης δοκιμαστικής αποκατάστασης καταστροφών, τόσο σε κάποια προγραμματισμένη χρονική στιγμή, όσο και σε κάποια η οποία δεν έχει προκαθοριστεί.	ΝΑΙ		
	Να προσφέρεται η δυνατότητα σχεδιασμού και παραμετροποίησης των σχεδίων αποκατάστασης από καταστροφή από τον Οργανισμό, καθώς και ομαδοποίησης και προτεραιοποίησης της αποκατάστασης των εφαρμογών στα σχέδια αυτά. Επιπλέον, να είναι δυνατή η ενσωμάτωση της προσφερόμενης λύσης με εξειδικευμένα για την εκάστοτε εφαρμογή σενάρια αποκατάστασης καταστροφών.	ΝΑΙ		
	Κατά την προστασία των εικονικών μηχανών να προσφέρεται η δυνατότητα application consistent σημείων ανάκαμψης.	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	<p>Να προσφέρεται η δυνατότητα replication κατ'ελάχιστον για τις παρακάτω εφαρμογές τοπικής υποδομής:</p> <ul style="list-style-type: none"> • MicrosoftActiveDirectory • IIS • SQL • SharePoint <p>υποστηρίζοντας τους εγγενείς μηχανισμούς υψηλής διαθεσιμότητας.</p>	NAI		
	<p>Η προσφερόμενη λύση να διαθέτει παραμετροποίηση δικτυακών ρυθμίσεων των προστατευόμενων εικονικών μηχανών, καθώς και συνεργασία με δικτυακές υπηρεσίες του παρόχου υπολογιστικού νέφους.</p>	NAI		
	<p>Ο πάροχος δημοσίου υπολογιστικού νέφους να προσφέρει κανάλι πρόσθετων επιλογών τύπου Marketplace, μέσω του οποίου να προσφέρονται εξειδικευμένες λύσεις αποκατάστασης καταστροφών από αντίστοιχους επίσημους συνεργάτες και κατασκευαστές λογισμικού.</p>	NAI		

7.2.4.4 Λύση Προστασίας Βάσεων Δεδομένων

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
1.	Να αναφερθεί ο κατασκευαστής, η έκδοση και η ημερομηνία διάθεσης.	NAI		
2.	Να προσφερθεί η απαραίτητη αδειοδότηση για την κάλυψη εξυπηρετητών βάσεων δεδομένων. Η προσφερόμενη αδειοδότηση δε θα πρέπει να θέτει περιορισμούς στη διακίνηση των δεδομένων.	≥20		
3.	Υλοποίηση σε διάταξη υψηλής διαθεσιμότητας active- passive	NAI		
4.	Διαχείριση μέσω κεντρικής κονσόλας διαχείρισης (GUI).	NAI		
5.	Σύνδεση «παθητικά» στο δίκτυο σε promiscuousmode κυρίως για τον εντοπισμό απειλών (alert).	NAI		
6.	Σύνδεση με πλήρη διαφάνεια στο δίκτυο «σε σειρά» (inlinebridge) με πλήρεις δυνατότητες ανίχνευσης και καταστολής απειλών.	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
7.	Ανίχνευση και καταστολή γνωστών επιθέσεων και απειλών σε επίπεδο υπηρεσίας (DBService) και εφαρμογής Βάσης Δεδομένων (π.χ. MSSQL, Oracle, κτλ).	ΝΑΙ		
8.	Υποστήριξη της ανάλυσης της δομής ενός SQLtransaction για τον προσδιορισμό όλης της πληροφορίας που σχετίζεται με ένα query. Επίσης θα πρέπει να παρέχει δυνατότητα περαιτέρω συσχετισμού χαρακτηριστικών (attributes) για τον ακριβή προσδιορισμό των στοιχείων πρόσβασης.	ΝΑΙ		
9.	Διάθεση εργαλείου ανάλυσης SQL γραμματικής για την κατανόηση σύνθετων SQLstatements.	ΝΑΙ		
10.	Εκμάθηση της κανονικής και νόμιμης λειτουργίας της βάσης δεδομένων και δημιουργία «προφίλ» ασφαλούς λειτουργίας αυτής, με αυτόματη διαδικασία, αποτρέποντας κάθε είδους δικτυακή κίνηση – πρόσβαση προς την βάση, η οποία αντιτίθεται στο «προφίλ» ασφαλούς λειτουργίας της βάσης δεδομένων, μέσω ανάλυσης της δικτυακής κίνησης και εντός εύλογου χρονικού διαστήματος. Να τεκμηριωθεί αναλυτικά.	ΝΑΙ		
11.	Αποτροπή της επιστροφής ευαίσθητων πληροφοριών προς τον client ως αποτέλεσμα κάποιου μη εξουσιοδοτημένου SQLquery αναλύοντας το περιεχόμενο των SQLqueryresponses. Να τεκμηριωθεί αναλυτικά.	ΝΑΙ		
12.	Η προτεινόμενη λύση πρέπει να υποστηρίζει κατ' ελάχιστον την προστασία των συγκεκριμένων τύπων βάσεων δεδομένων, καθώς και κάθε νεότερη έκδοση αυτών	<ul style="list-style-type: none"> • MS-SQL • Oracle • S4/HANA 		
13.	Πλήρη παρακολούθηση και καταγραφή της πρόσβασης και των ενεργειών των διαχειριστών στη βάση. Αυτό θα πρέπει να γίνεται είτε η πρόσβαση	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	πραγματοποιείται φυσικά στην λύση (locallogon) είτε μέσω κονσόλας διαχείρισης π.χ. remotedesktop, ssh, Xwindows κ.ά. Η λειτουργία αυτή δεν θα πρέπει να εισάγει φόρτο στη βάση δεδομένων και δεν θα πρέπει να βασίζεται στην ενεργοποίηση των εγγενών μηχανισμών audit του λειτουργικού συστήματος ή της βάσης.			
14.	Ο μηχανισμός καταγραφής της λύσης ασφάλειας θα πρέπει να επιτρέπει την πλήρη καταγραφή προσβάσεων στη βάση δεδομένων τουλάχιστον για τα παρακάτω: <ul style="list-style-type: none"> ▪ Database and Schema ▪ User or User groups (any/ all or only specific users all users, including sys dba) ▪ Source Application (any/ all or only specific items) ▪ Source IP Address ▪ Stored Procedures (any/ all or only specific items) ▪ Tables or tables groups (any/ all or only specific items) ▪ Column ▪ Operations ▪ User operation ▪ OS User name ▪ OS Computer name ▪ Query response size ▪ Query response time ▪ SQL exceptions ▪ Login/ logout ▪ Privilege operations Query executed	ΝΑΙ		
15.	Πλήρη παρακολούθηση και καταγραφή της πρόσβασης και των ενεργειών των χρηστών στις βάσεις οι οποίες πραγματοποιούνται μέσω κονσόλας διαχείρισης π.χ. remotedesktop, ssh, Xwindows κ.ά. Να τεκμηριωθεί αναλυτικά.	ΝΑΙ		
16.	Ο μηχανισμός καταγραφής των προσβάσεων και ενεργειών των χρηστών	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	δεν θα πρέπει να εισάγει φόρτο στη βάση δεδομένων και δεν θα πρέπει να βασίζεται στην ενεργοποίηση των εγγενών μηχανισμών καταγραφής του λειτουργικού συστήματος ή της βάσης (nativeOS/ DBaudit). Να τεκμηριωθεί αναλυτικά.			
17.	Ο μηχανισμός καταγραφής της λύσης ασφάλειας να επιτρέπει την λεπτομερή καταγραφή των ενεργειών των χρηστών στη βάση δεδομένων σε επίπεδο: <ul style="list-style-type: none"> • Local OS user • Database user Source OS user	NAI		
18.	Η κονσόλα διαχείρισης να παρέχει τη δημιουργία διαφορετικών ρόλων πρόσβασης και διαχείρισης (π.χ. viewonly, περιορισμένη διαχείριση, πλήρης πρόσβαση κτλ.) .	NAI		
19.	Η κονσόλα διαχείρισης θα πρέπει να επιτρέπει τη δημιουργία κανόνων συσχέτισης (correlationrules) ανάμεσα στα γεγονότα ασφάλειας που ανιχνεύονται. Να τεκμηριωθεί αναλυτικά.	NAI		
20.	Η λύση θα πρέπει να υποστηρίζει masking.	NAI		
21.	Η κονσόλα διαχείρισης θα πρέπει να επιτρέπει την δημιουργία και παραγωγή αναλυτικών αναφορών με βάση κατ' ελάχιστον τα συγκεκριμένα κριτήρια. <ul style="list-style-type: none"> • Ημερομηνία/ Ώρα • Διεύθυνση προέλευσης (sourceIPaddress) • Hostname προέλευσης • DB user name (login) • Διεύθυνση προορισμού (Destination IP address) • Server name προορισμού (DB name) • Client application Τύπος απειλής/ επίθεσης	NAI		
22.	Η κονσόλα διαχείρισης θα πρέπει να παρέχει εργαλείο προτυποποιημένων	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	αναφορών με έτοιμες αναφορές για την τεκμηρίωση της καταγραφής των γεγονότων του συστήματος. Να τεκμηριωθεί αναλυτικά.			
23.	Χρήση εικονικής μηχανής τύπου VMware για την υλοποίηση της λύσης	ΝΑΙ		
24.	Ενοποίηση με το υπάρχον σύστημα εφεδρείας netbackup (για λήψη των απαιτούμενων αντιγράφων ασφαλείας).	ΝΑΙ		
25.	Η λύση θα πρέπει να μπορεί να υποστηρίξει λειτουργικά συστήματα (βάσεων δεδομένων) τουλάχιστον τύπων Unix/ Linux, AIX, Windows.	ΝΑΙ		
26.	Δυνατότητα παρακολούθησης χωρίς τη SPAN πόρτα ή άλλη πόρτα από τα switches του δικτύου της για την παρακολούθηση (mirroring) της δικτυακής κίνησης. Εάν απαιτείται παρακολούθηση της δικτυακής κίνησης, ο Ανάδοχος πρέπει να παρέχει την απαραίτητη networktapping υποδομή και τις απαραίτητες υπηρεσίες υλοποίησης.	ΝΑΙ		
27.	Να αναφερθεί με λεπτομέρεια η αρχιτεκτονική της προτεινόμενης λύσης και τα υποσυστήματα που θα απαιτηθεί να υλοποιηθούν.	ΝΑΙ		
28.	Να αναφερθούν επιπλέον χαρακτηριστικά.	ΝΑΙ		
29.	Δεν θα επιφέρει επιβάρυνση στην λειτουργικότητα της εφαρμογής και της βάσης δεδομένων.	ΝΑΙ		
30.	Τα γεγονότα ασφαλείας θα πρέπει να προωθούνται για περαιτέρω ανάλυση και συσχέτισμό στην προσφερόμενη λύση SIEM.	ΝΑΙ		

7.2.4.5 Πλατφόρμα Κυβερνοασφάλειας – Εκτεταμένης Ανίχνευσης & Απόκρισης (Cyber Security)

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
1.	Η πλατφόρμα πρέπει να έχει τη δυνατότητα συλλογής και επεξεργασίας από πολλαπλών τύπων πηγές δεδομένων και όχι μόνο αρχείων καταγραφής, κινούμενη στη φιλοσοφία του bigdatasecurityanalytics.	ΝΑΙ		
2.	Με την εκμετάλλευση αυτοματοποιημένης επεξεργασίας και μηχανικής μάθησης, το σύστημα θα πρέπει να μπορεί να λειτουργεί αποτελεσματικά ως ένα ολοκληρωμένο κέντρο αναφοράς και αυτόματης πρότασης και λήψης αντιμέτρων	ΝΑΙ		
3.	Το σύστημα θα πρέπει κατ' ελάχιστον να συνοδεύεται από τεχνολογίες SIEM, Sandbox,NTA, ThreatIntelligenceκαι IDS και να μην απαιτείται η ξεχωριστή προμήθεια λογισμικού.	ΝΑΙ		
4.	Το προσφερόμενο σύστημα θα πρέπει να έχει τη δυνατότητα να υποστηρίζει και το μοντέλο MDR (ManagedDetection&Response) και θα πρέπει να υποστηρίζει το σύνολο του κύκλου ζωής αναγνώρισης και αντιμετώπισης απειλών, που αναλύεται στα στάδια: <ul style="list-style-type: none"> • Συλλογή (Collect) • Εντοπισμός (Detect) • Έρευνα (Investigate) • Απόκριση (Respond) 	ΝΑΙ		
5.	Το υπο προμήθεια σύστημα θα πρέπει να περιλαμβάνει την προμήθεια, εγκατάσταση και παραμετροποίηση αισθητήρων ασφαλείας (φυσικών ή εικονικών), οι οποίοι θα εφαρμόζουν λειτουργίες ML-IDS, antivirus, sandboxing και NTA.	ΝΑΙ		
	Χαρακτηριστικά NextGenSoc			

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
6.	Μοντέρνο περιβάλλον χρήσης (GUI) που ενσωματώνει απαραίτητες λειτουργίες παρακολούθησης και διαχείρισης.	ΝΑΙ		
7.	Πρόσβαση με χρήση ρόλων χρηστών (RBAC – RoleBasedAccess) για την διαχείριση δικαιωμάτων (userprivilegemanagement)	ΝΑΙ		
8.	Υποστήριξη πολλαπλών ενοίκων (multi-tenant) για την ξεχωριστή διαχείριση οντοτήτων, φυσικών δικτύων κτλ	ΝΑΙ		
9.	Εφαρμογή ξεχωριστού μοντέλου μηχανικής μάθησης ανά tenant για τη βελτίωση ακρίβειας των αποτελεσμάτων και τη μείωση των εσφαλμένων θετικών συμβάντων (falsepositives), εφαρμόζοντας ξεχωριστά συμπεριφορικά μοντέλα.	ΝΑΙ		
10.	Εξελιγμένες δυνατότητες μηχανικής μάθησης που να συμπεριλαμβάνουν τόσο supervised όσο και unsupervised διαδικασίες, τεχνολογίες graphML και να συνδυάζονται μεταξύ τους για την παραγωγή βέλτιστων αποτελεσμάτων	ΝΑΙ		
11.	Δυνατότητες ενσωμάτωσης με εργαλεία και τεχνολογίες ασφαλείας Firewalls, WAF, SWG, EDR, SOAR κτλ	ΝΑΙ		
12.	Υποστήριξη API για ενσωμάτωση με τεχνολογίες HoneyPots, εργαλεία OSINT κτλ.	ΝΑΙ		
13.	Μία ενοποιημένη, υψηλής απόδοσης, αποθήκη δεδομένων (“BigData” HighSpeedLake)	ΝΑΙ		
14.	Δυνατότητα εγκατάστασης τόσο σε φυσικό εξοπλισμό, όσο και σε εικονικό ή περιβάλλον cloud	ΝΑΙ		
15.	Κατανεμημένη και επεκτάσιμη αρχιτεκτονική που να υποστηρίζει ωστόσο και “AllInOne” σενάρια.	ΝΑΙ		
16.	Υψηλή διαθεσιμότητας με τη χρήση clusters και ευέλικτη τήρηση και αποθήκευση δεδομένων.	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
17.	Μηχανισμοί Συλλογής που να μπορούν να εγκατασταθούν τόσο σε φυσικό όσο και σε εικονικό περιβάλλον	ΝΑΙ		
18.	Το σύστημα θα πρέπει να ακολουθεί ανοιχτή αρχιτεκτονική που να επιτρέπει την εισαγωγή δεδομένων από οποιαδήποτε συσκευή με τη χρήση IntegrationAPIs.	ΝΑΙ		
19.	Κεντριοποιημένη διαχείριση	ΝΑΙ		
20.	Απλό ενοποιημένο μοντέλο αδειών χωρίς επιπλέον κόστη	ΝΑΙ		
	Next-GenerationSIEM			
21.	Η πλατφόρμα θα πρέπει να βασίζεται σε μια ενοποιημένη αποθήκη δεδομένων βασισμένη στην αρχιτεκτονική του bigdatalake και τα δεδομένα θα πρέπει κατ'ελάχιστον να μπορούν να εισαχθούν μέσω syslog.	ΝΑΙ		
22.	Απλός όσο και εξεζητημένος μηχανισμός αναζήτησης που να βασίζεται σε λογικούς τελεστές (Booleanmodifiers)	ΝΑΙ		
23.	Οι αναζητήσεις να μπορούν να εφαρμοστούν ως μόνιμα φίλτρα σε όλο το περιβάλλον για ταχύτερη διερεύνηση και ανάλυση περιστατικών.	ΝΑΙ		
24.	Υψηλής απόδοσης και άμεσες ανταποκρίσεις στην αναζήτηση και το φιλτράρισμα στο bigdata	ΝΑΙ		
25.	Πρόσβαση σε πηγές δεδομένων και όχι μόνο σε syslog δεδομένα	ΝΑΙ		
26.	Συλλογή δεδομένων από δικτυακή κίνηση (μέσω TAP ή MirrorTraffic). Τα πακέτα θα πρέπει να γίνονται reduce, να κανονικοποιούνται και να μετατρέπονται σε αξιοποιήσιμα μετα-δεδομένα για την ενσωμάτωση στο bigdatalake.	ΝΑΙ		
27.	Συλλογή δεδομένων από user sources όπως το Microsoft AD μέσω API Connector	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
28.	Συλλογή δεδομένων από πηγές νέφους (cloud) Office365 μέσω Connectors	NAI		
29.	Τα δεδομένα από πηγές πρέπει να κανονικοποιούνται, να εμπλουτίζονται και να συσχετίζονται αυτόματα από το σύστημα	NAI		
30.	Πηγές εμπλουτισμού πρέπει να περιλαμβάνονται γεωγραφικού προσδιορισμού (Geo-Awareness), IPReputation, ThreatIntelligence και DPIApplicationawareness.	NAI		
31.	Μοντέρνο περιβάλλον χρήστη με λειτουργίες SIEM που περιλαμβάνουν ερωτήματα και δημιουργίες κανόνων.	NAI		
32.	Πρόσθετο για παραδοσιακή απεικόνιση SIEM (π.χ. Kibana)	NAI		
	Εντοπισμός KillChain (KillChainDetections)			
33.	Το σύστημα πρέπει να έχει ενσωματωμένους μηχανισμούς εντοπισμών σε κάθε φάση του CyberSecurityKillChain, συμπεριλαμβάνοντας Reconnaissance, Delivery, Exploitation, Installation, Command&Control, andActions&Exfiltrations	NAI		
34.	Το σύστημα πρέπει να περιλαμβάνει ενσωματωμένη βάση υπογραφών IDS, ενισχυμένη από ανάλυση μηχανικής μάθησης (ML-IDS)	NAI		
35.	Η πλατφόρμα πρέπει να υποστηρίζει πολλαπλά ThreatIntelligenceFeeds, συμπεριλαμβάνοντας εμπορικές πηγές, open-source, anti-phishing κ.α.	NAI		
36.	Η πλατφόρμα πρέπει να επιτρέπει ενσωμάτωση με 3 rd partyfeeds μέσω STIX/TAXII και/η MISP	NAI		
37.	Η πλατφόρμα πρέπει να έχει ενσωματωμένες δυνατότητες APTsandboxing για να αναγνωρίζει και να περιορίζει άγνωστα αρχεία, και για εντοπισμό ransomware, spyware.	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Ανάλυση Δικτύου (Network Traffic Analysis)			
38.	Η πλατφόρμα πρέπει να ενσωματώνει λειτουργικότητα DeepPacketInspection(DPI) για την αναγνώριση τουλάχιστον 4000 εφαρμογών και να δομεί σχετικά συμπεριφορικά μοντέλα.	NAI		
39.	Τα δεδομένα κίνησης δικτύου πρέπει να μετασχηματίζονται σε κατάλληλα μετα-δεδομένα που περιλαμβάνουν και το payload, για την αντίστοιχη προαιρετική μείωση ανάγκης αποθηκευτικών χώρων.	NAI		
40.	Η πλατφόρμα πρέπει να ενσωματώνει λειτουργικότητα NTADetections, συμπεριλαμβάνοντας ApplicationUsageAnomalies, LongAppSessionAnomalies, και UnapprovedAssetActivity	NAI		
41.	Το σύστημα θα πρέπει να εντοπίζει ανωμαλίες στη συμπεριφορά των Firewalls, denialanomalies ή ruleusageanomalies	NAI		
	UserBehaviorAnalytics (UBA)			
42.	Το σύστημα πρέπει να πραγματοποιεί ανάλυση και εντοπισμό ανωμαλιών στη συμπεριφορά του χρήστη (userbehavior)	NAI		
43.	Το σύστημα πρέπει να ενσωματώνει μοντέλα εντοπισμού ανωμαλιών αδύνατου ταξιδιού (ImpossibleTravelAnomaly) ή ώρες αυθεντικοποίησης (LogInTimeAnomaly)	NAI		
44.	Εντοπισμούς NTA, έτσι κι εδώ όλα τα detections και τα σχετικά events στα logs και σε πηγές πρέπει να συσχετίζονται αυτόματα.	NAI		
	EndpointBehaviorAnalytics (EBA)			
45.	Το σύστημα θα πρέπει να μπορεί να εισάγει δεδομένα από τρίτα συστήματα εντοπισμού ευπαθειών (vulnerabilityscanners) Nessus, Tenable, Rapid7 και να συσχετίζει τα ευρήματα με σχετικά γεγονότα ασφαλείας.	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
46.	Το σύστημα θα πρέπει να μπορεί να ανακαλύψει όλα τα assets σε ένα περιβάλλον και να τα κατηγοριοποιεί με βάση τη διεύθυνση MAC και IP.	ΝΑΙ		
47.	Η λίστα των ανακαλυφθέντων/εντοπισθέντων assets θα πρέπει να μπορεί να επαυξάνεται και να παραμετροποιείται με τη χρήση αρχείων csv με λίστες assets και περιγραφές.	ΝΑΙ		
48.	Το σύστημα πρέπει να μπορεί να καταγράφει όλους συσχετισμούς με ένα asset με IP διευθύνσεις, ιστορικά στοιχεία για τη χρήση εφαρμογών κτλ.	ΝΑΙ		
	Ορατότητα Δικτύου και Υπηρεσιών (Network&ServiceVisibility)			
49.	Το σύστημα θα πρέπει να περιλαμβάνει δυνατά εργαλεία απεικόνισης δικτύων και υπηρεσιών, μαζί με analytics, με στόχο να προσφέρει ορατότητα επιδόσεις δικτύου (networkperformance), applicationusage κτλ.	ΝΑΙ		
	Κυνήγι Απειλών και Διερεύνηση (Threat Hunting & Investigation)			
50.	Το σύστημα πρέπει να έχει ενσωματωμένα σχετικά εργαλεία, προκαθορισμένες αναζητήσεις και ερωτήματα, και οπτικοποιήσεις (visualizations).	ΝΑΙ		
51.	Τα visualizations πρέπει να είναι παραμετροποιήσιμα	ΝΑΙ		
52.	Το σύστημα πρέπει να προσφέρει εξελιγμένες δυνατότητες συσχετισμένες αναζητήσεις, που επιτρέπουν αναλυτές να συνδέσουν πολλαπλά ανεξάρτητα ερωτήματα με κοινά κριτήρια προκειμένου να δομήσουν πληροφορίες από attacksequences ή να απομονώσουν κοινές πληροφορίες.	ΝΑΙ		
53.	Όλα τα ερωτήματα θα πρέπει να μπορούν να αποθηκευθούν, επεξεργαστούν, κλωνοποιηθούν κτλ από χρήστες.	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
54.	Τα visualizations πρέπει να μπορούν να αποθηκευθούν σαν customdashboards.	NAI		
55.	Τα ερωτήματα θα πρέπει να μπορούν να συνδυαστούν με ενέργειες/αποκρίσεις για PlayBooks	NAI		
	Playbooks / Integrated Orchestration & Response (SOAR)			
56.	Το σύστημα πρέπει να συμπεριλαμβάνει μια βιβλιοθήκη με έτοιμα ενσωματωμένα playbooks, που είναι αυτό-εκτελέσιμα ερωτήματα με ενσωματωμένες ενέργειες.	NAI		
57.	Οι ενσωματωμένες ενέργειες/αποκρίσεις θα πρέπει να συμπεριλαμβάνουν: <ul style="list-style-type: none"> Alerts – Αποστολή e-mail/slack message κτλ Actions – Άνοιγμα case, εκτέλεση εντολής API, δημιουργία security event κτλ Responses – Μπλοκάρισμα μιας IP στο Firewall, απενεργοποίηση χρήστη στο AD, εκτέλεση δέσμης ενεργειών κτλ 	NAI		
58.	Παράλληλα με αυτοματοποιημένες ενέργειες, εξωτερικές ενέργειες το μπλοκάρισμα μια IP ή χρήστη θα πρέπει να είναι διαθέσιμες στο χρήστη μέσω του UI ώστε να μπορούν παράλληλα να υλοποιηθούν ως μέρος διερεύνησης/αντιμετώπισης ή ανάλυσης.	NAI		
59.	Δυνατότητα ενσωμάτωσης με εμπορικά εργαλεία SOAR	NAI		
	Ειδοποιήσεις (Alarming)			
60.	Το σύστημα θα πρέπει να προσφέρει έναν έξυπνο, μοντέρνο και παραμετροποιήσιμο μηχανισμό ειδοποιήσεων που να δύναται να οριστεί με βάση παραλήπτες και άλλα κριτήρια (scoreseverity, killchaincategory, etc.)	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
61.	Οι ειδοποιήσεις πρέπει να μπορούν να αποσταλούν με email ή slack μηνύματα και τα μηνύματα πρέπει να είναι παραμετροποιήσιμα ως το περιεχόμενο και τα σχετικά δεδομένα.	ΝΑΙ		
	Αναφορές (Reporting)			
62.	Το σύστημα πρέπει να περιέχει ένα σύγχρονο εξελιγμένο μηχανισμό αναφορών που θα επιτρέπει παράλληλα εύκολη δημιουργία νέων αναφορών με draganddrop και αποθήκευσή για χρήση σε οποιοδήποτε σημείο.	ΝΑΙ		
63.	Οι αναφορές θα πρέπει να παράγονται με χρονοπρογραμματισμό και να αποστέλλονται σε διαφορετικούς χρήστες.	ΝΑΙ		
64.	Οι αναφορές πρέπει να είναι δυνατόν να αποστέλλονται με email σαν pdf ή csv ή να γράφονται σε αρχείο.	ΝΑΙ		
65.	Το σύστημα θα πρέπει να περιλαμβάνει πληθώρα έτοιμων αναφορών και templates.	ΝΑΙ		
	Portal			
66.	Πρόσβαση των χρηστών βάση ρόλου (UserRBACaccess) στο Portal με συνολική ή περιορισμένη πρόσβαση πληροφορίες.	ΝΑΙ		
67.	Custom Dashboards ανά ρόλο χρήστη.	ΝΑΙ		
68.	Χρονοπρογραμματισμένες αναφορές για κάθε tenant, tenantgroup και RBACusers.	ΝΑΙ		
69.	Η πρόσβαση των χρηστών πρέπει να μπορεί να περιορίζεται σε Read-Only, limitedview, μέχρι fullvisibilityandaccess.	ΝΑΙ		

7.2.4.6 Λογισμικό κυβερνοασφάλειας ΑΙ, συμπεριλαμβανομένης εγκατάστασης, εκπαίδευσης και υποστήριξης 24/7. 1000 Άδειες

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Να αναφερθούν το όνομα και η έκδοση του προσφερόμενου λογισμικού και η χρονολογία διάθεσης της προσφερόμενης έκδοσης	ΝΑΙ		
	Η άδεια χρήσης μπορεί να διατίθεται με την μορφή Λογισμικού ως Υπηρεσία και θα παρέχεται για ελάχιστο χρονικό διάστημα τριάντα (30) μηνών. Να αναφερθεί η συνολική χρονική διάρκεια.	ΝΑΙ		
	Αυτόματη ανακάλυψη (discovery) και ταξινόμηση (classification) όλων των στοιχείων (assets)	ΝΑΙ		
	Δυνατότητα αυτόματης αναγνώρισης της λειτουργίας, των μοτίβων κυκλοφορίας και των πρωτοκόλλων εκτέλεσης για κάθε κεντρικό υπολογιστή ή ομάδα κεντρικών υπολογιστών και τον τύπο συσκευής κάθε κεντρικού υπολογιστή.	ΝΑΙ		
	Δυνατότητα αυτόματης αναγνώρισης χρηστών, πελατών (clients), όλων των φυσικών και εικονικών συσκευών και σχέσεων μεταξύ τους.	ΝΑΙ		
	Δημιουργία αυτόματων χαρτών που δείχνουν σχέσεις και εξαρτήσεις μεταξύ συστημάτων, διακομιστών και εφαρμογών.	ΝΑΙ		
	Αυτόματη αναγνώριση και ανάλυση διαφόρων πρωτοκόλλων AD (LDAP, Kerberos, DNS, DHCP).	ΝΑΙ		
	Συσχέτιση αναγνωρισμένων πληροφοριών μέσω άντλησης - διασύνδεσης από AD	ΝΑΙ		
	Αυτόματη αναγνώριση και ανάλυση πρωτοκόλλων επικοινωνίας (FTP, RDP, Telnet, SSH, syslog, SNMP, SMTP, POP3, NTP, SMPP κ.λπ.),	ΝΑΙ		
	Αυτόματη αναγνώριση και ανάλυση πρωτοκόλλων βάσεων δεδομένων (να υποστηρίζεται κατ' ελάχιστον η βάση MSSQL, με επιθυμητή πλέον την PostgreSQL, MySQL)	ΝΑΙ		
	Ανάλυση κίνησης δικτύου και πρωτοκόλλων από L2 έως L7	ΝΑΙ		
	Παρακολούθηση συσκευών IoT	ΝΑΙ		
	Να αναλύει την πρωτότυπη κυκλοφορία πακέτων δικτύου ή τις ροές επισκεψιμότητας σε πραγματικό χρόνο.			
	Παρακολούθηση της απόδοσης του δικτύου και των εφαρμογών. Παρακολούθηση της συμπεριφοράς, δημιουργία προφίλ και ανάλυση της φυσιολογικής συμπεριφοράς του δικτύου και αναγνώριση / ειδοποίηση για μη φυσιολογική συμπεριφορά	ΝΑΙ		
	Χρήση πολλών αλγορίθμων τεχνητής νοημοσύνης και αρκετών τεχνικών μηχανικής μάθησης, όπως η βαθιά μάθηση, η εποπτευόμενη μηχανική μάθηση και η μη εποπτευόμενη μηχανική μάθηση.	ΝΑΙ		

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Παρακολούθηση της κίνησης στο δίκτυο για τον εντοπισμό απειλών εσωτερικού	ΝΑΙ		
	Κρυπτογραφημένη Ανάλυση Κυκλοφορίας (ETA) στη λύση για τον εντοπισμό ύποπτης κίνησης στο δίκτυο και τον εντοπισμό κακόβουλου περιεχομένου στην κρυπτογραφημένη κίνηση.	ΝΑΙ		
	Ανίχνευση απειλών			
	Προσδιορισμός τυχόν ύποπτης συμπεριφοράς στο δίκτυο και επισήμανση αυτών των συμπεριφορών σε πραγματικό χρόνο. Μηχανισμοί και μέθοδοι για την ανίχνευση απειλών σε πραγματικό χρόνο	ΝΑΙ		
	Δυνατότητα εντοπισμού βάσει ψηφιακής υπογραφής	ΝΑΙ		
	Προσδιορισμός νέων και άγνωστων συμπεριφορών επίθεσης χωρίς χρήση ψηφιακών υπογραφών ή κανόνων,	ΝΑΙ		
	Ανίχνευση διαφορετικών τύπων συμβάντων ασφαλείας (ICMP flood, Beaconsing, remote Powershell, Brute force login κ.λπ.),	ΝΑΙ		
	Εντοπισμός κρυπτογραφημένης κίνησης κακόβουλου λογισμικού.	ΝΑΙ		
	Ανίχνευση της μη συμμόρφωσης και της παραβίασης των οδηγιών ασφαλείας πληροφοριών, όπως παραβίαση πολιτικής, μη ασφαλή πρωτόκολλα, παρωχημένα πρωτόκολλα κρυπτογράφησης και κρυπτογραφήματα (ciphers), νέες συσκευές ή συσκευές rogue, κοινή χρήση αρχείων, αποθήκευση cloud κ.λπ.	ΝΑΙ		
	Εντοπισμός μη εξουσιοδοτημένης πρόσβασης αρχείων και άρνησης πρόσβασης σε αρχεία.	ΝΑΙ		
	Οι εντοπισμοί να αναφέρονται στο CVEDB για την ευπάθεια ή το πλαίσιο MITERATT&CK.	ΝΑΙ		
	Κλιμάκωση συμβάντων ασφαλείας σε διαφορετικά μοντέλα ειδοποιήσεων / παραβίασης (Anomalies, Data exfiltration, dDoS, Exploitation, Lateral movement, Reconnaissance, Botnet (Command&Control) traffic, Remote execution, malware propagation, Man in the Middle (MitM) attack).	ΝΑΙ		
	Δυνατότητα αυτόματης διαφοροποίησης μεταξύ των κανονικών συμπεριφορών και εκείνων που είναι πιο πιθανό να στοχεύονται ως απειλές botnet	ΝΑΙ		
	Οι ειδοποιήσεις και οι ανωμαλίες συγκεντρώνονται και συσχετίζονται για τη δημιουργία συμβάντων και μπορούν να φιλτραριστούν κατά συσκευή, χρήστη και τύπο παραβίασης.	ΝΑΙ		

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Οι ειδοποιήσεις και οι δυσλειτουργίες συγκεντρώνονται και συσχετίζονται για τη δημιουργία συμβάντων και εμφανίζουν αυτόματα τη βαθμολογία κινδύνου και τη φάση επίθεσης της ανίχνευσης.	ΝΑΙ		
	Αυτοματοποίηση διερεύνησης, χρησιμοποιώντας μηχανική εκμάθηση, για ανίχνευση και ιεράρχηση συμβάντων με διαφορετικά επίπεδα σοβαρότητας σε πραγματικό χρόνο	ΝΑΙ		
	Τροφοδότηση πληροφοριών απειλών (threatintelligencefeed),	ΝΑΙ		
	Πλήρης fullpacketcapture (PCAP) αποθήκευση & ανάλυση για ανίχνευση απειλών	ΝΑΙ		
	Απόκριση Περιστατικών			
	Μηχανισμός απόκρισης που μπορεί να ενεργοποιηθεί με τη δράση του χειριστή ή αυτόνομα ανάλογα με το επίπεδο ορατότητας, σοβαρότητας / κινδύνου και βεβαιότητας που απαιτείται από την ομάδα ασφαλείας για την αυτόματη απόκριση.	ΝΑΙ		
	Αυτόνομη ανταπόκριση σε πραγματικό χρόνο σε περιστατικά υψηλού κινδύνου ή για περιορισμό απειλών σε εξέλιξη	ΝΑΙ		
	Λειτουργικότητα απόκρισης σε συντονισμό με λύσεις τελικού σημείου (EndpointresponseEDR).	ΝΑΙ		
	Λειτουργικότητα απόκρισης σε συντονισμό με εργαλεία ελέγχου πρόσβασης δικτύου (NetworkAccessControlNAC).	ΝΑΙ		
	Εκτέλεση αναδρομικής αναζήτησης απειλών χρησιμοποιώντας μεταδεδομένα δικτύου.	ΝΑΙ		
	Η πλήρης διατήρηση πακέτων να υποστηρίζει τουλάχιστον 30 ημέρες	ΝΑΙ		
	Η διατήρηση μεταδεδομένων να υποστηρίζει τουλάχιστον 90 ημέρες	ΝΑΙ		
	Διαχείριση			
	Πρόσβαση βάσει ρόλου για πολλούς χρήστες σε λειτουργίες δικτύου και ομάδες ασφαλείας.	ΝΑΙ		
	Προσαρμόσιμες προβολές με διάφορες πληροφορίες διαθέσιμες μέσω ξεχωριστών ταμπλό, ανάλογα με το ρόλο του χρήστη.	ΝΑΙ		
	Προσαρμόσιμες προβολές με διάφορους τύπους πληροφοριών σύμφωνα με διαφορετικές περιπτώσεις χρήσης.	ΝΑΙ		

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Εσωτερική ορατότητα δικτύου, που απαιτείται για γρήγορο εντοπισμό και αντιμετώπιση πολλών προβλημάτων δικτύου.	ΝΑΙ		
	Ενσωμάτωση πληροφοριών χρήστη με στατιστικά στοιχεία κίνησης δικτύου για την παροχή λεπτομερών πληροφοριών στη δραστηριότητα των χρηστών οπουδήποτε στο δίκτυο.	ΝΑΙ		
	Δυνατότητα του αναλυτή να διερευνήσει τα δεδομένα (drilldown) σε ένα επιλεγμένο συμβάν.	ΝΑΙ		
	Δυνατότητα αναλυτικής προβολής (drilldown) σε κοινόχρηστα αρχεία στο δίκτυο.	ΝΑΙ		
	Δυνατότητα αναζήτησης συμβάντων σε αναλυμένα δεδομένα χρησιμοποιώντας ερωτήματα.	ΝΑΙ		
	Ανάλυση συσχετισμένων συμβάντων σε ένα γραφικό χρονοδιάγραμμα	ΝΑΙ		
	Κεντρική διαχείριση για διαμόρφωση συστήματος όπως ενημερώσεις (patches) O/S για όλες τις συσκευές,	ΝΑΙ		
	Το κεντρικό σύστημα διαχείρισης θα ενσωματώνει τις απόψεις (views) από όλους τους ιστότοπους που παρακολουθούνται και τα αντίστοιχα δεδομένα / πληροφορίες	ΝΑΙ		
	Κεντρικό σύστημα διαχείρισης για διαμόρφωση και λειτουργία λήψης δεδομένων	ΝΑΙ		
	Λοιπές Απαιτήσεις			
	Η λύση να προσφέρεται για εικονικά περιβάλλοντα όπως το ESXi και HyperV	ΝΑΙ		
	Παρακολούθηση σε ιδιωτικά/ δημόσια/ υβριδικά περιβάλλοντα cloud όπως το Azure κλπ.	ΝΑΙ		
	Παρακολούθηση της κυκλοφορίας μέσω SPAN / TAP / Mirror	ΝΑΙ		
	Ενσωμάτωση με λύση SIEM για χειρισμό και συσχέτιση ειδοποιήσεων.	ΝΑΙ		
	Τα μεταδεδομένα να μπορούν να προωθηθούν σε μια λύση SIEM.	ΝΑΙ		
	Ενσωμάτωση με τυπικά συστήματα υποστήριξης για τη διαχείριση συμβάντων.	ΝΑΙ		
	Ενσωμάτων με πλατφόρμες SOAR	ΝΑΙ		
	Υποστήριξη ειδοποιήσεων μέσω email σε συγκεκριμένη ομάδα χρηστών	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Ειδικές (ad hoc) και προγραμματισμένες αναφορές που παρουσιάζουν στατιστικές πληροφορίες για θέματα ασφάλειας και δικτύου για μια συγκεκριμένη χρονική περίοδο	ΝΑΙ		
	Εφαρμογή για κινητά για ειδοποίηση και διαχείριση συμβάντων.	ΝΑΙ		
	Ο ανάδοχος θα πρέπει να παρέχει διαρκώς επικαιροποιημένο υλικό εκπαίδευσης επί της λύσης του στο οποίο θα συμπεριλαμβάνεται και η χειροκίνητη ανίχνευση τεχνικών και τακτικών περιστατικών κυβερνοασφάλειας.	ΝΑΙ		

7.2.4.7 Λύση Διαβάθμισης και Σήμανσης Εγγράφων

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
1.	Οι endpointagents του Συστήματος Διαβάθμισης Δεδομένων, πρέπει να είναι συμβατοί με Λειτουργικά Συστήματα: Windows 10, WindowsServer 2008 R2, 2012, 2016, 2019 , , MacOS / X, AndroidEnterprise, IOS.	ΝΑΙ		
2.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να καλύπτει τετρακόσια (400) τερματικά του οργανισμού	ΝΑΙ		
3.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να έχει δυνατότητα να θέτει σήμανση σε έγγραφα της ακόλουθης μορφής: 1. ΣουίταMS Office (π.χ. Word, Excel, Power Point, Visio, Microsoft Project, OneNote). 2. Outlook email (π.χ. msg, pst, ost) 3.Αρχεία PDF 4. Αρχείακειμένου (π.χ. TXT, ASC, ANS, ACL, HTML, XML, ODM, OTT, INFO, PAP, PAGES) 5. Συμπιεσμένααρχεία (π.χ. ZIP, 7zip, RAR, WinRAR, BZip, Gzip, Tar, Bz2) 6. Αρχείαβίντεο (π.χ. mpg, mp4, amv, wmv, mov, avi, mkv) 7. Αρχείαήχου (π.χ. mp3, wma, wav, DVR-MS, WTV) 8. Αρχείαεικόνας (π.χ. JPEG, TIFF, GIF, BMP, PNG, AI, CDR, ADT, PSD, PUB)	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	9. Αρχεία βάσης δεδομένων (π.χ. ACCDB, ADT, DB, MDB, MYD, MYI, ORA, SQL, SDF, sqlite, 10. Κρυπτογραφημένα αρχεία (π.χ. ssh, pub, rpkr, cert, crt, der, p7b, PEM, PFX, AXX, EEA, TC, BPW, KDB, KDBX) 11. Άλλοι τύποι αρχείων (π.χ. CMD, BAT, JSP, PL, PHP, ASP, PYO, VBS)			
4.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να διαβαθμίζει τα έγγραφα με τρόπο, ώστε η πληροφορία για το επίπεδο διαβάθμισης (π.χ. πληροφορίες μεταδεδομένων) να μην μπορεί να διαγραφεί ή τροποποιηθεί από τον απλό χρήστη.	NAI		
5.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να επιβάλλει πολιτικές σχετικά με το αρχικό επίπεδο διαβάθμισης που θα έχει κάθε νέο έγγραφο (π.χ. οποιοδήποτε νέο έγγραφο δημιουργείται πρέπει να διαβαθμίζεται αυτόματα ως Εσωτερικό).	NAI		
6.	Η πληροφορία για το επίπεδο διαβάθμισης πρέπει να ακολουθεί ένα διαβαθμισμένο έγγραφο κατά τη διάρκεια κάθε είδους μεταφοράς (π.χ. μέσω email, μέσω διαδικτύου, εφαρμογών cloud, μέσω FTP / SFTP, αντιγραφή σε οποιονδήποτε τύπο αφαιρούμενου μέσου, εάν κρυπτογραφεί και αποκρυπτογραφεί, σε περίπτωση συμπίεσης)	NAI		
7.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να είναι σε θέση να επιβάλλει τουλάχιστον 4 διαφορετικά επίπεδα ταξινόμησης (π.χ. Δημόσιο, Εσωτερικό, Εμπιστευτικό και αυστηρά Εμπιστευτικό) και να έχει δυνατότητα να υποστηρίξει έως και πρακτικά απεριόριστα επίπεδα διαβάθμισης	NAI		
8.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει επίσης να μπορεί να διαφοροποιεί και να επιβάλλει διαφορετικές πολιτικές σε διαφορετικά επίπεδα διαβάθμισης εγγράφων (υποκατάταξη) με βάση τα τμήματα του οργανισμού, όπως αποτυπώνονται στο κέντρικό κατάλογο	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	χρηστών του οργανισμού (ActiveDirectory). Για παράδειγμα, θα μπορούσε να έχει ένα διαβαθμισμένο έγγραφο ως Εμπιστευτικό / Τμήμα Οικονομικών και άλλο έγγραφο, ως Εμπιστευτικό / Τμήμα εξυπηρέτησης κοινού, κ.λπ.			
9.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να μπορεί να καθορίζει την πολιτική χρονικής διατήρησης ανάλογα με το επίπεδο διαβάθμισης και τον τύπο του εγγράφου	ΝΑΙ		
10.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να έχει δυνατότητες σάρωσης των εγγράφων και εντοπισμού χαρακτηριστικών σημείων του περιεχομένου π.χ. λέξεις-κλειδιά, regular expressions, περιεχόμενα λεξικών κ.λπ.	ΝΑΙ		
11.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να μπορεί να υποστηρίζει και να επιβάλλει διαφορετικές τεχνικές διαβάθμισης, όπως οι ακόλουθες: 5. Χειροκίνητη Διαβάθμιση (π.χ. με ένα κλικ ενός κουμπιού, επιλέγοντας μεταξύ των 4 διαφορετικών επιπέδων και υπο-επιπέδων. 6. Ημιαυτόματη ταξινόμηση (π.χ. με βάση το περιεχόμενο του εγγράφου για να δώσει κάποιες ενδείξεις στον χρήστη για το τι επίπεδο διαβάθμισης πρέπει να θέσει) Μαζική ταξινόμηση (Το εργαλείο πρέπει να ταξινομήσει όλα τα αρχεία σε έναν συγκεκριμένο folder με βάση το απαιτούμενο επίπεδο διαβάθμισης ή με βάση τη σάρωση περιεχομένου, π.χ. σε περίπτωση που ανακαλύπτει προσωπικά δεδομένα σε αυτό κ.λπ.)	ΝΑΙ		
12.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να έχει δυνατότητα ρύθμισης για το αν επιτρέπεται ή όχι η αλλαγή του επιπέδου διαβάθμισης από τους χρήστες (π.χ. αναβάθμιση ή υποβάθμιση).	ΝΑΙ		
13.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να δίνει την δυνατότητα αυτόματης	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	διαβάθμισης εγγράφων κατά την αποθήκευση των εγγράφων .			
14.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να εκτελεί μαζική σάρωσης εγγράφων που είναι αποθηκευμένα είτε σε τοπικούς servers είτε σε εφαρμογές αποθήκευσης εγγράφων στο νέφος και αυτόματης διαβάθμισης με βάση το περιεχόμενο τους. Η διαχείριση των σχετικών ενεργειών πρέπει να εκτελείται από την κεντρική κονσόλα του συστήματος.	ΝΑΙ		
15.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να μπορεί να σαρώνει μεγάλο όγκο εγγράφων ώστε να διαβαθμιστούν έγγραφα που έχουν παραχθεί στο παρελθόν και διατηρούνται στα πληροφοριακά συστήματα του ΔΕΔΔΗΕ.	ΝΑΙ		
16.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να εκτελεί αυτόματο καθορισμό των επιπέδων διαβάθμισης με βάση τον εντοπισμό χαρακτηριστικών λέξεων και φράσεων στο περιεχόμενο των εγγράφων.	ΝΑΙ		
17.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να εκτελεί αυτόματο καθορισμό των επιπέδων διαβάθμισης με βάση τον εντοπισμό σειρών χαρακτήρων που ακολουθούν συγκεκριμένους κανόνες (regular expressions). Η διαχείριση των σχετικών ενεργειών πρέπει να εκτελείται από την κεντρική κονσόλα του συστήματος.	ΝΑΙ		
18.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να μπορεί να επιβάλει την αλλαγή του επιπέδου διαβάθμισης με βάση την ημερομηνία δημιουργίας ή τροποποίησης του εγγράφου (πχ αλλαγή επιπέδου διαβάθμισης από «εμπιστευτικό» σε «δημόσιο» μετά από καθορισμένο χρόνο από την ημερομηνία δημιουργίας ενός εγγράφου).	ΝΑΙ		
19.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να παρέχει στατιστικά για την εξέλιξη της αυτόματης διαβάθμισης των υφιστάμενων	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	εγγράφων από την κεντρική κονσόλα της λύσης.			
20.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να συντάσσει καταλόγο (inventory) με τα έγγραφα που έχουν εντοπιστεί με βάση κάποια πολιτική η οποία λαμβάνει υπ όψιν το περιεχόμενο τους ή/και τα επίπεδα διαβάθμισης τους. Η διαχείριση των σχετικών ενεργειών πρέπει να εκτελείται από την κεντρική κονσόλα του συστήματος.	ΝΑΙ		
21.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να είναι σε θέση να σαρώσει, να αναγνωρίσει και να διαβαθμίσει δεδομένα που είναι αποθηκευμένα σε συστήματα διαμοιρασμού εγγράφων: <ul style="list-style-type: none"> • Sharepoint • OneDrive • Dropbox • Box • Windows Filesharing 			
22.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να μπορεί να τοποθετεί οπτική σήμανση χαρακτηριστικής του επιπέδου διαβάθμισης εντός των εγγράφων της οικογένειας MsOffice (word, exec, powerpoint)	ΝΑΙ		
23.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να μπορεί να θέτει αυτόματα σήμανση εντός των εγγράφων με βάση το επίπεδο ταξινόμησής τους (π.χ. υδατογράφημα, υποσέλιδο, κεφαλίδα κ.λπ.)	ΝΑΙ		
24.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να μπορεί να προσαρμόζει τη σήμανση στις απαιτήσεις του ΔΕΔΔΗΕ (πχ χρώματα, λεκτικά, θέση, κλπ)	ΝΑΙ		
25.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να μπορεί να τοποθετεί σήμανση χαρακτηριστική του επιπέδου διαβάθμισης εντός μηνυμάτων ηλεκτρονικής αλληλογραφίας της εφαρμογής MsOutlook.	ΝΑΙ		
26.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να μπορεί να θέτει αυτόματα σήμανση στα εικονίδια εγγράφων (π.χ. τα εικονίδια επιφάνειας εργασίας κάθε εγγράφου) με	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	βάση το επίπεδο διαβάθμισης τους (π.χ. κόκκινη ετικέτα για αυστηρά εμπιστευτικό, πορτοκαλί ετικέτα για εμπιστευτικό, κίτρινη ετικέτα Εσωτερικό και πράσινη ετικέτα για Δημόσιας χρήσης).			
27.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να μπορεί να επισημάνει τα έγγραφα με μεταδεδομένα (metadata) στα οποία περιλαμβάνονται όλες οι πληροφορίες για τα επίπεδα και υποεπίπεδα διαβάθμισης των εγγράφων	ΝΑΙ		
28.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να μπορεί να προσθέσει στα μεταδεδομένα κάθε εγγράφου και πληροφορία για την πολιτική διατήρησης ανάλογα με το επίπεδο διαβάθμισης και τον τύπο του εγγράφου.	ΝΑΙ		
29.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να προστατεύει τα μεταδεδομένα από διαγραφή ή τροποποίηση από τον απλό χρήστη.	ΝΑΙ		
30.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να μπορεί να διατηρεί τα μεταδεδομένα επί του εγγράφου κατά τη διάρκεια κάθε είδους μεταφοράς (π.χ. μέσω email, μέσω διαδικτύου, εφαρμογών cloud, ftp/sftp, αντιγραφής, κρυπτογράφηση/αποκρυπτογράφησης, συμπίεσης, κλπ).	ΝΑΙ		
31.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να είναι απολύτως συμβατό με το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) (π.χ. τα μεταδεδομένα τα σχετικά με το επίπεδο διαβάθμισης πρέπει να αναγνωρίζονται από το εργαλείο DLP το οποίο θα εφαρμόζει κατάλληλες πολιτικές ελέγχου).	ΝΑΙ		
32.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να είναι πλήρως συμβατό με την λύση IRM του ΔΕΔΔΗΕ. Τα μεταδεδομένα σχετικά με το επίπεδο διαβάθμισης πρέπει να αναγνωρίζονται από την λύση IRM.	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
33.	Το Σύστημα Διαβάθμισης Δεδομένων θα πρέπει να συνεργάζεται με εργαλεία Εξωτερικής κρυπτογράφησης.	ΝΑΙ		
34.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να έχει χαρακτηριστικά ανοικτής αρχιτεκτονικής ώστε να εξασφαλίζεται η διαλειτουργικότητα του με τα υφιστάμενα πληροφοριακά συστήματα του ΔΕΔΔΗΕ.	ΝΑΙ		
35.	Μετά από μαζική σάρωση εγγράφων σε servers ή σε εφαρμογές αποθήκευσης εγγράφων (πχ sharepoint), το Σύστημα Διαβάθμισης Δεδομένων πρέπει να παράγει αναφορές και στατιστικά καθώς και τα αντίστοιχα γραφήματα τους .	ΝΑΙ		
36.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να μπορεί να εξάγει τις αναφορές υπό μορφή αρχείου.	ΝΑΙ		
37.	Η κονσόλα διαχείρισης του Συστήματος Διαβάθμισης Δεδομένων θα πρέπει να συλλέγει καταγραφές συμβάντων (logs) από τα τερματικά χρηστών, στις ακόλουθες περιπτώσεις: 1. Εάν ένας χρήστης αλλάξει το επίπεδο ταξινόμησης ενός εγγράφου (π.χ. μείωση του επιπέδου ταξινόμησης) 2. Εάν έχει σταλεί προειδοποίηση για κάποια ενέργεια (alert) ή έχει ζητηθεί αιτιολόγηση από τον χρήστη για κάποια ενέργεια.	ΝΑΙ		
38.	Το Σύστημα Διαβάθμισης Δεδομένων θα έχει την Δυνατότητα μεταφοράς των καταγραφών των ενεργειών χρηστών σε syslogserver.	ΝΑΙ		
39.	Το Σύστημα Διαβάθμισης Δεδομένων θα πρέπει να υποστηρίζει πλήρως την ελληνική γλώσσα, (π.χ. πληροφορίες αναδυόμενων παραθύρων, ενσωματωμένα κουμπιά σε εφαρμογές του Office κ.λπ.).	ΝΑΙ		
40.	Η αρχιτεκτονική του Συστήματος Διαβάθμισης Δεδομένων , θα πρέπει να περιλαμβάνει μια κεντρική κονσόλα διαχείρισης από την οποία δημιουργούνται	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	και προωθούνται οι κατάλληλες πολιτικές στα τερματικά των χρηστών.			
41.	Ο agent του Συστήματος Διαβάθμισης Δεδομένων δεν πρέπει να καταναλώνει περισσότερο από 5% των πόρων σταθμού εργασίας / διακομιστή, βάσει δεδομένων και έγκυρων μετρήσεων.	ΝΑΙ		
42.	Θα πρέπει να υπάρχει δυνατότητα ελέγχου και εντοπισμού κακόβουλης απενεργοποίησης του agent .	ΝΑΙ		
43.	Μετά από μαζική σάρωση εγγράφων σε servers ή σε εφαρμογές αποθήκευσης εγγράφων (πχ sharepoint), το Σύστημα Διαβάθμισης Δεδομένων πρέπει να μπορεί να αρχειοθετεί αυτόματα τα διαβαθμισμένα έγγραφα που φτάνουν στην ημερομηνία λήξης σύμφωνα με την πολιτική διατήρησης.	ΝΑΙ		
44.	Η σειρά εφαρμογής ή προτεραιότητα των πολιτικών διαβάθμισης, θα πρέπει να είναι σαφής και να καθορίζεται είτε από την σειρά της δήλωσής τους.	ΝΑΙ		
45.	Το Σύστημα Διαβάθμισης Δεδομένων πρέπει να υποστηρίζει λειτουργίες διαχείρισης πολιτικής όπως, μεταξύ άλλων, προσθήκη πολιτικής, κατάργηση πολιτικής, ενεργοποίηση πολιτικής, απενεργοποίηση πολιτικής, προσθήκη, κατάργηση και αλλαγή κανόνων πολιτικής, αλλαγή παραμέτρων πολιτικής, σύνδεση πολιτικής με συγκεκριμένους agents, πολιτική δοκιμών κ.λπ.	ΝΑΙ		
46.	Ο ανάδοχος πρέπει να παρέχει διαγράμματα αρχιτεκτονικής για το πώς θα υλοποιηθεί το Σύστημα και τους υπολογιστικούς πόρους που απαιτούνται για τη φιλοξενία του Συστήματος και για την Πρόληψη απώλειας δεδομένων.	ΝΑΙ		
47.	Ο ανάδοχος θα είναι υπεύθυνος για την εγκατάσταση της πλήρους υποδομής που απαιτείται για την υλοποίηση του Συστήματος (π.χ. εγκατάσταση λογισμικού	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	και λειτουργικού συστήματος, DB, εφαρμογής κ.λπ.).			
48.	Ο ανάδοχος θα είναι υπεύθυνος να εγκαταστήσει τους απαιτούμενους agents στους τερματικούς σταθμούς εργασίας των χρηστών.	ΝΑΙ		
49.	Ο ανάδοχος θα είναι υπεύθυνος για τη δημιουργία όλων των συμφωνημένων πολιτικών διαβάθμισης με βάση τις ανάγκες του αναθέτοντος οργανισμού και τις αντίστοιχες πολιτικές της εταιρείας αλλά και τα αποτελέσματα της μελέτης αξιολόγησης.	ΝΑΙ		
50.	Ο ανάδοχος πρέπει να παρέχει την κατάλληλη εκπαίδευση σε υπεύθυνους πληροφορικής του αναθέτοντος οργανισμού σχετικά με την λειτουργία του Συστήματος, αλλά και στο σύνολο των χρηστών της εταιρείας ώστε όλοι οι χρήστες να γνωρίζουν πως μπορούν να χρησιμοποιήσουν το σύστημα, σύμφωνα με τις απαιτήσεις της παραγράφου Error! Reference source not found..	ΝΑΙ		

7.2.4.8 Λύση Προστασίας Δεδομένων από Διαρροή

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
1.	Οι agents του συστήματος αποτροπής διαρροής δεδομένων που εγκαθίστανται στα τερματικά (endpoints), πρέπει να είναι συμβατοί με Λειτουργικά Συστήματα: Windows 10, WindowsServer 2008 R2, 2012, 2016, 2019 , , MacOS / X,	ΝΑΙ		
2.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) πρέπει να έχει τέλεια συμβατότητα με το εργαλείο διαβάθμισης και σήμανσης εγγράφων και με την λύση IRM .	ΝΑΙ		
3.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να καλύπτει τετρακόσια (400) τερματικά του οργανισμού	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
4.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να μπορεί να ανιχνεύει την ενέργεια και να λαμβάνει μέτρα (πχ αποτροπή / αιτιολόγηση / ενημέρωση) εάν ένας χρήστης αντιγράψει και επικολλήσει δεδομένα σε έναν μη έμπιστο προορισμό.	NAI		
5.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) πρέπει να μπορεί να επιθεωρεί την κυκλοφορία SSL (SSLinspection) εάν απαιτείται αλλά και να υποστηρίζει εξαιρέσεις (targetsw Whitelisting).	NAI		
6.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να μπορεί να παρέχει σε πραγματικό χρόνο καταγραφών της διακίνησης των δεδομένων στα πληροφοριακά συστήματα.	NAI		
7.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να μπορεί να καταγράφει τις κινήσεις που δεν είναι συμβατές με την αποδεκτή πολιτική διακίνησης δεδομένων,	NAI		
8.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να παρακολουθεί μέσω κεντρικής κονσόλα διαχείρισης την συνολική εικόνα διακίνησης των δεδομένων δηλ. ποια είδη δεδομένων χρησιμοποιούνται, ή διαβιβάζονται και από ποιους	NAI		
9.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να ανιχνεύει τις κινήσεις που αφορούν ενέργειες επί των δεδομένων στα τελικά σημεία όπως για παράδειγμα copy/paste σε εξωτερική μονάδα δίσκου ή USBstick, εκτυπώσεις αρχείων, λειτουργία printscreen.	NAI		
10.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να ανιχνεύει την διακίνηση δεδομένων από μέσα προς τα έξω, μέσω των κεντρικών δικτυακών υποδομών και μέσω των διαφόρων	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	πρωτοκόλλων επικοινωνίας ftp, http, https, smtp, αλλά και στιγμιαίο μήνυμα (IM).			
11.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να δημιουργεί incidents τα οποία πρέπει να διαβαθμίζονται αυτόματα σε διάφορα επίπεδα διαβάθμισης (πχ low, high, serious), με βάση τις πολιτικές και την κατηγοριοποίηση των δεδομένων.	ΝΑΙ		
12.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει αποστέλλει ενημερώσεις ασφαλείας με διάφορα μέσα επικοινωνίας παραβίασης (πχ. Email, sms, κλπ)	ΝΑΙ		
13.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να είναι σε θέση να σαρώσει, να εντοπίσει και να αποτρέψει τη διαρροή (με βάση τις πολιτικές) που είναι αποθηκευμένα στις ακόλουθες μορφές: 1. Αρχεία Excel 2. Αρχεία με οριοθετημένες στήλες (συγκεκριμένη γραμμογράφηση) 3. Δεδομένα που αποθηκεύονται σε γνωστές βάσεις δεδομένων όπως Oracle, MS-SQL, PostgreSQL, MongoDB, DB2 και χρησιμοποιεί η εταιρεία. 4. Δεδομένα που αποθηκεύονται σε συστήματα διαμοιρασμού εγγράφων: <ul style="list-style-type: none"> • Filenet • Sharepoint • OneDrive • OwnCloud • Windows Filesharing 	ΝΑΙ		
14.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) πρέπει να περιέχει δυνατότητες αναγνώρισης δεδομένων σε όλα τα πληροφοριακά συστήματα του οργανισμού, βάσει πολιτικών περιεχομένου (π.χ. λέξεις-κλειδιά, regular expressions, περιεχόμενα λεξικών κ.λπ.). Ο εγκαταστάτης θα πρέπει να παρέχει υπηρεσίες ανάπτυξης Regular expressions οι οποίες να καλύπτουν την αναγνώριση των ακόλουθων δεδομένων: 1. Αριθμοί Φορολογικού Μητρώου (ΑΦΜ)	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	2. Τηλεφωνικά νούμερα (Ελληνικά κινητά ή σταθερά τηλέφωνα) 3. Αριθμοί Ελληνικών Ταυτοτήτων. 4. Ελληνικά ονόματα (π.χ. πιθανώς με τεχνική λεξικού) 5. Διευθύνσεις (π.χ. πιθανώς με τεχνική λεξικού) 6. Αριθμοί πιστωτικών ή χρεωστικών καρτών 7. Αριθμοί λογαριασμών IBAN 8. Αριθμός Παροχής 9. Αριθμός Μητρώου Μισθωτού			
15.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα ανακαλύπτει τα δεδομένα που αποθηκεύονται σε διάφορους τύπους πληροφοριακών συστημάτων ενός δικτύου (discovery), όπως σε Fileservers ή κεντρικά storage καθώς και πάνω σε σταθμούς εργασίας (endpoints).	NAI		
16.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα παρέχει πληροφορίες για το περιεχόμενο των δεδομένων και για την διακίνηση τους, που θα δώσουν στους διαχειριστές ασφάλειας του ΔΕΔΔΗΕ πλήρη εποπτεία για το ποιος μπορεί να διακινήσει, ποιες πληροφορίες, από ποιο σημείο, και με ποιον τρόπο.	NAI		
17.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα καθορίζει πολιτικές αναζήτησης με βάση τα χαρακτηριστικά ή το περιεχόμενο των αρχείων.	NAI		
18.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα καθορίζει με βάση τις απαιτήσεις του οργανισμού ποιες αναζητήσεις μπορούν να γίνουν σε εργάσιμες ώρες, και ποιες λόγω όγκου και επιβάρυνσης του δικτύου, πρέπει να γίνονται σε προγραμματισμένες μη εργάσιμες ώρες.	NAI		
19.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα καθορίζει τις περιοχές	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	καθώς και των Τελικών Σημείων που θα εκτελείται η αναζήτηση δεδομένων.			
20.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) πρέπει να αποτρέπει τη διαρροή εταιρικών πληροφοριών, που είναι: 1. Αποθηκευμένες σε Πληροφοριακά Συστήματα (in rest) 2. Σε διαμετακόμιση (in transit) 3. Σε χρήση (in use)	ΝΑΙ		
21.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) πρέπει να καλύπτει τις ακόλουθες ανάγκες του οργανισμού: 1. Πρόληψη απώλειας δεδομένων προς τον ιστό (forward Proxy) 2. Πρόληψη απώλειας δεδομένων στο email 3. Πρόληψη απώλειας δεδομένων στο OWA - Outlook Web Access (web mail reverse proxy) 4. Πρόληψη απώλειας δεδομένων στο δίκτυο / VPN 5. Πρόληψη απώλειας δεδομένων από τα τερματικά (π.χ. αποτροπή εξαγωγής δεδομένων σε αφαιρούμενες συσκευές)	ΝΑΙ		
22.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) πρέπει να έχει δυνατότητα να εφαρμόσει τους ακόλουθους κανόνες / τύπους ενεργειών επί των δεδομένων : 1. Επιτρεπτή ενέργεια (allow) 2. Αποτροπή (block) 3. προειδοποίηση και αιτιολόγηση (π.χ. αίτημα προς τον τελικό χρήστη να περιγράψει τον λόγο για τον οποίο θέλει να κάνει την ενέργεια) 4. Καραντίνα 5. Κρυπτογράφηση Ο Οργανισμός θα μπορεί να επιλέξει για ποιες από τις παραπάνω ενέργειες θα πρέπει να δημιουργούνται άμεσα alerts σε καθορισμένους ρόλους	ΝΑΙ		
23.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να μπορεί να ανιχνεύει και να αποτρέπει τη διαρροή δεδομένων (βάσει πολιτικών), μέσω οποιουδήποτε πιθανού	ΝΑΙ		



A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	καναλιού επικοινωνίας δεδομένων, και οπωσδήποτε από τα ακόλουθα: 1. HTTP / HTTPS 2. FTP / FTPS 3. SMB (Κοινή χρήση αρχείων) 4. SSH / Telnet 5. VPN / OpenVPN (TLS / SSL / IPSEC / PPTP / PPTPS) 6. RDP 7. POP / POP3 / IMAP / IMAP4 / SMTP 8. IRC / SNMP 9. RPC / NFS 10. Rsync			
24.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να μπορεί να εντοπίζει και να αποτρέπει διαρροές δεδομένων ηλεκτρονικού ταχυδρομείου μέσω: 1. Microsoft Outlook 2. Outlook Web Anywhere (OWA) 3. Outlook Active Sync	ΝΑΙ		
25.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP), θα πρέπει να μπορεί να εντοπίζει και να αποτρέπει διαρροές δεδομένων από τους τερματικούς σταθμούς που επιχειρούνται μέσω των ακόλουθων καναλιών: 1. Wi-Fi 2. USB 3. Κάρτες Micro / Mini / Midi SD 4. CD / DCD 5. NFS / SMB	ΝΑΙ		
26.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να μπορεί να ανιχνεύει και να αποτρέπει διαρροές δεδομένων μέσω οποιουδήποτε τύπου εφαρμογών cloud, όπως: 1. Skype / Skype for business 2. DropBox 3. Evernote	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	4. OneDrive 5. iCloud 6. GoogleDrive 7. OneNote 8. Yammer 9. Jabber 10. Logmein 11. Citrix 12. TeamViewer 13. WebEx 14. Gmail 15. Facebook 16. Twitter 17. Instagram 18. Yammer 19. Wetransfer 20. Γιουσέντιτ 21. YouTransfer 22. Sendanywhere 23. FileDrop 24. BOX25. Filenet 26. Sharepoint 27. Teams 28. Etc.			
27.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να μπορεί να αναγνωρίζει, να ταξινομεί και να αποτρέπει τη διαρροή (βάσει πολιτικών) εγγράφων της ακόλουθης μορφής: 1. Σουίταγραφείου (π.χ. Word, Excel, Power Point, Visio, Microsoft Project, one-note κ.λπ.). 2. Email Outlook (π.χ. msg, pst, ost, κλπ) 3. Αρχεία PDF 4. Αρχείακειμένου (π.χ. TXT, ASC, ANS, ACL, O, HTML, XML, ODM, OTT, INFO, PAP, PAGES κ.λπ.)	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	<p>5. Συμπιεσμένα αρχεία (π.χ. ZIP, 7zip, RAR, WinRAR, BZip, Gzip, Tar, Bz2 κ.λπ.)</p> <p>6. Αρχεία βίντεο (π.χ. mpg, mp4, amv, wmv, mov, avi, mkv κ.λπ.)</p> <p>7. Αρχεία ήχου (π.χ. mp3, wma, wav, DVR-MS, WTV κ.λπ.)</p> <p>8. Αρχεία εικόνων (π.χ. JPEG, TIFF, GIF, BMP, PNG, AI, CDR, ADT, PSD, PUB κ.λπ.)</p> <p>9. Αρχεία βάσης δεδομένων (π.χ. ACCDB, ADT, DB, MDB, MYD, MYI, ORA, SQL, SDF, sqlite,</p> <p>10. Κρυπτογραφημένα αρχεία (π.χ. ssh, pub, ppk, cert, crt, der, p7b, PEM, PFX, AXX, EEA, TC, BPW, KDB, KDBX κ.λπ.)</p> <p>11. Άλλοι τύποι αρχείων (π.χ. CMD, BAT, JSP, PL, PHP, ASP, PYO, VBS κ.λπ.)</p>			
28.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να μπορεί να ανιχνεύει την ενέργεια και να λαμβάνει μέτρα (πχ αποτροπή / αιτιολόγηση / ενημέρωση) εάν ένας χρήστης προσπαθήσει να εκτυπώσει ή να αντιγράψει την οθόνη (printscreen)	ΝΑΙ		
29.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να έχει ενσωματωμένη δυνατότητα να φιλτράρει την δικτυακή κίνηση, να ανιχνεύει την ενέργεια και να λαμβάνει μέτρα (πχ αποτροπή / αιτιολόγηση / ενημέρωση) εάν ένα έγγραφο με τύπο εικόνας περιέχει διαβαθμισμένες πληροφορίες (π.χ. δυνατότητες OCR)	ΝΑΙ		
30.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) προστατεύει τα δεδομένα, με συγκεκριμένες διαδικασίες και με προκαθορισμένες αυτοματοποιημένες πολιτικές βασισμένες πάνω στις πολιτικές ασφαλείας που ορίζει η εταιρεία αλλά και με εκτεταμένο εύρος ενσωματωμένων πολιτικών ανά γεωγραφική περιοχή και επιχειρηματική δραστηριότητα.	ΝΑΙ		
31.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα εκτελεί συγκεκριμένες κινήσεις όταν οι ενέργειες του χρήστη	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	παραβαίνουν την πολιτική ασφάλειας του Οργανισμού.			
32.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα καταγράφει την ενέργεια του χρήστη (Monitor)	ΝΑΙ		
33.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα προειδοποιεί τον χρήστη (Alert)	ΝΑΙ		
34.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα αποτρέπει αυτόματα μία ενέργειας του χρήστη (Block),	ΝΑΙ		
35.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα μπορεί να απαιτεί από τον χρήστη αιτιολόγησης μίας ενέργειας (Justify).	ΝΑΙ		
36.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα μπορεί να παραμετροποιεί τους κανόνες που καθορίζουν το είδος της ενέργειας που θα εκτελέσει το σύστημα DLP, ώστε να λαμβάνουν υπ όψιν την ταυτότητα του χρήστη που επιχειρεί την διακίνηση των δεδομένων, το είδος των δεδομένων, τον υπο διακίνηση δεδομένων, τον όγκο των υπο διακίνηση δεδομένων, την πηγή και τον αποδέκτη των δεδομένων, κλπ.	ΝΑΙ		
37.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να κατηγοριοποιεί δεδομένα των εφαρμογών συνολικά	ΝΑΙ		
38.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα μπορεί να δημιουργεί κανόνες ελέγχου για συγκεκριμένες κατηγορίες τελικών σημείων	ΝΑΙ		
39.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) δεν θα έχει περιορισμούς στον αριθμό των κανόνων ελέγχου και θα μπορεί να εφαρμόζει πολλαπλούς κανόνες	ΝΑΙ		
40.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα εφαρμόζει κανόνες με	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	βάση το σύστημα/εφαρμογή που προέρχονται τα δεδομένα			
41.	<p>Η κονσόλα διαχείρισης του Συστήματος Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να συλλέγει δεδομένα από οποιονδήποτε αισθητήρα DLP (με βάση agents ή με βάση το δίκτυο) και θα πρέπει να μπορεί να παρέχει τις ακόλουθες αναφορές:</p> <ol style="list-style-type: none"> 1. Χρήστες οι οποίοι έχουν τον μεγαλύτερο αριθμό ενεργοποίησης κανόνων (triggered policies). 2. Συμβάντα για τα οποία ενεργοποιήθηκε η πολιτική αποτροπής (Block) 3. Συμβάντα για τα οποία ενεργοποιήθηκε αιτιολόγησης (Justify) 6. Προσπάθειες (επιτυχείς ή ανεπιτυχείς) που έχουν γίνει για την απομάκρυνση εταιρικών δεδομένων όταν το τερματικό ήταν εκτός εταιρικού δικτύου ή όταν ήταν συνδεδεμένο στο εταιρικό δίκτυο. 7. Περιστατικά για τα οποία ενεργοποιήθηκε Καραντίνα 8. Αναφορές ανά κανόνα ή ανά πολιτική 	ΝΑΙ		
42.	Οι αναφορές και τα στατιστικά στοιχεία θα πρέπει να είναι διαθέσιμα σε μορφή excel ή CSV και επιπλέον να περιλαμβάνουν γραφήματα.	ΝΑΙ		
43.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) πρέπει να παράγει αρχεία καταγραφής συμβάντων από τις ενέργειες των χρηστών (logs), τα οποία θα πρέπει να μεταφέρονται εύκολα σε πλατφόρμα SIEM (να περιγραφεί ο τρόπος διασύνδεσης). Επίσης, το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) πρέπει να έχει τη δυνατότητα αποστολής μόνο ανώνυμων δεδομένων (απόκρυψη του ονόματος χρήστη).	ΝΑΙ		
44.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα μπορεί να δημιουργεί αναφορές σε διάφορα επίπεδα συμπεριλαμβανομένου πλήρες ιστορικού ανά ένδειξη/περιστατικό	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
45.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα μπορεί να δημιουργεί αναφορές που καλύπτουν τις απαιτήσεις του Νομοθετικού/Κανονιστικού πλαισίου	ΝΑΙ		
46.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα μπορεί να δημιουργεί αναφορές ανά χρήστη, τελικό σημείο, κατηγορία ένδειξης/περιστατικού, κλπ	ΝΑΙ		
47.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα μπορεί να δημιουργεί αναφορές που δίνουν την αποτύπωση της συνολικής εικόνα των εγκαταστάσεων της εφαρμογής σε επίπεδο εταιρείας και στατιστικών στοιχείων των κανόνων	ΝΑΙ		
48.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα έχει την δυνατότητα να μεταφέρει αυτοματοποιημένα τις καταγραφές σε συστήματα SIEM.	ΝΑΙ		
49.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) πρέπει να έχει ενσωματωμένη δυνατότητα να εντοπίζει και να απεικονίζει στην κονσόλα πληροφορία βασισμένη σε αποδεκτά στατιστικά μοντέλα για ποιοι είναι οι πιο επικίνδυνοι χρήστες για διαρροή δεδομένων.			
50.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) να υποστηρίζει μέσω παραμετροποίησης την ελληνική γλώσσα (π.χ. πληροφορίες αναδυόμενων παραθύρων)	ΝΑΙ		
51.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να αναγνωρίζει εάν ένας σταθμός εργασίας είναι συνδεδεμένος στο εταιρικό δίκτυο ή εκτός σύνδεσης εταιρικού δικτύου και να λαμβάνει τα κατάλληλα μέτρα σε κάθε περίπτωση (βάσει των πολιτικών DLP)	ΝΑΙ		
52.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να είναι σε θέση να αναγνωρίζει οποιονδήποτε τύπο κρυπτογραφημένων αρχείων και να δίνει την	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	δυνατότητα αποτροπής αποστολή τους εκτός της εταιρείας.			
53.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) πρέπει να είναι σε θέση να κρυπτογραφεί (βάσει πολιτικών) έγγραφα που έχουν χαρακτηριστεί ως εμπιστευτικά (μέσω εφαρμογής διαβάθμισης εγγράφων), όταν επιχειρείται η εξαγωγή τους από τον σταθμό εργασίας (endpoint) σε αποσπώμενα μέσα αποθήκευσης (USB).	ΝΑΙ		
54.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) πρέπει να έχει δυνατότητα ψευδοανωνυμοποίησης σχετικά με τα λεπτομερή αποτελέσματα των ενεργειών των χρηστών. Τα αποτελέσματα της ανάλυσης θα πρέπει να προβάλλονται μόνο μετά από αίτημα παροχής στοιχείων σε περίπτωση συμβάντος και με την τεχνική splitknowledge (π.χ. διαπιστευτήρια του CISO και του διευθυντή IT).	ΝΑΙ		
55.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να υποστηρίζει την ελληνική γλώσσα, σε αναδυόμενα παράθυρα (pop-us). Επιπλέον, θα πρέπει να αναγνωρίζει ελληνικούς χαρακτήρες που μπορεί να περιλαμβάνονται σε έγγραφα.	ΝΑΙ		
56.	Ο agent του Συστήματος Αποτροπής Διαρροής Δεδομένων (DLP) δεν πρέπει να καταναλώνει περισσότερο από 5% των πόρων σταθμού εργασίας / διακομιστή, βάσει δεδομένων και έγκυρων μετρήσεων.	ΝΑΙ		
57.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) πρέπει να είναι απολύτως συμβατό με το Σύστημα Διαβάθμισης Δεδομένων (π.χ. τα μεταδεδομένα τα σχετικά με το επίπεδο διαβάθμισης οποιουδήποτε αρχείου πρέπει να αναγνωρίζονται, από το εργαλείο DLP το οποίο θα εφαρμόζει κατάλληλες πολιτικές ελέγχου) και με τα υπόλοιπα συστήματα του Οργανισμού.	ΝΑΙ		
58.	Ο agent που εγκαθίσταται στο τερματικό χρήστη πρέπει να προστατεύεται από	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	περιπτώσεις κακόβουλης απενεργοποίησης. Θα πρέπει να υπάρχει άμεση ενημέρωση (alert) σε περίπτωση που εντοπιστεί περίπτωση μη εξουσιοδοτημένης απενεργοποίησης			
59.	Η σειρά εφαρμογής ή προτεραιότητα των κανόνων / πολιτικών θα πρέπει να είναι σαφής και να καθορίζεται είτε από την σειρά της δήλωσής τους ή ρητά με αριθμό προτεραιότητας ή σπουδαιότητας.	ΝΑΙ		
60.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) πρέπει να υποστηρίζει λειτουργίες διαχείρισης πολιτικής όπως, μεταξύ άλλων, προσθήκη πολιτικής, κατάργηση πολιτικής, ενεργοποίηση πολιτικής, απενεργοποίηση πολιτικής, προσθήκη, κατάργηση και αλλαγή κανόνων πολιτικής, αλλαγή παραμέτρων πολιτικής, σύνδεση πολιτικής με συγκεκριμένους agents, πολιτική δοκιμών κ.λπ.	ΝΑΙ		
61.	Το "UserInterface" του συστήματος πρέπει να καθορίζεται με βάση τους ρόλους του συστήματος. Πρέπει να διακρίνονται κατ'ελάχιστον οι ρόλοι (α) διαχειριστής, (β) υπεύθυνος ασφαλείας, (γ) κοινός χρήστης	ΝΑΙ		
62.	Ο agent του συστήματος Αποτροπής Διαρροής Δεδομένων (DLP) θα μπορεί να εγκαθίσταται εξ αποστάσεως και θα είναι συμβατός με άλλα εργαλεία που λειτουργούν στα τελικά σημεία (antivirus κλπ)	ΝΑΙ		
63.	Οι agents του Συστήματος Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να είναι δυνατόν να εγκατασταθούν στα τελικά σημεία (endpoint) εξ αποστάσεως	ΝΑΙ		
64.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα έχει την δυνατότητα εγκατάστασης δικτυακών στοιχείων για την παρακολούθηση της διακίνησης δεδομένων μέσω του κεντρικού δικτύου,	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
65.	Οι κανόνες θα εφαρμόζονται τόσο σε online όσο και offline κατάσταση του τελικού σημείου	ΝΑΙ		
66.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα δίνει την δυνατότητα Ενεργοποίησης/Απενεργοποίησης κανόνων εξ αποστάσεως μόνο από συγκεκριμένους εξουσιοδοτημένους χρήστες	ΝΑΙ		
67.	Οι άμεσες ενημερώσεις θα διαχειρίζονται εύκολα και κεντρικοποιημένα	ΝΑΙ		
68.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να μπορεί να διακρίνει ρόλους χρηστών στην κεντρική κονσόλα διαχείρισης	ΝΑΙ		
69.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) δεν θα πρέπει να δίνει την δυνατότητα απενεργοποίησης της εφαρμογής από τον τελικό χρήστη	ΝΑΙ		
70.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να υποστηρίζει διεπαφές (RESTAPI) ώστε να εξασφαλίζεται η διαλειτουργικότητα του με τα υφιστάμενα πληροφοριακά συστήματα του ΔΕΔΔΗΕ.	ΝΑΙ		
71.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να μπορεί να διαχειρίζεται μεγάλο όγκου δεδομένων	ΝΑΙ		
72.	Το Σύστημα Αποτροπής Διαρροής Δεδομένων (DLP) θα πρέπει να είναι επεκτάσιμο	ΝΑΙ		
73.	Ο ανάδοχος πρέπει να παρέχει διαγράμματα αρχιτεκτονικής για το πώς θα υλοποιηθεί το Σύστημα και τους υπολογιστικούς πόρους που απαιτούνται για τη φιλοξενία του Συστήματος και για την Πρόληψη απώλειας δεδομένων.	ΝΑΙ		
74.	Ο ανάδοχος θα είναι υπεύθυνος για την εγκατάσταση της πλήρους υποδομής που απαιτείται για την υλοποίηση του Συστήματος (π.χ. εγκατάσταση λογισμικού	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	και λειτουργικού συστήματος, DB, εφαρμογής κ.λπ.).			
75.	Ο ανάδοχος θα είναι υπεύθυνος να εγκαταστήσει τους απαιτούμενους agents στους τερματικούς σταθμούς εργασίας των χρηστών.	ΝΑΙ		
76.	Ο ανάδοχος θα είναι υπεύθυνος για τη δημιουργία όλων των συμφωνημένων πολιτικών διαβάθμισης με βάση τις ανάγκες του φορέα.	ΝΑΙ		
77.	Ο ανάδοχος πρέπει να παρέχει την κατάλληλη εκπαίδευση σχετικά με τη λειτουργία του Συστήματος ώστε όλοι οι χρήστες να γνωρίζουν πως μπορούν να χρησιμοποιήσουν το σύστημα	ΝΑΙ		

7.2.4.9 Λύση Διαχείρισης Δικαιωμάτων Εγγράφων

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
1.	Η λύση πρέπει να επιτρέπει τον καθορισμό του είδους των δικαιωμάτων που έχει κάθε χρήστης επί του εγγράφου (πχ μόνο ανάγνωση, επεξεργασία, ορισμός δικαιούχων, κλπ)	ΝΑΙ		
2.	Η λύση πρέπει να επιτρέπει στους διαχειριστές να παρακολουθούν τις ενέργειες πρόσβασης (επιτυχείς ή αποτυχημένες) από τελικούς χρήστες.			
3.	Η λύση πρέπει να επιτρέπει σε επιλεγμένους χρήστες να παρακολουθούν τις ενέργειες πρόσβασης (επιτυχείς ή αποτυχημένες) από τελικούς χρήστες.			
4.	Η λύση πρέπει να δίνει τη δυνατότητα εξ αποστάσεως αναίρεσης των δικαιωμάτων που έχουν παραχωρηθεί σε χρήστες ή διαγραφής ενός εγγράφου	ΝΑΙ		
5.	Η λύση πρέπει να δίνει τη δυνατότητα ορισμού ημερομηνιών λήξης της ισχύος των δικαιωμάτων πρόσβασης.	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
6.	Η λύση πρέπει να δίνει τη δυνατότητα σε διαχειριστές να καθορίζουν πολιτικές πρόσβασης και σε χρήστες να εφαρμόζουν αυτές τις πολιτικές πρόσβασης σε έγγραφα.	ΝΑΙ		
7.	Η λύση Λύση Διαχείρισης Δικαιωμάτων Εγγράφων θα πρέπει να προσφερθεί για καλύπτει τετρακόσιους (400) χρήστες	ΝΑΙ		
8.	Η λύση πρέπει να έχει την δυνατότητα να αποδίδει συγκεκριμένα δικαιώματα πρόσβασης είτε σε μεμονωμένους χρήστες είτε σε ομάδες χρηστών.	ΝΑΙ		
9.	Η λύση πρέπει να έχει την δυνατότητα να εφαρμόζει πολιτικές απόδοσης δικαιωμάτων πρόσβασης τόσο σε επίπεδο εταιρείας όσο και σε συγκεκριμένους χρήστες.			
10.	Η λύση πρέπει να επιτρέπει σε επιλεγμένους χρήστες (όχι μόνο διαχειριστές) να διαχειρίζονται πολιτικές απόδοσης δικαιωμάτων πρόσβασης.			
11.	Η λύση πρέπει να δίνει την δυνατότητα καθορισμού των διαδικτυακών διευθύνσεων από τις οποίες επιτρέπεται η πρόσβαση στα έγγραφα.	ΝΑΙ		
12.	Η λύση πρέπει να αναγνωρίζει και να αυθεντικοποιεί τους χρήστες που ανήκουν στον οργανισμό μέσω πλήρους λειτουργικής διασύνδεσης με το AD του οργανισμού.	ΝΑΙ		
13.	Η λύση πρέπει να έχει την δυνατότητα απόδοσης συγκεκριμένων δικαιωμάτων πρόσβασης σε χρήστες που ανήκουν σε συγκεκριμένες ομάδες του οργανισμού (ActiveDirectorygroups).	ΝΑΙ		
14.	Η λύση πρέπει να δίνει την δυνατότητα να καθορίζονται ονομαστικά οι χρήστες (εσωτερικοί ή εξωτερικοί) στους οποίους επιτρέπεται η πρόσβαση σε έγγραφα του οργανισμού καθώς και το είδος της πρόσβασης που παρέχεται.	ΝΑΙ		
15.	Η λύση πρέπει να δίνει την δυνατότητα να καθορίζονται ομάδες χρηστών στις οποίες			

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	επιτρέπεται η πρόσβαση σε έγγραφα του οργανισμού.			
16.	Η λύση πρέπει να έχει την δυνατότητα αποστολής ειδοποιήσεων/προσλήσεων (invitations) σε εξωτερικούς χρήστες στους οποίους παραχωρείται πρόσβαση σε ένα έγγραφο.	ΝΑΙ		
17.	Οι χρήστες στους οποίους αποδίδεται δικαίωμα πρόσβασης σε ένα έγγραφο πρέπει να μπορούν να διαχειρίζονται το έγγραφο χωρίς την χρήση ειδικών προγραμμάτων (transparency).	ΝΑΙ		
18.	Η λύση πρέπει να δίνει την δυνατότητα καθορισμού δικαιωμάτων πρόσβασης σε οποιονδήποτε τύπο αρχείου			
19.	Η λύση πρέπει να δίνει την δυνατότητα καθορισμού δικαιωμάτων πρόσβασης είτε σε διακριτά έγγραφα είτε σε όλα τα έγγραφα που διατηρούνται σε συγκεκριμένα διακριτά σημεία διατήρησης (φακέλους ή μέσα αποθήκευσης).	ΝΑΙ		
20.	Η λύση πρέπει να δίνει δυνατότητα καθορισμού δικαιωμάτων πρόσβασης σε αρχεία που διατηρούνται σε τοπικούς σταθμούς εργασίας, servers, σε εφαρμογές νέφους (Office365, Sharepoint, OneDrive, κλπ).	ΝΑΙ		
21.	Ο τρόπος διαχείρισης των δικαιωμάτων πρόσβασης των εγγράφων θα πρέπει να είναι ίδιος ανεξάρτητα από το μέσο διατήρησης των αρχείων.	ΝΑΙ		
22.	Η λύση πρέπει να έχει πλήρη συμβατότητα με τις εφαρμογές του Office 365 και να δίνει δυνατότητα στους χρήστες των εφαρμογών να καθορίζουν τα δικαιώματα επί των δεδομένων μέσα από το περιβάλλον των ίδιων των εφαρμογών ή μέσω της εφαρμογής.	ΝΑΙ		
23.	Η λύση πρέπει να έχει πλήρη συμβατότητα με τις εφαρμογές Outlook και Exchange.	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
24.	Η λύση πρέπει να έχει δυνατότητα καθορισμού δικαιωμάτων πρόσβασης σε αρχεία pdf.	ΝΑΙ		
25.	Η λύση πρέπει να έχει την δυνατότητα λειτουργικής διασύνδεσης με την λύση DLP του Οργανισμού (DataLossPrevention) και τη λύση Διαβάθμισης Εγγράφων καθώς και τις υπόλοιπες εφαρμογές του Οργανισμού.	ΝΑΙ		
26.	Δυνατότητα Διασύνδεσης με το SIEM του οργανισμού	ΝΑΙ		
27.	Ο ανάδοχος πρέπει να παρέχει την κατάλληλη εκπαίδευση σχετικά με τη λειτουργία του Συστήματος ώστε όλοι οι χρήστες να γνωρίζουν πως μπορούν να χρησιμοποιήσουν το σύστημα	ΝΑΙ		

7.2.4.10 Λύση Διαχείρισης Λογαριασμών και Δικαιωμάτων Πρόσβασης Χρηστών

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Να αναφερθεί το όνομα, η έκδοση, η ημερομηνία ανακοίνωσης και ο κατασκευαστής της προσφερόμενης πλατφόρμας.	ΝΑΙ		
	Ο κατασκευαστής της προσφερόμενης πλατφόρμας λογισμικού Identity&AccessRightsManagement IAM θα πρέπει να διαθέτει τοπική παρουσία με τοπικό γραφείο εκπροσώπησης / θυγατρική στην Ελλάδα	ΝΑΙ		
	ΗπροσφερόμενηΛύσηIdentity&AccessRightsManagementIAM θακαλύπτειχίλιους (1.000) λογαριασμούς.	ΝΑΙ		
	Η προτεινόμενη αρχιτεκτονική υλοποίησης της πλατφόρμας θα πρέπει να περιλαμβάνει λειτουργία σε διάταξη υψηλής διαθεσιμότητας.	ΝΑΙ		
	Η προτεινόμενη αρχιτεκτονική υλοποίησης της πλατφόρμας θα πρέπει να υποστηρίζει λειτουργία 24x7.	ΝΑΙ		
	Χρήση μιας κεντρικής ενιαίας σχεσιακής βάσης δεδομένων για την διαχείριση του συνόλου των δεδομένων της προτεινόμενης πλατφόρμας.	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Η προτεινόμενη αρχιτεκτονική υλοποίησης της πλατφόρμας θα πρέπει να προσφέρει τη δυνατότητα οριζόντιας και κάθετης κλιμάκωσης.	ΝΑΙ		
	Η δυνατότητα οριζόντιας κλιμάκωσης θα προβλέπει δυναμική προσθήκη επιπλέον κόμβων στη βάση δεδομένων και στους εξυπηρετητές εφαρμογών της πλατφόρμας χωρίς καμιά διακοπή της υπηρεσίας. Κάθε νέος κόμβος που θα προστίθεται θα γίνεται άμεσα ενεργός και θα αναλαμβάνει μέρος του φόρτου εργασίας και των συνδέσεων των εφαρμογών.	ΝΑΙ		
	Οι προσφερόμενες άδειες χρήσης λογισμικού της πλατφόρμας IAM θα επιτρέπουν στον φορέα εάν το επιθυμεί να μεταφέρει και να λειτουργήσει την πλατφόρμα IAM σε υποδομές PublicCloud. Η προσφερόμενη λύση θα πρέπει να μπορεί να μεταφερθεί και να λειτουργήσει κατ'ελάχιστων στις ακόλουθες υποδομές Δημόσιου Νέφους (PublicCloudInfrastructure): α) Microsoft Azure, β) Amazon Web Services.			
	Όλα τα δομικά συστατικά της προτεινόμενης πλατφόρμας λογισμικού θα πρέπει να λειτουργούν σε διάταξη υψηλής διαθεσιμότητας και ισοκατανομής φόρτου εργασίας	ΝΑΙ		
	Υποστήριξη κεντριοποιημένης πολιτικής με χρήση των ακόλουθων στοιχείων: • Χρήστες (users) • Ρόλοι χρηστών (roles) • Δικαιώματα (permissions) • Εφαρμογές (applications) • Εξαιρέσεις (exclusions) • Κίνδυνοι (risks) Οργανισμοί (organizations)	ΝΑΙ		
	Υποστήριξη εκχώρησης της δυνατότητας εκτέλεσης των διαθέσιμων διαχειριστικών ενεργειών στο σύστημα είτε απευθείας σε χρήστες, είτε σε ομάδες χρηστών (delegatedadministration).	ΝΑΙ		
	Εργαλείο αναζήτησης βάση πολλαπλών κριτηρίων.	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Δυνατότητα επαναφοράς του συνθηματικού χρήστη στις εφαρμογές από τον χρήστη, χωρίς τη διαμεσολάβηση διαχειριστή (self-servicepasswordreset).	ΝΑΙ		
	Η πλατφόρμα θα πρέπει να υποστηρίζει πολλαπλά πρωτόκολλα για αυθεντικοποίηση και εξουσιοδότηση (Active Directory/ADFS, LDAP, OpenID, OAuth, Identity Management Systems etc).	ΝΑΙ		
	Να περιγραφεί η διαδικασία εξουσιοδότησης και συγκεκριμένα η διαδικασία δημιουργίας ρόλων και ανάθεσης δικαιωμάτων εξουσιοδότησης.	ΝΑΙ		
	Η πλατφόρμα θα πρέπει να παρέχει δυνατότητες προσαρμογής της διεπαφής χρήσης καθώς και των connectors και των διαδικασιών.	ΝΑΙ		
	Η πλατφόρμα θα πρέπει να υποστηρίζει την παραμετροποίηση τήρησης των αποθηκευμένων διαπιστευτηρίων (saved/cachedcredentials).	ΝΑΙ		
	Η πλατφόρμα θα πρέπει να διασφαλίζει την εξουσιοδοτημένη πρόσβαση σε υπηρεσίες και δεδομένα.	ΝΑΙ		
	Η πλατφόρμα θα πρέπει να παρέχει τη δυνατότητα ανάθεσης μόνο των τελείως απαραίτητων δικαιωμάτων σε κάθε χρήστη ανάλογα με τον ρόλο του και εφαρμόζοντας την αρχή του LeastPrivilege.	ΝΑΙ		
	Η πλατφόρμα θα πρέπει να υποστηρίζει το RESTAPIs για εισερχόμενες διεπαφές με τρίτα συστήματα.	ΝΑΙ		
	Να διατεθούν και να υλοποιηθούν adaptersμε τον ActiveDirectoryκαι με μία βάση (Oracleή MSSQL) του Φορέα	ΝΑΙ		
	Η προτεινόμενη πλατφόρμα θα πρέπει να έχει τη δυνατότητα διασύνδεσης με ActiveDirectory για την παραμετροποίηση των ρόλων των χρηστών.	ΝΑΙ		
	Η πλατφόρμα θα πρέπει να υποστηρίζει το RoleBasedAccessControl (RBAC) μοντέλο. Θα πρέπει να ανατεθούν σε χρήστες επιχειρησιακοί ρόλοι που θα μεταφράζονται σε δικαιώματα εφαρμογών και θα ανταποκρίνονται στη θέση τους στον οργανισμό.	ΝΑΙ		
	Η πλατφόρμα θα πρέπει να υποστηρίζει MultiFactorAuthentication.	ΝΑΙ		
	Δυνατότητα δημιουργίας ροών αιτημάτων χρήσης μέσω γραφικού περιβάλλοντος, με τα παρακάτω χαρακτηριστικά:	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	<ul style="list-style-type: none"> Υποστήριξη παράλληλων και σειριακών διεργασιών με αιτήματα έγκρισης από ευέλικτα καθοριζόμενους χρήστες (approvaltasks). Δυνατότητα προώθησης συγκεκριμένων αιτημάτων έγκρισης σε άλλους χρήστες. Δυνατότητα προσωρινής εκχώρησης των δικαιωμάτων έγκρισης σε άλλο χρήστη (και με ημερομηνία λήξης). Δυνατότητα παρακολούθησης της κατάστασης ενός αιτήματος (και για χρήστες μη εγγεγραμμένους στο σύστημα). Δυνατότητα έγκρισης/απόρριψης ενός αιτήματος από το e-mail του χρήστη. <p>Δυνατότητα έναρξης αιτημάτων για δημιουργία λογαριασμού χωρίς την ανάγκη κατοχής λογαριασμού χρήσης στο σύστημα.</p>			
	Δυνατότητα υποστήριξης αυτόματων μεταβολών στις προσβάσεις ενός χρήστη ανάλογα με τις κινήσεις που γίνονται στο trustedsource (HRMS) σύστημα (πρόσληψη, μετακίνηση, αλλαγή θέσης, τερματισμός).	NAI		
	Αυτοματοποιημένη μεταβολή των δικαιωμάτων πρόσβασης στα συνδεδεμένα (connected) συστήματα.	NAI		
	Δυνατότητα αποδοχής ή άρνησης των αιτήσεων πρόσβασης στις εφαρμογές.	NAI		
	Δυνατότητα προσωρινής εκχώρησης των δικαιωμάτων έγκρισης σε άλλο χρήστη (και με ημερομηνία λήξης).	NAI		
	Δυνατότητα παρακολούθησης της κατάστασης ενός αιτήματος (και για χρήστες μη εγγεγραμμένους στο σύστημα).	NAI		
	Να παρέχεται έτοιμο λογισμικό, χωρίς την ανάγκη ανάπτυξης κώδικα, για τη σύνδεση με συστήματα αποθήκευσης χρηστών (userrepositories). Να αναφερθούν τα υποστηριζόμενα συστήματα	NAI		
	Να παρέχονται εύκολα παραμετροποιήσιμοι οδηγοί (wizards) για την σύνδεση και διαχείριση χρηστών σε συστήματα ευρέως χρησιμοποιούμενων τεχνολογιών (π.χ CSV αρχεία, συστήματα, συστήματα με webservices διεπαφές, πίνακες σε βάσεις δεδομένων με ειδική μορφή).	NAI		
	Δυνατότητα διασύνδεσης εφαρμογών ως disconnected, με την αποστολή εργασίας (task) στον διαχειριστή ενός	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	συστήματος, ώστε να μπορούν να συνδεθούν δυνητικά όλες οι εφαρμογές του οργανισμού.			
	Η πλατφόρμα θα πρέπει να διαθέτει connectors τα οποία θα πρέπει να υποστηρίζουν εργασίες για το provisioning (δημιουργία, ενημέρωση, κατάργηση) των χρηστών στα διασυνδεδεμένα συστήματα καθώς και το reconciliation αυτών (ανάκτηση χρήστη και των δικαιωμάτων του). Οι προσβάσεις που έχουν αποδοθεί εκτός των διαδικασιών της λύσης, θα πρέπει να έχουν την αντίστοιχη ένδειξη για να μπορούν να ληφθούν αποφάσεις είτε χειροκίνητα (κατάργηση τους από τον διαχειριστή του συστήματος) είτε αυτόματα (κατάργηση τους μέσω διεργασίας).	ΝΑΙ		
	Ορισμός πολιτικών εξαιρέσεων και διαχωρισμού των προσβάσεων ανάλογα με τον ρόλο του χρήστη (Segregation of Duties). Θα πρέπει να εφαρμόζονται οι πολιτικές κατά το αίτημα ενός χρήστη για πρόσβαση καθώς και να μπορεί να προγραμματιστεί περιοδικός έλεγχος που θα αναθέτει μια εργασία αποκατάστασης (remediation task) σε εξουσιοδοτημένους χρήστες.	ΝΑΙ		
	Καταγραφή του συνόλου των γεγονότων του συστήματος και παραγωγή έτοιμων αναφορών (out of the box reports) κατ'ελάχιστον για τα ακόλουθα: <ul style="list-style-type: none"> • Πολιτικές πρόσβασης ανά ρόλο χρηστών και συνδεδεμένο σύστημα • Κατάσταση αιτημάτων έγκρισης και εγκριτικών ροών εργασίας • Κατάσταση χρηστών ανά σύστημα και ρόλο χρηστών Δικαιώματα πρόσβασης ανά χρήστη, ρόλο, οργανισμό, και συνδεδεμένο σύστημα	ΝΑΙ		
	Το σύστημα θα πρέπει να υποστηρίζει τον σχεδιασμό νέων αναφορών μέσω wizards.	ΝΑΙ		
	Η πλατφόρμα θα πρέπει να προσφέρει δυνατότητες καταγραφής.	ΝΑΙ		
	Θα πρέπει να διαλειτουργεί με κεντρική logging ή SIEM υποδομή.	ΝΑΙ		
	Υποστήριξη κατηγοριοποίησης γεγονότων βασιζόμενοι σε τύπο (π.χ. error, warning, information, debug etc.) και σημαντικότητα (π.χ. critical, major, normal etc.) με τρόπο που να είναι εύκολο το φιλτράρισμα σε αναφορές.	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Το επίπεδο καταγραφής θα πρέπει να είναι προσαρμόσιμο.	ΝΑΙ		
	Να περιγράφουν οι δυνατότητες καταγραφής της πλατφόρμας αναφέροντας: <ul style="list-style-type: none"> ενέργειες και γεγονότα που καταγράφονται τεχνολογίες που χρησιμοποιούνται εκτυπωτικές δυνατότητες	ΝΑΙ		
	Η πλατφόρμα θα πρέπει να διατηρεί ιστορικά αρχεία (logs) με ασφαλή τρόπο που να αποτρέπει οποιαδήποτε απόπειρα τροποποίησης.	ΝΑΙ		
	Η γραφική διεπαφή της προσφερόμενης πλατφόρμας θα πρέπει να είναι διαθέσιμη σε πολλαπλά είδη συσκευών (desktop, tablet, mobile).	ΝΑΙ		
	Η γραφική διεπαφή της προσφερόμενης πλατφόρμας θα πρέπει να διατίθεται μέσω webbrowser.	ΝΑΙ		
	Υποστήριξη πολιτικών πρόσβασης με βάση τα παρακάτω κριτήρια: <ul style="list-style-type: none"> Εφαρμογή για την οποία ζητείται η πρόσβαση Ταυτότητα χρήστη Ομάδα χρήστη IP διεύθυνση Ώρα εισόδου	ΝΑΙ		
	Δυνατότητα υποστήριξης πολλαπλών μηχανισμών αυθεντικοποίησης όπως: <ul style="list-style-type: none"> Αναγνωριστικό Χρήστη/Κωδικός Πρόσβασης One Time Password Passwordless Authentication	ΝΑΙ		
	Δυνατότητα καθορισμού χρόνου λήξης ανενεργού συνόδου χρήσης (idlelogout).	ΝΑΙ		
	Καταγραφή και αναφορά της IP διεύθυνσης των συνδεδεμένων χρηστών.	ΝΑΙ		
	Παροχή API για την δημιουργία κατά παραγγελία μεθόδων αυθεντικοποίησης (customauthenticationmodules).	ΝΑΙ		
	Υψηλή διαθεσιμότητα αξιοποιώντας εγγενώς τεχνολογίες caching, διαμοιρασμού φορτίου, failover.	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Δυνατότητα ορισμού επιπέδων αυθεντικοποίησης μεταξύ των διαφόρων μεθόδων αυθεντικοποίησης (multi-level authentication) και αντιστοίχιση των επιπέδων με τις προσφερόμενες υπηρεσίες. Στην περίπτωση απόπειρας πρόσβασης σε υπηρεσία υψηλότερου επιπέδου από το τρέχον επίπεδο αυθεντικοποίησης του χρήστη, ο χρήστης θα πρέπει να προτρέπει για επιπρόσθετη αυθεντικοποίηση, (step-up authentication).	ΝΑΙ		
	Υποστήριξη δυνατοτήτων κληρονόμησης δικαιωμάτων από χρήστες ή ομάδες.	ΝΑΙ		
	Υποστήριξη του πρωτοκόλλου SAML 2.0.	ΝΑΙ		
	Υποστήριξη OAuth 2.0/OpenIDConnect	ΝΑΙ		
	Υποστήριξη αυτόματης αντιστοίχισης της ταυτότητας μεταξύ ενός απομακρυσμένου και ενός τοπικού χρήστη (account mapping).	ΝΑΙ		
	Δυνατότητα προτροπής της συγκατάβασης από τον χρήστη, για την σύνδεση ή όχι μεταξύ της τοπικής και απομακρυσμένης ταυτότητας (opt-in, opt-out sso)	ΝΑΙ		
	Να αναφερθούν λεπτομερώς οι δυνατότητες ολοκλήρωσης με υποδομή LDAP καταλόγου.	ΝΑΙ		
	Η πλατφόρμα πρέπει να προσφέρει ένα RoleMining εργαλείο για την ανάλυση των user accounts και των entitlements σε εφαρμογές και να προτείνει υποψήφιους επιχειρησιακούς ρόλους.	ΝΑΙ		
	Το RoleMining εργαλείο θα πρέπει να διαλειτουργεί με την πλατφόρμα για να: <ul style="list-style-type: none"> Φορτώνει δεδομένα από IDM πλατφόρμα που είναι απαραίτητα για ανάλυση Δημοσιεύει τον υποψήφιο ρόλο σε IDM πλατφόρμα για να γίνει διαθέσιμη σε αιτήσεις χρηστών	ΝΑΙ		
	Το RoleMining εργαλείο θα πρέπει να επιτρέπει κλιμακωτή φόρτωση υποψήφιων ρόλων σε IDM πλατφόρμα για να ενημερωθούν αλλαγές σε ρόλους αλλά και να φορτωθούν νέοι ρόλοι που δημιουργήθηκαν μετά το αρχικό load.	ΝΑΙ		
	Το RoleMining εργαλείο θα πρέπει να προσφέρει τη δυνατότητα σύγκρισης υποψήφιων ρόλων με τους υφιστάμενους ρόλους για τον εντοπισμό πιθανών διπλών ρόλων.	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Το RoleMining εργαλείο θα πρέπει προσφέρει τη δυνατότητα συγκέντρωσης δεδομένων από διαφορετικές πηγές (IDM και CSV αρχεία).	ΝΑΙ		
	Το RoleMining εργαλείο θα πρέπει προσφέρει δυνατότητες what-ifanalysis πριν δημοσιεύσει τους ρόλους σεIDM πλατφόρμα.	ΝΑΙ		
	Να αναφερθεί το όνομα, η έκδοση του προσφερόμενου Συστήματος Διαχείρισης Βάσεων Δεδομένων (Σ.Δ.Β.Δ.) και η χρονολογία διάθεσης της προσφερόμενης έκδοσης	ΝΑΙ		
	Υποστηριζόμενες πλατφόρμες υλικού και λογισμικού: - Unix και Linux - Windows	ΝΑΙ		
	Συνοπτική περιγραφή της αρχιτεκτονικής του προσφερόμενου Σ.Δ.Β.Δ., του τρόπου συνεργασίας με το Λ.Σ. και του τρόπου αξιοποίησης της φυσικής αρχιτεκτονικής του συστήματος	ΝΑΙ		
	Ο ανάδοχος πρέπει να παρέχει την κατάλληλη εκπαίδευση, ώστε όλοι οι χρήστες να γνωρίζουν πως μπορούν να χρησιμοποιήσουν το σύστημα	ΝΑΙ		

7.2.4.11 Λύση Διαχείρισης Προνομιούχων Λογαριασμών Πρόσβασης

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
1.	Να αναφερθεί το λογισμικό και ο κατασκευαστής.	ΝΑΙ		
2.	Αριθμός Υποστηριζόμενων Διαχειριστών	≥40		
3.	Αριθμός υποστηριζόμενων συνεργατών (namedusers)	≥15		
4.	Η προσφερόμενη λύση θα πρέπει να υποστηρίζει μηχανισμούς υψηλής διαθεσιμότητας.	ΝΑΙ		
5.	Η προσφερόμενη λύση θα πρέπει να υποστηρίζει διατάξεις Active/ Active και Active/ Passive.	ΝΑΙ		
6.	Η προσφερόμενη λύση θα πρέπει να υποστηρίζει την δυνατότητα οριζόντιας	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	κλιμάκωσης σε περιπτώσεις υψηλού φόρτου.			
7.	Η προσφερόμενη λύση θα πρέπει να υποστηρίζει την κλιμακούμενη αύξηση του αριθμού των χρηστών και των υποστηριζόμενων συστημάτων.	ΝΑΙ		
8.	Η προσφερόμενη λύση δεν θα πρέπει να χρειάζεται ενδιάμεσους "jumpservers" για την διαχείριση των συνδέσεων με τα υπό διαχείριση συστήματα.			
9.	Η πρόσβαση στην προσφερόμενη λύση θα πρέπει να υλοποιείται με χρήση διεθνών αναγνωρισμένων μηχανισμών κρυπτογράφησης .	ΝΑΙ		
10.	Η προσφερόμενη λύση θα πρέπει να υποστηρίζει, κατ' ελάχιστα, την διασύνδεση με τα ακόλουθα συστήματα: <ul style="list-style-type: none"> • Windows • (Windows 10, Windowsserver 2012, 2016 και 2019 και μεταγενέστερες). • Unix / Linux (Oracle Enterprise Linux, RHEL, AIX, Ubuntu). • Databases (DB2, Oracle, MSSQL, MongoDB, PostgreSQL). • Network devices (Checkpoint, Fortigate firewalls, HP και Cisco switches, routers, Cisco balancers, κτλ.) • Εικονικά Συστήματα. • Εφαρμογές Web. 	ΝΑΙ		
11.	Η προσφερόμενη λύση θα πρέπει να υποστηρίζει την εφαρμογή διαφορετικών πολιτικών συνθηματικών καθώς και εναλλαγής/ διαχείρισης περιόδων σύνδεσης.	ΝΑΙ		
12.	Η προσφερόμενη λύση θα πρέπει να υποστηρίζει την εφαρμογή ελέγχου ταυτότητας πολλαπλών παραγόντων (MFA) για τους διαχειριστές καθώς και μηχανισμούς ελέγχου ενός παράγοντα για όλες τις εταιρικές εφαρμογές ιστού και κινητών.	ΝΑΙ		



A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
13.	Η προσφερόμενη λύση θα πρέπει να υποστηρίζει μηχανισμούς ελέγχου ταυτότητας βασισμένους στον βαθμό επικινδυνότητας του χρήστη.	ΝΑΙ		
14.	Η προσφερόμενη λύση θα πρέπει να διαθέτει μηχανισμό προ-ελέγχου ταυτότητας για τις εφαρμογές που ανακτούν κωδικούς από ασφαλή αποθετήριο (securestore).	ΝΑΙ		
15.	Η προσφερόμενη λύση θα πρέπει να διαθέτει μηχανισμό ελέγχου πρόσβασης σε οποιοδήποτε σύστημα, υπηρεσία ή/ και εφαρμογή, που συνδέονται χρήστες με αυξημένα δικαιώματα καθώς και να παρέχει την δυνατότητα περιορισμού των δικαιωμάτων "superuser".	ΝΑΙ		
16.	Η προσφερόμενη λύση θα πρέπει να παρέχει την δυνατότητα σύνδεσης με αυξημένα δικαιώματα σε συστήματα, υπηρεσίες και εφαρμογές όταν αυτό απαιτείται.	ΝΑΙ		
17.	Η προσφερόμενη λύση θα πρέπει παρέχει την δυνατότητα εκχώρησης ρόλων στους λογαριασμούς χρηστών με σκοπό την διασφάλιση της αρχής του ελάχιστου δικαιώματος (leastprivilege) και αποφυγή παραχώρησης αυξημένων δικαιωμάτων πρόσβασης όταν δεν απαιτείται.	ΝΑΙ		
18.	Η προσφερόμενη λύση θα πρέπει να παρέχει την δυνατότητα τερματισμού ή αποκλεισμού μιας συνόδου (session) η οποία έχει υλοποιηθεί με λογαριασμό με αυξημένα δικαιώματα είτε λόγω αδράνειας είτε μετά από αίτημα του διαχειριστή.	ΝΑΙ		
19.	Η προσφερόμενη λύση θα πρέπει να παρέχει την δυνατότητα περιορισμού απομακρυσμένης πρόσβασης και ενεργειών σε συστήματα, υπηρεσίες ή/και εφαρμογές του οργανισμού.	ΝΑΙ		
20.	Η προσφερόμενη λύση θα πρέπει να παρέχει ένα ενοποιημένο περιβάλλον για τη διαχείριση πολλαπλών απομακρυσμένων	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	συνδέσεων RemoteDesktop και SSH από την ίδια κονσόλα.			
21.	Η προσφερόμενη λύση θα πρέπει να υποστηρίζει την δημιουργία συνεδρίας αυξημένων δικαιωμάτων για σύνδεση των διαχειριστών σε συστήματα Linux και συσκευές δικτύου μέσω SSH.	NAI		
22.	Η προσφερόμενη λύση θα πρέπει να υποστηρίζει την δημιουργία συνεδρίας αυξημένων δικαιωμάτων για σύνδεση των διαχειριστών σε συστήματα Windows μέσω RDP.	NAI		
23.	Τα δεδομένα της προσφερόμενης λύσης θα πρέπει να διατηρούν τα ίδια επίπεδα ασφάλειας και κρυπτογράφησης κατά την διαδικασία λήψης αντίγραφου ασφαλείας	NAI		
24.	Η προσφερόμενη λύση θα πρέπει να διαθέτει διαδικτυακή πύλη μέσω της οποίας οι χρήστες (εξωτερικοί και εσωτερικοί) θα αποκτούν πρόσβαση στα εξουσιοδοτημένα συστήματα.	NAI		
25.	Η προσφερόμενη λύση θα πρέπει να διαθέτει υποσύστημα για κινητές συσκευές μέσω της οποίας θα είναι διαθέσιμη η αποδοχή ή απόρριψη ροών έγκρισης.	NAI		
26.	Η προσφερόμενη λύση θα πρέπει να διαθέτει εφαρμογή για κινητές συσκευές η οποία θα λειτουργεί σαν εναλλακτική μέθοδος σύνδεσης κάνοντας χρήση λογαριασμού με αυξημένα δικαιώματα.	NAI		
27.	Η προσφερόμενη λύση θα πρέπει να παρέχει την δυνατότητα ανάκτησης κωδικού πρόσβασης μέσω SDK. Τα διαπιστευτήρια που σχετίζονται με την εφαρμογή θα πρέπει να αποθηκεύονται σε ένα ασφαλή αποθηκευτικό χώρο.	NAI		
28.	Η βάση δεδομένων της προσφερόμενης λύσης θα πρέπει να χρησιμοποιεί κρυπτογράφηση με κλειδί AES256 (AdvancedEncryptionStandards).	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
29.	Η προσφερόμενη λύση θα πρέπει να παρέχει δυνατότητα αναβάθμισης.	ΝΑΙ		
30.	Η προσφερόμενη λύση θα πρέπει να διασυνδέεται με κεντρικό κατάλογο χρηστών (ActiveDirectory). Να αναφερθούν οι δυνατότητες	ΝΑΙ		
31.	Η προσφερόμενη λύση θα πρέπει να παρέχει δυνατότητα αυθεντικοποίησης διαχειριστών που δεν ανήκουν στον Φορέα (εξωτερικοί συνεργάτες)	ΝΑΙ		
32.	Η πρόσβαση στην προσφερόμενη λύση θα πρέπει να επιτυγχάνεται με την χρήση των τρεχόντων διαπιστευτηρίων των χρηστών και χωρίς την ύπαρξη λογισμικού (agentless) στους σταθμούς εργασίας τους.	ΝΑΙ		
33.	Η προσφερόμενη λύση θα πρέπει να υποστηρίζει την δημιουργία κατά απαίτηση (adhoc) σύνδεσης με συγκεκριμένο τύπου τερματικού στην περίπτωση έλλειψης προεπιλεγμένης διασύνδεσης.	ΝΑΙ		
34.	Η προσφερόμενη λύση θα πρέπει να διαχειρίζεται διαπιστευτήρια βασισμένα στις πολιτικές που ορίζονται στα τελικά συστήματα καθώς και να επιτρέπει την διαχείριση των κλειδιών SSH και API για περιβάλλοντα νέφους.	ΝΑΙ		
35.	Η προσφερόμενη λύση θα πρέπει να εντοπίζει, να εισάγει και να διαχειρίζεται λογαριασμούς σε όλο το περιβάλλον του οργανισμού.	ΝΑΙ		
36.	Κατά τη δημιουργία νέου λογαριασμού με αυξημένα δικαιώματα, η προσφερόμενη λύση θα πρέπει να εντοπίζει και να ενημερώνει για την ύπαρξη προηγούμενου λογαριασμού με το ίδιο αναγνωριστικό σε οποιοδήποτε σύστημα, εφαρμογή και/ ή υπηρεσία, για την αποφυγή επαναχρησιμοποίησης του.	ΝΑΙ		
37.	Η προσφερόμενη λύση θα πρέπει να προστατεύει τις πληροφορίες που είναι απαραίτητες για την αυθεντικοποίηση των	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	χρηστών με αυξημένα δικαιώματα για την αποφυγή μια πιθανής εκμετάλλευσης από μη εξουσιοδοτημένους χρήστες.			
38.	Η προσφερόμενη λύση θα πρέπει να μπορεί να περιορίζει τις αποτυχημένες προσπάθειες σύνδεσης για την αποφυγή επιθέσεων τύπου bruteforce/ dictionaryattack και να ενημερώνει αυτόματα συγκεκριμένους χρήστες εντός της εταιρείας.	NAI		
39.	Να αναφερθούν οι μηχανισμοί ασφαλείας.	NAI		
40.	Η προσφερόμενη λύση θα πρέπει να υποστηρίζει την κρυπτογράφηση των αποθηκευμένων διαπιστευτηρίων χρησιμοποιώντας διεθνώς αναγνωρισμένους αλγόριθμους κρυπτογράφησης όπως AES-256, RSA-2048 κ.λπ.	NAI		
41.	Η προσφερόμενη λύση θα πρέπει να χρησιμοποιεί κρυπτογραφημένο κανάλι επικοινωνίας για την μεταφορά των δεδομένων από/ προς το αποθετήριο.			
42.	Η προσφερόμενη λύση θα πρέπει να μπορεί να αλλάζει αυτόματα, τα συνθηματικά που εισάγονται στο αποθετήριο.			
43.	Η προσφερόμενη λύση θα πρέπει να διασφαλίζει την εναλλαγή των συνθηματικών των λογαριασμών των χρηστών με υψηλά προνόμια.	NAI		
44.	Η προσφερόμενη λύση θα πρέπει να διασφαλίζει την εναλλαγή των συνθηματικών, όπου η ύπαρξη των λογαριασμών με αυξημένα δικαιώματα είναι απαραίτητη π.χ. κώδικας σε αρχεία παραμετροποίησης, συνδέσεις με βάσεις δεδομένων κ.λπ.			
45.	Η προσφερόμενη λύση θα πρέπει να παρέχει δυνατότητα αποθήκευσης στο αποθετήριο, διαπιστευτήρια που δεν πρέπει να γίνουν αλλαγή (π.χ. λογαριασμοί έκτακτης ανάγκης).			

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
46.	Η προσφερόμενη λύση θα πρέπει να παρέχει τη δυνατότητα αλλαγής των συνθηματικών που ανήκουν σε συστήματα καταλόγου, όπως και σε εκείνα που ανήκουν σε συστήματα Windows και Linux.	ΝΑΙ		
47.	Η προσφερόμενη λύση θα πρέπει να μπορεί να περιορίσει το χρόνο ισχύος των συνθηματικών που χρησιμοποιούνται από λογαριασμούς με αυξημένα προνόμια επιτρέποντας την δημιουργία εξαιρέσεων στην γενική πολιτική.	ΝΑΙ		
48.	Η προσφερόμενη λύση θα πρέπει να επιτρέπει την δημιουργία συνθηματικών μίας χρήσης και να διατηρεί ιστορικό των διαπιστευτηρίων για την αποφυγή επαναχρησιμοποίησης τους σύμφωνα με τους περιορισμούς χρόνου που έχει θέσει ο οργανισμός.	ΝΑΙ		
49.	Για περιστασιακές περιπτώσεις, η προσφερόμενη λύση θα πρέπει να διαθέτει μηχανισμό αυτόματης αλλαγή συνθηματικών.	ΝΑΙ		
50.	Η προσφερόμενη λύση θα πρέπει να δυνατότητα επιβολής της πολιτικής ασφάλειας του ΔΕΔΔΗΕ σχετικά με τους κωδικούς πρόσβασης και δυνατότητα να υποστηρίζει τις σχετικές κανονιστικές απαιτήσεις και τις βέλτιστες πρακτικές.			
51.	Η προσφερόμενη λύση θα πρέπει να επιβάλει κανόνες για την συνθετότητα των κωδικών, που περιλαμβάνουν μήκος κωδικών, μίξη αλφανουμερικών και ειδικών χαρακτήρων, διάκριση μεταξύ κεφαλαίων και μικρών (upper και lower).			
52.	Η προσφερόμενη λύση θα πρέπει να δίνει την δυνατότητα στους administrators για αλλαγή των κωδικών • σε συγκεκριμένα διαστήματα με βάση την πολιτική του οργανισμού. • σε περιοδική βάση, • μετά από κάθε πρόσβαση εφόσον κριθεί	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	αναγκαίο • κωδικών κατ' εντολή.			
53.	Η προσφερόμενη λύση θα πρέπει να παρέχει τους απαραίτητους μηχανισμούς παρακολούθησης, καταγραφής και ελέγχου της χρήσης των λογαριασμών με αυξημένα δικαιώματα σε οποιοδήποτε σύστημα, εφαρμογή και/ ή υπηρεσία.	NAI		
54.	Η προσφερόμενη λύση θα πρέπει υποστηρίζει την προώθηση όλων των ενεργειών των χρηστών στο SIEM της εταιρείας .	NAI		
55.	Η προσφερόμενη λύση θα πρέπει να παρέχει τους απαραίτητους μηχανισμούς προστασίας από διαγραφή ή/ και τροποποίηση των συμβάντων ασφαλείας.	NAI		
56.	Η προσφερόμενη λύση θα πρέπει να παρέχει την δυνατότητα παρακολούθησης των συνοδών SSH που πραγματοποιούνται από τον τελικό χρήστη σε διακομιστή Linux ή άλλη δικτυακή συσκευή, με δυο διαφορετικούς τρόπους: • καταγραφή της περιόδου λειτουργίας σε δευτερόλεπτα για όσο διάστημα είναι ενεργή η σύνδεση • καταγραφή όλων των εντολών και ενεργειών που εκτελούνται κατά τη διάρκεια της συνόδου	NAI		
57.	Η προσφερόμενη λύση θα πρέπει να παρέχει την δυνατότητα εύρεσης των εντολών που εκτέλεσε ο χρήστης μέσω των καταγραφών της συνόδου SSH	NAI		
58.	Η προσφερόμενη λύση θα πρέπει να παρέχει την δυνατότητα παρακολούθησης των συνοδών RDP που πραγματοποιούνται από τον τελικό χρήστη σε διακομιστή Windows με δυο διαφορετικούς τρόπους: • καταγραφή της συνόδου σε δευτερόλεπτα για όσο διάστημα είναι ενεργή • καταγραφή όλων των εντολών και ενεργειών που εκτελούνται κατά τη διάρκεια της συνόδου	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
59.	Δυνατότητα καταγραφής (videorecording) των ενεργειών των χρηστών και για νομικές/κανονιστικές απαιτήσεις			
60.	Όλες οι ενέργειες του διαχειριστή της εφαρμογής θα πρέπει να υπάρχει η δυνατότητα να αποστέλλονται στο SIEM			
61.	Η προσφερόμενη λύση θα πρέπει να παρέχει στους διαχειριστές της λύσης την δυνατότητα <ul style="list-style-type: none"> • δυναμικής παροχής πρόσβασης - πχ. χρονικού περιορισμού της πρόσβασης (πχ. Πρόσβαση για τις επόμενες Χ ώρες) • διακοπής πρόσβασης μέσω του Συστήματος εφόσον κριθεί αναγκαίο • έγκρισης της πρόσβασης από τρίτον χρήστη • πολλαπλών τρόπων έγκρισης για άμεση ενεργοποίηση 	NAI		
62.	Η προσφερόμενη λύση θα μπορεί να επιβάλει επιπλέον κανόνων ελέγχου πρόσβασης που δεν καθορίζονται μόνο από το ρόλο του χρήστη όπως ο χρόνος της πρόσβασης (ημέρα, βράδυ, εργάσιμες ημέρες αργίες).	NAI		
63.	Η προσφερόμενη λύση θα μπορεί να περιορίζει την πρόσβαση από συγκεκριμένα δικτυακά σημεία.	NAI		
64.	Η προσφερόμενη λύση θα μπορεί να μεσολαβεί μεταξύ του διαχειριστή και του υπό διαχείριση συστήματος προωθώντας εντολές του διαχειριστή χωρίς ο ίδιος να γνωρίζει τον κωδικό πρόσβασης στο υπό διαχείριση σύστημα (sessionproxy).	NAI		
65.	Δυνατότητα πλήρους καταγραφής των ενεργειών του διαχειριστή ώστε να αποδεικνύεται η συμμόρφωση με Νομικές/Κανονιστικές απαιτήσεις.	NAI		
66.	Η προσφερόμενη λύση θα πρέπει διαθέτει μηχανισμούς ανάλυσης της συμπεριφοράς των χρηστών, με σκοπό τον εντοπισμό των ανωμαλιών ή των περιπτώσεων απόκλισης από την συνηθισμένη ασυνήθιστη	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	δραστηριότητα ή ανωμαλιών σε πραγματικό χρόνο. Και να ενημερώνει αυτόματα συγκεκριμένους ρόλους και θέσεις εντός της εταιρείας.			
67.	Η προσφερόμενη λύση θα πρέπει να υποστηρίζει την δημιουργία προτύπου αναφοράς (baseline) σύμφωνα με την συμπεριφορά των χρηστών. Το ως άνω πρότυπο θα βασίζεται σε αλγόριθμους μηχανικής εκμάθησης που αναλύουν την συμπεριφορά σε βάθος χρόνου, τη συμπεριφορά πρόσβασης, την σπουδαιότητα των διαπιστευτηρίων και την συμπεριφορά των απλών χρηστών. Μόλις ένας χρήστης παρεκκλίνει από το ως άνω πρότυπο, θα βαθμολογείται η επικινδυνότητα σε πραγματικό χρόνο.	ΝΑΙ		
68.	Η προσφερόμενη λύση θα πρέπει να βαθμολογεί την συμπεριφορά των χρηστών βάσει της επικινδυνότητας.	ΝΑΙ		
69.	Η προσφερόμενη λύση θα πρέπει να μπορεί να καταγράψει τους λογαριασμούς με αυξημένα δικαιώματα και τους χρήστες που έχουν πρόσβαση σε αυτούς. Επιπλέον οι χρήστες ή/ και τα διαπιστευτήρια θα πρέπει να μπορούν να ομαδοποιηθούν ώστε να μπορεί να διαπιστωθεί εάν ένα διαπιστευτήριο περιέχεται σε μια ομάδα ή εάν οι χρήστες έχουν πρόσβαση σε διαπιστευτήρια ή στοιχεία που ανήκουν σε άλλα τμήματα.	ΝΑΙ		
70.	Η Λύση Διαχείρισης Προνομιούχων Λογαριασμών Πρόσβασης θα μπορεί να ανακαλύπτει λογαριασμούς με αυξημένα δικαιώματα ώστε να αποφεύγεται το ενδεχόμενο ύπαρξης κάποιου λογαριασμού ο οποίος δεν έχει πέσει στην αντίληψη της ομάδας πληροφορικής και οποίος ενδεχομένως χρησιμοποιείται κακόβουλα ώστε να παρακάμψει τα εφαρμοζόμενα μέτρα προστασίας και λογοδοσίας (auditing).	ΝΑΙ		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
71.	Η Λύση Διαχείρισης Προνομιούχων Λογαριασμών Πρόσβασης θα μπορεί να διαχειρίζεται κεντρικά και αυτοματοποιημένα τους λογαριασμούς με αυξημένα δικαιώματα σε όλα τα συστήματα με τα οποία θα διασυνδεθεί.	NAI		
72.	Η Λύση Διαχείρισης Προνομιούχων Λογαριασμών Πρόσβασης θα μπορεί να εντοπίζει εύκολα τα διαπιστευτήρια των διαχειριστών που δεν ελέγχονται μέσω του Συστήματος	NAI		
73.	Η Λύση Διαχείρισης Προνομιούχων Λογαριασμών Πρόσβασης θα μπορεί να εντοπίζει εύκολα τα διαπιστευτήρια εντός εφαρμογών (hard-coded/embedded application credentials) και περιορισμό αυτών.	NAI		
74.	Η Λύση Διαχείρισης Προνομιούχων Λογαριασμών Πρόσβασης θα μπορεί να εκδίδει ειδοποιήσεις (alerts) σε κάθε περίπτωση που θα διαπιστωθεί η ύπαρξη κάποιου μη αναμενόμενου λογαριασμού.	NAI		
75.	Η προσφερόμενη λύση θα διατηρεί λεπτομερείς αναφορές σχετικά με την χρήση των κωδικών πρόσβασης από τους διαχειριστές των συστημάτων (logging).	NAI		
76.	Η προσφερόμενη λύση θα διατηρεί λεπτομερείς αναφορές με το ποια πολιτική διαχείρισης κωδικών εφαρμόζεται σε κάθε σύστημα και ποιες εξαιρέσεις ισχύουν.	NAI		
77.	Η προσφερόμενη λύση θα διατηρεί λεπτομερείς αναφορές σε διάφορα επίπεδα συμπεριλαμβανομένου πλήρους ιστορικού ενεργειών ανά διαχειριστή/σύστημα.	NAI		
78.	Η προσφερόμενη λύση θα διατηρεί λεπτομερείς αναφορές για το ποιος απόκτησε πρόσβαση με αυξημένα δικαιώματα, τότε και για ποιον λόγο.	NAI		
79.	Η προσφερόμενη λύση θα παρέχει Δυνατότητα αποστολής των καταγραφών σε σύστημα SIEM	NAI		

A/A	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
80.	Ο ανάδοχος πρέπει να παρέχει την κατάλληλη εκπαίδευση ώστε όλοι οι χρήστες να γνωρίζουν πως μπορούν να χρησιμοποιήσουν το σύστημα	ΝΑΙ		

7.3 ΠΑΡΑΡΤΗΜΑ ΙΙΙ – ΕΥΡΩΠΑΙΚΟ ΕΝΙΑΙΟ ΕΓΓΡΑΦΟ ΣΥΜΒΑΣΗΣ (ΕΕΕΣ)

ΕΥΡΩΠΑΙΚΟ ΕΝΙΑΙΟ ΕΓΓΡΑΦΟ ΣΥΜΒΑΣΗΣ (ΕΕΕΣ)

Από τις 2-5-2019, οι αναθέτουσες αρχές συντάσσουν το ΕΕΕΣ με τη χρήση της νέας ηλεκτρονικής υπηρεσίας Promitheus ESPDint (<https://espdint.eprocurement.gov.gr/>), που προσφέρει τη δυνατότητα ηλεκτρονικής σύνταξης και διαχείρισης του Ευρωπαϊκού Ενιαίου Εγγράφου Σύμβασης (ΕΕΕΣ). Η σχετική ανακοίνωση είναι διαθέσιμη στη Διαδικτυακή Πύλη του ΕΣΗΔΗΣ www.promitheus.gov.gr

Συνημμένα της παρούσας διακήρυξης περιλαμβάνονται:

- Πρότυπο του Ευρωπαϊκού Ενιαίου Εγγράφου Σύμβασης (ΕΕΕΣ) της παρούσας διακήρυξης σε μορφή αρχείου pdf ψηφιακά υπογεγραμμένο, το οποίο αποτελεί αναπόσπαστο μέρος της διακήρυξης.
- Το Ευρωπαϊκό Ενιαίο Έγγραφο Σύμβασης (ΕΕΕΣ) σε μορφή αρχείου.xml το οποίο θα μπορούν να χρησιμοποιήσουν οι ενδιαφερόμενοι οικονομικοί φορείς, προκειμένου να το συμπληρώσουν.
- Επισημαίνεται ότι οι προσφέροντες για το μέρος IV Κριτήρια επιλογής του ΕΕΕΣ συμπληρώνουν μόνο την ενότητα α «Γενική ένδειξη για όλα τα κριτήρια επιλογής».

7.4 ΠΑΡΑΡΤΗΜΑ IV – Υπόδειγμα Βιογραφικού Σημειώματος

ΒΙΟΓΡΑΦΙΚΟ ΣΗΜΕΙΩΜΑ

ΠΡΟΣΩΠΙΚΑ ΣΤΟΙΧΕΙΑ

Επώνυμο:	Όνομα:
Πατρώνυμο:	Μητρώνυμο:
Ημερομηνία Γέννησης: _ / _ / _	Τόπος Γέννησης:
Τηλέφωνο:	E-mail:
Fax:	
Διεύθυνση Κατοικίας:	

ΕΚΠΑΙΔΕΥΣΗ

Όνομα Ιδρύματος	Τίτλος Πτυχίου	Ειδικότητα	Ημερομηνία Απόκτησης Πτυχίου



ΚΑΤΗΓΟΡΙΑ ΣΤΕΛΕΧΟΥΣ

(στο προτεινόμενο, από τον υποψήφιο Οικονομικό Φορέα,
σχήμα διοίκησης Έργου)

ΕΠΑΓΓΕΛΜΑΤΙΚΗ ΕΜΠΕΙΡΙΑ

Έργο	Εργοδότης	Θέση ⁸ και Καθήκοντα στο Έργο	Απασχόληση στο Έργο	
			Περίοδος (από - έως)	Α/Μ
			__ / __ / __ - __ / __ / __	
			__ / __ / __ - __ / __ / __	
			__ / __ / __ - __ / __ / __	

⁸Ως ΘΕΣΕΙΣ ενδεικτικά αναφέρονται : manager, senior consultant, consultant, business expert κλπ.

7.5 ΠΑΡΑΡΤΗΜΑ V – Υπόδειγμα Τεχνικής Προσφοράς

Ο φάκελος «Τεχνική Προσφορά» πρέπει να περιλαμβάνει τις παρακάτω ενότητες, τα περιεχόμενα των οποίων περιγράφονται παρακάτω. Η προσφορά θα πρέπει να καλύπτει το σύνολο των απαιτήσεων του έργου που αναφέρονται στην διακήρυξη και να παρέχει τα πλήρη στοιχεία που απαιτούνται για την αξιολόγησή της.

Τα περιεχόμενά της θα πρέπει να καλύπτουν τουλάχιστον τα παρακάτω κεφάλαια και υποενότητες:

1. Εισαγωγή: παρουσίαση του προσφέροντος, της καταλληλότητάς του για την υλοποίηση του έργου
2. Περιβάλλον έργου – Ειδικές απαιτήσεις: Συνολική αντίληψη του υποψήφιου για το έργο και τους σκοπούς και στόχους του, ειδικές απαιτήσεις - ιδιαιτερότητες, κρίσιμοι παράγοντες επιτυχίας, κίνδυνοι του έργου και προτάσεις αντιμετώπισης.
3. Εξοπλισμός: Περιγραφή χαρακτηριστικών προσφερόμενου εξοπλισμού, σε σχέση με τις επιχειρησιακές και τεχνολογικές διαστάσεις του έργου
4. Λογισμικό: Λειτουργικές απαιτήσεις εφαρμογών.
5. Υπηρεσίες: Μεθοδολογία παροχής των απαιτούμενων υπηρεσιών, συμβατότητα μεθοδολογίας με τις συνθήκες λειτουργίας της αναθέτουσας αρχής
6. Μεθοδολογία υλοποίησης: Μεθοδολογία υλοποίησης και διασφάλισης ποιότητας, ανάλυση σε δραστηριότητες/ εργασίες, προϊόντα, χρονοδιάγραμμα
7. Συμπληρωμένοι Πίνακες Συμμόρφωσης του Παραρτήματος II.
8. Διοίκηση του έργου (σχήμα διοίκησης, μεθοδολογία επικοινωνίας κλπ)
9. Πίνακες Οικονομικής Προσφοράς Χωρίς Τιμές

7.6 ΠΑΡΑΡΤΗΜΑ VI – Υπόδειγμα Οικονομικής Προσφοράς

1. Εξοπλισμός

Α/Α	ΠΕΡΙΓΡΑΦΗ	ΤΥΠΟΣ	ΠΟΣΟΤΗΤΑ	ΑΞΙΑ ΧΩΡΙΣ ΦΠΑ [€]		ΦΠΑ [€]	ΣΥΝΟΛΙΚΗ ΑΞΙΑ ΜΕ ΦΠΑ [€]	* ΚΟΣΤΟΣ ΣΥΝΤΗΡΗΣΗΣ ΧΩΡΙΣ ΦΠΑ [€]		
				ΤΙΜΗ ΜΟΝΑΔΑΣ	ΣΥΝΟΛΟ			1 ^ο έτος	2 ^ο έτος	3 ^ο έτος
ΣΥΝΟΛΟ										

* Το ΚΟΣΤΟΣ ΣΥΝΤΗΡΗΣΗΣ αφορά στα έτη μετά την ελάχιστη **ζητούμενη** Περίοδο Εγγύησης.

2. Εφαρμογές – Λογισμικά

Α/Α	ΠΕΡΙΓΡΑΦΗ	ΤΥΠΟΣ	ΠΟΣΟΤΗΤΑ (Σε Ανθρώπινες)	ΑΞΙΑ ΧΩΡΙΣ ΦΠΑ [€]		ΦΠΑ [€]	ΣΥΝΟΛΙΚΗ ΑΞΙΑ ΜΕ ΦΠΑ [€]	* ΚΟΣΤΟΣ ΣΥΝΤΗΡΗΣΗΣ ΧΩΡΙΣ ΦΠΑ [€]		
				ΤΙΜΗ ΜΟΝΑΔΑΣ	ΣΥΝΟΛΟ			1 ^ο έτος	2 ^ο έτος	3 ^ο έτος
ΣΥΝΟΛΟ										

* Το ΚΟΣΤΟΣ ΣΥΝΤΗΡΗΣΗΣ αφορά στα έτη μετά την ελάχιστη **ζητούμενη** Περίοδο Εγγύησης

3. Υπηρεσίες

Α/Α	ΠΕΡΙΓΡΑΦΗ	Ανθρωπο μήνες	ΑΞΙΑ ΧΩΡΙΣ ΦΠΑ [€]		ΦΠΑ [€]	ΣΥΝΟΛΙΚΗ ΑΞΙΑ ΜΕ ΦΠΑ [€]
			ΤΙΜΗ ΜΟΝΑΔΑΣ	ΣΥΝΟΛΟ		
1.	Πρωτοβάθμιος Έλεγχος – Σχεδιασμός RTSHM – Σχεδιασμός σεναρίων παρακολούθησης και λογισμικού					
2.	Δευτεροβάθμιος Έλεγχος					
3.	Μη Καταστροφικές Δοκιμαστικές Φορτίσεις και Επικαιροποίηση μελετών					
4.	Υπηρεσίες πιλοτικής λειτουργίας					
5.	Υπηρεσίες Παραγωγικής λειτουργίας					
6.	...					
7.	...					
...	Άλλες Υπηρεσίες ...					
ΣΥΝΟΛΟ						

4. Άλλες δαπάνες

Α/Α	ΠΕΡΙΓΡΑΦΗ	ΠΟΣΟΤΗΤΑ	ΑΞΙΑ ΧΩΡΙΣ ΦΠΑ [€]		ΦΠΑ [€]	ΣΥΝΟΛΙΚΗ ΑΞΙΑ ΜΕ ΦΠΑ [€]
			ΤΙΜΗ ΜΟΝΑΔΑΣ	ΣΥΝΟΛΟ		
ΣΥΝΟΛΟ						

5. Συγκεντρωτικός Πίνακας Οικονομικής Προσφοράς Έργου

Α/Α	ΠΕΡΙΓΡΑΦΗ	ΣΥΝΟΛΙΚΗ ΑΞΙΑ ΕΡΓΟΥ ΧΩΡΙΣ ΦΠΑ [€]	ΦΠΑ [€]	ΣΥΝΟΛΙΚΗ ΑΞΙΑ ΕΡΓΟΥ ΜΕ ΦΠΑ [€]
1	Εξοπλισμός (Πίνακας 1)			
2	Εφαρμογές – Υποσυστήματα (Πίνακας 2)			
3	Υπηρεσίες (Πίνακας 3)			
4	Άλλες δαπάνες (Πίνακας 4)			
	ΓΕΝΙΚΟ ΣΥΝΟΛΟ			

6. Συγκεντρωτικός Πίνακας Οικονομικής Προσφοράς Συντήρησης

ΕΤΟΣ*	ΕΤΗΣΙΑ ΣΥΝΤΗΡΗΣΗ ΕΞΟΠΛΙΣΜΟΥ (ΧΩΡΙΣ ΦΠΑ) [€]	ΕΤΗΣΙΑ ΣΥΝΤΗΡΗΣΗ ΛΟΓΙΣΜΙΚΩΝ (ΧΩΡΙΣ ΦΠΑ) [€]	ΣΥΝΟΛΙΚΗ ΕΤΗΣΙΑ ΑΞΙΑ ΣΥΝΤΗΡΗΣΗΣ (ΧΩΡΙΣ ΦΠΑ) [€]	ΦΠΑ [€]	ΣΥΝΟΛΙΚΗ ΕΤΗΣΙΑ ΑΞΙΑ ΣΥΝΤΗΡΗΣΗΣ (ΜΕ ΦΠΑ) [€]	ΕΤΗΣΙΟ ΠΟΣΟΣΤΟ ΣΥΝΤΗΡΗΣΗΣ**
1 ^ο						
2 ^ο						
3 ^ο						
ΣΥΝΟΛΟ						

* ΕΤΟΣ: μετά την παραλαβή της εκάστοτε εκτελεστικής σύμβασης

** Το **ΕΤΗΣΙΟ ΠΟΣΟΣΤΟ ΣΥΝΤΗΡΗΣΗΣ** (για την κάθε γραμμή του Πίνακα 6) προκύπτει διαιρώντας το ποσό που αναγράφεται στη στήλη «ΣΥΝΟΛΙΚΗ ΕΤΗΣΙΑ ΑΞΙΑ ΣΥΝΤΗΡΗΣΗΣ (ΧΩΡΙΣ ΦΠΑ)» του ίδιου Πίνακα με το «ΓΕΝΙΚΟ ΣΥΝΟΛΟ» που αναγράφεται στη στήλη «ΣΥΝΟΛΙΚΗ ΑΞΙΑ ΕΡΓΟΥ (ΧΩΡΙΣ ΦΠΑ)» του **Πίνακα 5**

7.7 ΠΑΡΑΡΤΗΜΑ VII – Άλλες Δηλώσεις

7.8 ΠΑΡΑΡΤΗΜΑ VIII – Υποδείγματα Εγγυητικών Επιστολών

I. Εγγυητική Επιστολή Συμμετοχής

ΕΚΔΟΤΗΣ (Πλήρης επωνυμία).....

Ημερομηνία έκδοσης.....

Προς: Την Κοινωνία της Πληροφορίας ΜΑΕ

Λεωφ. Συγγρού 194, 176 71 Καλλιθέα Αθήνα

Εγγύηση μας υπ' αριθμ. ποσού ευρώ

Με την παρούσα εγγυόμαστε, ανέκκλητα και ανεπιφύλακτα παραιτούμενοι του δικαιώματος της διαιρέσεως και διζήσεως, μέχρι του ποσού των ευρώ.....υπέρ του

{σε περίπτωση φυσικού προσώπου}: (ονοματεπώνυμο, πατρώνυμο), ΑΦΜ: οδός..... αριθμός..... ΤΚ.....

{Σε περίπτωση μεμονωμένης εταιρίας}: της Εταιρίας ΑΦΜ: οδός αριθμός ... ΤΚ ,}

{ή σε περίπτωση Ένωσης ή Κοινοπραξίας}: των Εταιριών

α) (πλήρη επωνυμία) ΑΦΜ..... οδός..... αριθμός..... ΤΚ.....

β) (πλήρη επωνυμία) ΑΦΜ..... οδός..... αριθμός..... ΤΚ.....

γ) (πλήρη επωνυμία) ΑΦΜ..... οδός..... αριθμός..... ΤΚ.....

μελών της Ένωσης ή Κοινοπραξίας, ατομικά για κάθε μια από αυτές και ως αλληλέγγυα και εις ολόκληρο υποχρεών μεταξύ τους εκ της ιδιότητάς τους ως μελών της Ένωσης ή Κοινοπραξίας,}

για τη συμμετοχή του/της/τους σύμφωνα με την (αριθμό/ημερομηνία) Διακήρυξη της (Αναθέτουσας Αρχής) με καταληκτική ημερομηνία υποβολής των προσφορών, για την ανάδειξη αναδόχου για την ανάθεση της σύμβασης: "(τίτλος σύμβασης)"/ για το/α τμήμα/τα

Η παρούσα εγγύηση καλύπτει μόνο τις από τη συμμετοχή στην ανωτέρω απορρέουσες υποχρεώσεις του/της (υπέρ ου η εγγύηση) καθ' όλο τον χρόνο ισχύος της.

Το παραπάνω ποσό τηρείται στη διάθεσή σας και θα καταβληθεί ολικά ή μερικά χωρίς καμία από μέρους μας αντίρρηση, αμφισβήτηση ή ένσταση και χωρίς να ερευνηθεί το βάσιμο ή μη της απαίτησής σας μέσα σε πέντε(5) ημέρες από την απλή έγγραφη ειδοποίησή σας.

Η παρούσα ισχύει μέχρι και την (ο χρόνος ισχύος πρέπει να είναι μεγαλύτερος τουλάχιστον κατά τριάντα (30) ημέρες μετά τη λήξη χρόνου ισχύος της Προσφοράς)

Σε περίπτωση κατάρπτωσης της εγγύησης, το ποσό της κατάρπτωσης υπόκειται στο εκάστοτε ισχύον πάγιο τέλος χαρτοσήμου.

Αποδεχόμαστε να παρατείνουμε την ισχύ της εγγύησης ύστερα από έγγραφο της Υπηρεσίας σας, στο οποίο επισυνάπτεται η συναίνεση του υπέρ ου για την παράταση της προσφοράς, σύμφωνα με την παρ. 2.2.2 της παρούσας, με την προϋπόθεση ότι το σχετικό αίτημά σας θα μας υποβληθεί πριν από την ημερομηνία λήξης της.

(Εξουσιοδοτημένη υπογραφή)

II. Εγγυητική Επιστολή Καλής Εκτέλεσης

ΕΚΔΟΤΗΣ (Πλήρης επωνυμία).....

Ημερομηνία έκδοσης.....

Προς: Την Κοινωνία της Πληροφορίας ΜΑΕ

Λεωφ. Συγγρού 194, 176 71 Καλλιθέα Αθήνα

Εγγύηση μας υπ' αριθμ. ποσού ευρώ

Με την παρούσα εγγυόμαστε, ανέκκλητα και ανεπιφύλακτα παραιτούμενοι του δικαιώματος της διαιρέσεως και διζήσεως, μέχρι του ποσού των ευρώ.....υπέρ του

{σε περίπτωση φυσικού προσώπου}: (ονοματεπώνυμο, πατρώνυμο), ΑΦΜ: οδός..... αριθμός.....ΤΚ.....

{Σε περίπτωση μεμονωμένης εταιρίας}: της Εταιρίας ΑΦΜ: οδός αριθμός ... ΤΚ},

{ή σε περίπτωση Ένωσης ή Κοινοπραξίας}: των Εταιριών

α) (πλήρη επωνυμία) ΑΦΜ..... οδός..... αριθμός.....ΤΚ.....

β) (πλήρη επωνυμία) ΑΦΜ.....οδός..... αριθμός.....ΤΚ.....

γ) (πλήρη επωνυμία) ΑΦΜ.....οδός..... αριθμός.....ΤΚ.....

ατομικά και για κάθε μία από αυτές και ως αλληλέγγυα και εις ολόκληρο υπόχρεων μεταξύ τους, εκ της ιδιότητάς τους ως μελών της ένωσης ή κοινοπραξίας,

για την καλή εκτέλεση της υπ αριθ σύμβασης "(τίτλος σύμβασης)", σύμφωνα με την (αριθμό/ημερομηνία) Διακήρυξης.

Το παραπάνω ποσό τηρείται στη διάθεσή σας και θα καταβληθεί ολικά ή μερικά χωρίς καμία από μέρους μας αντίρρηση, αμφισβήτηση ή ένσταση και χωρίς να ερευνηθεί το βάσιμο ή μη της απαίτησής σας μέσα σε πέντε(5) ημέρες από την απλή έγγραφη ειδοποίησή σας.

Η παρούσα ισχύει μέχρι και την (**διάρκεια ισχύος σύμφωνα με την παρ.4.1 της παρούσας**)

Σε περίπτωση κατάρπτωσης της εγγύησης, το ποσό της κατάρπτωσης υπόκειται στο εκάστοτε ισχύον πάγιο τέλος χαρτοσήμου.

(Εξουσιοδοτημένη υπογραφή)

III. Εγγυητική Επιστολή Προκαταβολής

ΕΚΔΟΤΗΣ:

Ημερομηνία έκδοσης:

Προς:

Κοινωνία της Πληροφορίας Μ.Α.Ε.

Λεωφ. Συγγρού 194, 176 71 Καλλιθέα Αθήνα

ΑΦΜ:999983307

Εγγύηση μας υπ' αριθμ. ποσού ευρώ

Με την παρούσα εγγυόμαστε, ανέκκλητα και ανεπιφύλακτα παραιτούμενοι του δικαιώματος της διαιρέσεως και διζήσεως, μέχρι του ποσού των ευρώ.....υπέρ του

{σε περίπτωση φυσικού προσώπου}: (ονοματεπώνυμο, πατρώνυμο), ΑΦΜ: οδός..... αριθμός.....ΤΚ.....

{Σε περίπτωση μεμονωμένης εταιρίας}: της Εταιρίας ΑΦΜ: οδός αριθμός ... ΤΚ ,}

{ή σε περίπτωση Ένωσης ή Κοινοπραξίας}: των Εταιριών

α) (πλήρη επωνυμία) ΑΦΜ..... οδός..... αριθμός.....ΤΚ.....

β) (πλήρη επωνυμία) ΑΦΜ.....οδός..... αριθμός.....ΤΚ.....

γ) (πλήρη επωνυμία) ΑΦΜ.....οδός..... αριθμός.....ΤΚ.....

μελών της Ένωσης ή Κοινοπραξίας, ατομικά για κάθε μια από αυτές και ως αλληλέγγυα και εις ολόκληρο υπόχρεων μεταξύ τους εκ της ιδιότητάς τους ως μελών της Ένωσης ή Κοινοπραξίας.}

για την λήψη προκαταβολής για τη χορήγηση του ...% (συμπληρώνετε το συνολικό ποσοστό της λαμβανόμενης προκαταβολής) της συμβατικής αξίας μη περιλαμβανομένου του ΦΠΑ, ευρώ (συμπληρώνετε το συνολικό ποσό της λαμβανόμενης προκαταβολής) σύμφωνα με τη σύμβαση με αριθμό.....και τη Διακήρυξή σας με αριθμό....., στο πλαίσιο του διαγωνισμού της (συμπληρώνετε την ημερομηνία διενέργειας του διαγωνισμού) για εκτέλεση του έργου (συμπληρώνετε τον τίτλο του έργου) συνολικής αξίας (συμπληρώνετε το συνολικό συμβατικό τίμημα με διευκρίνιση εάν περιλαμβάνει ή όχι τον ΦΠΑ), και μέχρι του ποσού των ευρώ (συμπληρώνετε το ποσό το οποίο καλύπτει η συγκεκριμένη εγγυητική επιστολή), , πλέον τόκων επί της προκαταβολής αυτής που θα καταλογισθούν σε βάρος της Εταιρείας ή, σε περίπτωση Ένωσης ή Κοινοπραξίας, υπέρ των Εταιρειών της Ένωσης ή Κοινοπραξίας, υπέρ της οποίας εγγυόμαστε σε εφαρμογή του άρθρου 72 του Ν. 4412/2016 (ΦΕΚ Α/147/8-08-2016) , στο οποίο και μόνο περιορίζεται η εγγυήσή μας.

Το παραπάνω ποσό της εγγύησης τηρείται στη διάθεσή σας, το οποίο και υποχρεούμαστε να σας καταβάλουμε ολικά ή μερικά, μέσα σε πέντε (5) ημέρες από την έγγραφη ειδοποίησή σας.

Η παρούσα ισχύει μέχρι και την(Σημείωση προς την Τράπεζα: **διάρκεια ισχύος σύμφωνα με την παρ.4.1 της παρούσας**)».

Σε περίπτωση κατάπτωσης της εγγύησης, το ποσό της κατάπτωσης υπόκειται στο εκάστοτε ισχύον πάγιο τέλος χαρτοσήμου.

(Εξουσιοδοτημένη υπογραφή)

IV. Εγγυητική Επιστολή Καλής Λειτουργίας

ΕΚΔΟΤΗΣ:

Ημερομηνία έκδοσης:

Προς:

Κύριο του Έργου

Εγγύηση μας υπ' αριθμ. ποσού ευρώ

Με την παρούσα εγγυόμαστε, ανέκκλητα και ανεπιφύλακτα παραιτούμενοι του δικαιώματος της διαιρέσεως και διζήσεως, μέχρι του ποσού των ευρώ.....υπέρ του

{σε περίπτωση φυσικού προσώπου}:(ονοματεπώνυμο, πατρώνυμο),ΑΦΜ: οδός..... αριθμός.....ΤΚ.....

{Σε περίπτωση μεμονωμένης εταιρίας}: της Εταιρίας ΑΦΜ: οδός αριθμός ... ΤΚ},

{ή σε περίπτωση Ένωσης ή Κοινοπραξίας}: των Εταιριών

α) (πλήρη επωνυμία) ΑΦΜ..... οδός..... αριθμός.....ΤΚ.....

β) (πλήρη επωνυμία) ΑΦΜ.....οδός..... αριθμός.....ΤΚ.....

γ) (πλήρη επωνυμία) ΑΦΜ.....οδός..... αριθμός.....ΤΚ.....

μελών της Ένωσης ή Κοινοπραξίας, ατομικά για κάθε μια από αυτές και ως αλληλέγγυα και εις ολόκληρο υποχρεων μεταξύ τους εκ της ιδιότητάς τους ως μελών της Ένωσης ή Κοινοπραξίας,}

για την καλή λειτουργία του αντικειμένου της σύμβασης με αριθμό.....και τη Διακήρυξή σας με αριθμό....., στο πλαίσιο του διαγωνισμού της (συμπληρώνετε την ημερομηνία διενέργειας του διαγωνισμού)

Το παραπάνω ποσό της εγγύησης τηρείται στη διάθεσή σας, το οποίο και υποχρεούμαστε να σας καταβάλουμε ολικά ή μερικά, μέσα σε πέντε (5) ημέρες από την έγγραφη ειδοποίησή σας.

Η παρούσα ισχύει μέχρι και την(Σημείωση προς την Τράπεζα: **διάρκεια ισχύος σύμφωνα με την παρ.ΧΧ της παρούσας**)».

Σε περίπτωση κατάρπτωσης της εγγύησης, το ποσό της κατάρπτωσης υπόκειται στο εκάστοτε ισχύον πάγιο τέλος χαρτοσήμου.

(Εξουσιοδοτημένη υπογραφή)

7.9 ΠΑΡΑΡΤΗΜΑ ΙΧ – ΕΝΗΜΕΡΩΣΗ ΓΙΑ ΤΗΝ ΕΠΕΞΕΡΓΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Η Αναθέτουσα Αρχή ενημερώνει υπό την ιδιότητά της ως υπεύθυνης επεξεργασίας το φυσικό πρόσωπο που υπογράφει την προσφορά ως Προσφέρων ή ως Νόμιμος Εκπρόσωπος Προσφέροντος, ότι το ίδιο ή και τρίτοι, κατ' εντολή και για λογαριασμό του, θα επεξεργάζονται τα ακόλουθα δεδομένα ως εξής:

I. Αντικείμενο επεξεργασίας είναι τα δεδομένα προσωπικού χαρακτήρα που περιέχονται στους φακέλους της προσφοράς και τα αποδεικτικά μέσα τα οποία υποβάλλονται στην Αναθέτουσα Αρχή, στο πλαίσιο του παρόντος Διαγωνισμού, από το φυσικό πρόσωπο το οποίο είναι το ίδιο Προσφέρων ή Νόμιμος Εκπρόσωπος Προσφέροντος.

II. Σκοπός της επεξεργασίας είναι η αξιολόγηση του Φακέλου Προσφοράς, η ανάθεση της Σύμβασης, η προάσπιση των δικαιωμάτων της Αναθέτουσας Αρχής, η εκπλήρωση των εκ του νόμου υποχρεώσεων της Αναθέτουσας Αρχής και η εν γένει ασφάλεια και προστασία των συναλλαγών. Τα δεδομένα ταυτοπροσωπίας και επικοινωνίας θα χρησιμοποιηθούν από την Αναθέτουσα Αρχή και για την ενημέρωση των Προσφερόντων σχετικά με την αξιολόγηση των προσφορών.

III. Αποδέκτες των ανωτέρω (υπό Α) δεδομένων στους οποίους κοινοποιούνται είναι:

(α) Φορείς στους οποίους η Αναθέτουσα Αρχή αναθέτει την εκτέλεση συγκεκριμένων ενεργειών για λογαριασμό της, δηλαδή οι Σύμβουλοι, τα υπηρεσιακά στελέχη, μέλη Επιτροπών Αξιολόγησης, Χειριστές του Ηλεκτρονικού Διαγωνισμού και λοιποί εν γένει προστηθέντες της, υπό τον όρο της τήρησης σε κάθε περίπτωση του απορρήτου.

(β) Το Δημόσιο, άλλοι δημόσιοι φορείς ή δικαστικές αρχές ή άλλες αρχές ή δικαιοδοτικά όργανα, στο πλαίσιο των αρμοδιοτήτων τους.

(γ) Έτεροι συμμετέχοντες στο Διαγωνισμό, στο πλαίσιο της αρχής της διαφάνειας και του δικαιώματος προδικαστικής και δικαστικής προστασίας των συμμετεχόντων στο Διαγωνισμό, σύμφωνα με το νόμο.

IV. Τα δεδομένα θα τηρούνται για χρονικό διάστημα για χρονικό διάστημα ίσο με τη διάρκεια της εκτέλεσης της σύμβασης, και μετά τη λήξη αυτής για χρονικό διάστημα πέντε ετών, για μελλοντικούς φορολογικούς-δημοσιονομικούς ή ελέγχους χρηματοδοτών ή άλλους προβλεπόμενους ελέγχους από την κείμενη νομοθεσία, εκτός εάν η νομοθεσία προβλέπει διαφορετική περίοδο διατήρησης. Σε περίπτωση εκκρεμοδικίας αναφορικά με δημόσια σύμβαση τα δεδομένα τηρούνται μέχρι το πέρας της εκκρεμοδικίας. Μετά τη λήξη των ανωτέρω περιόδων, τα προσωπικά δεδομένα θα καταστρέφονται.

V. Το φυσικό πρόσωπο που είναι είτε Προσφέρων είτε Νόμιμος Εκπρόσωπος του Προσφέροντος, μπορεί να ασκεί κάθε νόμιμο δικαίωμά του σχετικά με τα δεδομένα προσωπικού χαρακτήρα που το αφορούν, απευθυνόμενο στον υπεύθυνο προστασίας προσωπικών δεδομένων της Αναθέτουσας Αρχής.

VI. Η Αναθέτουσα Αρχή έχει υποχρέωση να λαμβάνει κάθε εύλογο μέτρο για τη διασφάλιση του απορρήτου και της ασφάλειας της επεξεργασίας των δεδομένων και της προστασίας τους από τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση από οποιονδήποτε και κάθε άλλης μορφή αθέμιτη επεξεργασία.