ΕΦΗΜΕΡΙΔΑ
ΤΗΣ ΚΥΒΕΡΝΗΣΕΩΣ
ΤΗΣ ΕΛΛΗΝΙΚΗΣ ΔΗΜΟΚΡΑΤΙΑΣ

22 Σεπτεμβρίου 2020 | ΤΕΥΧΟΣ ΔΕΥΤΕΡΟ | Αρ. Φύλλου **4071**

ΑΠΟΦΑΣΕΙΣ

Αριθμ. Φ. 120/402565/Σ.3497

Κύρωση του Εθνικού Κανονισμού Βιομηχανικής Ασφαλείας (ΕΚΒΑ)

Ο ΥΠΟΥΡΓΟΣ ΕΘΝΙΚΗΣ ΑΜΥΝΑΣ

Έχοντας υπόψη:

1. Την παρ. 2 του άρθρου 68 του ν. 3433/2006 «Προμήθειες αμυντικού υλικού των Ενόπλων Δυνάμεων» (Α΄20).

2. Το άρθρο 90 του Κώδικα Νομοθεσίας για την Κυβέρνηση και τα κυβερνητικά όργανα, που κυρώθηκε με το άρθρο πρώτο του π.δ. 63/2005 (Α΄98), σε συνδυασμό με την παρ. 22 του άρθρου 119 του ν. 4622/2019 (Α΄ 133).

3. Το γεγονός ότι, όπως προκύπτει από την υπ' αρ. 268/2020 εισήγηση του προϊσταμένου των οικονομικών υπηρεσιών του Υπουργείου Εθνικής Άμυνας, από τις διατάξεις της παρούσας δεν προκαλείται δαπάνη σε βάρος του κρατικού προϋπολογισμού, αποφασίζουμε:

Άρθρο 1
Κύρωση ΕΚΒΑ

Κυρώνεται ο Εθνικός Κανονισμός Βιομηχανικής Ασφάλειας (ΕΚΒΑ), ο οποίος τυγχάνει εφαρμογής από κάθε οικονομικό φορέα που αποκτά πρόσβαση σε Εθνικές Διαβαθμισμένες Πληροφορίες - Υλικά (ΕΔΠΥ).

Άρθρο 2
Καταργούμενες διατάξεις

Καταργείται ο ΕΚΒΑ, ο οποίος κυρώθηκε με την υπό στοιχεία Φ.120/1/136775/Σ.486/2005 απόφαση του Υπουργού Εθνικής Άμυνας (Β΄ 336).

ΠΙΝΑΚΑΣ
ΚΑΤΑΧΩΡΗΣΗΣ ΤΡΟΠΟΠΟΙΗΤΙΚΩΝ ΔΙΑΤΑΓΩΝ

Α/Α Τροποποίησης	Αριθμός και Ημερ/νια Δγης Τροποποίησης	Ημερομηνία Καταχώρησης Τροποποίησης	Ο καταχωρήσας την τροποποίηση		
			Βαθμός	Ονοματεπώνυμο	Μονογραφή

Οδηγίες:

1. Επιφέρατε μεταβολές στον παρόντα Κανονισμό μόνο κατόπιν διαταγής του ΓΕΕΘΑ/Ε’ ΚΛΑΔΟΥ/ΔΝΣΗ ΑΣΦΑΛΕΙΑΣ (Ε3).

2. Στη θέση κάθε μεταβολής και στο περιθώριο της σελίδας του κειμένου, αναγράψατε ένα Κεφαλαίο Τ και τον α/α της τροποποίησης (π.χ. Τ1, Τ2 κοκ.).

3. Καταχωρίσατε στον παραπάνω πίνακα κάθε τέτοια διαταγή, για επιβεβαίωση ότι έγιναν οι μεταβολές.

ΠΙΝΑΚΑΣ ΣΥΝΤΜΗΣΕΩΝ

Α

ΑΑΑ	Αύξων Αριθμός Αντιτύπων
ΑΑΠ	Άκρως Απόρρητο
ΑΔ	Αδιαβάθμητο
ΑΕΑ	Αριθμός Εκδοθέντων Αντιτύπων
ΑΕΛ	Αρχή Επιχειρησιακής Λειτουργίας
ΑΚ	Ανάλυση Κινδύνου
ΑΠ	Απόρρητο

Γ

ΓΔΑΕΕ/ΔΑΕΤΕ	Γενική Διεύθυνση Αμυντικών Εξοπλισμών και Επενδύσεων / Διεύθυνση Αμυντικών Επενδύσεων και Τεχνολογικών Ερευνών
ΓΕΕΘΑ	Γενικό Επιτελείο Εθνικής Άμυνας

Δ

ΔΑΑ	Διορισμένη Αρχή Ασφαλείας
ΔΑΛ	Διαδικασία Ασφαλούς Λειτουργίας
ΔΑΠΑΣ	Δήλωση Απαιτήσεων Ασφαλείας Συστήματος
ΔΙΑΛ	Διαχειριστής Λειτουργίας

Ε

ΕΑΑ	Εθνική Αρχή Ασφαλείας
ΕΑΑΕΠ	Εθνική Αρχή Ασφαλείας Επικοινωνιών – Πληροφορικής
ΕΑΔΑ	Εθνική Αρχή Διαπίστευσης Ασφαλείας
ΕΑΣ	Έλεγχος Ασφαλείας Συστήματος
ΕΔ	Ένοπλες Δυνάμεις
ΕΔΠΥ	Εθνική Διαβαθμισμένη Πληροφορία - Υλικό
ΕΕ	Ευρωπαϊκή Ένωση
ΕΕΒΑ	Επιτροπή Επιθεωρήσεων Βιομηχανικής Ασφαλείας
ΕΚΑ	Εθνικός Κανονισμός Ασφαλείας
ΕΚΒΑ	Εθνικός Κανονισμός Βιομηχανικής Ασφαλείας
ΕΛ.ΑΣ	Ελληνική Αστυνομία
ΕΠ	Εμπιστευτικό

Η

Η/Υ	Ηλεκτρονικός Υπολογιστής

Ι

ΙΕΠΥΑ	Ιδιωτική Επιχείρηση Παροχής Υπηρεσιών Ασφαλείας

Ν

ΝΑΤΟ	Οργανισμός Ασφαλείας Βορειοατλαντικού Συμφώνου (NORTH ATLANTIC TREATY ORGANIZATION)
ΝΠΔΔ	Νομικό Πρόσωπο Δημοσίου Δικαίου

Π

π.δ.	Προεδρικό Διάταγμα
ΠΑΕ	Πιστοποιητικό Ασφάλειας Εγκατάστασης
ΠΧ	Περιορισμένης Χρήσης

Σ

ΣΑΕ	Σχέδιο Ασφαλείας Εγκατάστασης

ΣΕΠ	Σύστημα Επικοινωνιών Πληροφορικής
	Υ
ΥΑΔ	Υπεύθυνος Ασφαλείας Δικτύου
ΥΑΣ	Υπεύθυνος Ασφαλείας Συστήματος
ΥΑΤ	Υπεύθυνος Ασφαλείας Τοποθεσίας
ΥΠΕΘΑ	Υπουργείο Εθνικής Άμυνας

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΜΕΡΟΣ ΠΡΩΤΟ

ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΕΘΝΙΚΩΝ ΔΙΑΒΑΘΜΙΣΜΕΝΩΝ ΠΛΗΡΟΦΟΡΙΩΝ ΚΑΙ ΥΛΙΚΩΝ

ΚΕΦΑΛΑΙΟ Α

ΓΕΝΙΚΑ

ΚΕΦΑΛΑΙΟ Β

ΔΙΑΔΙΚΑΣΙΕΣ ΑΣΦΑΛΕΙΑΣ

ΚΕΦΑΛΑΙΟ Γ

ΣΥΜΒΑΣΕΙΣ

ΚΕΦΑΛΑΙΟ Δ

ΠΑΡΑΒΑΣΕΙΣ - ΠΑΡΑΒΙΑΣΕΙΣ ΑΣΦΑΛΕΙΑΣ

ΚΕΦΑΛΑΙΟ Ε

ΕΠΙΣΚΕΨΕΙΣ - ΕΠΙΘΕΩΡΗΣΕΙΣ - ΠΙΣΤΟΠΟΙΗΤΙΚΟ ΑΣΦΑΛΕΙΑΣ ΕΓΚΑΤΑΣΤΑΣΗΣ

ΜΕΡΟΣ ΔΕΥΤΕΡΟ

ΠΡΟΣΤΑΣΙΑ ΕΔΠΥ ΠΟΥ ΤΥΓΧΑΝΟΥΝ ΔΙΑΧΕΙΡΙΣΗΣ ΑΠΟ ΣΥΣΤΗΜΑΤΑ ΕΠΙΚΟΙΝΩΝΙΩΝ – ΠΛΗΡΟΦΟΡΙΚΗΣ

ΚΕΦΑΛΑΙΟ ΣΤ

ΓΕΝΙΚΑ

Άρθρο

ΚΕΦΑΛΑΙΟ Ζ

ΟΡΓΑΝΩΣΗ ΑΣΦΑΛΕΙΑΣ

ΚΕΦΑΛΑΙΟ Η

ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΣΕΠ

ΚΕΦΑΛΑΙΟ Θ

ΣΥΝΤΗΡΗΣΗ – ΠΡΟΜΗΘΕΙΑ – ΔΙΑΠΙΣΤΕΥΣΗ – ΑΞΙΟΛΟΓΗΣΗ ΚΑΙ ΠΙΣΤΟΠΟΙΗΣΗ ΣΕΠ

ΚΕΦΑΛΑΙΟ Ι
ΔΙΑΔΙΚΑΣΙΑ ΔΙΑΠΙΣΤΕΥΣΗΣ
ΣΥΣΤΗΜΑΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ – ΠΛΗΡΟΦΟΡΙΚΗΣ (ΣΕΠ)

Άρθρο

ΠΑΡΑΡΤΗΜΑΤΑ

ΥΠΟΔΕΙΓΜΑΤΑ

ΕΘΝΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ ΒΙΟΜΗΧΑΝΙΚΗΣ ΑΣΦΑΛΕΙΑΣ (ΕΚΒΑ)

ΜΕΡΟΣ ΠΡΩΤΟ

ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΕΘΝΙΚΩΝ ΔΙΑΒΑΘΜΙΣΜΕΝΩΝ ΠΛΗΡΟΦΟΡΙΩΝ ΚΑΙ ΥΛΙΚΩΝ

ΚΕΦΑΛΑΙΟ Α

ΓΕΝΙΚΑ

ΑΡΘΡΟ 1

ΕΙΣΑΓΩΓΗ

1. Ο παρών Κανονισμός αποτελεί τον Εθνικό Κανονισμό Βιομηχανικής Ασφάλειας (ΕΚΒΑ), αντικείμενο του οποίου είναι η καθιέρωση μέτρων και διαδικασιών για τη διασφάλιση της προστασίας των Εθνικών Διαβαθμισμένων Πληροφοριών – Υλικών (ΕΔΠΥ) από τους οικονομικούς φορείς που αποκτούν πρόσβαση σε αυτές, σύμφωνα με τις διατάξεις του.

2. Ειδικότερα σε ότι αφορά στην προστασία διαβαθμισμένων πληροφοριών και υλικών στο πλαίσιο του ΝΑΤΟ και της ΕΕ, εκτός των προβλέψεων του ΕΚΒΑ και της Εθνικής νομοθεσίας, εφαρμόζονται αντίστοιχα ο Κανονισμός Ασφάλειας του Βορειοατλαντικού Συμφώνου (ΝΑΤΟ) C-M (2002) 49 της 17 Ιουν 2002 και η απόφαση του Συμβουλίου της Ευρωπαϊκής Ένωσης (ΕΕ) 2013/488/ΕC, λαμβάνοντας υπόψη τις σχετικές συνθήκες και τις γενικές αρχές του Διεθνούς και Ευρωπαϊκού Δικαίου, καθώς και τις αναθεωρήσεις αυτών που έχουν γίνει αποδεκτές από τη χώρα μας.

3. Επί των θεμάτων ελέγχου ασφαλείας προσωπικού για διαβαθμισμένα έργα υποδομής που αφορούν στον Κανονισμό Ασφαλείας Έργων Υποδομής ΝΑΤΟ και Εθνικών/1959 (Φ.3587/02/Β.Σ.Τ.902/15 Ιουν 1959/ΓΕΕΘΑ/ΑΙΙ-Ε.Κ.Φ./Α.ΜΕΟ), εφαρμόζονται οι διατάξεις του παρόντος Κανονισμού, όσον αφορά τα υποβαλλόμενα δικαιολογητικά και τα κωλύματα.

4. Όπου για την εφαρμογή των κειμένων των ανωτέρω παραγράφων 2 και 3 απαιτείται η σύμπραξη της Εθνικής Αρχής Ασφαλείας ή της Διορισμένης Αρχής Ασφαλείας, εφαρμόζονται οι διαδικασίες ελέγχου ασφαλείας και εξουσιοδοτήσεων του παρόντος Κανονισμού.

ΑΡΘΡΟ 2

ΟΡΙΣΜΟΙ

Για τις ανάγκες του παρόντος κανονισμού ορίζονται ως:

1. Ανάγκη Γνώσης

Η αρχή σύμφωνα με την οποία προσδιορίζεται θετικά ότι ένας ενδεχόμενος παραλήπτης έχει την απαίτηση για πρόσβαση, γνώση ή κατοχή ΕΔΠΥ, προκειμένου να επιτελέσει επίσημη εργασία ή υπηρεσία.

2. Ανάδοχος (Καλείται και Κύριος Ανάδοχος)

Κάθε οικονομικός φορέας στον οποίο έχει ανατεθεί με σύμβαση η κατασκευή ή η μελέτη έργου, ή η προμήθεια αγαθών ή η παροχή υπηρεσιών.

3. Αναθέτουσα Αρχή

Ο φορέας που σύμφωνα με την νομοθεσία συμβάλλεται με τον ανάδοχο και αναθέτει σε αυτόν την κατασκευή ή μελέτη έργου, ή την προμήθεια αγαθών ή την παροχή υπηρεσιών.

4. Αποστολέας

Το άτομο ή ο οργανισμός αρμόδιος για την αποστολή των ΕΔΠΥ στον παραλήπτη.

5. Αρχή των «δύο ατόμων»

Η αρχή σύμφωνα με την οποία παρεμποδίζεται η περίπτωση ένα και μόνο άτομο να έχει πλήρη γνώση ή έλεγχο των κλειδών ασφαλείας (κωδικές λέξεις εισόδου και μηχανισμών ταυτοποίησης ή ταυτοπροσωπίας) του λογισμικού ή να έχει πρόσβαση ή να στελεχώνει χώρους Συστημάτων Επικοινωνιών Πληροφορικής (ΣΕΠ), που πραγματοποιείται χειρισμός διαβαθμισμένων πληροφοριών.

6. Ασφάλεια

Η προστασία των ΕΔΠΥ από οποιοδήποτε κίνδυνο παράβασης, παραβίασης, κλοπής, παραποίησης, καταστροφής από άτομα ή δυνάμεις που στόχο έχουν να βλάψουν την Εθνική Ασφάλεια και Άμυνα της Χώρας, καθώς και τα συμφέροντά αυτής.

7. Ασφάλεια (ΣΕΠ)

Είναι η εφαρμογή μέτρων ασφαλείας για την προστασία των πληροφοριών από ανεπιθύμητη εκμετάλλευση, αποκάλυψη, καταστροφή και παρακώλυση εξυπηρέτησης των νόμιμων χρηστών, που επιτυγχάνονται μέσω υποκλοπής, ατυχήματος, φυσικής καταστροφής, παραπλάνησης, παρείσφρησης ή μέσω εκδήλωσης όποιας άλλης παράνομης πρόσβασης στα ΣΕΠ. Σε αυτά τα μέτρα, περιλαμβάνεται η ασφάλεια ΣΕΠ, η φυσική ασφάλεια, η ασφάλεια προσωπικού και η ασφάλεια πληροφοριών.

8. Ασφάλεια Υπολογιστών

Είναι η εφαρμογή χαρακτηριστικών ασφαλείας υλικού (hardware), λογισμικού (software) ή συνδυασμού αυτών σε ένα σύστημα υπολογιστών, για να προστατευτεί ή να εμποδιστεί η μη εξουσιοδοτημένη αποκάλυψη, χειρισμός, τροποποίηση, διαγραφή πληροφοριών και η άρνηση παροχής υπηρεσίας.

9. Βιομηχανική Ασφάλεια

Η εφαρμογή μέτρων διασφάλισης της προστασίας των ΕΔΠΥ από τους οικονομικούς φορείς κατά τις διαπραγματεύσεις, πριν από την ανάθεση της σύμβασης και καθ’ όλη τη διάρκεια του κύκλου ζωής των διαβαθμισμένων συμβάσεων.

10. Διαβαθμισμένη Σύμβαση

Οποιαδήποτε σύμβαση για την οποία απαιτείται πρόσβαση σε ΕΔΠΥ από άτομα που εμπλέκονται στην σύνταξη αυτής ή σε διαπραγματεύσεις πριν από την σύμβαση.

11. Διαπίστευση ΣΕΠ

Είναι η εξουσιοδότηση και έγκριση που δίδεται σε ένα ΣΕΠ, ώστε να επεξεργάζεται διαβαθμισμένες πληροφορίες στο επιχειρησιακό του περιβάλλον. Μία

τέτοια διαπίστευση δίδεται, αφού έχουν εφαρμοσθεί όλες οι κατάλληλες διαδικασίες ασφαλείας και έχει επιτευχθεί ένα επαρκές επίπεδο προστασίας των μέσων του ΣΕΠ.

12. Διασύνδεση ΣΕΠ

Για τον παρόντα Κανονισμό, ως διασύνδεση ορίζεται η απ' ευθείας σύνδεση (μονής ή πολλαπλής κατεύθυνσης), δύο ή περισσοτέρων ΣΕΠ για την ανταλλαγή δεδομένων. Όταν τα ανωτέρω δύο ή περισσότερα ΣΕΠ συνδέονται με δημόσιο δίκτυο, χρησιμοποιώντας αυτό αποκλειστικά ως τηλεπικοινωνιακό φορέα και τα διακινούμενα δεδομένα κρυπτογραφούνται από πιστοποιημένο (σύμφωνα με τις διατάξεις του παρόντος Κανονισμού) κρυπτογραφικό υλικό, τότε η σύνδεση αυτή, δε θεωρείται διασύνδεση με το δημόσιο δίκτυο.

13. Έγγραφο

Με τον όρο αυτό χαρακτηρίζεται κάθε έντυπο ή ηλεκτρονικό μέσο, που περιέχει καταγεγραμμένη πληροφορία, ανεξάρτητα από τη μορφή και τα χαρακτηριστικά της.

14. Εγκατάσταση

Κάθε κτίριο ή ομάδα κτιρίων που αποτελούν ένα συγκρότημα, εργοστάσιο, εργαστήριο, γραφείο, εταιρεία, εμπορική επιχείρηση συμπεριλαμβανομένων και των αποθηκών, που όταν συσχετιστούν με τη λειτουργία και την τοποθεσία, αποτελούν μία ενότητα ή έναν οικονομικό φορέα.

15. Εθνική Άμυνα

Είναι η σύνθετη έννοια, που περιλαμβάνει κάθε μορφή υπεράσπισης συντεταγμένων κρατικών δυνάμεων ενός έθνους, έναντι κάθε απειλής, επιβουλής ή διεκδίκησης, που άμεσα ή έμμεσα απειλούν την ύπαρξη, την επιβίωση και την ακεραιότητά του.

16. Εθνική Ασφάλεια

Συλλογικός όρος, που ενσωματώνει τα πεδία της Εθνικής Άμυνας, της Εσωτερικής Ασφάλειας και των Εξωτερικών Σχέσεων.

17. Εθνική Διαβαθμισμένη Πληροφορία και Υλικό (ΕΔΠΥ)

Με τον όρο αυτό, νοείται κάθε πληροφορία και υλικό, που έχει χαρακτηριστεί με βαθμό ασφαλείας σύμφωνα με τις διατάξεις του παρόντος Κανονισμού και των οποίων η άνευ αδείας κοινολόγηση, δύναται να βλάψει ποικιλοτρόπως τα εθνικά συμφέροντα της Χώρας.

18. Εθνικό Συμφέρον

Όρος που αφορά στη διασφάλιση της συλλογικής ελευθερίας και της επιβίωσης ενός έθνους – κράτους, στη διατήρηση των συντελεστών ισχύος του, στη διαφύλαξη των πολιτικών και οικονομικών δραστηριοτήτων του, με σκοπό την προστασία της φυσικής, οικονομικής, πολιτικής και πολιτισμικής ταυτότητάς του, από οποιαδήποτε επιβουλή ή απειλή.

19. Εμπορευματοκιβώτιο

Μεγάλο κυτίο από σκληρή κατασκευή με άνοιγμα που κλειδώνει, το οποίο έχει τη δυνατότητα μεταφοράς.

20. Εξουσιοδότηση Ασφαλείας Προσωπικού

Έγγραφο που εκδίδεται από την Εθνική Αρχή Ασφαλείας (ΕΑΑ), σύμφωνα με τις προβλέψεις του παρόντος Κανονισμού, με το οποίο πιστοποιείται η δυνατότητα του συγκεκριμένου προσωπικού, να λαμβάνει γνώση, να διαχειρίζεται και να συμβάλει στην ασφάλεια και προστασία ΕΔΠΥ συγκεκριμένης διαβάθμισης, για ορισμένη χρονική διάρκεια και για συγκεκριμένο οικονομικό φορέα.

21. Εσωτερική Ασφάλεια

Όρος που αναφέρεται στην προστασία της πολιτικής σταθερότητας, της οικονομικής ευημερίας, της κοινωνικής προόδου και συνοχής, της περιβαλλοντικής ισορροπίας, καθώς και της απρόσκοπτης προσβασιμότητας σε υπηρεσίες, από κάθε απειλή, κυρίως του οργανωμένου εγκλήματος και της τρομοκρατίας, αλλά και από κάθε φυσική ή ανθρωπογενή καταστροφή.

22. Κρίσιμες Υποδομές Χώρας

Με τον όρο αυτό νοούνται τα περιουσιακά στοιχεία, συστήματα ή μέρη αυτών τα οποία είναι ουσιώδη για τη διατήρηση των λειτουργιών ζωτικής σημασίας της κοινωνίας, της υγείας, της ασφάλειας, της οικονομικής και κοινωνικής ευημερίας των μελών της, και των οποίων η διακοπή ή η καταστροφή έχει σημαντικό αντίκτυπο για τη Χώρα, ως αποτέλεσμα της αδυναμίας διατήρησης των λειτουργιών αυτών.

23. Κύκλος ζωής ΣΕΠ

Είναι η συνολική διάρκεια ύπαρξης ενός ΣΕΠ που περιλαμβάνει την έναρξη της διαδικασίας, την αρχική σύλληψη, τον προγραμματισμό, την ανάλυση απαιτήσεων, το σχεδιασμό, την ανάπτυξη, τη δοκιμή, την εφαρμογή, τη λειτουργία του, τη συντήρηση και τον παροπλισμό.

24. Οικονομικός φορέας

Κάθε εργολήπτης, εργολάβος, υπεργολάβος, προμηθευτής, πάροχος υπηρεσιών, ήτοι κάθε φυσικό ή νομικό πρόσωπο, ένωση προσώπων ή φορέας του Δημοσίου ή κοινοπραξία των υπόψη προσώπων ή φορέων, που προσφέρει αντίστοιχα την εκτέλεση εργασιών ή έργων, την προμήθεια προϊόντων ή την παροχή υπηρεσιών στην αγορά.

25. Παραλήπτης

Ο ανάδοχος, ο οικονομικός φορέας, ή άλλος οργανισμός που λαμβάνει το υλικό από τον αποστολέα για περαιτέρω διαχείριση ή άλλους λόγους. Δεν περιλαμβάνει τους μεταφορείς ή τους μεσάζοντες.

26. Πιστοποιητικό Ασφάλειας Εγκατάστασης (ΠΑΕ)

Έγγραφο που εκδίδεται από την ΕΑΑ, με το οποίο πιστοποιείται ότι μία εγκατάσταση ενός οικονομικού φορέα μπορεί να παράσχει ασφάλεια σε διαβαθμισμένες πληροφορίες. Οποτεδήποτε συναντάται ο όρος Πιστοποιητικό Βιομηχανικής Ασφάλειας νοείται το ΠΑΕ και οι πράξεις εξουσιοδοτήσεως ασφάλειας προσωπικού του οικονομικού φορέα.

27. Πληροφορία

Με τον όρο αυτό νοείται κάθε είδους γνώση, η οποία μπορεί να μεταδοθεί με οποιοδήποτε μέσο και μορφή.

28. Στελέχη

Τα άτομα εκείνα τα οποία βρίσκονται σε διευθυντικές θέσεις, πέραν των ιδιοκτητών ή διευθυντών, τα οποία διευθύνουν έναν οικονομικό φορέα.

29. Σύστημα Επικοινωνιών Πληροφορικής (ΣΕΠ)

Καλείται κάθε σύστημα, το οποίο επεξεργάζεται, αποθηκεύει και διαβιβάζει πληροφορίες με ηλεκτρονικά μέσα. Ένα ΣΕΠ περιλαμβάνει το σύνολο των στοιχείων που απαιτούνται για τη λειτουργία του, συμπεριλαμβανομένων της υποδομής, της οργάνωσης, του προσωπικού και των πληροφοριών. Τα όρια ενός συστήματος καθορίζονται, γενικά, ως τα στοιχεία που ευρίσκονται υπό τον έλεγχο μιας μόνο Αρχής Επιχειρησιακής Λειτουργίας ΣΕΠ. Ένα ΣΕΠ μπορεί να περιέχει υποσυστήματα, μερικά από τα οποία είναι επίσης ολοκληρωμένα ΣΕΠ. Για λόγους απλοποίησης, αντί των όρων «επεξεργάζεται», «αποθηκεύει» και «διαβιβάζει» γίνεται χρήση του όρου «χειρίζεται».

30. Τρόπος ασφαλούς λειτουργίας ΣΕΠ

α. Αποκλειστικός

Είναι ο τρόπος λειτουργίας ασφαλείας, κατά τον οποίο όλα τα άτομα με πρόσβαση στο ΣΕΠ, είναι εξουσιοδοτημένα για το επίπεδο διαβάθμισης του συνόλου των πληροφοριών, που χειρίζεται το ΣΕΠ. Για όλα τα άτομα ισχύει η αρχή «ανάγκη γνώσης». Όλα τα άλλα χαρακτηριστικά ασφαλείας συμμορφώνονται με απαιτήσεις του ανώτερου επιπέδου διαβάθμισης που χειρίζεται το ΣΕΠ ή των επικοινωνιών.

β. Υψηλού Επιπέδου (Μονοεπίπεδος)

Είναι ο τρόπος λειτουργίας ασφαλείας, κατά τον οποίο όλα τα άτομα με πρόσβαση στο ΣΕΠ, είναι εξουσιοδοτημένα για το ανώτατο επίπεδο διαβάθμισης των πληροφοριών που χειρίζεται το σύστημα, ενώ δεν έχουν όλα τα άτομα πλήρη πρόσβαση σε πληροφορίες, υπηρεσίες και πόρους του συστήματος. Η πρόσβαση των ατόμων ακολουθεί την αρχή «ανάγκη γνώσης». Η έλλειψη ανάγκης κοινής γνώσης, δείχνει ότι υπάρχει απαίτηση τα χαρακτηριστικά ασφαλείας των συστημάτων να παρέχουν επιλεκτική πρόσβαση σε πληροφορίες και διαχωρισμό των πληροφοριών μέσα στο ΣΕΠ. Άλλα χαρακτηριστικά ασφαλείας συμμορφώνονται με τις απαιτήσεις του υψηλότερου επίπεδου διαβάθμισης που χειρίζεται το σύστημα.

γ. Πολλαπλού Επιπέδου (Πολυεπίπεδος)

Είναι ο τρόπος λειτουργίας κατά τον οποίο ένα μέρος από τα άτομα με πρόσβαση στο ΣΕΠ είναι εξουσιοδοτημένα για το ανώτατο επίπεδο διαβάθμισης των πληροφοριών, που χειρίζονται από το ΣΕΠ και επί πλέον ένα μέρος από τα άτομα με πρόσβαση στο ΣΕΠ έχουν βασική «ανάγκη γνώσης», για τις πληροφορίες που χειρίζεται το σύστημα. Αυτός ο τρόπος λειτουργίας επιτρέπει από κοινού, το χειρισμό πληροφοριών διαφορετικών επιπέδων διαβάθμισης, επειδή υπάρχει στο σύστημα μηχανισμός ελέγχου των επιπέδων διαβάθμισης. Η έλλειψη ανάγκης εξουσιοδότησης όλων των ατόμων για το ανώτατο επίπεδο, μαζί με την έλλειψη βασικής απαραίτητης γνώσης, δείχνει ότι υπάρχει απαίτηση για πιστοποιημένα χαρακτηριστικά ασφαλείας υπολογιστών, τα οποία να παρέχουν επιλεκτική πρόσβαση σε πληροφορίες και διαχωρισμό πληροφοριών μέσα στο ΣΕΠ. Σε αυτόν τον τρόπο λειτουργίας, επιτρέπεται ο χειρισμός πολλών ειδών κατηγοριοποιημένων πληροφοριών από προσωπικό που φέρει ανάλογη εξουσιοδότηση.

δ. Κατηγοριοποιημένος

Είναι τρόπος λειτουργίας ασφαλείας ανάλογος του μονοεπίπεδου, κατά τον οποίο όμως το σύστημα επιτρέπεται να χειριστεί, είτε περισσότερα του ενός είδη κατηγοριοποιημένων πληροφοριών ή συνδυασμό εθνικά διαβαθμισμένων, με κατηγοριοποιημένες πληροφορίες. Οι χρήστες απαιτούνται να φέρουν εθνική εξουσιοδότηση τουλάχιστον «ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ», ώστε να μπορούν να κυκλοφορούν ασυνόδευτοι στο χώρο του συστήματος, ενώ φέρουν και όποια άλλη εξουσιοδότηση απαιτείται για το χειρισμό των πληροφοριών στις οποίες έχουν πρόσβαση.

ε. Ελεγχόμενος

Είναι ο τρόπος λειτουργίας ανάλογος του πολυεπίπεδου, κατά τον οποίο δεν υπάρχει πιστοποίηση όλων των απαραίτητων δυνατοτήτων ενός συστήματος, οπότε κατά την πιστοποίηση αναφέρονται ξεκάθαρα οι περιορισμοί του συστήματος, καθώς και τα χαρακτηριστικά του συστήματος στα οποία υπάρχει εμπιστοσύνη. Κατά τη διαπίστευση του συστήματος, αποφασίζονται ανάλογοι περιορισμοί στις σχετικές διαβαθμίσεις που μπορεί να χειριστεί το σύστημα. Επίσης και διαφορετικά μέρη του ιδίου συστήματος δύνανται να λειτουργούν με διαφορετικό τρόπο ασφαλείας. Στις περιπτώσεις αυτές, υπάρχουν τα κατάλληλα και όπου απαιτείται πιστοποιημένα μέτρα ασφαλείας που εγκρίνονται κατά τη διαπίστευση, ώστε να εξασφαλίζεται η στεγανότητα μεταξύ των μερών ενός συστήματος που λειτουργούν με διαφορετική μέθοδο ασφαλείας.

31. Υλικό

Ο όρος αυτός περιλαμβάνει τα έγγραφα, καθώς επίσης και κάθε είδος μηχανήματος, εξοπλισμού και οπλισμού, το οποίο είτε βρίσκεται στο στάδιο μελέτης ή κατασκευής, είτε έχει ήδη κατασκευασθεί.

32. Υπαρχείο

Με τον όρο αυτό καθορίζεται ιδιαίτερος χώρος ασφαλείας, μέσα σε μόνιμες, ισχυρές από πλευράς κατασκευής κτιριακές εγκαταστάσεις, που αποτελείται από ένα ή περισσότερα συνεχόμενα δωμάτια (χώρους), τα οποία προστατεύονται ισχυρά με διαδοχικές πόρτες και παράθυρα, όπου διαφυλάσσεται, δακτυλογραφείται, αναπαράγεται και διακινείται υλικό βαθμού ασφαλείας «ΑΠΟΡΡΗΤΟ» και άνω.

33. Χώρος ΣΕΠ

Είναι ο χώρος που περιέχει έναν ή περισσότερους Η/Υ, τις τοπικές περιφερειακές μονάδες τους και μονάδες αποθήκευσης, τις μονάδες ελέγχου, τον εξοπλισμό δικτύου και επικοινωνιών, συμπεριλαμβανομένου και του χώρου απομακρυσμένων τερματικών / σταθμών εργασίας που περιέχει εξοπλισμό Η/Υ με τις τοπικές του συσκευές, τα τερματικά / σταθμούς εργασίας και οποιοδήποτε σχετικό εξοπλισμό επικοινωνιών.

34. Χώροι Ασφαλείας

Είναι οι χώροι στους οποίους τηρούνται και διακινούνται ΕΔΠΥ διαβάθμισης «ΕΜΠΙΣΤΕΥΤΙΚΟ» και άνω. Οι χώροι αυτοί είναι οργανωμένοι και κατάλληλα διαμορφωμένοι με τέτοιο τρόπο ώστε η είσοδος και η εκτέλεση εργασίας να επιτρέπεται μόνο σε κατάλληλα εξουσιοδοτημένο προσωπικό.

ΑΡΘΡΟ 3
ΓΕΝΙΚΕΣ ΑΡΧΕΣ ΑΣΦΑΛΕΙΑΣ

1. Οι αρχές βιομηχανικής ασφάλειας που εφαρμόζονται από κάθε οικονομικό φορέα, είναι:

α. Η εξουσιοδότηση σύμφωνα με τις διατάξεις του παρόντος Κανονισμού όλου του προσωπικού που πρόκειται να χειρισθεί ΕΔΠΥ ή να αποκτήσει πρόσβαση σε αυτό, καθώς και η τήρηση των μέτρων ασφαλείας από όλο το προσωπικό που χειρίζεται ή αποκτά πρόσβαση σε ΕΔΠΥ.

β. Η απομάκρυνση από τα καθήκοντα χειρισμού διαβαθμισμένου υλικού, του προσωπικού για το οποίο επήλθε μεταγενέστερα κώλυμα και του οποίου η εξουσιοδότηση ασφαλείας αίρεται, κατόπιν αιτήσεως του οικονομικού φορέα ή αυτοδίκαια από την ΕΑΑ.

γ. Ο αποκλεισμός στην πρόσβαση μη εξουσιοδοτημένων ατόμων γενικά σε ΕΔΠΥ ή σε χώρους όπου αυτό φυλάσσεται.

δ. Ο καθορισμός τρόπων διασφάλισης της προστασίας ΕΔΠΥ σε περιπτώσεις καταστάσεων έκτακτης ανάγκης.

ε. Η πιστή εφαρμογή της θεμελιώδους αρχής «ανάγκη γνώσης».

ΑΡΘΡΟ 4
ΟΡΓΑΝΩΣΗ ΥΠΗΡΕΣΙΩΝ ΑΣΦΑΛΕΙΑΣ

1. Το Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ):

α. Είναι η Εθνική Αρχή Ασφαλείας (ΕΑΑ) [National Security Authority (NSA)] της Χώρας, με αρμόδια Διεύθυνση το ΓΕΕΘΑ/Ε΄ ΚΛΑΔΟ/Ε3.

β. Έχει την ευθύνη, ως ΕΑΑ:

(1) Για τον καθορισμό της εθνικής πολιτικής όσον αφορά στην ασφάλεια και την προστασία των ΕΔΠΥ.

(2) Για την ασφάλεια και την προστασία των διαβαθμισμένων πληροφοριών-υλικών του ΝΑΤΟ και της ΕΕ αντίστοιχα.

γ. Συντονίζει τις αρμόδιες, για θέματα ασφαλείας, Υπηρεσίες των Υπουργείων, Δημοσίων Υπηρεσιών, Οργανισμών Τοπικής Αυτοδιοίκησης και Ενόπλων Δυνάμεων, επί των μέτρων ασφαλείας, για την προστασία των ΕΔΠΥ.

δ. Εκδίδει το ΠΑΕ των οικονομικών φορέων, αφού λάβει υπόψη τη θετική εισήγηση της αρμόδιας επιτροπής του άρθρου 13, παράγραφος 2 και το αποστέλλει στη Διορισμένη Αρχή Ασφαλείας (ΔΑΑ).

ε. Εξουσιοδοτεί το προσωπικό των οικονομικών φορέων για το χειρισμό ΕΔΠΥ.

στ. Συμμετέχει με εκπροσώπους στην επιτροπή επιθεωρήσεως που συγκροτεί το Υπουργείο Εθνικής Άμυνας/Γενική Διεύθυνση Αμυντικών Εξοπλισμών και Επενδύσεων/Διεύθυνση Αμυντικών Επενδύσεων και Τεχνολογικών Ερευνών (ΥΠΕΘΑ/ΓΔΑΕΕ/ΔΑΕΤΕ).

2. Το ΥΠΕΘΑ/ΓΔΑΕΕ/ΔΑΕΤΕ είναι η Διορισμένη Αρχή Ασφαλείας (ΔΑΑ) [Designated Security Authority (DSA)] και ευθύνεται για:

α. Την παροχή οδηγιών προς τους οργανισμούς, οικονομικούς φορείς και όλους εκείνους που ασχολούνται με το αμυντικό υλικό, ή γενικότερα το χειρισμό ΕΔΠΥ.

β. Τον έλεγχο για την εφαρμογή του παρόντος κανονισμού από φυσικά και νομικά πρόσωπα ή ενώσεις προσώπων που υλοποιούν ερευνητικά, αναπτυξιακά προγράμματα, ειδικές μελέτες επ’ ωφελεία των Ενόπλων Δυνάμεων (ΕΔ), καθώς και προγράμματα ή συμβάσεις που ενδέχεται να εμπεριέχουν ΕΔΠΥ.

γ. Την τήρηση μητρώου εξουσιοδοτημένων οικονομικών φορέων και προσωπικού αυτών.

δ. Τη συγκρότηση επιτροπής επιθεωρήσεων βιομηχανικής ασφάλειας και τη διαβίβαση του Πιστοποιητικού Ασφάλειας Εγκατάστασης στον οικονομικό φορέα που ελέγχθηκε.

3. Γραφεία ασφαλείας οικονομικών φορέων

α. Σε κάθε οικονομικό φορέα στον οποίο απαιτείται η τήρηση ΕΔΠΥ σύμφωνα με τις διατάξεις του παρόντα κανονισμού συστήνεται γραφείο ασφαλείας.

β. Τα γραφεία ασφαλείας των οικονομικών φορέων, είναι αρμόδια για την τήρηση και προστασία των ΕΔΠΥ, σύμφωνα με τις διατάξεις παρόντος. Η έδρα των γραφείων είναι εντός των κτιριακών εγκαταστάσεων για τους οποίους λαμβάνεται ΠΑΕ του οικονομικού φορέα και κατά προτίμηση σε χώρο πλησίον της κυρίας εισόδου.

γ. Η σύνθεση του γραφείου ασφαλείας καθορίζεται από τη διοίκηση του οικονομικού φορέα, ανάλογα με τις ανάγκες και το μέγεθος αυτού. Το προσωπικό στελέχωσης αποτελείται κατ’ ελάχιστο από τον υπεύθυνο ασφαλείας και τον βοηθό / αναπληρωτή του.

4. Ο υπεύθυνος ασφαλείας του οικονομικού φορέα είναι αρμόδιος:

α. Έναντι της διοίκησης επί θεμάτων ασφαλείας.

β. Για το συντονισμό των μέσων και μέτρων ασφαλείας που αφορούν στο εκάστοτε συγκεκριμένο έργο, πρόγραμμα ή σύμβαση.

γ. Για το συντονισμό των αναγκών ασφαλείας του οικονομικού φορέα με τα σώματα ασφαλείας και την οποιαδήποτε πολιτική υπηρεσία προστασίας που ίσως χρησιμοποιηθεί.

δ. Για το σχεδιασμό και την εφαρμογή των μέτρων ασφαλείας και διαδικασιών του οικονομικού φορέα, σύμφωνα με τις διατάξεις του παρόντος Κανονισμού και την αναθεώρηση αυτών όποτε απαιτείται.

ε. Για τα περιγραφόμενα στο Παράρτημα «Α».

ΑΡΘΡΟ 5
ΒΑΘΜΟΙ ΑΣΦΑΛΕΙΑΣ

1. Ο βαθμός της παρεχόμενης προστασίας ανταποκρίνεται στην κρισιμότητα και στη σπουδαιότητα της πληροφορίας ή του υλικού, το οποίο επιβάλλεται να προστατευθεί. Για το σκοπό αυτό, οι ΕΔΠΥ είναι αναγκαίο να προστατεύονται ανάλογα με τη διαβάθμιση που δίδεται από τον εκδότη και να κοινοποιούνται σε περιορισμένο προσωπικό κατάλληλα εξουσιοδοτημένο, ακολουθώντας τη θεμελιώδη

αρχή «ανάγκη γνώσης».

2. Οι Εθνικοί βαθμοί ασφαλείας, βάσει των οποίων διαβαθμίζονται οι ΕΔΠΥ, είναι οι εξής:

α. ΕΤΝΑ ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ (ΕΤΝΑ ΑΑΠ)

(1) Ο χαρακτηρισμός αυτός δίδεται σε υλικό και πληροφορίες, των οποίων η αποκάλυψη σε μη εξουσιοδοτημένο προσωπικό, πρόκειται να προκαλέσει εξαιρετικά σοβαρές ζημίες στην εθνική άμυνα και ασφάλεια, καθώς και στα ζωτικά συμφέροντα της Χώρας, όπως:

(α) Μαζική απώλεια ζωής ανθρώπων.

(β) Δραστική μείωση της μαχητικής ισχύος της Χώρας, θέτοντας σε άμεσο κίνδυνο την εδαφική της ακεραιότητα.

(γ) Ανεξέλεγκτη δράση εγχώριων ή/και διεθνών οργανώσεων εγκλήματος και τρομοκρατίας.

(δ) «Κατάρρευση» της λειτουργίας κρίσιμων υποδομών της Χώρας.

(ε) Ανεπανόρθωτες ζημιές στο περιβάλλον εσωτερικής ασφάλειας της Χώρας και στις διεθνείς της σχέσεις.

(2) Ο όρος «ΕΤΝΑ», δεν αποτελεί από μόνος του βαθμό ασφαλείας, αλλά ένδειξη που προέρχεται από τη λέξη «ΕΘΝΙΚΟ», για να είναι δυνατή η αναγραφή της με τα ίδια τυπογραφικά στοιχεία και στην ελληνική και στις γλώσσες που χρησιμοποιούν το λατινικό αλφάβητο.

β. ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ (ΑΑΠ)

Ο χαρακτηρισμός αυτός δίδεται σε υλικό και πληροφορίες, των οποίων η αποκάλυψη σε μη εξουσιοδοτημένο προσωπικό, είναι δυνατό να προκαλέσει σοβαρές ζημίες στην εθνική άμυνα και ασφάλεια, καθώς και στα ζωτικά συμφέροντα της Χώρας, όπως:

(1) Απώλεια ζωής σημαντικού αριθμού ανθρώπων.

(2) Σημαντική μείωση της μαχητικής ισχύος των ΕΔ.

(3) Να καταστήσει αδύνατη την έρευνα και τη δίωξη εγχώριων ή/και διεθνικών σοβαρών και οργανωμένων μορφών εγκλήματος και της τρομοκρατίας, από τις Αρχές επιβολής του νόμου.

(4) Άμεση και υπαρκτή διακινδύνευση της λειτουργίας κρίσιμων υποδομών της Χώρας.

(5) Πρόκληση σοβαρών ζημιών στο περιβάλλον εσωτερικής ασφάλειας της Χώρας και στις διεθνείς της σχέσεις.

γ. ΑΠΟΡΡΗΤΟ (ΑΠ)

Ο χαρακτηρισμός αυτός δίδεται σε υλικό και πληροφορίες, των οποίων η αποκάλυψη σε μη εξουσιοδοτημένο προσωπικό, είναι δυνατό να προκαλέσει ζημίες στην εθνική άμυνα και ασφάλεια, καθώς και στα ζωτικά συμφέροντα της Χώρας, όπως:

(1) Απώλεια ζωής ανθρώπων.

(2) Μείωση της μαχητικής ισχύος των ΕΔ.

(3) Να παρεμποδίσει μακροπρόθεσμα την έρευνα και τη δίωξη εγχώριων ή/και διεθνικών σοβαρών και οργανωμένων μορφών εγκλήματος και της τρομοκρατίας, από τις Αρχές επιβολής του νόμου.

(4) Να θέσει σε σοβαρό κίνδυνο τις λειτουργίες κρίσιμων υποδομών της Χώρας.

(5) Να προκαλέσει ζημιές στο περιβάλλον εσωτερικής ασφάλειας της Χώρας και στις διεθνείς της σχέσεις.

δ. ΕΜΠΙΣΤΕΥΤΙΚΟ (ΕΠ)

Ο χαρακτηρισμός αυτός δίδεται σε υλικό και πληροφορίες, των οποίων η αποκάλυψη σε μη εξουσιοδοτημένο προσωπικό, ενδέχεται να βλάψει την εθνική άμυνα και ασφάλεια, καθώς και τα ζωτικά συμφέροντα της Χώρας, όπως:

(1) Να θέσει σε κίνδυνο την προσωπική ασφάλεια ανθρώπων, ή ομάδων ανθρώπων.

(2) Να βλάψει τη μαχητική ισχύ των ΕΔ.

(3) Να παρεμποδίσει ή/και να αποκαλύψει την έρευνα και τη δίωξη εγχώριων, ή/και διεθνικών σοβαρών και οργανωμένων μορφών εγκλήματος και της τρομοκρατίας, από τις Αρχές επιβολής του νόμου.

(4) Να θέσει σε κίνδυνο τις λειτουργίες κρίσιμων υποδομών της Χώρας.

(5) Να βλάψει το περιβάλλον εσωτερικής ασφάλειας της Χώρας και τις διεθνείς της σχέσεις.

ε. ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ (ΠΧ)

Ο χαρακτηρισμός αυτός δίδεται σε υλικό και πληροφορίες, των οποίων η αποκάλυψη σε μη εξουσιοδοτημένο προσωπικό, είναι δυνατό να επηρεάσει δυσμενώς την εθνική άμυνα και ασφάλεια, καθώς και τα ζωτικά συμφέροντα της Χώρας, όπως:

(1) Να επιδράσει δυσμενώς στη μαχητική ισχύ των ΕΔ.

(2) Να διαταράξει τις λειτουργίες κρίσιμων υποδομών της Χώρας.

(3) Να επηρεάσει δυσμενώς το περιβάλλον εσωτερικής ασφάλειας της Χώρας και τις διεθνείς της σχέσεις.

3. Απαγορεύεται η ανάρτηση διαβαθμισμένης πληροφορίας στο διαδίκτυο.

4. Κάθε υλικό ή πληροφορία που δεν φέρει χαρακτηρισμό σύμφωνα με την ανωτέρω παράγραφο 2, χαρακτηρίζεται ως ΑΔΙΑΒΑΘΜΗΤΟ (ΑΔ). Ο χαρακτηρισμός αυτός, δεν συνιστά βαθμό ασφαλείας. Υλικό ή πληροφορία με χαρακτηρισμό «ΑΔΙΑΒΑΘΜΗΤΟ», επιτρέπεται να αναρτηθεί στο διαδίκτυο, μόνο εφόσον αυτό ορίζεται ρητά στο προ του κειμένου μέρος, με την ένδειξη «ΑΝΑΡΤΗΤΕΟ ΣΤΟ ΔΙΑΔΙΚΤΥΟ», τηρουμένης πάντοτε της αρχής «ανάγκη γνώσης».

5. Υλικά ή πληροφορίες, τα οποία ανάλογα με το περιεχόμενο ή το αντικείμενό τους απαιτούν ειδική μεταχείριση, σημαίνονται με πρόσθετο χαρακτηρισμό, ο οποίος γράφεται σε παρένθεση αμέσως μετά τον βαθμό ασφαλείας, όπως παρακάτω:

α. ΕΙΔΙΚΟΥ ΧΕΙΡΙΣΜΟΥ (ΕΧ)

Αυτός ο χαρακτηρισμός χρησιμοποιείται όταν κρίνεται αναγκαίο, μόνο σε υλικό ή πληροφορία που έχει βαθμό ασφαλείας από «ΑΠΟΡΡΗΤΟ» και πάνω, όπως «ΑΠΟΡΡΗΤΟ (ΕΧ)».

β. ΠΡΟΣΩΠΙΚΟ (ΠΡΣΚΟ)

Αυτός ο χαρακτηρισμός ακολουθεί τη διαβάθμιση ασφαλείας υλικού ή πληροφορίας, όταν λαμβάνει γνώση του περιεχομένου, ειδικά προσδιορισμένος παραλήπτης, όπως «ΑΠΟΡΡΗΤΟ (ΠΡΣΚΟ)».

γ. ΚΡΥΠΤΟ – ΚΡΥΠΤΑΣΦΑΛΕΙΑ

Αυτός ο χαρακτηρισμός χρησιμοποιείται σε ΕΔΠΥ που είναι σχετικά με κρυπτοϋλικά – κρυπτασφάλεια.

6. Οι βαθμοί ασφαλείας των ΕΔΠΥ σε αντιστοιχία με τους αντίστοιχους συμμαχικούς (ΝΑΤΟ και Ευρωπαϊκής Ένωσης), έχουν όπως στον παρακάτω πίνακα:

ΑΝΑΛΟΓΙΚΟΣ ΠΙΝΑΚΑΣ ΒΑΘΜΩΝ ΑΣΦΑΛΕΙΑΣ

ΕΘΝΙΚΟΣ	ΝΑΤΟ	ΕΕ
ΕΤΝΑ ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ	-	-
ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ	COSMIC TOP SECRET	EU TOP SECRET
ΑΠΟΡΡΗΤΟ	NATO SECRET	EU SECRET
ΕΜΠΙΣΤΕΥΤΙΚΟ	NATO CONFIDENTIAL	EU CONFIDENTIAL
ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ	NATO RESTRICTED	EU RESTRICTED

ΚΕΦΑΛΑΙΟ Β
ΔΙΑΔΙΚΑΣΙΕΣ ΑΣΦΑΛΕΙΑΣ

ΑΡΘΡΟ 6
ΦΥΣΙΚΗ ΑΣΦΑΛΕΙΑ

1. Φυσική ασφάλεια είναι η εφαρμογή φυσικών και τεχνικών μέτρων προστασίας προκειμένου να εμποδίζεται αναρμόδια πρόσβαση σε ΕΔΠΥ. Τα μέτρα φυσικής Ασφάλειας σχεδιάζονται έτσι ώστε να μην επιτρέπεται η λαθραία ή βίαιη είσοδος αναρμόδιων, να αποτρέπονται, να παρεμποδίζονται και να ανιχνεύονται οι μη εξουσιοδοτημένες ενέργειες και να καθίσταται δυνατός ο διαχωρισμός του προσωπικού όσον αφορά στην πρόσβασή του σε ΕΔΠΥ βάσει της «ανάγκης γνώσης».

2. Ο βαθμός της παρεχόμενης προστασίας που κατά περίπτωση εφαρμόζεται, είναι ανάλογος του επιπέδου διαβάθμισης των ΕΔΠΥ. Τα συστήματα ασφαλείας επιθεωρούνται σε τακτά χρονικά διαστήματα και ο εξοπλισμός συντηρείται τακτικά, ενώ η αποτελεσματικότητα κάθε μέτρου ασφαλείας και ολόκληρου του συστήματος ασφαλείας, επαναξιολογείται με διαρκείς ελέγχους.

3. Κατά τη διάρκεια των εργάσιμων ωρών και ημερών, το προσωπικό που εργάζεται σε χώρους ασφαλείας και χειρίζεται ΕΔΠΥ είναι υπεύθυνο για την προστασία τους. Ο έλεγχος εξακολουθεί μετά τη λήξη του ωραρίου εργασίας από εντεταλμένο προς αυτό προσωπικό ασφαλείας του οικονομικού φορέα. Αν χρησιμοποιείται προσωπικό από ιδιωτική εταιρεία παροχής υπηρεσιών ασφαλείας (ΙΕΠΥΑ), αυτό είναι εξουσιοδοτημένο σύμφωνα με τις προβλέψεις του παρόντος Κανονισμού, με μέριμνα του οικονομικού φορέα και όχι της ΙΕΠΥΑ.

4. Οι εγκαταστάσεις του οικονομικού φορέα, στις οποίες φυλάσσονται ΕΔΠΥ, προστατεύονται από μη εξουσιοδοτημένη πρόσβαση, να πληρούν τις ελάχιστες προδιαγραφές ασφαλείας του Παραρτήματος «Δ», να ελέγχονται πλήρως από τον ίδιο οικονομικό φορέα και να μην υπάρχει πρόσβαση σε αυτές άλλου οικονομικού φορέα ή προσωπικού αυτού.

5. Οι χώροι ασφαλείας και το υπαρχείο πληρούν τις ελάχιστες προδιαγραφές ασφαλείας του Παραρτήματος «Δ».

ΑΡΘΡΟ 7
ΕΞΟΥΣΙΟΔΟΤΗΣΗ ΑΣΦΑΛΕΙΑΣ ΠΡΟΣΩΠΙΚΟΥ

1. Οι εξουσιοδοτήσεις ασφαλείας προσωπικού είναι πέντε (5) κατηγοριών:

α.	ΕΤΝΑ ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ	(ΕΤΝΑ ΑΑΠ)
β.	ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ	(ΑΑΠ)
γ.	ΑΠΟΡΡΗΤΟ	(ΑΠ)
δ.	ΕΜΠΙΣΤΕΥΤΙΚΟ	(ΕΠ)
ε.	ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ	(ΠΧ)

2. Η κατηγορία της εξουσιοδότησης ασφαλείας του προσωπικού βρίσκεται σε αντιστοιχία με το βαθμό ασφάλειας των ΕΔΠΥ, που χειρίζεται ο εξουσιοδοτημένος οικονομικός φορέας και δεν είναι ανώτερη από το ΠΑΕ.

3. Η εξουσιοδότηση ασφαλείας προσωπικού αφορά κατά βάση στους Έλληνες υπηκόους. Κατ΄ εξαίρεση μπορεί να εκδοθεί για τους αλλοδαπούς, όταν τούτο κρίνεται απολύτως αναγκαίο, για την υποστήριξη ενός προγράμματος έργου, σύμβασης ή λειτουργίας και κατόπιν ελέγχου ασφαλείας από την ΕΑΑ, σε συνεργασία με αρμόδιες αρχές της χώρας που είναι υπήκοος ο αλλοδαπός, με την προϋπόθεση ύπαρξης συμφωνίας προστασίας και ανταλλαγής διαβαθμισμένων πληροφοριών (Security Agreement on Classified Information) με την Ελλάδα.

4. Με βάση τη θεμελιώδη αρχή «ανάγκη γνώσης», η γνώση και ο χειρισμός ΕΔΠΥ δεν επεκτείνεται σε όλο το προσωπικό του οικονομικού φορέα, αλλά περιορίζεται σε αυτό που είναι απόλυτα αναγκαίο να έχει πρόσβαση.

5. Η ανάθεση των καθηκόντων ασφάλειας σε προσωπικό του οικονομικού φορέα είναι απαραίτητη και προηγείται της εξουσιοδότησης ασφάλειας του προσωπικού που πρόκειται να αποκτήσει πρόσβαση σε ΕΔΠΥ. Η πρόσβαση σε ΕΔΠΥ δεν επιτρέπεται σε προσωπικό του οικονομικού φορέα πριν την εξουσιοδότησης ασφαλείας αυτού.

6. Στο προσωπικό του οικονομικού φορέα που απαιτείται να λάβει εξουσιοδότηση ασφαλείας περιλαμβάνονται τα πρόσωπα που ασκούν πράξεις διαχείρισης ή διοίκησης του οικονομικού φορέα, τα μέλη του διοικητικού ή διαχειριστικού οργάνου του οικονομικού φορέα, οι ιδιοκτήτες ή οι κύριοι μέτοχοι επί ανωνύμου εταιρείας, οι διευθυντές και τα ανώτερα στελέχη, οι υπεύθυνοι ασφαλείας, καθώς και όλα τα φυσικά πρόσωπα ανεξαρτήτως ιθαγένειας, τα οποία πρόκειται να αποκτήσουν πρόσβαση σε ΕΔΠΥ και τα οποία καθορίζονται με μέριμνα του ασκούντος τη διαχείριση ή διοίκηση του οικονομικού φορέα.

7. Η εξουσιοδότηση ασφαλείας του προσωπικού, πραγματοποιείται όπως παρακάτω:

α. Καθορίζονται εγγράφως, με μέριμνα του διευθύνοντος συμβούλου ή του ασκούντος τη διαχείριση/διοίκηση, όλα τα φυσικά πρόσωπα του οικονομικού φορέα που απαιτείται να έχουν πρόσβαση και να διαχειρίζονται ΕΔΠΥ.

β. Το προς εξουσιοδότηση προσωπικό υπογράφει υπεύθυνη δήλωση εξουσιοδότησης (Υπόδειγμα 2). Επίσης, συμπληρώνει πίνακα προσωπικών στοιχείων εις τριπλούν (Υπόδειγμα 1). Τα παραπάνω έντυπα, θεωρημένα για το γνήσιο της υπογραφής από αρμόδια κρατική αρχή, συνοδεύονται από το δελτίο υποβολής στοιχείων καταλληλόλητας (Υπόδειγμα 3).

γ. Τα παραπάνω δικαιολογητικά, μετά από έλεγχο της πληρότητας και ορθότητας των αναγραφόμενων στοιχείων, υποβάλλονται στη ΔΑΑ η οποία τα αποστέλλει στην ΕΑΑ. Η ΕΑΑ διαβιβάζει τα απαραίτητα δικαιολογητικά σε αρμόδιες αρχές, προκειμένου να προβούν στον έλεγχο ασφαλείας του προσωπικού του οικονομικού φορέα. Η ΕΑΑ διατηρεί οποτεδήποτε το δικαίωμα επανάληψης της διαδικασίας του ελέγχου ασφαλείας του ως άνω προσωπικού, ακόμη και μετά την εξουσιοδότηση.

δ. Σε περιπτώσεις εξουσιοδότησης ασφαλείας προσωπικού «ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ» και άνω, πέραν των ανωτέρω δικαιολογητικών, απαιτείται βεβαίωση από την αναθέτουσα αρχή που να πιστοποιεί:

(1) Την εμπλοκή του οικονομικού φορέα.

(2) Το βαθμό ασφαλείας της σύμβασης.

(3) Τη χρονική διάρκεια ισχύος της σύμβασης.

ε. Όταν ολοκληρωθεί ο έλεγχος ασφαλείας του προσωπικού για το οποίο απαιτείται η έκδοση εξουσιοδότησης ασφαλείας για το χειρισμό ή πρόσβαση σε ΕΔΠΥ και διαπιστωθεί ότι είναι κατάλληλο προς αυτό και ότι δεν υφίσταται σε βάρος του κάποιο από τα κωλύματα της επόμενης παραγράφου, εκδίδεται από την ΕΑΑ η εξουσιοδότηση ασφαλείας και τηρείται στη ΔΑΑ και στον οικονομικό φορέα.

στ. Τα κωλύματα που εμποδίζουν την έκδοση ή προκαλούν την άρση της εξουσιοδότησης ασφάλειας προσωπικού είναι τα εξής:

(1) Εκκρεμής αμετάκλητη παραπομπή για κακούργημα καθώς και αμετάκλητη παραπομπή για κλοπή, απάτη, υπεξαίρεση (κοινή ή στην υπηρεσία), εκβίαση, πλαστογραφία, ψευδή βεβαίωση, ψευδορκία, ψευδή ανωμοτί κατάθεση, δωροδοκία, καταπίεση, απιστία περί την υπηρεσία, παραβίαση απορρήτου, παραβίαση υπηρεσιακού απορρήτου, ψευδή καταμήνυση, συκοφαντική δυσφήμιση, παράβαση καθήκοντος, ανυποταξία, λιποταξία, οποιοδήποτε έγκλημα κατά του πολιτεύματος, κατά της Χώρας, κατά της ελεύθερης άσκησης των πολιτικών δικαιωμάτων, κατά της γενετήσιας ελευθερίας ή οικονομικής εκμετάλλευσης της γενετήσιας ζωής, παράβαση της νομοθεσίας περί ναρκωτικών, παραβάσεις της νομοθεσίας περί όπλων, πυρομαχικών, εμπρησμού, έκρηξης, εκρηκτικών υλών, εκρηκτικών μηχανισμών, σύστασης εγκληματικής οργάνωσης ή ένταξης σε αυτή ως μέλος, καθώς και τρομοκρατικών πράξεων. Επίσης, να μην έχουν καταδικαστεί οποτεδήποτε για κακούργημα ή για τα παραπάνω αναφερόμενα αδικήματα.

(2) Εκκρεμής ποινική δίωξη για έγκλημα στο οποίο έχει διαταχθεί προσωρινή κράτηση ή προφυλάκιση, από τον εκάστοτε εισαγγελέα.

(3) Οιαδήποτε σχέση με υπηρεσίες πληροφοριών ξένων Κρατών, οργανώσεις, ή συλλόγους, ή άτομα, που ενδέχεται να θέσουν σε κίνδυνο την Εθνική Ασφάλεια και το Πολίτευμα της Χώρας.

8. Κάθε οικονομικός φορέας, για τον οποίο έχει εκδοθεί ΠΑΕ, τηρεί μητρώο καταχώρησης εξουσιοδοτημένου προσωπικού (Υπόδειγμα 4).

9. Η διάρκεια ισχύος μιας εξουσιοδοτήσεως ασφαλείας βαθμού μέχρι και ΕΠ δεν μπορεί να υπερβαίνει τα δέκα (10) έτη, ενώ η αντίστοιχη διάρκεια για βαθμό ΑΠ και άνω, δεν μπορεί να υπερβαίνει τα πέντε (5) έτη.

10. Σε περίπτωση που απαιτείται η έκδοση βεβαίωσης εξουσιοδότησης ασφαλείας για προσωπικό ενός οικονομικού φορέα, για συμμετοχή του σε διαβαθμισμένη δραστηριότητα, αυτό πραγματοποιείται με μέριμνα της ΔΑΑ, κατόπιν αιτήσεως του οικονομικού φορέα. Η έκδοση βεβαίωσης εξουσιοδότησης ασφαλείας προϋποθέτει την εξουσιοδότηση ασφαλείας του υπόψη προσωπικού, σύμφωνα με τις προβλέψεις του παρόντος Κανονισμού.

11. Η άρση της εξουσιοδότησης ασφάλειας προσωπικού πραγματοποιείται από την ΕΑΑ, κατόπιν σχετικής έγγραφης αίτησης του οικονομικού φορέα, επισυναπτόμενου του Υποδείγματος 5, μόλις παύσουν να συντρέχουν οι λόγοι που στοιχειοθέτησαν την έκδοσή της.

12. Η εξουσιοδότηση ασφαλείας προσωπικού αίρεται σε κάθε περίπτωση, όταν στο εξουσιοδοτημένο προσωπικό επέρχονται μεταγενέστερα κωλύματα, όπως νομικής υφής ή έλλειψης ουσιαστικών προσόντων, τα οποία διαπιστώνονται από τον οικονομικό φορέα. Αυτός οφείλει να ενημερώσει άμεσα την ΕΑΑ και να προβεί σε ενέργειες για άρση της εξουσιοδότησης ασφαλείας σύμφωνα με την ανωτέρω

παράγραφο.

13. Η ΕΑΑ διατηρεί το δικαίωμα άρσης της εξουσιοδότησης ασφαλείας προσωπικού σε περίπτωση που διαπιστωθούν μεταγενέστερα κωλύματα της παραγράφου 7στ του παρόντος άρθρου.

ΑΡΘΡΟ 8
ΑΣΦΑΛΕΙΑ ΕΔΠΥ

1. Ο χειρισμός των ΕΔΠΥ, καθώς και η αναπαραγωγή τους γίνεται αποκλειστικά και μόνο από άτομα, που έχουν εξουσιοδοτηθεί προς τούτο, τουλάχιστον μέχρι του βαθμού ασφάλειας των εγγράφων. Οι ΕΔΠΥ, σε οποιαδήποτε μορφή, φέρουν σε εμφανές σημείο το βαθμό ασφάλειάς τους.

2. Τα παραρτήματα και οι προσθήκες των ΕΔΠΥ αναγράφονται σε πίνακα στην πρώτη σελίδα αυτού, ή στα περιεχόμενα, ενώ οι σελίδες είναι αριθμημένες και στην πρώτη σελίδα αναφέρεται ο συνολικός αριθμός τους.

3. Εάν κάποιο ΕΔΠΥ περιέχει τμήματα διαφορετικής διαβάθμισης, τότε το υλικό φέρει τον υψηλότερο βαθμό ασφάλειας από τους υπάρχοντες εσωτερικά αυτού. Οι παρακάτω πρόσθετες διαδικασίες εφαρμόζονται κατά περίπτωση:

α. Σε διαγράμματα, χάρτες και σχέδια η διαβάθμιση αναγράφεται στην εσωτερική πλευρά και στην εξωτερική όταν αυτά είναι διπλωμένα ή τυλιγμένα.

β. Φωτογραφικό υλικό, κινηματογραφικό υλικό, καθώς και κάθε άλλο μέσο στο οποία υπάρχει διαβαθμισμένη πληροφορία σημαίνεται εμφανώς με τη μέγιστη διαβάθμιση που περιέχει.

γ. Μέσα αποθήκευσης και μεταφοράς ψηφιακών δεδομένων φέρουν τη σήμανση της διαβάθμισης τυπωμένη ή σφραγισμένη.

4. Ο βαθμός ασφάλειας αναγράφεται χωριστά από οποιοδήποτε άλλο χαρακτηρισμό του υλικού. Τα γράμματα που χρησιμοποιούνται για τις διαβαθμίσεις είναι διαφορετικών τυπογραφικών στοιχείων ή με άλλο χρώμα ανατύπωσης και μεγαλύτερα από εκείνα που χρησιμοποιούνται στο κείμενο του εγγράφου.

5. Ο αποχαρακτηρισμός ή η υποβάθμιση του υλικού γίνεται μόνο από τον εκδότη ή κατόπιν αδείας του.

6. Η διανομή των ΕΔΠΥ γίνεται μόνο προς όσους έχουν ανάγκη γνώσης και αντίστοιχη εξουσιοδότηση ασφαλείας.

7. Ο εκδότης των ΕΔΠΥ καθορίζει τους αποδέκτες. Ο παραλήπτης δύναται να πραγματοποιήσει ευρύτερη διανομή, εάν τούτο απαιτηθεί σύμφωνα με τα αναφερόμενα στη προηγούμενη παράγραφο, μόνο κατόπιν εγκρίσεως του εκδότη. Η διανομή των ΕΔΠΥ πραγματοποιείται με ευθύνη της Γραμματείας.

8. Κάθε οικονομικός φορέας διαθέτει οργανωμένη κεντρική γραμματεία για τη διακίνηση όλων των εισερχομένων και εξερχόμενων ΕΔΠΥ, ενώ κάθε τμήμα της, διαθέτει, εάν είναι αποδέκτης ΕΔΠΥ, πρωτόκολλο εισερχομένων και εξερχόμενων διαβαθμισμένων εγγράφων.

ΚΕΦΑΛΑΙΟ Γ
ΣΥΜΒΑΣΕΙΣ

ΑΡΘΡΟ 9
ΔΙΑΒΑΘΜΙΣΗ ΑΣΦΑΛΕΙΑΣ ΣΥΜΒΑΣΕΩΝ

1. Ο βαθμός της απαιτούμενης προστασίας των ΕΔΠΥ που περιέχονται σε συμβάσεις ανταποκρίνεται στην αξία και στη σπουδαιότητα αυτών.

2. Για να εξασφαλισθεί ο βαθμός προστασίας των διαβαθμισμένων συμβάσεων εφαρμόζονται οι ακόλουθες βασικές αρχές:

α. Ο καθορισμός της διαβάθμισης είναι αρμοδιότητα του φορέα που αναθέτει τη σύμβαση.

β. Η διαβάθμιση ασφαλείας δίδεται στα μέρη εκείνα της σύμβασης που απαιτείται να προστατεύονται, σύμφωνα με το επίπεδο διαβάθμισης ΕΔΠΥ που περιέχουν, ενώ δεν γίνεται κατάχρηση των χαρακτηρισμών διαβάθμισης.

γ. Η συνολική διαβάθμιση ασφαλείας της σύμβασης δεν επιτρέπεται να είναι κατώτερη από την ανώτατη διαβάθμιση οποιουδήποτε μέρους της. Τα μέρη της σύμβασης που φέρουν κατώτερο βαθμό ασφαλείας από τη συνολική διαβάθμιση ασφαλείας της σύμβασης, προστατεύονται ανάλογα με το βαθμό ασφαλείας τους.

δ. Υποβίβαση του βαθμού ασφαλείας μίας σύμβασης ή τμήματος αυτής γίνεται μόνο από την αναθέτουσα αρχή, σε συνεργασία με τις ΕΑΑ/ΔΑΑ.

ΑΡΘΡΟ 10
ΑΣΦΑΛΕΙΑ ΣΥΜΒΑΣΕΩΝ

1. Η αρχή που αναθέτει την εκτέλεση μιας σύμβασης προμήθειας αγαθών, ή κατασκευής ή μελέτης έργου, ή παροχής υπηρεσιών, καθορίζει την κατάλληλη διαβάθμιση ασφαλείας που τη χαρακτηρίζει και είναι υπεύθυνη για την παρακολούθηση των λαμβανομένων μέτρων και διαδικασιών ασφαλείας σε όλα τα στάδια της σύμβασης, σύμφωνα με τις οδηγίες των αρμοδίων αρχών ασφαλείας (ΕΑΑ-ΔΑΑ), τις διατάξεις του παρόντος κανονισμού και της κείμενης νομοθεσίας.

2. Οι απαιτήσεις και τα αναγκαία μέτρα για την προστασία και την ασφάλεια των ΕΔΠΥ, όπως προβλέπονται από τις διατάξεις του παρόντος κανονισμού και την κείμενη νομοθεσία, απαιτείται να λαμβάνονται υπόψη πριν από την υπογραφή των συμβάσεων.

3. Κατά την υλοποίηση των συμβάσεων, οι απαιτήσεις και τα αναγκαία μέτρα για την προστασία και την ασφάλεια των ΕΔΠΥ, απαιτείται να συμμορφώνονται με τις διατάξεις του παρόντος κανονισμού και την κείμενη νομοθεσία.

4. Σύμβαση εργολαβίας ή υπεργολαβίας με αντικείμενο την προμήθεια αγαθών, ή την κατασκευή ή μελέτη έργου, ή την παροχή υπηρεσιών στις οποίες περιέχονται ΕΔΠΥ, συνάπτεται:

α. Με οικονομικούς φορείς οι οποίοι έχουν την καταστατική και πραγματική έδρα τους στην Ελλάδα, τηρουμένου του παρόντος κανονισμού με την υποχρεωτική έκδοση ΠΑΕ από την ΕΑΑ.

β. Με οικονομικούς φορείς που έχουν τη φυσική και πραγματική τους έδρα σε κράτος εκτός ΕΕ, το οποίο έχει συνάψει υποχρεωτικά συμφωνία προστασίας διαβαθμισμένων πληροφοριών με την Ελλάδα. Οι εν λόγω οικονομικοί φορείς διαθέτουν ΠΑΕ, καθώς και αντίστοιχου επιπέδου διαπίστευση ΣΕΠ εφόσον απαιτείται η διαχείριση ΕΔΠΥ μέσω ΣΕΠ, από την ΕΑΑ της χώρας που έχουν έδρα.

γ. Με οικονομικούς φορείς που δρουν για λογαριασμό του ΝΑΤΟ, για τους οποίους ισχύουν τα αναγραφόμενα στο ανωτέρω εδάφιο.

δ. Με οικονομικούς φορείς που έχουν τη φυσική και πραγματική τους έδρα σε κράτη-μέλη (κ-μ) της ΕΕ, για τα οποία, σύμφωνα με την κοινοτική οδηγία 2009/81/ΕΚ και τον εφαρμοστικό νόμο ν.3978/2011, οι διαπιστεύσεις ασφαλείας θεωρούνται κατ’ αρχάς ισότιμες με εκείνες που εκδίδονται σύμφωνα με την ελληνική νομοθεσία, με την επιφύλαξη της δυνατότητας του Υπουργείου Εθνικής Άμυνας να διενεργήσει και να λάβει υπόψη του περαιτέρω έρευνες με δική του πρωτοβουλία, εάν θεωρηθεί αναγκαίο. Στο πλαίσιο αυτό η ΕΑΑ δύναται να εξετάζει κατά περίπτωση την απαίτηση ύπαρξης συμφωνίας προστασίας διαβαθμισμένων πληροφοριών κ-μ της ΕΕ με τη Ελλάδα, για λόγους Εθνικής άμυνας και ασφαλείας. Η ύπαρξη ΠΑΕ, καθώς και αντίστοιχου επιπέδου διαπίστευση ΣΕΠ εφόσον απαιτείται η διαχείριση ΕΔΠΥ μέσω ΣΕΠ, είναι υποχρεωτική από την ΕΑΑ της χώρας που έχουν έδρα.

5. Οι διεθνείς ή εθνικοί οικονομικοί φορείς, που υποβάλλουν προσφορές, έχουν εξασφαλίσει ότι το προσωπικό τους που έχει πρόσβαση σε ΕΔΠΥ κατέχει ανάλογη εξουσιοδότηση ασφαλείας.

6. Συνεργασία του προσφέροντα με έτερο οικονομικό φορέα επιτρέπεται μόνο κατόπιν υποβολής αιτήματος, μέσω της αναθέτουσας αρχής, στην ΕΑΑ ή ΔΑΑ και έγκρισης, με την προϋπόθεση οι εγκαταστάσεις και το προσωπικό του οικονομικού φορέα να είναι κατάλληλα εξουσιοδοτημένα σύμφωνα με τον παρόντα Κανονισμό.

7. Στην περίπτωση που κατά το προσυμβατικό στάδιο, παρέχονται ΕΔΠΥ σε οικονομικό φορέα, ο οποίος τελικά δεν υποβάλλει προσφορά ή δεν επιλέγεται, υποχρεούται να επιστρέψει όλες τις ΕΔΠΥ, που έχει λάβει, μετά την κατακύρωση του διαγωνισμού.

8. Οι ανάδοχοι που πρόκειται να αποκτήσουν πρόσβαση ή να χειριστούν ΕΔΠΥ σε οποιοδήποτε στάδιο της σύμβασης εφαρμόζουν τις διαδικασίες του παρόντος Κανονισμού για την προστασία των ΕΔΠΥ.

9. Οι ανάδοχοι δεν δύναται να αναπαράγουν ΕΔΠΥ, παρά μόνον κατόπιν έγκρισης του εκδότη τους.

10. Οι ανάδοχοι έχουν τις παρακάτω υποχρεώσεις:

α. Δημιουργούν τους χώρους ασφαλείας όπου εκτελείται το διαβαθμισμένο έργο και αναρτούν σε αυτούς πίνακα με το εξουσιοδοτημένο προς τούτο προσωπικό, απαγορεύοντας την πρόσβαση σε προσωπικό που δεν είναι κατάλληλα εξουσιοδοτημένο.

β. Λαμβάνουν έγκριση από την ΕΑΑ ή την ΔΑΑ, κατόπιν υποβολής σχετικού αιτήματος μέσω της αναθέτουσας αρχής, προτού αναθέσουν τμήματα διαβαθμισμένης σύμβασης σε υπεργολάβους, ώστε να ελεγχθεί η ύπαρξη διαπιστεύσεων ασφαλείας (ΠΑΕ, Εξουσιοδοτήσεις προσωπικού, ΣΕΠ εφόσον απαιτείται).

γ. Μεριμνούν ώστε όλες οι υπεργολαβικές δραστηριότητες που αναλαμβάνονται είναι σύμφωνες με τις προδιαγραφές του παρόντος Κανονισμού και δεν παρέχουν ΕΔΠΥ σε υπεργολάβο χωρίς προηγούμενη γραπτή συγκατάθεση της ΕΑΑ ή της ΔΑΑ.

δ. Συμμορφώνονται επί παντός θέματος, που αφορά στους κανόνες ασφαλείας του παρόντος Κανονισμού και σε κάθε οδηγία και τροποποίηση που εκδίδεται για την εφαρμογή του.

ε. Αναφέρουν κάθε νομική μεταβολή τους, ιδίως κυριότητα, αλλαγή έδρας, ή άλλη πληροφορία για την κατάστασή τους.

στ. Αναφέρουν αμέσως κάθε παραβίαση ή παράβαση ασφαλείας στην Αναθέτουσα Αρχή, η οποία με τη σειρά της ενημερώνει την ΕΑΑ.

ζ. Κατά κανόνα, οφείλουν να επιστρέψουν στην αναθέτουσα αρχή, άμα τη λύσει της διαβαθμισμένης σύμβασης, τις ΕΔΠΥ που έχουν στην κατοχή τους. Στην περίπτωση που οι ανάδοχοι έχουν δικαίωμα διατήρησης των ΕΔΠΥ μετά τη λύση της σύμβασης, οι διατάξεις ασφαλείας του παρόντος Κανονισμού συνεχίζουν να τηρούνται και το απόρρητο των ΕΔΠΥ προστατεύεται από τους αναδόχους.

η. Εκπαιδεύουν συνεχώς το προσωπικό τους σε θέματα ασφαλείας και το ενημερώνουν για τις ισχύουσες οδηγίες και κανονισμούς ασφαλείας.

θ. Παρέχουν εγκαίρως πληροφορίες στην ΕΑΑ για το προσωπικό που επιθυμούν να απασχολήσουν για την εκτέλεση της σύμβασης, ώστε να προηγηθεί η διαδικασία ελέγχου και εξουσιοδότησής ασφαλείας του.

ι. Συμμορφώνονται με οποιαδήποτε διαδικασία ορίστηκε και αφορά στη σύμβαση.

ΚΕΦΑΛΑΙΟ Δ
ΠΑΡΑΒΑΣΕΙΣ - ΠΑΡΑΒΙΑΣΕΙΣ ΑΣΦΑΛΕΙΑΣ

ΑΡΘΡΟ 11
ΠΑΡΑΒΑΣΕΙΣ - ΠΑΡΑΒΙΑΣΕΙΣ ΑΣΦΑΛΕΙΑΣ

1. Κάθε παρέκκλιση από τις διατάξεις ασφαλείας του Κανονισμού αυτού, που προέρχεται είτε από παράλειψη, είτε από πλημμελή εφαρμογή του από τον οικονομικό φορέα, αποτελεί παράβαση των κανόνων ασφαλείας των ΕΔΠΥ.

2. Κάθε διαρροή, υποκλοπή, απώλεια, καταστροφή ΕΔΠΥ ανεξάρτητα από τους παράγοντες που την προκάλεσαν, αποτελεί παραβίαση ασφαλείας.

3. Όλοι οι οικονομικοί φορείς και οι εργολήπτες καλούνται να αναφέρουν άμεσα στις ΕΑΑ, ΔΑΑ, στην αναθέτουσα αρχή της σύμβασης και στην αρμόδια Εισαγγελική Αρχή κάθε ένδειξη απώλειας ή υποκλοπής ΕΔΠΥ. Οι αναφορές των ως άνω συμβάντων περιλαμβάνουν οπωσδήποτε τις εξής λεπτομέρειες:

α. Γενική περιγραφή των συνθηκών.

β. Τον πιθανό τόπο και χρόνο (ημέρα και ώρα) κατά τον οποία έλαβε χώρα το συμβάν.

γ. Το χρόνο και τα στοιχεία αυτού που ανέφερε και αυτού που διαπίστωσε το συμβάν.

δ. Τη διαβάθμιση ασφαλείας των ΕΔΠΥ που παραβιάστηκαν.

ε. Μια σύντομη περιγραφή του περιεχομένου των ΕΔΠΥ. Ειδικά στην περίπτωση διαρροής εγγράφου αναφέρονται και τα εξής:

(1) Η αρχή έκδοσης.

(2) Το θέμα.

(3) Τα σχετικά.

(4) Η ημερομηνία.

(5) Ο αριθμός αντιτύπων.

(6) Η γλώσσα.

(7) Κάθε συναφής πληροφορία.

στ. Εκτίμηση της πιθανότητας υποκλοπής, όπως «βέβαιη», «δυνατή», «πιθανή», ή «απίθανη».

ζ. Δήλωση για το αν ενημερώθηκε η εκδίδουσα Αρχή ΕΔΠΥ.

ΚΕΦΑΛΑΙΟ Ε
ΕΠΙΣΚΕΨΕΙΣ - ΕΠΙΘΕΩΡΗΣΕΙΣ - ΠΙΣΤΟΠΟΙΗΤΙΚΟ ΑΣΦΑΛΕΙΑΣ ΕΓΚΑΤΑΣΤΑΣΗΣ

ΑΡΘΡΟ 12
ΕΠΙΣΚΕΨΕΙΣ

1. Οι διατάξεις του παρόντος άρθρου αφορούν σε επισκέψεις οικονομικών φορέων, που απαιτείται να πραγματοποιηθούν στο πλαίσιο διαβαθμισμένων συμβάσεων, σε διαβαθμισμένες εγκαταστάσεις:

α. Κρατικών Υπηρεσιών

β. Εθνικών Οργανισμών

γ. Ενόπλων Δυνάμεων

δ. Οικονομικών φορέων

2. Οι οικονομικοί φορείς που πρόκειται να πραγματοποιήσουν την επίσκεψη υποβάλλουν αίτημα στη ΔΑΑ, σύμφωνα με το υπόδειγμα 15, τουλάχιστον είκοσι εργάσιμες ημέρες προ της επίσκεψης. Η ΔΑΑ είτε εγκρίνει την επίσκεψη, εάν πρόκειται για εγκαταστάσεις οικονομικού φορέα, είτε διαβιβάζει το αίτημα στον αρμόδιο φορέα στον οποίο υπάγεται η προς επίσκεψη εγκατάσταση για έγκριση, με παράλληλη ενημέρωση της ΕΑΑ.

3. Για την έγκριση της επίσκεψης, λαμβάνονται υπόψη τα ακόλουθα:

α. Η επίσκεψη σχετίζεται με κάποια διαβαθμισμένη σύμβαση.

β. Οι επισκέπτες διαθέτουν κατάλληλη εξουσιοδότηση ασφαλείας και ανάγκη γνώσης, στο πλαίσιο της σύμβασης, των ΕΔΠΥ στις οποίες πρόκειται να αποκτήσουν πρόσβαση κατά την επίσκεψη.

4. Σε περίπτωση διεθνών επισκέψεων, οι αιτήσεις υποβάλλονται έγκαιρα στη ΔΑΑ, η οποία, μέσω των αρμόδιων διπλωματικών ή προξενικών αρχών, αποστέλλει για έγκριση το αίτημα στις ΕΑΑ/ΔΑΑ των προς επίσκεψη Κρατών. Οι επισκέπτες οφείλουν να συμμορφώνονται με τους κανονισμούς ασφάλειας του φιλοξενούντος Κράτους.

5. Οι φορείς, της ανωτέρω παραγράφου 1, που δέχονται επισκέψεις διασφαλίζουν ότι:

α. Οι επισκέψεις πληρούν τις προϋποθέσεις της παραγράφου 3 του παρόντος άρθρου.

β. Οι επισκέπτες έχουν πρόσβαση μόνο σε ΕΔΠΥ που σχετίζονται με το σκοπό της επίσκεψης.

γ. Τηρούνται αρχεία για όλους τους επισκέπτες (όνομα, οργανισμός, ημερομηνία, ώρα και σκοπός επίσκεψης) για χρονικό διάστημα δύο (2) ετών.

ΑΡΘΡΟ 13
ΕΠΙΘΕΩΡΗΣΕΙΣ ΒΙΟΜΗΧΑΝΙΚΗΣ ΑΣΦΑΛΕΙΑΣ

1. Για την παρακολούθηση και τον έλεγχο τήρησης των διατάξεων ασφαλείας του παρόντος κανονισμού καθώς και για την πρόληψη τυχόν συνεπειών, από πα-

ραλείψεις, ή πλημμελή εφαρμογή των προβλεπόμενων μέτρων ασφαλείας από τους οικονομικούς φορείς που χειρίζονται ΕΔΠΥ, συγκροτείται επιτροπή επιθεωρήσεων βιομηχανικής ασφαλείας, η οποία με μέριμνα της ΔΑΑ, προβαίνει σε τακτικές, ή έκτακτες και απροειδοποίητες επιθεωρήσεις, οι οποίες αποσκοπούν στον περιορισμό των πιθανοτήτων διαρροής, παραβίασης, ή υποκλοπής των ΕΔΠΥ.

2. Η συγκρότηση της επιτροπής επιθεωρήσεων βιομηχανικής ασφαλείας γίνεται με μέριμνα της ΔΑΑ, ως ακολούθως:

α. Πρόεδρος, επιτελής του ΥΠΕΘΑ/ΓΔΑΕΕ.

β. Μέλος, επιτελής του ΥΠΕΘΑ/ΓΔΑΕΕ/ΔΑΕΤΕ/ΤΕΒΣ.

γ. Μέλος, επιτελής του ΓΕΕΘΑ/Ε3 (Βιομηχανική Ασφάλεια).

δ. Μέλος, επιτελής του ΓΕΕΘΑ/Ε3 (Ηλεκτρονική Ασφάλεια).

ε. Μέλος, επιτελής από ΓΕΣ, ΓΕΝ και ΓΕΑ [ένας (1) από κάθε ΓΕ, σύνολο τρεις (3)].

3. Για τη συγκρότηση της επιτροπής επιθεωρήσεων βιομηχανικής ασφαλείας προτείνονται από τους ανωτέρω αρμόδιους φορείς ένα κύριο μέλος και τουλάχιστον ένα αναπληρωματικό ανά φορέα.

4. Η ανωτέρω επιτροπή, μετά από κάθε επιθεώρηση, αποστέλλει στην ΕΑΑ έκθεση επιθεώρησης ασφαλείας εγκαταστάσεων, στην οποία σημειώνονται οι τυχόν παρατηρήσεις και ανάλογα προτείνεται η έκδοση ή μη πιστοποιητικού ασφαλείας εγκαταστάσεων. Η επιθεώρηση που πραγματοποιείται βασίζεται στους ενδείκτες επιθεωρήσεως του παρόντος Κανονισμού (Υπόδειγμα 12).

5. Σε περίπτωση που απαιτείται η πιστοποίηση Συστήματος Επικοινωνιών – Πληροφορικής του οικονομικού φορέα, ισχύουν οι προβλέψεις του δευτέρου μέρους του παρόντος Κανονισμού.

ΑΡΘΡΟ 14
ΑΠΑΙΤΟΥΜΕΝΑ ΓΙΑ ΤΗ ΧΟΡΗΓΗΣΗ ΠΙΣΤΟΠΟΙΗΤΙΚΟΥ ΑΣΦΑΛΕΙΑΣ ΕΓΚΑΤΑΣΤΑΣΗΣ

1. Προκειμένου να ξεκινήσει η διαδικασία εξουσιοδότησης του οικονομικού φορέα, απαιτείται η υποβολή στη ΔΑΑ των κάτωθι:

α. Βεβαίωση καταχωρήσεως του αιτούντος οικονομικού φορέα και των οικονομικών φορέων-μετόχων αυτής στο προβλεπόμενο από την οικεία νομοθεσία εμπορικό μητρώο.

β. ΦΕΚ σύστασης του οικονομικού φορέα (σε περίπτωση Ανώνυμης Εταιρίας-Α.Ε.).

γ. Κύκλος εργασιών και υπηρεσιών του οικονομικού φορέα.

δ. Ενιαίο έντυπο αναγγελίας πρόσληψης και συμπληρωματικός πίνακας πρόσληψης (Ε4).

ε. Πράξη διοικητικού συμβουλίου ή άλλο έγγραφο για τον ορισμό του υπεύθυνου ασφαλείας και του βοηθού ή των βοηθών του.

στ. Τα δικαιολογητικά εξουσιοδότησης του προσωπικού, σύμφωνα με τα περιγραφόμενα στην υποπαράγραφο 7β του άρθρου 7.

ζ. Σύμβαση που έχει υπογράψει ο οικονομικός φορέας με εταιρεία καθαρισμού, σε περίπτωση που ο καθαρισμός των χώρων της δεν γίνεται από δικό της προσωπικό.

η. Σύμβαση που έχει υπογράψει ο οικονομικός φορέας με ΙΕΠΥΑ, σε περίπτωση φύλαξης της βιομηχανικής μονάδας από ΙΕΠΥΑ.

θ. Πιστοποιητικό πυροπροστασίας από την Πυροσβεστική Υπηρεσία.

ι. Κάτοψη των εγκαταστάσεων του οικονομικού φορέα όπου απεικονίζεται το υπαρχείο.

ια. Αντίγραφο του σχεδίου ασφαλείας, συμφώνως προς το Υπόδειγμα του Παραρτήματος «Γ», υπογεγραμμένο από τον υπεύθυνο ασφαλείας και το πρόσωπο που ασκεί τη διοίκηση του οικονομικού φορέα.

ιβ. Άδειες οπλοφορίας (αν υπάρχουν), για λόγους ασφαλείας.

ιγ. Τον πίνακα της παραγράφου 4 του Υποδείγματος 12 του παρόντος συμπληρωμένο και υπογεγραμμένο.

ΑΡΘΡΟ 15
ΧΟΡΗΓΗΣΗ ΠΙΣΤΟΠΟΙΗΤΙΚΟΥ ΑΣΦΑΛΕΙΑΣ ΕΓΚΑΤΑΣΤΑΣΗΣ

1. Οποιοσδήποτε οικονομικός φορέας που πρόκειται να αποκτήσει πρόσβαση σε ΕΔΠΥ απαιτείται να κατέχει πιστοποιητικό ασφαλείας εγκατάστασης (Υπόδειγμα 14), το οποίο σε συνδυασμό με τις εξουσιοδοτήσεις προσωπικού συνιστούν το πιστοποιητικό βιομηχανικής ασφάλειας.

2. Εφόσον έχουν συλλεχθεί όλα τα απαιτούμενα δικαιολογητικά και πληρούνται όλες οι προϋποθέσεις σύμφωνα με το άρθρο 14 παρόντος, ακολουθεί η επιθεώρηση του οικονομικού φορέα για τη χορήγηση του Πιστοποιητικού Ασφάλειας Εγκαταστάσεων, κατά τον οποίο αξιολογούνται τα κάτωθι:

α. Η ακεραιότητα του οικονομικού φορέα.

β. Η κυριότητα, ο έλεγχος, ή η δυνατότητα άσκησης αθέμιτης επιρροής, που δύναται να θεωρηθεί ως κίνδυνος κατά της ασφάλειας.

γ. Η κατάσταση ασφαλείας του προσωπικού, σύμφωνα με το άρθρο 7.

3. Το ΠΑΕ ενός οικονομικού φορέα χορηγείται για συγκεκριμένο χρόνο και λαμβάνοντας υπόψη τη θετική πρόταση της επιτροπής του άρθρου 13 του παρόντος Κανονισμού.

4. Η αρχική έκδοση πιστοποιητικού ασφάλειας εγκαταστάσεων των οικονομικών φορέων χορηγείται ταυτόχρονα με την εξουσιοδότηση ασφάλειας του προσωπικού τους. Για την αρχική έκδοση απαιτείται διάστημα τουλάχιστον έξι μηνών από την υποβολή αίτησης και των δικαιολογητικών του άρθρου 14.

5. Η διάρκεια ισχύος του ΠΑΕ ενός οικονομικού φορέα είναι έως πέντε (5) έτη, ενώ για την ανανέωσή του απαιτείται αίτηση του οικονομικού φορέα τουλάχιστον έξι μήνες πριν τη λήξη του.

6. Κάθε χωριστή εγκατάσταση του οικονομικού φορέα, στην οποία γίνεται χειρισμός ΕΔΠΥ, επιθεωρείται από την επιτροπή βιομηχανικής ασφάλειας και λαμβάνει ξεχωριστό ΠΑΕ.

7. Κατά τη διαδικασία χορήγησης ΠΑΕ ή και μετά από αυτήν, η ΕΑΑ, δύναται να κάνει χρήση οποιουδήποτε νόμιμου μέσου προκειμένου να λαμβάνει γνώση για την κατάσταση ασφαλείας του οικονομικού φορέα, η οποία δύναται να επιφέρει επιπτώσεις στην ισχύ του χορηγηθέντος πιστοποιητικού.

8. Η ΕΑΑ έχει τη δυνατότητα ανάκλησης του ΠΑΕ εφόσον διαπιστωθεί ότι δεν πληρούνται πλέον οι προϋποθέσεις των διατάξεων του παρόντος Κανονισμού, που τηρούνταν κατά την έκδοση του ΠΑΕ. Επιπλέον, για τους ίδιους λόγους η ΔΑΑ δύναται να αιτηθεί από την ΕΑΑ την εξέταση ανάκλησης ΠΑΕ.

9. Οποιαδήποτε αλλαγή των στοιχείων ή των προδιαγραφών ασφαλείας της εγκατάστασης, που ίσχυαν κατά την επιθεώρηση και έκδοση του ΠΑΕ του οικονομικού φορέα, επιφέρει αυτοδίκαια την παύση ισχύος του ΠΑΕ και αποτελεί αιτία επανελέγχου κατόπιν νέας αιτήσεώς του.

10. Σε περίπτωση λήξης ισχύος ή ανάκλησης του ΠΑΕ του οικονομικού φορέα, αυτός πρέπει, με μέριμνα του διευθύνοντος συμβούλου και του υπευθύνου ασφαλείας, να επιστρέψει τα ΕΔΠΥ που έχει στην κατοχή του στους εκδότες/δημιουργούς τους.

ΜΕΡΟΣ ΔΕΥΤΕΡΟ

ΠΡΟΣΤΑΣΙΑ ΕΔΠΥ ΠΟΥ ΤΥΓΧΑΝΟΥΝ ΔΙΑΧΕΙΡΙΣΗΣ ΑΠΟ ΣΥΣΤΗΜΑΤΑ ΕΠΙΚΟΙΝΩΝΙΩΝ – ΠΛΗΡΟΦΟΡΙΚΗΣ

ΚΕΦΑΛΑΙΟ ΣΤ

ΓΕΝΙΚΑ

ΑΡΘΡΟ 16

ΕΙΣΑΓΩΓΗ

1. Στο κεφάλαιο αυτό καθορίζεται η Εθνική Πολιτική Ασφαλείας, δηλαδή τα τεχνικά και διαδικαστικά μέτρα ασφαλείας, τα οποία απαιτείται να εφαρμόζονται από οικονομικούς φορείς σε περιπτώσεις όπου στο πλαίσιο χορήγησης πιστοποιητικού βιομηχανικής ασφαλείας διαθέτουν Συστήματα Επικοινωνών – Πληροφορικής (ΣΕΠ) που πρόκειται να διαχειριστούν ΕΔΠΥ.

2. Επιπλέον, καθορίζονται οι αρμόδιες εθνικές αρχές, οι οποίες είναι υπεύθυνες για την εξασφάλιση της συμμόρφωσης με την Εθνική Πολιτική Ασφαλείας, σε σχέση με τα ΣΕΠ.

3. Σε όλα τα ΣΕΠ στα οποία πρόκειται να γίνεται διαχείριση ΕΔΠΥ, πριν τη λειτουργία τους, υποβάλλονται σε διαδικασία διαπίστευσης, προκειμένου να βεβαιωθεί ότι έχουν εφαρμοστεί όλα τα ενδεδειγμένα μέτρα ασφαλείας και ότι έχει επιτευχθεί, ικανοποιητικό επίπεδο προστασίας τόσο των διαβαθμισμένων πληροφοριών, όσο και των ΣΕΠ. Με την ολοκλήρωση της διαδικασίας διαπίστευσης το ΣΕΠ θεωρείται διαβαθμισμένο και ως εκ τούτου δύναται να διαχειριστεί ΕΔΠΥ ανάλογου βαθμού ασφαλείας. Οι ενέργειες διαπίστευσης ενός ΣΕΠ αναλύονται στο Παράρτημα «Ι», τηρουμένων των μέτρων και διαδικασιών ασφαλείας που περιγράφονται στο Παράρτημα «ΙΓ».

ΑΡΘΡΟ 17

ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ

1. Τα μέτρα ασφαλείας παρέχουν προστασία από τη μη εξουσιοδοτημένη αποκάλυψη πληροφοριών, δηλαδή την απώλεια του εμπιστευτικού τους χαρακτήρα.

2. Για τη δημιουργία ασφαλούς περιβάλλοντος λειτουργίας σε κάθε ΣΕΠ, καθορίζεται και εφαρμόζεται ένα σύνολο μέτρων ασφαλείας, που αφορά στη φυσική ασφάλεια, στην ασφάλεια προσωπικού, στην ασφάλεια επικοινωνιών – πληροφορικής και στην ασφάλεια πληροφοριών.

3. Μέτρα ασφαλείας υπολογιστών, υλικού και λογισμικού, απαιτούνται για την εφαρμογή της αρχής «ανάγκη γνώσης» και για την παρεμπόδιση και εντοπισμό της τυχόν αποκάλυψης πληροφοριών σε μη εξουσιοδοτημένο προσωπικό. Ο βαθμός ασφαλείας των ΣΕΠ, καθορίζεται κατά τη διάρκεια σύνταξης της Δήλωσης Απαιτήσεων Ασφαλείας Συστήματος (ΔΑΠΑΣ). Η διαδικασία διαπίστευσης, εξουσιοδοτεί το σύστημα για χειρισμό πληροφοριών συγκεκριμένου βαθμού ασφαλείας λαμβάνοντας υπόψη τα μέτρα ασφαλείας του περιβάλλοντος λειτουργίας του συστήματος.

ΑΡΘΡΟ 18
ΔΗΛΩΣΗ ΑΠΑΙΤΗΣΕΩΝ ΑΣΦΑΛΕΙΑΣ ΣΥΣΤΗΜΑΤΟΣ (ΔΑΠΑΣ)

1. Για κάθε διαβαθμισμένο ΣΕΠ, δηλαδή με διαβάθμιση «ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ» και άνω, απαιτείται η σύνταξη ΔΑΠΑΣ από την Αρχή Επιχειρησιακής Λειτουργίας (ΑΕΛ) του οικονομικό φορέα, η οποία υποβάλλεται μέσω της ΔΑΑ στην αρμόδια Εθνική Αρχή Διαπίστευσης Ασφαλείας (ΕΑΔΑ) προς έγκριση.

2. Η ΔΑΠΑΣ συντάσσεται για κάθε ΣΕΠ ξεχωριστά, ενώ επικαιροποιείται, κατά την αναβάθμιση – εξέλιξη του συστήματος στα διάφορα στάδια του κύκλου ζωής του.

3. Η ΔΑΠΑΣ αποτελεί την υποχρεωτική συμφωνία μεταξύ της ΑΕΛ του ΣΕΠ και της ΕΑΔΑ, βάσει της οποίας πρόκειται να διαπιστευτεί το ΣΕΠ.

4. Η ΔΑΠΑΣ είναι μια πλήρης και σαφής δήλωση των πολιτικών ασφαλείας που τηρούνται, καθώς και των λεπτομερών απαιτήσεων ασφαλείας. Βασίζεται στην εθνική πολιτική ασφαλείας και σε μια ανάλυση κινδύνων ή επιβάλλεται από παραμέτρους, που καλύπτουν το επιχειρησιακό περιβάλλον, το κατώτατο επίπεδο εξουσιοδότησης προσωπικού, την ανώτατη διαβάθμιση των χειριζόμενων πληροφοριών, τους ασφαλείς τρόπους λειτουργίας ή τα αιτήματα του χρήστη.

5. Οδηγίες για τη σύνταξη μίας ΔΑΠΑΣ, καθορίζονται στο Παράρτημα «ΙΑ».

ΚΕΦΑΛΑΙΟ Ζ
ΟΡΓΑΝΩΣΗ ΑΣΦΑΛΕΙΑΣ

ΑΡΘΡΟ 19
ΕΘΝΙΚΗ ΑΡΧΗ ΑΣΦΑΛΕΙΑΣ

Το ΓΕΕΘΑ, ως Εθνική Αρχή Ασφαλείας (ΕΑΑ), καθορίζει την Εθνική Πολιτική Ασφαλείας διαβαθμισμένων πληροφοριών. Το ΓΕΕΘΑ/Ε' ΚΛΑΔΟΣ/Ε3, χειρίζεται τα θέματα που αφορούν στην ασφάλεια των ΣΕΠ.

ΑΡΘΡΟ 20
ΕΘΝΙΚΗ ΑΡΧΗ ΑΣΦΑΛΕΙΑΣ ΕΠΙΚΟΙΝΩΝΙΩΝ – ΠΛΗΡΟΦΟΡΙΚΗΣ (ΕΑΑΕΠ)

1. Η Εθνική Υπηρεσία Πληροφοριών/ ΔΙ.ΚΥ Διεύθυνση, σύμφωνα με την περ.6 του άρθρου 2 του π.δ. 1/2017 (Α’ 2), το οποίο τροποποιήθηκε με την περ.3 του άρθρου 22 του ν. 4625/2019, και του π.δ. 325/2003 (Α’ 273), είναι η Τεχνικής Φύσεως Αρχή Ασφαλείας Πληροφοριών (INFOSEC). Ως εκ τούτου, στον παρόντα Κανονισμό αναφέρεται ως Εθνική Αρχή Ασφαλείας Επικοινωνιών – Πληροφορικής (ΕΑΑΕΠ), για θέματα TEMPTEST και λογισμικού. Στα πλαίσια αυτά, είναι υπεύθυνη για την αξιολόγηση και πιστοποίηση από πλευράς ασφαλείας του υλικού και λογισμικού των ΣΕΠ. Ανάμεσα στις αρμοδιότητές της είναι η παροχή τεχνικών συμβουλών και τεχνικής επικουρίας στην ΕΑΔΑ, καθώς και η συμμετοχή της στη διαδικασία και στις ομάδες διαπίστευσης ΣΕΠ κατά περίπτωση. Για θέματα ασφαλείας επικοινωνιών – πληροφορικής, που απαιτούν εξειδικευμένη γνώση, απαιτείται η συνεργασία των φορέων, με την Εθνική Υπηρεσία Πληροφοριών.

2. Η Εθνική Υπηρεσία Πληροφοριών (ΕΥΠ) στο πλαίσιο των καθηκόντων της ως Εθνική Αρχή Ασφαλείας Επικοινωνιών – Πληροφορικής ορίζεται και ως Εθνική Αρχή επί θεμάτων TEMPEST με αρμοδιότητες:

α. Τον καθορισμό των μέτρων έναντι των ανεπιθύμητων ηλεκτρομαγνητικών ακτινοβολιών σε συνεργασία με την ΕΑΑ.

β. Την εκτέλεση αντίστοιχων ελέγχων στις εγκαταστάσεις, όπου απαιτείται.

3. Η ΕΥΠ είναι επιπλέον υπεύθυνη για την παραγωγή των εθνικών κλειδών και κωδικών.

ΑΡΘΡΟ 21
ΕΘΝΙΚΗ ΑΡΧΗ ΔΙΑΠΙΣΤΕΥΣΗΣ ΑΣΦΑΛΕΙΑΣ (ΕΑΔΑ)

1. Η ΕΑΔΑ είναι ο Ε' ΚΛΑΔΟΣ του ΓΕΕΘΑ, ο οποίος συγκροτεί επιτροπές διαπίστευσης με συμμετοχή κατά περίπτωση των καταλλήλων εμπλεκομένων φορέων και της ΕΑΑΕΠ ή μεταβιβάζει την αρμοδιότητα για τη διαδικασία αυτή σε κατάλληλους φορείς.

2. Η ΕΑΔΑ, είναι υπεύθυνη για τη χορήγηση έγκρισης λειτουργίας σε ένα ΣΕΠ με ορισμένο επίπεδο διαβάθμισης, συμπεριλαμβανομένων και των ειδικών κατηγοριών διαβάθμισης, στο επιχειρησιακό του περιβάλλον.

3. Η ΕΑΔΑ, έχει την τελική ευθύνη για τη διαπίστευση ασφαλείας ενός ΣΕΠ και τη δικαιοδοσία να επιβάλλει αντίστοιχα πρότυπα ασφαλείας.

4. Η ΕΑΔΑ καθορίζει μια πολιτική ή στρατηγική διαπίστευσης, ως τμήμα της συνολικής πολιτικής της ασφαλείας, που αναφέρει σαφώς τις συνθήκες, υπό τις οποίες καλείται να διαπιστεύσει ένα ΣΕΠ.

5. Η διαδικασία διαπίστευσης ενός ΣΕΠ και οι αρμοδιότητες των εμπλεκόμενων φορέων κατά τα στάδια αυτής, περιγράφονται στο Κεφάλαιο Ι και στο Παράρτημα «Ι».

ΑΡΘΡΟ 22
ΑΡΧΗ ΕΠΙΧΕΙΡΗΣΙΑΚΗΣ ΛΕΙΤΟΥΡΓΙΑΣ (ΑΕΛ)

1. Η ΑΕΛ ενός ΣΕΠ, η οποία είτε ενεργεί ως διαχειριστής συστήματος, είτε ορίζει αυτόν, είναι το άτομο ή το τμήμα του οικονομικού φορέα, που μεταβιβάζεται η ευθύνη για την εκμετάλλευση και τη λειτουργία του ΣΕΠ. Αυτή η ευθύνη υφίσταται σε όλο τον κύκλο ζωής του ΣΕΠ, από το στάδιο σχεδίασης, του καθορισμού των προδιαγραφών, του ελέγχου της εγκατάστασης, της διαπίστευσης, της λειτουργίας, της τροποποίησης, έως το τέλος λειτουργίας του. Κατά τη διάρκεια των διαφόρων φάσεων του κύκλου ζωής του ΣΕΠ, ο ρόλος της ΑΕΛ μπορεί να μεταβιβασθεί από ένα τμήμα σε άλλο εντός του οικονομικού φορέα.

2. Η ΑΕΛ ενός ΣΕΠ αιτείται τη συνεργασία της ΕΑΔΑ και της ΕΑΑΕΠ, καθ' αρμοδιότητα, με σκοπό την εξασφάλιση της εφαρμογής των προβλέψεων ασφαλείας, όταν:

α. Σχεδιάζει την ανάπτυξη ή απόκτηση ενός ΣΕΠ.

β. Εισηγείται αλλαγές στον εξοπλισμό ενός υπάρχοντος ΣΕΠ.

γ. Εισηγείται τη διασύνδεση ενός ΣΕΠ με άλλο ΣΕΠ.

δ. Εισηγείται αλλαγές στον τρόπο ασφαλούς λειτουργίας ενός ΣΕΠ.

ε. Εισηγείται αλλαγές στο υπάρχον λογισμικό ή την αποδοχή νέου λογισμικού, που πιθανόν έχει επίδραση στην ασφάλεια ενός ΣΕΠ.

στ. Εισηγείται την ανάληψη έργου υψηλότερης διαβάθμισης από αυτήν, για την οποία έχει διαπιστευτεί ένα ΣΕΠ.

ζ. Σχεδιάζει, εισηγείται ή αναλαμβάνει οποιαδήποτε άλλη δραστηριότητα που μπορεί να επηρεάσει την ασφάλεια ενός διαπιστευμένου ΣΕΠ, όπως η αύξηση του αριθμού των χρηστών.

3. Η ΑΕΛ, κατευθυνόμενη από την ΕΑΑΕΠ, αποφασίζει για το υλικό και το λογισμικό που πρόκειται να εγκατασταθεί στο ΣΕΠ, ενώ σε συνεργασία με την ΕΑΔΑ, αποφασίζει τα πρότυπα και τις πρακτικές που χρησιμοποιούνται για την ανάπτυξη, την εγκατάσταση και τον έλεγχο του ΣΕΠ. Επιπλέον, η ΑΕΛ είναι υπεύθυνη για την αιτιολόγηση, επιλογή, εφαρμογή και έλεγχο εκείνων των τεχνικών χαρακτηριστικών ασφαλείας, τα οποία έχουν σχεδιαστεί ως τμήμα του συνολικού ΣΕΠ. Τα μέτρα ασφαλείας και η δομή διαχείρισης, για την εφαρμογή και την εποπτεία ασφαλείας σε όλο τον κύκλο ζωής ενός ΣΕΠ, με τον καθορισμό ανάλογων ευθυνών, τίθενται από το στάδιο καθορισμού των αρχικών απαιτήσεων.

4. Το σύνολο των ευθυνών και αρμοδιοτήτων ΑΕΛ, αναγράφεται στο Παράρτημα «ΙΕ».

ΑΡΘΡΟ 23
ΥΠΕΥΘΥΝΟΣ ΑΣΦΑΛΕΙΑΣ ΣΥΣΤΗΜΑΤΟΣ (ΥΑΣ)

1. Ο ΥΑΣ ορίζεται από την ΑΕΛ με τη σύμφωνη γνώμη της ΕΑΔΑ και ευθύνεται για την ανάπτυξη, υλοποίηση και τήρηση των μέτρων ασφαλείας του ΣΕΠ, περιλαμβανομένης της προετοιμασίας των Διαδικασιών Ασφαλούς Λειτουργίας (ΔΑΛ).

2. Επιπλέον, για μεγαλύτερα ΣΕΠ, όπως, είναι δυνατό να ορίζονται επιπλέον άτομα (για παράδειγμα, σε ειδικές περιοχές, Τμήματα ή Διευθύνσεις ενός οικονομικού φορέα), τα οποία εκτελούν τα καθήκοντα αυτά.

3. Το σύνολο των ευθυνών και αρμοδιοτήτων του ΥΑΣ, περιγράφεται στο Παράρτημα «ΙΕ».

ΑΡΘΡΟ 24
ΥΠΕΥΘΥΝΟΣ ΑΣΦΑΛΕΙΑΣ ΔΙΚΤΥΟΥ (ΥΑΔ)

1. Όταν δύο ή περισσότερα ΣΕΠ διασυνδέονται μεταξύ τους ή στην περίπτωση ενός μεγάλου ενιαίου ΣΕΠ, ορίζεται ένας ΥΑΔ για το συντονισμό των μέτρων ασφαλείας δικτύου, ο οποίος συνεργάζεται με τους υπεύθυνους για την ασφάλεια των επικοινωνιών. Στη διασύνδεση συστημάτων διαφορετικών φορέων τα ενδιαφερόμενα μέρη συμφωνούν αμοιβαία για το άτομο που ορίζεται στη θέση του ΥΑΔ.

2. Το σύνολο των ευθυνών και αρμοδιοτήτων του ΥΑΔ, περιγράφεται στο Παράρτημα «ΙΕ».

ΑΡΘΡΟ 25
ΥΠΕΥΘΥΝΟΣ ΑΣΦΑΛΕΙΑΣ ΤΟΠΟΘΕΣΙΑΣ (ΥΑΤ)

1. Ο ΥΑΤ ορίζεται από την ΑΕΛ, ως υπεύθυνος για την εφαρμογή και την τήρηση των μέτρων ασφαλείας, που εφαρμόζονται σε συγκεκριμένη τοποθεσία του οικονομικού φορέα.

2. Η τοποθεσία μπορεί να είναι μία ευρύτερη περιοχή ή σύνολο περιοχών που περιλαμβάνουν πολλούς χώρους ΣΕΠ. Η ευθύνη ασφαλείας για κάθε μία απομακρυσμένη περιοχή τερματικού / χώρου εργασίας καθορίζεται σαφώς. Τα καθήκοντα του ΥΑΤ μπορεί να καλύπτονται από τον υπεύθυνο ασφαλείας του οικονομικού φορέα, ως μέρος των γενικών καθηκόντων του.

3. Το σύνολο των ευθυνών και αρμοδιοτήτων του ΥΑΤ, περιγράφεται στο Παράρτημα «ΙΕ».

ΚΕΦΑΛΑΙΟ Η
ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΣΕΠ

ΑΡΘΡΟ 26
ΑΣΦΑΛΕΙΑ – ΕΚΠΑΙΔΕΥΣΗ ΠΡΟΣΩΠΙΚΟΥ

1. Όλοι οι χρήστες ΣΕΠ [απλοί χρήστες, χρήστες με ειδικά προνόμια, Διαχειριστές Λειτουργίας (ΔΙΑΛ), Υπεύθυνος Ασφαλείας Συστήματος (ΥΑΣ), Υπεύθυνος Ασφαλείας Δικτύου (ΥΑΔ), Υπεύθυνοι Ασφαλείας Τοποθεσίας (ΥΑΤ), προσωπικό που απαρτίζει την ΑΕΛ] είναι εξουσιοδοτημένοι, σύμφωνα με τις προβλέψεις του παρόντος Κανονισμού, για χειρισμό διαβαθμισμένων πληροφοριών αντίστοιχου βαθμού ασφαλείας με αυτόν του ΣΕΠ, ενώ ευθύνονται για την ασφάλεια του ΣΕΠ που χρησιμοποιούν, τελώντας υπό την εποπτεία του ΥΑΣ και του ΥΑΤ. Η αποτελεσματικότητα της ασφάλειας μπορεί να επιτευχθεί μόνο όταν όλοι οι χρήστες είναι ενημερωμένοι, έχουν πλήρη γνώση των καθηκόντων τους και ενεργούν για την ασφάλεια του ΣΕΠ που χρησιμοποιούν.

2. Η εκπαίδευση ασφαλείας είναι αναγκαίο να πραγματοποιείται σε διάφορα επίπεδα, ανάλογα με τα καθήκοντα του προσωπικού (προσωπικό ανάπτυξης ΣΕΠ, προσωπικό Αρχής ασφαλείας, υπεύθυνοι ασφαλείας ΣΕΠ και χρήστες). Η εκπαίδευση είναι συνεχής, ώστε να διασφαλίζεται η ενημέρωση του προσωπικού, επί των νέων απειλών και κινδύνων που προκύπτουν από τις τεχνολογικές εξελίξεις.

3. Τα ΣΕΠ σχεδιάζονται ώστε, να διευκολύνεται η ανάθεση καθηκόντων και ευθυνών στο προσωπικό και να εφαρμόζεται η αρχή των «δύο ατόμων». Η ΔΑΠΑΣ πρέπει σαφώς να δηλώνει τις καταστάσεις εκείνες στις οποίες εφαρμόζεται η αρχή των «δύο ατόμων».

ΑΡΘΡΟ 27
ΦΥΣΙΚΗ ΑΣΦΑΛΕΙΑ

1. Οι χώροι ΣΕΠ και οι απομακρυσμένοι χώροι τερματικών / σταθμών εργασίας στους οποίους χειρίζονται διαβαθμισμένες πληροφορίες ή όπου είναι δυνατή η πρόσβαση σε τέτοιες πληροφορίες, ορίζονται ως ελεγχόμενοι χώροι.

2. Τα μέτρα φυσικής ασφαλείας που λαμβάνονται για την προστασία αυτών των χώρων, είναι τα παρακάτω:

α. Επιλογή κατάλληλων χώρων για την ομαλή και ανεμπόδιστη λειτουργία των μηχανημάτων και συσκευών που εγκαθίστανται.

β. Επιτήρηση των χώρων καθ' όλο το 24ωρο.

γ. Αποφυγή σήμανσης για υποδήλωση, κατά περίπτωση, της ταυτότητας διαφόρων κέντρων ή σταθμών.

δ. Προστασία θυρών και παραθύρων με μεταλλικά κιγκλιδώματα.

ε. Απαγόρευση της εισόδου στους προαναφερόμενους χώρους, αναρμόδιων και μη εξουσιοδοτημένων προσώπων.

στ. Ελεγχόμενη είσοδος και έξοδος ατόμων και υλικού.

ζ. Εφοδιασμός του εργαζόμενου προσωπικού με ειδική κάρτα ή ταυτότητα ή ηλεκτρονικό κλειδί για την είσοδό του, στους προαναφερόμενους χώρους.

η. Στελέχωση των υπόψη χώρων από τουλάχιστον δύο εξουσιοδοτημένα άτομα, εφαρμόζοντας την αρχή των «δύο ατόμων».

θ. Έγκριση εσόδου, από τον υπεύθυνο ασφαλείας χώρου, στα άτομα που αιτούνται προσωρινή ή επανειλημμένη πρόσβαση στους χώρους αυτούς ως επισκέπτες. Οι επισκέπτες εποπτεύονται συνεχώς, ώστε να απαγορεύεται η μη εξουσιοδοτημένη πρόσβαση σε διαβαθμισμένες πληροφορίες.

ι. Ελεγχόμενη είσοδος ιδιόκτητου ηλεκτρονικού εξοπλισμού, όπως ραδιόφωνα, κινητά τηλέφωνα και Η/Υ, εντός των διαβαθμισμένων χώρων.

3. Με βάση τον κίνδυνο κατά της ασφάλειας και ανάλογα με τη διαβάθμιση των πληροφοριών που υφίστανται επεξεργασία, μπορεί να υπάρξει απαίτηση εφαρμογής της αρχής «δύο ατόμων» ακόμα και σε χώρους διαφορετικούς από τους χώρους του ΣΕΠ, εάν αυτοί μπορούν να επηρεάσουν την ασφαλή λειτουργία αυτού. Οι χώροι αυτοί, καθορίζονται κατά τη διάρκεια του σταδίου σχεδίασης του έργου και προσδιορίζονται στη ΔΑΠΑΣ.

4. Όταν ένα ΣΕΠ πρόκειται να διαχωριστεί από κάποιο άλλο ΣΕΠ στο οποίο ανήκε αρχικά, τότε, λαμβανομένου υπόψη του φυσικού περιβάλλοντος, άλλων διαδικαστικών ή τεχνικών μέτρων ασφαλείας, της αρχιτεκτονικής υλικού και του ρόλου του, είναι δυνατό να απαιτείται τροποποίηση στους κανόνες ασφαλείας. Σε τέτοιες περιπτώσεις, η ΕΑΔΑ ορίζει κατάλληλους κανόνες για τη σύνθεση του ΣΕΠ, το επίπεδο των διαβαθμισμένων πληροφοριών που επεξεργάζονται και τα ειδικά χαρακτηριστικά που αναγνωρίζονται στο νέο ανεξάρτητο ΣΕΠ.

ΑΡΘΡΟ 28
ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΩΝ

1. Η πρωτοκόλληση, η διακίνηση και ο χειρισμός των έγγραφων που λαμβάνονται από ένα ΣΕΠ και φέρουν διαβαθμισμένες πληροφορίες, γίνονται σύμφωνα με τις διατάξεις του παρόντα Κανονισμού.

2. Όταν οι πληροφορίες διακινούνται από ένα ΣΕΠ σε άλλο, προστατεύονται τόσο κατά τη διάρκεια της μεταφοράς, όσο και στο ΣΕΠ που τις δέχεται, κατά τρόπο ανάλογο με την αρχική διαβάθμιση και κατηγορία διαβάθμισης των πληροφοριών. Ως συνέπεια του προαναφερόμενου επισημαίνεται ότι, το ΣΕΠ που δέχεται την διαβαθμισμένη πληροφορία είναι απαραίτητο να διαθέτει διαπίστευση εν ισχύ, τουλάχιστον ίδιου ή μεγαλύτερου βαθμού, με την πληροφορία που πρόκειται να δεχθεί.

3. Όλα τα μέσα αποθήκευσης πληροφοριών φυλάσσονται με τρόπο που αρμόζει, είτε στην υψηλότερη διαβάθμιση των αποθηκευμένων πληροφοριών, είτε στο επίπεδο διαβάθμισης κάθε μέσου.

4. Τα επαναχρησιμοποιούμενα αποθηκευτικά μέσα που χρησιμοποιούνται για την καταχώριση διαβαθμισμένων πληροφοριών, διατηρούν την υψηλότερη διαβάθμιση για την οποία χρησιμοποιήθηκαν στο παρελθόν, μέχρις ότου οι πληροφορίες υποβαθμιστούν ή λάβουν νέα διαβάθμιση ή αποχαρακτηριστούν ή καταστραφούν σύμφωνα με προβλεπόμενες διαδικασίες, ως Παράρτημα «Θ».

ΑΡΘΡΟ 29
ΕΛΕΓΧΟΣ ΚΑΙ ΚΑΤΑΓΡΑΦΗ ΤΩΝ ΕΝΕΡΓΕΙΩΝ

1. Η αυτόματη ή χειρόγραφη καταγραφή ενεργειών διατηρείται, ως ημερολόγιο πρόσβασης σε πληροφορίες με διαβάθμιση «ΑΠΟΡΡΗΤΟ» και άνω.

2. Η ελάχιστη χρονική περίοδος διατήρησης πληροφοριών διαβάθμισης «ΑΠΟΡΡΗΤΟ» και άνω ή ειδικής κατηγορίας ορίζεται στα δέκα (10) έτη, ενώ για πληροφορίες με διαβάθμιση «ΕΜΠΙΣΤΕΥΤΙΚΟ» και κάτω, η ελάχιστη χρονική περίοδος διατήρησης ορίζεται στα πέντε (5) έτη.

3. Τα ημερολόγια πρόσβασης σε οποιαδήποτε μορφή, ηλεκτρονική ή έντυπη, που φυλάσσονται στον χώρο ΣΕΠ:

α. Δύναται να τα χειρίζεται κάποιος ως μία διαβαθμισμένη ενότητα, υπό την προϋπόθεση ότι το υλικό αναγνωρίζεται, σημειώνεται με τη διαβάθμισή του και ελέγχεται μέσα στον χώρο ΣΕΠ, μέχρις ότου καταστραφεί ή αρχειοθετηθεί.

β. Διατηρούνται μέσα στο χώρο ΣΕΠ, μέχρις ότου το υλικό τεθεί υπό επίσημο έλεγχο εγγράφων ή καταστραφεί.

4. Όταν το ημερολόγιο πρόσβασης διαβιβάζεται σε έναν απομακρυσμένο χώρο τερματικών / σταθμών εργασίας από ένα χώρο ΣΕΠ, καθιερώνονται κατάλληλες διαδικασίες για τον έλεγχο αυτού, εγκεκριμένες από την ΕΑΔΑ. Για διαβάθμιση «ΑΠΟΡΡΗΤΟ» και άνω, οι διαδικασίες αυτές περιλαμβάνουν ειδικές οδηγίες για τον έλεγχο των πληροφοριών.

ΑΡΘΡΟ 30
ΧΕΙΡΙΣΜΟΣ ΚΑΙ ΕΛΕΓΧΟΣ
ΜΕΤΑΚΙΝΟΥΜΕΝΩΝ ΜΕΣΩΝ ΗΛΕΚΤΡΟΝΙΚΗΣ ΑΠΟΘΗΚΕΥΣΗΣ

1. Όλα τα μέσα αποθήκευσης των ΣΕΠ που είναι δυνατό να αφαιρεθούν, όπως σκληρός δίσκος, οπτικός δίσκος, μαγνητική ταινία, και στα οποία πρόκειται να αποθηκευτούν ΕΔΠΥ, αναγνωρίζονται, σημαίνονται κατάλληλα και ελέγχονται. Τα μέτρα και οι διαδικασίες ασφαλείας που τηρούνται και ελέγχονται κατά τη διαπίστευση του ΣΕΠ, ανά κατηγορία διαβάθμισης περιγράφονται στο Παράρτημα «ΙΓ».

2. Για ΣΕΠ που χειρίζονται πληροφορίες με διαβάθμιση «ΑΠΟΡΡΗΤΟ» και άνω, ισχύουν τα εξής:

α. Μετά το πέρας της εγκατάστασης του συστήματος από εξουσιοδοτημένο προσωπικό, αφαιρούνται υποχρεωτικά όλοι οι οδηγοί δισκετών, οπτικών δίσκων και λοιπών εξωτερικών μέσων αποθήκευσης, εξαιρουμένων αυτών που προβλέπονται από τη ΔΑΠΑΣ.

β. Η εισαγωγή δεδομένων ή λογισμικού στο σύστημα γίνεται από κεντρικό σημείο, με τυποποιημένες διαδικασίες, από ειδικά εξουσιοδοτημένο προσωπικό, όπως ορίζεται από τη ΔΑΠΑΣ.

γ. Η παραγωγή έντυπων προϊόντων, ελέγχεται επίσης κεντρικά, τα δε προϊόντα διακινούνται με τις διαδικασίες που προβλέπονται για τα έγγραφα αντιστοίχου βαθμού ασφαλείας.

δ. Οι θύρες επικοινωνίας των μερών του συστήματος που δεν απαιτούνται για τη λειτουργία του, καθώς και οι ρυθμίσεις προσθήκης συσκευών απενερ-

γοποιούνται από λογισμικό που προστατεύεται με μέτρα ασφαλείας αναλόγου επιπέδου.

ε. Λαμβάνονται ειδικά μέτρα προστασίας μη εξουσιοδοτημένης επέμβασης στο εσωτερικό των συσκευών, τα οποία καθορίζονται από τη ΔΑΠΑΣ.

στ. Διενεργούνται τακτικοί και έκτακτοι έλεγχοι για την τήρηση των παραπάνω, από τις αρμόδιες Αρχές Ασφαλείας.

ζ. Για το χειρισμό πληροφοριών «ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ» και άνω, χρησιμοποιείται αποκλειστικά μεμονωμένος Η/Υ, με διατάξεις ασφαλείας που περιγράφονται στο άρθρο 42.

ΑΡΘΡΟ 31
ΥΠΟΒΑΘΜΙΣΗ – ΑΠΟΧΑΡΑΚΤΗΡΙΣΜΟΣ ΜΕΣΩΝ ΑΠΟΘΗΚΕΥΣΗΣ

1. Τα μέσα αποθήκευσης που περιέχουν πληροφορίες με διαβάθμιση «ΑΠΟΡΡΗΤΟ» και άνω ή ειδικής κατηγορίας, δεν δύναται να υποβαθμιστούν.

2. Οι πληροφορίες με διαβάθμιση μέχρι «ΕΜΠΙΣΤΕΥΤΙΚΟ», που εγγράφονται σε ηλεκτρομαγνητικά, οπτικά ή άλλα επαναχρησιμοποιούμενα μέσα αποθήκευσης, διαγράφονται μόνο σύμφωνα με τις εγκεκριμένες διαδικασίες καθαρισμού και εξυγίανσης μέσων, ως Παράρτημα «Θ».

3. Τα μέσα αποθήκευσης όταν φθάσουν στο τέλος της ζωής τους, δηλαδή όταν παύσουν να λειτουργούν:

α. Καταστρέφονται, σύμφωνα με εγκεκριμένη διαδικασία στην περίπτωση που έχουν πληροφορίες με διαβάθμιση «ΑΠΟΡΡΗΤΟ» και άνω ή ειδικής κατηγορίας.

β. Αποχαρακτηρίζονται / εξυγιαίνονται, σύμφωνα με εγκεκριμένη διαδικασία για διαβάθμιση μέχρι «ΕΜΠΙΣΤΕΥΤΙΚΟ», οπότε μπορεί να αντιμετωπισθεί ως «ΑΔΙΑΒΑΘΜΗΤΟ». Αν το μέσο δεν μπορεί να αποχαρακτηριστεί / εξυγιανθεί για τεχνικούς ή άλλους λόγους, τότε καταστρέφεται, σύμφωνα με εγκεκριμένη διαδικασία.

4. Διαδικασίες αποχαρακτηρισμού και εξυγίανσης μέσων αποθήκευσης, ως Παράρτημα «Θ».

ΑΡΘΡΟ 32
ΕΓΚΑΤΑΣΤΑΣΗ ΚΑΙ ΑΣΦΑΛΕΙΑ ΑΚΤΙΝΟΒΟΛΙΩΝ

1. Η αρχική εγκατάσταση ΣΕΠ και οποιαδήποτε σημαντική αλλαγή σε αυτά, γίνεται από εξειδικευμένο τεχνικό προσωπικό που είναι εξουσιοδοτημένο για πρόσβαση σε διαβαθμισμένες πληροφορίες, σε επίπεδο ισοδύναμο με την υψηλότερη διαβάθμιση των πληροφοριών που χειρίζεται το ΣΕΠ, υπό τη μόνιμη εποπτεία προσωπικού ασφαλείας, το οποίο να διαθέτει επαρκείς τεχνικές γνώσεις για να ελέγχει τη διαδικασία.

2. Όλος ο εξοπλισμός εγκαθίσταται σύμφωνα με την τρέχουσα πολιτική και πρότυπα, ως Παράρτημα «Η».

3. Τα ΣΕΠ που χειρίζονται πληροφορίες με διαβάθμιση «ΕΜΠΙΣΤΕΥΤΙΚΟ»

και άνω, προστατεύονται κατάλληλα από τρωτότητες που οφείλονται στις διαφεύγουσες ακτινοβολίες, η μελέτη και ο έλεγχος των οποίων αναφέρονται ως «TEMPEST».

ΑΡΘΡΟ 33
ΔΙΑΔΙΚΑΣΙΕΣ ΑΣΦΑΛΟΥΣ ΛΕΙΤΟΥΡΓΙΑΣ (ΔΑΛ)

1. Οι ΔΑΛ [Security Operations Procedures (SecOPs)], είναι μία περιγραφή της εφαρμογής της πολιτικής ασφαλείας που υιοθετείται, των λειτουργικών διαδικασιών που ακολουθούνται και των ευθυνών του προσωπικού.

2. Οι ΔΑΛ προετοιμάζονται από την ΑΕΛ του ΣΕΠ, σε συντονισμό με την ΕΑΔΑ και τα λοιπά όργανα ασφαλείας. Η ΕΑΔΑ εγκρίνει τις ΔΑΛ, προτού εξουσιοδοτήσει την αποθήκευση, επεξεργασία ή τη διαβίβαση διαβαθμισμένων πληροφοριών.

3. Οδηγίες για τη σύνταξη των ΔΑΛ, καθορίζονται στο Παράρτημα «ΙΒ».

ΚΕΦΑΛΑΙΟ Θ
ΣΥΝΤΗΡΗΣΗ – ΠΡΟΜΗΘΕΙΑ – ΔΙΑΠΙΣΤΕΥΣΗ – ΑΞΙΟΛΟΓΗΣΗ ΚΑΙ ΠΙΣΤΟΠΟΙΗΣΗ ΣΕΠ

ΑΡΘΡΟ 34
ΣΥΝΤΗΡΗΣΗ

1. Οι συμβάσεις και οι διαδικασίες για την προγραμματισμένη και κατόπιν κλήσεως συντήρηση ΣΕΠ, που χειρίζονται διαβαθμισμένες πληροφορίες, ορίζουν ακριβώς τις απαιτήσεις και διαδικασίες για το προσωπικό συντήρησης που εισέρχεται σε έναν χώρο ΣΕΠ.

2. Οι απαιτήσεις ορίζονται σαφώς στη ΔΑΠΑΣ και οι διαδικασίες στις ΔΑΛ. Η συντήρηση βάσει συμβάσεως, που απαιτεί διαγνωστικές διαδικασίες μέσω απομακρυσμένης πρόσβασης, επιτρέπεται μόνο σε εξαιρετικές συνθήκες, υπό αυστηρό έλεγχο ασφαλείας και μόνο με την έγκριση της ΕΑΔΑ.

ΑΡΘΡΟ 35
ΠΡΟΜΗΘΕΙΑ ΥΛΙΚΟΥ – ΛΟΓΙΣΜΙΚΟΥ ΣΕΠ

1. Η προμήθεια υλικού και λογισμικού ενός διαβαθμισμένου ΣΕΠ, περιορίζεται όσο είναι δυνατό, σε εκείνα που έχουν σχεδιαστεί, κατασκευαστεί ή πιστοποιηθεί, σύμφωνα με εθνικώς αποδεκτά πρότυπα, στην Ελλάδα ή σε χώρα με την οποία υπάρχει συμφωνία προστασίας και ανταλλαγής διαβαθμισμένων πληροφοριών (συμφωνία ασφαλείας). Προμήθεια υλικού και λογισμικού, που αναπτύσσεται, κατασκευάζεται ή πιστοποιείται σε άλλες χώρες, πραγματοποιείται μόνο κατόπιν εγκρίσεως της ΕΑΔΑ και της ΕΑΑΕΠ, καθ' αρμοδιότητα.

2. Για τα ΣΕΠ που χειρίζονται πληροφορίες με διαβάθμιση «ΑΠΟΡΡΗΤΟ» και άνω, καθώς και πληροφορίες ειδικής κατηγορίας, το υλικό, το λογισμικό και τα βασικά προϊόντα ασφαλείας υπολογιστών, όπως προϊόντα λειτουργικών συστημάτων γενικού σκοπού, προϊόντα ασφαλείας περιορισμένης λειτουργικότητας και προϊόντα δικτύου, είτε έχει αξιολογηθεί και πιστοποιηθεί είτε είναι υπό αξιολόγηση και πιστοποίηση, σύμφωνα με Εθνικά, ΝΑΤΟ ή άλλα εγκεκριμένα κριτήρια, από τον φορέα αξιολόγησης ή πιστοποίησης (ΕΑΑΕΠ).

3. Για τα ΣΕΠ, που χειρίζονται πληροφορίες με διαβάθμιση «ΕΜΠΙΣΤΕΥΤΙΚΟ», γίνεται ουσιώδης εξέταση σύμφωνα με τις ανωτέρω προδιαγραφές.

ΑΡΘΡΟ 36
ΔΙΑΠΙΣΤΕΥΣΗ

1. Όλα τα ΣΕΠ, πριν την έναρξη αποθήκευσης, επεξεργασίας ή διαβίβασης διαβαθμισμένων πληροφοριών, διαπιστεύονται με βάση πληροφορίες που αναφέρονται στη ΔΑΠΑΣ, τις ΔΑΛ και οποιαδήποτε άλλα σχετικά έγγραφα, από την ΕΑΔΑ. Τα υποσυστήματα και τα απομακρυσμένα τερματικά / σταθμοί εργασίας διαπιστεύονται ως τμήμα όλων των ΣΕΠ, με τα οποία συνδέονται.

2. Όταν ένα ΣΕΠ χρησιμοποιείται εκτός της διαχείρισης ΕΔΠΥ και για την διαχείριση διαβαθμισμένης πληροφορίας και άλλων Διεθνών Οργανισμών, όπως

ΝΑΤΟ/ΕΕ, η ΕΑΔΑ και οι Διεθνείς Οργανισμοί συμφωνούν αμοιβαία για τη διαπίστευση. Για την κρυπτογράφηση, οι κλείδες που πρόκειται να χρησιμοποιηθούν συμφωνούνται κατά τη διαπίστευση. Όπου πρόκειται να χρησιμοποιηθούν εθνικές κλείδες παράγονται από την ΕΥΠ.

ΑΡΘΡΟ 37
ΑΞΙΟΛΟΓΗΣΗ ΚΑΙ ΠΙΣΤΟΠΟΙΗΣΗ

1. Πριν από τη διαπίστευση, σε ορισμένες περιπτώσεις ο τρόπος λειτουργίας ασφαλείας «πολλαπλού επιπέδου» απαιτεί τα χαρακτηριστικά ασφαλείας του υλικού και λογισμικού ενός ΣΕΠ, να έχουν αξιολογηθεί και πιστοποιηθεί με βάση τα κριτήρια που έχουν καθορισθεί από την ΕΑΑΕΠ. Τα κριτήρια αυτά, είναι ικανά να διασφαλίσουν τις πληροφορίες μικτής διαβάθμισης και να εξασφαλίζουν ελεγχόμενη πρόσβαση με βάση την εξουσιοδότηση των χρηστών.

2. Οι απαιτήσεις για την αξιολόγηση και πιστοποίηση, περιλαμβάνονται στο σχεδιασμό συστημάτων και δηλώνονται σαφώς στη ΔΑΠΑΣ, αμέσως μόλις καθοριστεί ο τρόπος ασφαλούς λειτουργίας (άρθρο 2, παράγραφος 28).

3. Οι περιπτώσεις, στις οποίες απαιτείται αξιολόγηση και πιστοποίηση, στα πλαίσια του τρόπου λειτουργίας ασφαλείας «πολλαπλού επιπέδου», είναι οι ακόλουθες:

α. ΣΕΠ που αποθηκεύουν, επεξεργάζονται ή διαβιβάζουν πληροφορίες με διαβάθμιση «ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ» ή πληροφορίες ειδικής κατηγορίας.

β. ΣΕΠ που αποθηκεύουν, επεξεργάζονται ή διαβιβάζουν πληροφορίες με διαβάθμιση «ΑΠΟΡΡΗΤΟ», όπου:

(1) Το ΣΕΠ διασυνδέεται με άλλο ΣΕΠ, για παράδειγμα υπό άλλη ΑΕΛ.

(2) Το ΣΕΠ έχει αριθμό χρηστών που δεν μπορεί να καθοριστεί επακριβώς, για παράδειγμα όπου συνδέεται άμεσα ή έμμεσα με δημόσιο δίκτυο.

4. Η αξιολόγηση και η πιστοποίηση διεξάγονται σύμφωνα με τις εγκεκριμένες κατευθυντήριες γραμμές και από ανεξάρτητες και αμερόληπτες επιτροπές τεχνικώς ειδικευμένου και κατάλληλα εξουσιοδοτημένου προσωπικού, οι οποίες συγκροτούνται από την ΕΑΑΕΠ.

5. Το ανωτέρω προσωπικό για τις επιτροπές αξιολόγησης παρέχουν η ΕΥΠ και οι φορείς επ' ωφελεία των οποίων λειτουργούν τα συστήματα. Ειδικότερα, οι αξιολογήσεις των κρυπτοσυστημάτων διεξάγονται αποκλειστικά από την ΕΥΠ.

6. Οι διαδικασίες αξιολόγησης και πιστοποίησης καθορίζουν την έκταση, στην οποία ο σχεδιασμός και η εφαρμογή ενός συγκεκριμένου ΣΕΠ ανταποκρίνονται σε καθορισμένες απαιτήσεις ασφαλείας, όπως δηλώνεται στη ΔΑΠΑΣ. Οι διαδικασίες αξιολόγησης και πιστοποίησης απαιτείται να αρχίζουν στο στάδιο προσδιορισμού του ΣΕΠ, να συνεχίζουν στο στάδιο υλοποίησης και να ολοκληρώνονται πριν την επιχειρησιακή λειτουργία του συστήματος.

7. Ο βαθμός των απαιτούμενων διαδικασιών αξιολόγησης και πιστοποίησης είναι δυνατό να ελαττωθεί, όταν τα ΣΕΠ βασίζονται σε υπάρχοντα προϊόντα ασφαλείας υπολογιστών, που έχουν αξιολογηθεί και πιστοποιηθεί σε εθνικό επίπεδο.

ΑΡΘΡΟ 38
ΑΝΑΝΕΩΣΗ ΤΗΣ ΔΙΑΠΙΣΤΕΥΣΗΣ

1. Για όλα τα ΣΕΠ, που αποθηκεύουν, επεξεργάζονται ή διαβιβάζουν διαβαθμισμένες πληροφορίες, η ΑΕΛ ενός ΣΕΠ καθορίζει τις διαδικασίες ελέγχου, οι οποίες εξασφαλίζουν ότι όλες οι αλλαγές του ΣΕΠ επανεξετάζονται ως προς τις συνέπειες που έχουν για την ασφάλειά του.

2. Οι αλλαγές, που αποτελούν αιτία για επαναδιαπίστευση ή που απαιτούν πρότερη έγκριση της ΕΑΔΑ, ορίζονται σαφώς στη ΔΑΠΑΣ. Μετά από οποιαδήποτε τροποποίηση, επισκευή ή διακοπή λειτουργίας, που μπορεί να επηρεάσει τα χαρακτηριστικά ασφαλείας του ΣΕΠ, η ΑΕΛ του συστήματος διενεργεί έλεγχο, ώστε να βεβαιωθεί η σωστή λειτουργία των χαρακτηριστικών ασφαλείας.

3. Όλα τα ΣΕΠ, που χειρίζονται διαβαθμισμένες πληροφορίες, επιθεωρούνται περιοδικά από την ΕΑΔΑ και από το φορέα στον οποίο ανήκει το ΣΕΠ. Ειδικότερα, τα ΣΕΠ που αποθηκεύουν, επεξεργάζονται ή διαβιβάζουν πληροφορίες «ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ» ή ειδικής κατηγορίας, επιθεωρούνται τουλάχιστον μία φορά κατ' έτος.

ΑΡΘΡΟ 39
ΑΣΦΑΛΕΙΑ ΦΟΡΗΤΩΝ ΥΠΟΛΟΓΙΣΤΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ (ΦΥΣ)

1. Στα ΦΥΣ παρέχεται προστασία όσον αφορά στην πρόσβαση, χειρισμό, αποθήκευση και μεταφορά, ανάλογη με το ανώτατο επίπεδο διαβάθμισης πληροφοριών που αποθηκεύτηκαν στο παρελθόν ή υπέστησαν επεξεργασία (μέχρις ότου υποβαθμιστούν ή αποχαρακτηριστούν σύμφωνα με τις εγκεκριμένες διαδικασίες).

2. Τα ΦΥΣ που λειτουργούν, είτε ανεξάρτητα, είτε σε δίκτυο, λογίζονται ως μέσα αποθήκευσης πληροφοριών με την ίδια έννοια όπως τα φορητά μέσα αποθήκευσης, και λαμβάνονται τα μέτρα και οι διαδικασίες ασφαλείας του Παραρτήματος «Ι».

ΑΡΘΡΟ 40
ΧΡΗΣΗ ΕΞΟΠΛΙΣΜΟΥ ΣΕΠ

1. Απαγορεύεται η χρήση Η/Υ, ΦΥΣ, μέσων αποθήκευσης, και υλικού – λογισμικού, για την αποθήκευση, επεξεργασία και διαβίβαση διαβαθμισμένων πληροφοριών που δεν έχουν προβλεφθεί και περιγραφή πλήρως κατά την διαδικασία της διαπίστευσης αυτού.

2. Απαγορεύεται να προσκομίζεται επιπλέον υλικό, λογισμικό και άλλα μέσα που είναι δυνατό να συνεργαστούν, να επηρεάσουν ή να θέσουν σε κίνδυνο την ασφαλή λειτουργία του ΣΕΠ, σε ελεγχόμενο χώρο στον οποίον αποθηκεύονται, υφίστανται επεξεργασία ή διαβιβάζονται ΕΔΠΥ. Εξαίρεση αποτελούν οι τυχόν προβλεπόμενες περιπτώσεις από τη ΔΑΠΑΣ του ΣΕΠ.

ΑΡΘΡΟ 41
ΧΡΗΣΗ ΕΞΟΠΛΙΣΜΟΥ ΣΕΠ ΤΡΙΤΩΝ ΓΙΑ ΑΝΑΓΚΕΣ ΕΡΓΟΥ

Η χρήση εξοπλισμού ΣΕΠ και λογισμικού που ανήκει σε προμηθευτές, για τη στήριξη του έργου του οικονομικού φορέα, δύναται να επιτραπεί από τον υπεύθυνο ασφαλείας του ΣΕΠ. Η χρήση του εξοπλισμού αυτού, υπόκειται σε διαδικασίες που προβλέπονται στη ΔΑΠΑΣ. Η χρήση εξοπλισμού ΣΕΠ, από υπαλλήλους σε άλλο οικονομικό φορέα δύναται επίσης να επιτραπεί με τον ίδιο τρόπο. Στην περίπτωση αυτή, ο εξοπλισμός ΣΕΠ τίθεται υπό τον έλεγχο του αρμοδίου οργάνου. Σε κάθε περίπτωση, εάν ο εξοπλισμός ΣΕΠ πρόκειται να χρησιμοποιηθεί για την αποθήκευση, επεξεργασία και διαβίβαση διαβαθμισμένων πληροφοριών, τότε ζητείται η έγκριση της αρμόδιας Επιτροπής Διαπίστευσης Ασφαλείας (ΕΔΑ).

ΚΕΦΑΛΑΙΟ Ι
ΔΙΑΔΙΚΑΣΙΑ ΔΙΑΠΙΣΤΕΥΣΗΣ
ΣΥΣΤΗΜΑΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ – ΠΛΗΡΟΦΟΡΙΚΗΣ (ΣΕΠ)

ΑΡΘΡΟ 42
ΓΕΝΙΚΗ ΠΕΡΙΓΡΑΦΗ

1. Η διαδικασία της διαπίστευσης έχει σκοπό τη δημιουργία ασφαλούς περιβάλλοντος για όλα τα ΣΕΠ, που χειρίζονται διαβαθμισμένες πληροφορίες, όπως αυτές χαρακτηρίζονται και κατατάσσονται στον παρόντα Κανονισμό. Έτσι, έχει εφαρμογή σε όλα τα είδη ΣΕΠ, από τους μεμονωμένους υπολογιστές (stand alone), τοπικά (LAN) και ευρεία δίκτυα (WAN) Η/Υ, μέχρι εκτεταμένα ΣΕΠ, συμπεριλαμβανομένων όλων των ΦΥΣ (όπως laptops, notebooks, smartphones κλπ). Μεταξύ των έργων της διαπίστευσης, είναι και η αποδοχή του αποδεκτού κινδύνου για την ασφάλεια ενός συστήματος, λαμβάνοντας υπόψη τις ιδιαιτερότητες αυτού. Η διαπίστευση είναι μια δυναμική διαδικασία, για την επίτευξη της οποίας, απαραίτητη προϋπόθεση αποτελεί η συνεχής ανησυχία και προσπάθεια της ΑΕΛ (άρθρο 22), για την ασφάλεια των πληροφοριών που χειρίζεται το ΣΕΠ, το οποίο, η ίδια συνήθως αναπτύσσει και χρησιμοποιεί.

2. Η καθιέρωση ορθών διαδικασιών για τη διαπίστευση των ΣΕΠ, είναι ζωτικής σημασίας, δεδομένου ότι μέσω αυτών παρέχονται οι αναγκαίες οδηγίες στους εμπλεκόμενους φορείς και προσωπικό, ώστε να διασφαλίζεται ότι έχει καθιερωθεί, υλοποιηθεί και διατηρείται ένα ικανοποιητικό επίπεδο ασφαλείας για αυτά. Κατά συνέπεια, η διαπίστευση ενός ΣΕΠ, αφορά σε όλα τα στάδια σχεδιασμού, υλοποίησης και επιχειρησιακής λειτουργίας αυτού, μέχρι τη χρονική στιγμή αποσύρσεώς του από την ενεργό δράση και της διάθεσης των τμημάτων του για άλλες χρήσεις ή για καταστροφή. Ενέργειες διαπίστευσης κατά τη διάρκεια του κύκλου ζωής ενός ΣΕΠ και αρμοδιότητες των εμπλεκομένων φορέων, ως Παράρτημα «Ι».

3. Όλα όσα διατυπώνονται στον παρόντα Κανονισμό, αφορούν σε ΣΕΠ, τα οποία χειρίζονται δεδομένα με διαβάθμιση ασφαλείας από «ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ» έως και «ΑΠΟΡΡΗΤΟ». Οι προδιαγραφές διαπίστευσης των ΣΕΠ που χειρίζονται δεδομένα με διαβάθμιση ασφαλείας «ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ» και άνω, αποτελούν αντικείμενο ειδικής μελέτης, λόγω των αυξημένων απαιτήσεων ασφαλείας σε:

α. Υλικό (όπως η αποκλειστική χρήση συσκευών / υλικού με προδιαγραφές TEMPEST, χρήση αποκλειστικά δικτύου οπτικών ινών, κατασκευή ειδικών χώρων αποκλειστικά για την εγκατάστασή τους κλπ).

β. Προσωπικό (περιορισμό των χρηστών στους ελάχιστους απαραίτητους, ανάθεση καθηκόντων ασφαλείας σε συγκεκριμένο και επαρκές προσωπικό το οποίο δεν έχει έτερα καθήκοντα κλπ).

γ. Διαδικασίες (όπως η απαραίτητη OFF LINE κρυπτογράφηση, η εφαρμογή πολλαπλών και αλληλοκαλυπτόμενων συστημάτων ελέγχου πρόσβασης και ταυτοποίησης κλπ).

4. Για τα ΣΕΠ που αποτελούνται από ένα και μόνο αυτόνομο σύστημα (stand alone):

α. Τηρούνται όλοι οι κανόνες ασφαλείας του παρόντος κανονισμού, προσαρμοσμένοι, λόγω του μεγέθους του ΣΕΠ. Κατά περίπτωση και εφόσον απαιτείται

δίνονται διευκρινιστικές οδηγίες από την ΕΑΔΑ.

β. Απαιτείται κατ’ ελάχιστον να υπάρχει συγκεκριμένος χειριστής, καθώς επίσης και υπεύθυνος ΥΑΣ, ο οποίος έχει και την κύρια ευθύνη για την εγκατάσταση, ενημέρωση, συντήρηση και απόσυρση αυτού καθώς και την συμπλήρωση ενημέρωση και τήρηση όλων των απαραίτητων εγγράφων.

γ. Δεν εκδίδεται πιστοποιητικό ηλεκτρονικής ασφάλειας και ακολουθεί την πορεία πιστοποίησης της εγκατάστασης η οποία αναθεωρείται ανά 5 έτη. Σε περίπτωση που απαιτείται πιστοποιητικό ηλεκτρονικής ασφάλειας αυτό χορηγείται βάσει των προβλέψεων του παρόντος κανονισμού με διάρκεια έως 3 έτη.

5. Για το χειρισμό εγγράφου βαθμού ασφαλείας «ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ» και άνω, σε ηλεκτρονική μορφή, χρησιμοποιείται μεμονωμένος (stand alone) Η/Υ, για τον οποίο ισχύουν κατά ελάχιστο τα παρακάτω:

α. Να μην έχει οποιαδήποτε διασύνδεση με έτερο ΣΕΠ ή άλλο δίκτυο.

β. Το προσωπικό που έχει πρόσβαση σε αυτόν, να είναι εξαιρετικά περιορισμένο και το απολύτως απαραίτητο και να διαθέτει εξουσιοδότηση ασφαλείας «ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ», ενώ ο Η/Υ να φυλάσσεται σε χώρο με αυξημένα μέτρα ασφαλείας.

γ. Οι εξωτερικές θύρες, καθώς και οι οδηγοί δισκέτας και CD/DVD του συγκεκριμένου Η/Υ, να είναι απενεργοποιημένοι και προσβάσιμοι μόνο από 2 συγκεκριμένους διαχειριστές.

δ. Να χρησιμοποιεί συγκεκριμένο εκτυπωτή, στον οποίο έχει πρόσβαση μόνο εξουσιοδοτημένο προσωπικό και ο χώρος που βρίσκεται πληροί τις προϋποθέσεις για το χειρισμό υλικού «ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ» και άνω, ενώ γίνεται αποτύπωση (αύξων αριθμός αντιτύπου, ποιος παρέλαβε αντίτυπα, ημερομηνία και ώρα) όλων των αντιτύπων που εκτυπώνονται.

6. Η διαδικασία της διαπίστευσης, η οποία καθορίζεται από την ΕΑΔΑ, είναι σύμφωνη με τα οριζόμενα στον ΕΚΒΑ και κατά συνέπεια, με τα αντίστοιχα θεσμικά κείμενα του ΝΑΤΟ και της ΕΕ. Επιπλέον, εφαρμόζεται στο πλαίσιο απόκτησης πιστοποιητικού βιομηχανικής ασφάλειας ενός φορέα που διαθέτει ΣΕΠ με το οποίο πρόκειται να χειριστεί διαβαθμισμένα δεδομένα, ανεξάρτητα εάν λειτουργεί αυτόνομα ή πρόκειται να διασυνδεθεί με έτερα ΣΕΠ (Εθνικά, ΕΕ ή ΝΑΤΟ). Στο πλαίσιο εφαρμογής της εν λόγω διαδικασίας, η ΕΑΔΑ μπορεί να συγκροτεί κατά περίπτωση επιτροπές που ονομάζονται Επιτροπές Διαπίστευσης Ασφαλείας (ΕΔΑ), στις οποίες συμμετέχει και εξειδικευμένο προσωπικό από την ΕΑΑΕΠ.

7. Όταν ένα ΣΕΠ χρησιμοποιείται εκτός από Εθνικό σκοπό και από Διεθνείς Οργανισμούς (όπως ΝΑΤΟ, ΕΕ), η ΕΑΔΑ και οι Διεθνείς Οργανισμοί συμφωνούν αμοιβαία για τη διαπίστευση.

8. Η διαδικασία της διαπίστευσης ΣΕΠ ξεκινά με αίτημα ενός οικονομικού φορέα που έχει ή πρόκειται να αποκτήσει πιστοποιητικό βιομηχανικής ασφάλειας προς τη ΔΑΑ. Η ΔΑΑ προωθεί το αίτημα προς την ΕΑΔΑ, η οποία δύναται να συγκροτεί κατά περίπτωση ΕΔΑ. Όλα τα απαιτούμενα έγγραφα (ΔΑΠΑΣ, ΔΑΛ κλπ) διαβιβάζονται από τον οικονομικό φορέα προς τη ΔΑΑ και εν συνεχεία στην ΕΑΔΑ.

9. Κατά τη διαδικασία διαπίστευσης ενός ΣΕΠ, εξετάζονται τα παρακάτω:

α. Το εύρος και οι δυνατότητές του.

β. Ο όγκος και η διαβάθμιση των πληροφοριών που χειρίζεται.

γ. Οι κάθε είδους χρήστες του και οι απαιτούμενες εξουσιοδοτήσεις αυτών.

δ. Το περιβάλλον και οι διάφορες περιοχές στις οποίες λειτουργεί.

ε. Η διασύνδεσή του με άλλα ΣΕΠ.

στ. Οι κίνδυνοι που σχετίζονται με την απώλεια πληροφοριών και τα μέτρα (τεχνικά και μη) αντιμετώπισής τους.

ζ. Η εκτίμηση ασφαλείας, ώστε να διασφαλισθεί ότι τα ληφθέντα μέτρα είναι επαρκή.

10. Η εμπλοκή προσωπικού της ΑΕΛ, εξειδικευμένου σε θέματα ασφαλείας, απαιτείται από τα αρχικά στάδια σχεδιασμού και καθ' όλη τη διάρκεια της ανάπτυξης, εγκατάστασης και επέκτασης ενός ΣΕΠ, έτσι ώστε να αποφεύγεται η εκ των υστέρων προσθήκη χαρακτηριστικών ασφαλείας, η οποία είναι υψηλού κόστους, χρονοβόρα και συχνά δεν ανταποκρίνεται στις σύγχρονες απαιτήσεις ασφαλείας.

11. Η αποτελεσματική ασφάλεια ενός ΣΕΠ, βασίζεται στην υλοποίηση ενός ισορροπημένου συνόλου μέτρων ασφαλείας, συμπεριλαμβανομένων των μέτρων φυσικής ασφαλείας, ασφαλείας προσωπικού, ασφαλείας ΕΔΠΥ και ασφαλείας επικοινωνιών – πληροφορικής, με σκοπό τη μείωση του κινδύνου (διαρροής των πληροφοριών που αυτό «χειρίζεται»), σε ένα αποδεκτό επίπεδο και την παροχή άμυνας σε βάθος.

12. Ανάλυση Κινδύνου (ΑΚ)

Είναι το σύνολο των ενεργειών με τις οποίες διασφαλίζεται ότι η πιθανότητα διαρροής των πληροφοριών, διατηρείται σε αποδεκτό επίπεδο, καθ' όλη τη διάρκεια ζωής ενός ΣΕΠ. Περιλαμβάνει τη μελέτη των απειλών, των τρωτοτήτων του ΣΕΠ και τον σχεδιασμό των κατάλληλων μέτρων με βάση την απειλή, καθώς και τον εναπομένοντα αποδεκτό κίνδυνο. Λόγω της κρισιμότητας της εν λόγω διεργασίας και για την πληρέστερη υλοποίησή της, κρίνεται σκόπιμη η χρήση λογισμικού ανάλυσης κινδύνου από την ΑΕΛ. Τα αποτελέσματα της ΑΚ, έχουν άμεση επίπτωση, τόσο στον αρχικό προϋπολογισμό, όσο και στο τελικό κόστος ενός ΣΕΠ, καθόσον υποδεικνύουν τα απαραίτητα μέτρα ασφαλείας για το συγκεκριμένο σύστημα. Σε περίπτωση, που αποφασιστεί να μην αντιμετωπιστούν συγκεκριμένοι κίνδυνοι λόγω κόστους η ΑΕΛ να αναλαμβάνει και την ανάλογη ευθύνη λειτουργίας του ΣΕΠ, υπό τη συγκεκριμένη διαμόρφωση, εφόσον βέβαια υφίσταται η συμφωνία της ΕΑΔΑ. Οδηγίες για τη Διαδικασία Ανάλυσης Κινδύνου Ασφαλείας, ως Παράρτημα «ΙΔ».

13. Διαχείριση Κινδύνου (ΔΚ)

Πρόκειται για τη διαδικασία της συνεχούς αξιολόγησης των πιθανών γεγονότων που πρόκειται να επηρεάσουν την ασφάλεια ενός ΣΕΠ, με σκοπό την αναπροσαρμογή τόσο της πολιτικής όσο και των μέτρων ασφάλειας. Πληροφορίες για τη Διαχείριση Κινδύνου, ως Παράρτημα «ΙΔ».

14. Δήλωση Απαιτήσεων Ασφαλείας Συστήματος (ΔΑΠΑΣ)

α. Αποτελεί τη συμφωνία μεταξύ της ΕΑΔΑ (ή ΕΔΑ εφόσον έχει οριστεί) και της ΑΕΛ για τη λειτουργία ενός ΣΕΠ, για το οποίο πληρούνται συγκεκριμένες προδιαγραφές ασφαλείας, ενώ οι εναπομείναντες κίνδυνοι, για τους οποίους δεν έχουν ληφθεί μέτρα ασφαλείας, βρίσκονται σε αποδεκτό επίπεδο. Η ΔΑΠΑΣ συντάσσεται από την ΑΕΛ και μπορεί να μεταβληθεί κατά τη διάρκεια ζωής του ΣΕΠ.

Οδηγίες για τη σύνταξη ΔΑΠΑΣ, ως Παράρτημα «ΙΑ».

β. Η ΔΑΠΑΣ, μπορεί να τροποποιείται στους παρακάτω τύπους, ανάλογα με τη φύση του ΣΕΠ:

(1) Δήλωση Απαιτήσεων Ασφαλείας Διασύνδεσης (ΔΑΠΑΔ)

Περιγράφει όλα τα θέματα ασφαλείας, που αφορούν στη διασύνδεση δύο ΣΕΠ.

(2) Δήλωση Απαιτήσεων Ασφαλείας Κοινότητας (ΔΑΠΑΚ)

Περιγράφει όλα τα θέματα ασφαλείας ενός ενιαίου συστήματος, το οποίο πληροί συγκεκριμένες προδιαγραφές και πρότυπα ασφαλείας και αποτελείται από περισσότερα των δύο ΣΕΠ που διασυνδέονται μεταξύ τους. Τα ΣΕΠ αυτά μπορεί να λειτουργούν, είτε κάτω από ένα ενιαίο περιβάλλον ασφαλείας, είτε κάτω από διαφορετικά.

(3) Δήλωση Απαιτήσεων Τεχνικής Ασφαλείας (ΔΑΤΑΣ)

Περιγράφει τις προδιαγραφές ενός συγκεκριμένου υλικού ή λογισμικού και χρησιμεύει για την εκπλήρωση των απαιτήσεων των αρμοδίων αρχών ασφαλείας και σχεδιασμού, στο πλαίσιο προμήθειας των συστημάτων.

15. Διαδικασίες Ασφαλούς Λειτουργίας (ΔΑΛ)

α. Η ΑΕΛ, προκειμένου να υλοποιήσει την πολιτική ασφαλείας, που υιοθετήθηκε μέσω της ΔΑΠΑΣ, προβαίνει στην έκδοση των ΔΑΛ, που είναι μία περιγραφή της εφαρμογής της πολιτικής ασφαλείας που υιοθετείται, των λειτουργικών διαδικασιών που ακολουθούνται και των ευθυνών του προσωπικού. Οδηγίες για τη σύνταξη ΔΑΛ, ως Παράρτημα «ΙΒ».

β. Για κάθε διοικητικά ή γεωγραφικά ανεξάρτητο χώρο λειτουργίας ενός ΣΕΠ, απαιτείται η έκδοση ξεχωριστής ΔΑΛ, η οποία όμως στηρίζεται στα καθοριζόμενα από τη ΔΑΠΑΣ.

γ. Ειδικά για τα ΣΕΠ με διαβάθμιση «ΕΜΠΙΣΤΕΥΤΙΚΟ» και άνω, απαιτείται η έγκριση του συνόλου των ΔΑΛ από την ΕΑΔΑ (ή ΕΔΑ εφόσον έχει οριστεί), πριν την ενεργοποίησή τους.

δ. Οι εξουσιοδοτημένοι χρήστες του ΣΕΠ δηλώνουν ενυπόγραφα ότι έχουν μελετήσει, κατανοήσει και δεσμεύονται να εφαρμόζουν τα προβλεπόμενα στις ΔΑΛ. Οι υπογεγραμμένες από τους χρήστες ΔΑΛ, τηρούνται από τον ΥΑΣ του οικονομικού φορέα, ενώ με μέριμνά του υπάρχει άμεση πρόσβαση σε αυτές.

ΑΡΘΡΟ 43
ΙΣΧΥΣ ΤΗΣ ΔΙΑΠΙΣΤΕΥΣΗΣ

1. Μετά την έγκριση των ΔΑΠΑΣ και ΔΑΛ από την ΕΑΔΑ (ή ΕΔΑ εφόσον έχει οριστεί) και την ολοκλήρωση της διαδικασίας διαπίστευσης του ΣΕΠ, ακολουθεί η έκδοση Πιστοποιητικού Διαπίστευσης Ασφαλείας του (Υπόδειγμα 13), στο οποίο καθορίζεται η ισχύς της διαπίστευσης. Ωστόσο, σε περίπτωση που διαπιστωθούν ελλείψεις στα δηλωθέντα από την ΑΕΛ μέτρα ασφαλείας και ανάλογα με την κρισιμότητα αυτών, η ΕΑΔΑ (ή ΕΔΑ εφόσον έχει οριστεί), δύναται να εκδώσει Άδεια Προσωρινής Λειτουργίας, περιορισμένου χρονικού διαστήματος, εντός του οποίου απαιτείται να αποκατασταθούν οι παρατηρήσεις – ελλείψεις που διαπιστώθηκαν.

2. Η φύση και η πολυπλοκότητα των ΣΕΠ που απαιτούν διαπίστευση, καθώς και η ανάγκη τεχνικής εξέλιξης, επέκτασης και διασύνδεσής τους με έτερα συστήματα, σε συνδυασμό με τη μεταβολή της απειλής και την ανάγκη συνεχούς επανεκτίμησης του αποδεκτού εναπομείναντα κινδύνου, επιβάλουν την ύπαρξη περιορισμών στην ισχύ της διαπίστευσης. Οι περιορισμοί ισχύος της διαπίστευσης, περιγράφονται σαφώς στην τελική πράξη διαπίστευσης ενός συγκεκριμένου ΣΕΠ, καθώς επίσης και οι ενέργειες στις οποίες προβαίνει κατά περίπτωση η ΑΕΛ, προκειμένου να διατηρήσει το συγκεκριμένο ΣΕΠ σε λειτουργία.

3. Οι παράγοντες που επηρεάζουν την ισχύ της διαπίστευσης είναι οι παρακάτω:

α. Χρόνος

Η χρονική διάρκεια ισχύος της διαπίστευσης, εξαρτάται κυρίως από τις τεχνολογίες ασφαλείας που ενσωματώνει το ΣΕΠ και ορίζεται έως τρία (3) χρόνια. Πριν το πέρας του προαναφερθέντος χρονικού διαστήματος, η ΑΕΛ υποβάλλει εκ νέου προς την ΕΑΔΑ, τη ΔΑΠΑΣ και τις ΔΑΛ, κατάλληλα τροποποιημένες ανάλογα με τις τυχόν εν ισχύ αλλαγές, προκειμένου το ΣΕΠ να λάβει νέα χρονική παράταση λειτουργίας. Σε περίπτωση που το ΣΕΠ δεν είναι δυνατό να διατηρήσει το επίπεδο διαβάθμισης σύμφωνα με την αρχική διαπίστευση, αποσύρονται από αυτό όλα τα δεδομένα που αντιστοιχούσαν στην προηγούμενη διαβάθμισή του. Σε περίπτωση ήδη διαπιστευμένου ΣΕΠ, η ΑΕΛ παρακολουθεί συνεχώς την εξέλιξη της τεχνολογίας στον τομέα, καθώς και τις σχετικές οδηγίες που εκδίδονται από τους αρμόδιους φορείς, προκειμένου να εντοπίζει τεχνικά θέματα που επηρεάζουν την ασφάλειά του και τα οποία αναφέρονται απαραιτήτως στις τροποποιημένες πλέον ΔΑΠΑΣ και ΔΑΛ.

β. Απειλή

Τα μέτρα ασφαλείας ενός ΣΕΠ, μελετώνται με βάση την απειλή, το αποδεκτό ρίσκο, καθώς και τους εναπομείναντες κινδύνους, όπως προκύπτουν από την ΑΚ και τον περιοδικό έλεγχο ασφαλείας που διενεργείται. Στο πιστοποιητικό διαπίστευσης ασφαλείας καθορίζονται οι προϋποθέσεις ισχύος της διαπίστευσης, με σκοπό την καθοδήγηση της ΑΕΛ, προκειμένου να προβαίνει στην επανεξέταση των εναπομεινάντων κινδύνων, όταν διαπιστώνεται μεταβολή στις αρχικές συνθήκες προσδιορισμού της απειλής και του αποδεκτού ρίσκου.

γ. Μεταβολές (Επέκταση – Τροποποίηση ΣΕΠ)

Κάθε μεταβολή (επέκταση ή κατάργηση υλικού, καθώς και τροποποίηση λογισμικού) του ΣΕΠ, μικρή ή μεγάλη, προκαλεί ανάλογη επανεκτίμηση των θεμάτων ασφαλείας, με επανυποβολή νέας ΔΑΠΑΣ και επαναδιαπίστευση του συγκεκριμένου ΣΕΠ από την ΕΑΔΑ.

Στρατηγός Κωνσταντίνος Φλώρος
Αρχηγός

Ακριβές Αντίγραφο

Ασμχος (ΕΑ) Νικόλαος Ζήκος
Επιτελής ΓΕΕΘΑ/Ε3/1

ΠΑΡΑΡΤΗΜΑΤΑ

«Α» Αρμοδιότητες Υπευθύνου Γραφείου Ασφαλείας και Βοηθών του
«Β» Σχέδιο Μεταφοράς ΕΔΠΥ
«Γ» Σχέδιο Ασφαλείας Εγκατάστασης Οικονομικού Φορέα
«Δ» Προδιαγραφές Ασφαλείας Εγκαταστάσεων – Υπαρχείου
«Ε» Διαδικασία Επιλογής και Εξουσιοδότησης Ασφαλείας Προσωπικού
«ΣΤ» Οδηγίες Χειρισμού ΕΔΠΥ
«Ζ» Κατάσταση Τηρουμένων Εντύπων - Βιβλίων
«Η» Ηλεκτρομαγνητική Προστασία
«Θ» Πίνακας Καθαρισμού και Εξυγίανσης Μέσων
«Ι» Ενέργειες Διαπίστευσης κατά τη Διάρκεια του Κύκλου Ζωής ενός ΣΕΠ
«ΙΑ» Οδηγίες για τη Σύνταξη της Δήλωσης Απαιτήσεων Ασφαλείας Συστήματος (ΔΑΠΑΣ)
«ΙΒ» Οδηγίες για τη Σύνταξη των Διαδικασιών Ασφαλούς Λειτουργίας (ΔΑΛ)
«ΙΓ» Μέτρα και Διαδικασίες Ασφαλείας ανά Διαβάθμιση ΣΕΠ
«ΙΔ» Διαδικασία Ανάλυσης Κινδύνου Ασφαλείας
«ΙΕ» Αρμοδιότητες και Καθήκοντα Αρχών και Προσωπικού Ασφαλείας

ΥΠΟΔΕΙΓΜΑΤΑ

ΓΕΝΙΚΟ ΕΠΙΤΕΛΕΙΟ ΕΘΝΙΚΗΣ ΑΜΥΝΑΣ
Ε΄ ΚΛΑΔΟΣ
ΔΝΣΗ ΑΣΦΑΛΕΙΑΣ
07 Σεπ 20

ΠΑΡΑΡΤΗΜΑ «Α» ΣΤΟΝ
ΕΚΒΑ

ΑΡΜΟΔΙΟΤΗΤΕΣ
ΥΠΕΥΘΥΝΟΥ ΓΡΑΦΕΙΟΥ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΒΟΗΘΩΝ ΤΟΥ

ΥΠΕΥΘΥΝΟΣ ΑΣΦΑΛΕΙΑΣ

1. Γενικά

Ο υπεύθυνος ασφαλείας του οικονομικού φορέα:

α. Είναι υπεύθυνος για όλα τα θέματα ασφαλείας έναντι της Διοίκησης.

β. Ενημερώνεται για τα προβλεπόμενα στον παρόντα Κανονισμό.

γ. Αναλαμβάνει καθήκοντα μετά την ημερομηνία εξουσιοδότησής του.

δ. Συνεργάζεται με τη ΔΑΑ για θέματα ασφαλείας στο πλαίσιο του ΕΚΒΑ.

ε. Ελέγχει το προσωπικό που χειρίζεται ΕΔΠΥ.

στ. Συνεργάζεται με τους υπεύθυνους ασφαλείας άλλων οικονομικών φορέων, όπως κυρίων αναδόχων και υπεργολάβων.

ζ. Τηρεί τα προβλεπόμενα έντυπα – βιβλία του Παραρτήματος «Ζ» του παρόντος Κανονισμού.

η. Ενημερώνει τη διοίκηση του οικονομικού φορέα καθώς και τις αρμόδιες αρχές για κάθε παραβίαση σε θέματα ασφαλείας, σύμφωνα με το άρθρο 11.

θ. Για την εκτέλεση των καθηκόντων του επικουρείται υποχρεωτικά από ένα βοηθό υπευθύνου ασφαλείας στον οποίο αναθέτει αρμοδιότητες και τον αναπληρώνει σε περίπτωση απουσίας του. Η ανάθεση αρμοδιοτήτων στο βοηθό δεν απαλλάσσει από τις ευθύνες του τον υπεύθυνο ασφαλείας. Εάν απαιτείται δύναται να ορισθούν περισσότεροι του ενός βοηθοί.

2. Αρμοδιότητες – Καθήκοντα Υπευθύνου Ασφαλείας

α. Ασφάλεια Προσωπικού

(1) Εφαρμόζει τις διαδικασίες του Άρθρου 7 και του Παραρτήματος «Ε» για την εξουσιοδότηση ασφαλείας προσωπικού του οικονομικού φορέα που πρόκειται να έχει πρόσβαση σε ΕΔΠΥ.

(2) Ενημερώνει, εκπαιδεύει και ελέγχει για την καταλληλότητα το προσωπικό σε θέματα ασφαλείας πριν την εξουσιοδότησή του.

(3) Ενημερώνει το προσωπικό στο οποίο πρόκειται να αρθεί η εξουσιοδότηση ασφαλείας και μεριμνά για τη σύνταξη, υπογραφή και υποβολή του Υποδείγματος 5.

(4) Ενημερώνει και εκπαιδεύει το προσωπικό του οικονομικού φορέα, ανά εξάμηνο, για θέματα και διαδικασίες ασφαλείας, νομικές συνέπειες σχετικές με παραβιάσεις και παραβάσεις ασφαλείας καθώς και για την εξ αμελείας ή εκ

προθέσεως διαρροή ΕΔΠΥ, αλλά και την υποχρέωση αναφοράς οποιασδήποτε παράβασης ή παραβίασης ασφαλείας.

(5) Σε περίπτωση φύλαξης του οικονομικού φορέα από ΙΕΠΥΑ, ενημερώνει το προσωπικό αυτής για θέματα και διαδικασίες ασφαλείας του οικονομικού φορέα.

(6) Διενεργεί συνεχείς ελέγχους για τη διαπίστωση εφαρμογής των μέτρων ασφαλείας ΕΔΠΥ από το εξουσιοδοτημένο προσωπικό.

(7) Χορηγεί ταυτότητες και δελτία εισόδου οπουδήποτε απαιτείται.

(8) Εφαρμόζει τις διαδικασίες του Άρθρου 12 για τη πραγματοποίηση επισκέψεων από/προς τον οικονομικό φορέα.

(9) Ενημερώνει το εξουσιοδοτημένο προσωπικό για τη λήψη μέτρων ασφαλείας εφ’ όσον σκοπεύει, για οποιονδήποτε λόγο, να ταξιδέψει στο εξωτερικό.

β. Φυσική Ασφάλεια

(1) Σχεδιάζει, εισηγείται και ελέγχει την υλοποίηση των μέτρων ασφαλείας που απαιτούνται για την προστασία των εγκαταστάσεων, στις οποίες φυλάσσονται ΕΔΠΥ.

(2) Συντάσσει το Σχέδιο Ασφάλειας Εγκαταστάσεως του οικονομικού φορέα, σύμφωνα με το Παράρτημα «Γ» του παρόντος, και το υποβάλλει στη ΔΑΑ. Μεριμνά για την εφαρμογή του και την αναθεώρησή του όποτε αυτό απαιτείται.

(3) Μεριμνά για την οργάνωση της αντιπυρικής προστασίας των εγκαταστάσεων του οικονομικού φορέα σε συνεργασία με την Πυροσβεστική Υπηρεσία, καθώς και για την προμήθεια, εγκατάσταση και συντήρηση των υλικών και μέσων πυρασφαλείας που απαιτούνται.

(4) Προβάλει στον οικονομικό φορέα τις απαιτήσεις σε προσωπικό ασφάλειας, υλικά και μέσα.

(5) Συγκεντρώνει και υποβάλει τα δικαιολογητικά που απαιτούνται, σύμφωνα με το Άρθρο 14 του Κανονισμού, για την έκδοση Πιστοποιητικού Ασφάλειας Εγκατάστασης του οικονομικού φορέα.

(6) Καθορίζει τους χώρους ασφαλείας και τα μέτρα ασφαλείας αυτών.

(7) Εκπονεί πρότυπα ασφαλείας για γραφεία, διαδρόμους, αποθήκες, ενισχυμένα γραφεία/αίθουσες και χρηματοκιβώτια όπου φυλάσσονται ΕΔΠΥ και μεριμνά για την προστασία των κωδικών και των συνδυασμών και την περιοδική αλλαγή αυτών, οποτεδήποτε υπάρξουν αντικαταστάσεις προσωπικού ή οποτεδήποτε υπάρχει υποψία διαρροής τους.

(8) Εκπονεί και εισηγείται μέτρα ελέγχου εισόδου, εξόδου για τις εγκαταστάσεις και παρακολουθεί την εφαρμογή τους.

(9) Ελέγχει περιοδικά τη λειτουργικότητα των συστημάτων συναγερμού και μεριμνά για τη συντήρηση και αναβάθμισή τους.

(10) Εκτελεί ελέγχους ασφαλείας εντός και εκτός ωραρίου εργασίας, δίδοντας ιδιαίτερη έμφαση σε γραφεία, αρχεία και άλλες εγκαταστάσεις, όπου φυλάσσονται ΕΔΠΥ.

(11) Ελέγχει την εφαρμογή των μέτρων ασφαλείας στο υπαρχείο και τους χώρους ασφαλείας του οικονομικού φορέα.

(12) Αναπτύσσει διαδικασίες και λαμβάνει μέτρα ασφαλείας των χώρων που διεξάγονται συσκέψεις, συνέδρια, ενημερώσεις και άλλες δραστηριότητες για την προστασία ΕΔΠΥ.

(13) Ελέγχει τις εγκαταστάσεις ή τους χώρους ασφαλείας που ο οικονομικός φορέας δεν χρησιμοποιεί προς εξακρίβωση ότι εντός αυτών δεν υφίσταται ΕΔΠΥ.

(14) Καθορίζει διαδικασίες για δραστηριότητες καθαρισμού και συντήρησης σε χώρους ασφαλείας.

(15) Συντάσσει οδηγίες με τα καθήκοντα των φρουρών ασφαλείας, των παρατηρητών και των δυνάμεων ασφαλείας και διεξάγει ασκήσεις με σκοπό να δοκιμασθεί η επάρκεια των συστημάτων και η κατανόηση των διαδικασιών από αυτούς που τα χειρίζονται.

(16) Δημιουργεί σύστημα ελέγχου για τα κλειδιά όλων των γραφείων της επιχείρησης και καθορίζει τα υπεύθυνα άτομα.

(17) Τηρεί όλα τα κλειδιά των χώρων ασφαλείας και του υπαρχείου και απασφαλίζει/ασφαλίζει τους χώρους αυτούς ο ίδιος ή οι βοηθοί του. Επίσης, τηρεί τα κλειδιά όλων των φωριαμών που περιέχουν ΕΔΠΥ.

γ. Ασφάλεια ΕΔΠΥ

(1) Καθιερώνει διαδικασίες για την καταγραφή όλων των εισερχομένων ΕΔΠΥ, τον έλεγχο και διανομή τους.

(2) Καθιερώνει διαδικασίες για τον έλεγχο όλων των φωτοαντιγράφων, μεταφράσεων και αποσπασμάτων διαβαθμισμένων πληροφοριών, μεριμνώντας για την καταγραφή και αρίθμησή τους.

(3) Καθορίζει τα προς καταστροφή ΕΔΠΥ, που δεν είναι πλέον απαραίτητα, και αφού λάβει τη σχετική έγκριση του εκδότη τους, προβαίνει στην καταστροφή αυτών, σύμφωνα με τις διαδικασίες που προβλέπονται στο Παράρτημα «ΣΤ».

(4) Μεριμνά για την εκπόνηση σχεδίων μεταφοράς των ΕΔΠΥ και εξασφαλίζει τη σωστή εφαρμογή τους.

(5) Εξασφαλίζει ότι ο οικονομικός φορέας φυλάσσει και χειρίζεται τις ΕΔΠΥ αναλόγως του επιπέδου διαβάθμισής τους.

(6) Εξασφαλίζει ότι άτομα που αποκτούν πρόσβαση σε ΕΔΠΥ έχουν εξουσιοδότηση ασφαλείας αντίστοιχη με την διαβάθμιση ασφαλείας αυτών.

(7) Εξασφαλίζει ότι η πρόσβαση σε ΕΔΠΥ από εξουσιοδοτημένους επισκέπτες διέπεται από την αρχή «ανάγκη γνώσης».

(8) Εξασφαλίζει την τήρηση των ρητρών ασφαλείας των συμβάσεων του οικονομικού φορέα και συνεργάζεται με τους υπεύθυνους ασφαλείας των επιμέρους αναδόχων με σκοπό την εφαρμογή μέτρων ασφαλείας από όλα τα εμπλεκόμενα μέρη.

δ. Ασφάλεια Επικοινωνιών – Πληροφορικής

(1) Χρησιμοποίηση των συσκευών – συστημάτων επικοινωνίας για

τη διαβίβαση πληροφοριών, μέχρι του βαθμού ασφαλείας για τον οποίον έχουν πιστοποιηθεί. Επιπλέον τοποθέτηση πινακίδων σε όλες τις συσκευές επικοινωνιών, που να φέρουν την ένδειξη του πιστοποιημένου βαθμού ασφαλείας, καθώς και το είδος ασφαλείας που προσφέρει η συσκευή.

(2) Χρησιμοποίηση κάθε δικτύου επικοινωνιών μόνο για το σκοπό που έχει σχεδιασθεί.

(3) Πιστή τήρηση των οδηγιών που αναφέρονται στην εγκατάσταση συσκευών επεξεργασίας και διαβιβάσεως διαβαθμισμένων πληροφοριών.

(4) Η χρήση κινητών τηλεφώνων απαγορεύεται εντός των υπαρχείων.

(5) Απενεργοποίηση των κινητών τηλεφώνων και παράδοσή και τοποθέτησή τους σε ασφαλισμένους χώρους εκτός των αιθουσών συζήτησης διαβαθμισμένων πληροφοριών.

(6) Τακτικός και έκτακτος έλεγχος των τηλεφωνικών γραμμών και κυκλωμάτων για πιθανή ύπαρξη συσκευών υποκλοπής, παροχετεύσεων ή παραλληλισμών.

(7) Τακτικός και έκτακτος έλεγχος του υπαρχείου και των χώρων όπου συζητούνται θέματα υψηλής διαβάθμισης για ύπαρξη συσκευών υποκλοπής.

(8) Έκδοση οδηγιών ασφαλούς λειτουργίας των ΣΕΠ και εκπαίδευση του αρμόδιου προσωπικού.

3. Επιθεωρήσεις

α. Παρευρίσκεται ο ίδιος ή ο αναπληρωτής του στις προγραμματισμένες και έκτακτες επιθεωρήσεις ασφαλείας που πραγματοποιούνται από τις αρμόδιες αρχές ασφαλείας.

β. Σχεδιάζει και εφαρμόζει ετήσιο πρόγραμμα εσωτερικής επιθεώρησης του οικονομικού φορέα, που αφορά στα γραφεία και τους χώρους του και συντάσσει σχετική αναφορά που υποβάλλει στη διοίκηση. Επίσης, πραγματοποιεί απροειδοποίητες επιθεωρήσεις ασφαλείας.

ΒΟΗΘΟΣ ΥΠΕΥΘΥΝΟΥ ΑΣΦΑΛΕΙΑΣ

1. Επικουρεί τον υπεύθυνο ασφαλείας σε θέματα ασφαλείας του οικονομικού φορέα και αναπληρώνει αυτόν σε περίπτωση απουσίας του.

2. Ενεργεί με βάση τις οδηγίες και τις αρμοδιότητες που του εκχωρεί ο υπεύθυνος ασφαλείας στο πλαίσιο εκτέλεσης των καθηκόντων του.

3. Εισηγείται κατά την κρίση του μέτρα βελτίωσης της ασφάλειας του οικονομικού φορέα.

Αντιναύαρχος Ιωάννης Δρυμούσης ΠΝ
Υπαρχηγός

Ακριβές Αντίγραφο

Ασμχος (ΕΑ) Νικόλαος Ζήκος
Επιτελής ΓΕΕΘΑ/Ε3/1

ΓΕΝΙΚΟ ΕΠΙΤΕΛΕΙΟ ΕΘΝΙΚΗΣ ΑΜΥΝΑΣ
Ε’ ΚΛΑΔΟΣ
ΔΝΣΗ ΑΣΦΑΛΕΙΑΣ
07 Σεπ 20

ΠΑΡΑΡΤΗΜΑ «Β» ΣΤΟΝ
ΕΚΒΑ

ΣΧΕΔΙΟ ΜΕΤΑΦΟΡΑΣ ΕΔΠΥ

1. Σκοπός Σχεδίου Μεταφοράς

Σκοπός του Σχεδίου αυτού είναι να καθορισθούν τα κατάλληλα μέτρα ασφαλείας που λαμβάνονται, καθώς και οι αναγκαίες προπαρασκευές και διαδικασίες που γίνονται για τη μεταφορά ΕΔΠΥ, ώστε να μην περιέλθει στα χέρια μη εξουσιοδοτημένου προσωπικού. Το Σχέδιο υποβάλλεται για έγκριση στην ΕΑΑ και περιλαμβάνει τις εξής ενότητες:

α. Περιγραφή ΕΔΠΥ

Περιλαμβάνει μία γενική περιγραφή των ΕΔΠΥ που πρόκειται να μεταφερθούν. Εάν κριθεί απαραίτητο, μπορεί να επισυναφθεί σε αυτό το σχέδιο ως παράρτημα ένας λεπτομερής, περιγραφικός πίνακας των ΕΔΠΥ που πρόκειται να μεταφερθούν.

β. Αναγνώριση Εξουσιοδοτημένων Εκπροσώπων Συμμετέχοντος Κράτους.

Καθορίζονται οι εξουσιοδοτημένοι εκπρόσωποι κάθε συμμετέχοντος στο πρόγραμμα / μελέτη με το όνομά τους και τα καθήκοντά τους οι οποίοι πρόκειται να παραλάβουν και να αναλάβουν αρμοδιότητες ασφαλείας του ΕΔΠΥ κατά τη μεταφορά του. Οι ταχυδρομικές διευθύνσεις, τα τηλέφωνα, οι αριθμοί συσκευών τηλεομοιοτυπίας, e-mail, καταγράφονται για τους εκπροσώπους κάθε χώρας.

γ. Σημεία Παράδοσης

(1) Καθορίζονται τα σημεία παράδοσης για κάθε συμμετέχοντα (π.χ Λιμάνια, Σιδηροδρομικοί Σταθμοί, Αεροδρόμια, κλπ) και ο τρόπος πραγματοποίησης της μεταβίβασης.

(2) Περιγράφονται οι ρυθμίσεις ασφαλείας που απαιτούνται κατά τη διάρκεια που το ΕΔΠΥ τοποθετείται στα σημεία παράδοσης.

(3) Καθορίζονται τυχόν πρόσθετες ρυθμίσεις ασφαλείας που μπορεί να απαιτηθούν λόγω της ιδιαίτερης φύσης της μετακίνησης των ΕΔΠΥ ή κάποιου από τα σημεία παράδοσης είτε πρόκειται για ενδιάμεσες στάσεις είτε για τελικό προορισμό (π.χ τμήμα εμπορευμάτων ενός αεροδρομίου ή σταθμός παραλαβής ενός λιμένος).

δ. Καθορισμός Μεταφορέων

Καθορίζονται οι εξουσιοδοτημένοι μεταφορείς και οι αντιπρόσωποι μεταφορικών εταιρειών, όπου αρμόζει, οι οποίοι εμπλέκονται στη μεταφορά ΕΔΠΥ.

ε. Εγκατάσταση Αποθήκευση / Διεκπεραιώσεως και Σημεία Μεταβίβασης

(1) Καταγράφονται από το συμμετέχοντα οι εγκαταστάσεις αποθήκευσης ή διεκπεραίωσης και τα σημεία μεταβίβασης που πρόκειται να χρησιμο-

ποιηθούν.

(2) Περιγράφονται οι ειδικές ρυθμίσεις ασφαλείας για την προστασία ΕΔΠΥ όταν αυτές βρίσκονται σε χώρο αποθήκευσης / διεκπεραιώσεως ή στο σημείο μεταβίβασης.

στ. Δρομολόγια

Καθορίζονται τα δρομολόγια των μεταφορών βάσει του σχεδίου, ενώ περιλαμβάνεται κάθε τμήμα του δρομολογίου από το σημείο εκκίνησης μέχρι τον τελικό προορισμό συμπεριλαμβανομένων όλων των διαβάσεων των συνόρων. Τα δρομολόγια περιγράφονται λεπτομερώς σε κάθε συμμετέχοντα με λογική σειρά φόρτωσης από σημείο σε σημείο. Εάν απαιτούνται στάσεις ή διανυκτερεύσεις καθορίζονται ρυθμίσεις ασφαλείας για κάθε σημείο στάθμευσης.

ζ. Ασφάλεια Λιμένων και Τελωνειακές Αρχές

Καθορίζονται οι ρυθμίσεις διεκπεραίωσης με τις τελωνειακές και λιμενικές αρχές ασφαλείας μέσω των οποίων μεταφέρεται το ΕΔΠΥ. Οι υπεύθυνοι των εγκαταστάσεων πιστοποιούν ότι ο απεσταλμένος είναι κατάλληλα εξουσιοδοτημένος σύμφωνα με τον παρόντα Κανονισμό, έχει μαζί του όλα τα απαραίτητα έγγραφα και ότι γνωρίζει τις προβλεπόμενες διαδικασίες για τη μεταφορά ΕΔΠΥ μέσω λιμένων και τελωνείου. Δύναται να προηγηθεί συντονισμός με τις τελωνειακές υπηρεσίες και την ασφάλεια λιμένος έτσι ώστε να επιτευχθούν ασφαλώς οι μεταφορές του προγράμματος / μελέτης. Οι διαδικασίες για τη διεκπεραίωση τελωνειακών ερευνών και σημείων ελέγχου για την επιβεβαίωση των κινήσεων στα αρχικά σημεία φόρτωσης περιλαμβάνονται σε αυτήν την ενότητα.

η. Μεταφορείς

Όταν χρησιμοποιούνται μεταφορείς καθορίζονται τα στοιχεία τους (ονοματεπώνυμο, καθήκοντα, αριθμός διαβατηρίου ή ταυτότητας), ενώ απαιτείται να έχουν την κατάλληλη εξουσιοδότηση ασφαλείας. Προ της μεταφοράς είναι αναγκαία η ενημέρωσή τους που είναι προσαρμοσμένη στον τύπο μεταφοράς (π.χ Αεροπορική, με Πλοίο, Φορτηγό, Τρένο κλπ) καθώς και για τις ευθύνες τους περί ασφαλείας ΕΔΠΥ. Για κάθε μεταφορά εκδίδεται μια «Ειδοποίηση Αποστολής» σύμφωνα με την Προσθήκη «1» του παρόντος Παραρτήματος.

θ. Αρμοδιότητες Αποδεκτών

Περιγράφονται οι αρμοδιότητες κάθε αποδέκτη του σχεδίου μεταφοράς για την έγκριση της μεταφοράς και τον έλεγχο όλων των συνοδευτικών εγγράφων και:

(1) Ενημερώνεται ο αποστολέας για τυχόν μεταβολές στα δρομολόγια ή στις μεθόδους που καθορίζονται στο σχέδιο.

(2) Ενημερώνεται ο αποστολέας για τυχόν συμφωνίες στα έγγραφα ή ελλείψεις στην φόρτωση.

(3) Δηλώνεται σαφώς στους αποδέκτες η ανάγκη για άμεση ενημέρωση των ΕΑΑ/ ΔΑΑ του αποστολέα για τυχόν διαπιστωμένη ή πιθανή υποκλοπή ΕΔΠΥ ή για τυχόν άλλες κρίσιμες καταστάσεις που μπορεί να θέσουν σε κίνδυνο τη μεταφορά.

ι. Λεπτομέρειες Κινήσεων ΕΔΠΥ

Η παρούσα ενότητα περιλαμβάνει τα εξής θέματα :

(1) Καθορισμό των σημείων συγκεντρώσεως αποστολών.

(2) Ανάγκες συσκευασίας που συμφωνούν με τους κανόνες Εθνικής ασφαλείας των συμμετεχόντων στο πρόγραμμα. Εξηγούνται οι ανάγκες για έγγραφα αποστολής, σφραγίδες, αποδείξεις, αποθήκευση και φοριαμούς ασφαλείας και να δηλώνεται κάθε ειδική ανάγκη των συμμετεχόντων στο πρόγραμμα / έργο.

(3) Απαιτούμενη αλληλογραφία για τα σημεία αποστολής.

(4) Έγγραφα εξουσιοδοτήσεως μεταφορέων και ρυθμίσεις μεταφορών.

(5) Διαδικασίες φύλαξης, σφράγισης, ελέγχου και αποστολής φόρτωσης. Περιγραφή των διαδικασιών, των σημείων φόρτωσης, περιλαμβανομένων και των αρχείων καταμέτρησης, των ευθυνών εποπτείας και έλεγχο των ρυθμίσεων καταμετρητής και φόρτωσης.

(6). Διαδικασίες πρόσβασης του μεταφορέα στα φορτία καθ’ οδόν.

(7) Διαδικασίες εκφόρτωσης στον τόπο προορισμού, οι οποίες περιλαμβάνουν καθορισμό των αποδεκτών και διαδικασίες αλλαγής συνοδών και ρυθμίσεις παραλαβής.

(8) Διαδικασίες έκτακτης επικοινωνίας. Καταγραφή καταλλήλων αριθμών τηλεφώνου και αρμοδίων χειριστών για ειδοποίηση σε περίπτωση έκτακτης ανάγκης.

(9) Διαδικασίες καθορισμού κάθε αποστολής και παροχής λεπτομερειών αυτής, ενώ η ειδοποίηση διαβιβάζεται όχι λιγότερο από δέκα (10) εργάσιμες ημέρες πριν από την διακίνηση- μεταφορά του ΕΔΠΥ.

(10) Σε περίπτωση έκτακτης ανάγκης, το διαβαθμισμένο υλικό καταστρέφεται με μέριμνα του εξουσιοδοτημένου προσωπικού εφόσον τέτοια ενέργεια κρίνεται αναγκαία προς αποφυγή υποκλοπής και έχει εγκριθεί από τον υπεύθυνο ασφαλείας του οικονομικού φορέα. Στην περίπτωση αυτή, ο υπεύθυνος ασφαλείας του οικονομικού φορέα εφαρμόζει άμεσα τις διαδικασίες του άρθρου 11 του παρόντος κανονισμού.

ια. Επιστροφή ΕΔΠΥ

Στην ενότητα αυτή καθορίζονται οι προϋποθέσεις επιστροφής ΕΔΠΥ προς τον εκδότη - κατασκευαστή ή την αποστέλλουσα χώρα (π.χ εγγύηση, επισκευή, δοκιμή, και αξιολόγηση, κλπ).

Σημείωση: Υποδείγματα αυτών των εντύπων περιλαμβάνονται, ως κρίνεται απαραίτητο, ως συνημμένα στο πεδίο.

(1) Κατάλογος συσκευασίας.

(2) Αποδείξεις ΕΔΠΥ.

(3) Λογαριασμοί φορτώσεων.

(4) Δήλωση εξαγωγής.

(5) Φορτωτικές.

(6) Άλλα απαιτούμενα έντυπα.

ιβ. Ειδοποίηση Αποστολής ΕΔΠΥ

(1) Όταν καταρτίζεται ένα σχέδιο μεταφορών προς υποστήριξη ενός

προγράμματος, έργου, ή συμβάσεως το οποίο προβλέπει περισσότερες από μια Διεθνείς αποστολές ΕΔΠΥ, απαιτείται μία διαδικασία καθορισμού ταυτότητας και παροχής λεπτομερειών κάθε αποστολής στον αποδέκτη, στο προσωπικό μεταφορών και στο προσωπικό που χρησιμοποιείται για την εξασφάλιση της ασφαλείας της αποστολής.

(2) Ο υπεύθυνος ασφαλείας της αποστέλλουσας εγκατάστασης διαβιβάζει, με πρόσφορο τρόπο, την «ειδοποίηση αποστολής» στον υπεύθυνο ασφαλείας της υπηρεσίας, ή του οικονομικού φορέα παραλήπτριας Χώρας καθώς και τις αρμόδιες Αρχές Ασφαλείας κάθε συμμετέχουσας Χώρας στο πρόγραμμα- έργο. Αντίγραφα της ειδοποιήσεως αποστέλλονται / χορηγούνται σε άλλες κρατικές υπηρεσίες ή οικονομικούς φορείς αναλόγως, καθώς και στον εξουσιοδοτημένο μεταφορέα των ΕΔΠΥ.

(3) Τύπος ειδοποίησης αποστολής, όπως στην Προσθήκη «1».

Αντιναύαρχος Ιωάννης Δρυμούσης ΠΝ
Υπαρχηγός

Ακριβές Αντίγραφο

Ασμχος (ΕΑ) Νικόλαος Ζήκος
Επιτελής ΓΕΕΘΑ/Ε3/1

ΠΡΟΣΘΗΚΕΣ

«1» Ειδοποίηση Αποστολής

ΓΕΝΙΚΟ ΕΠΙΤΕΛΕΙΟ ΕΘΝΙΚΗΣ ΑΜΥΝΑΣ
Ε’ ΚΛΑΔΟΣ
ΔΝΣΗ ΑΣΦΑΛΕΙΑΣ
07 Σεπ 20

ΠΡΟΣΘΗΚΗ «1» ΣΤΟ ΠΑΡΑΡΤΗΜΑ «Β»
του ΕΚΒΑ

ΕΙΔΟΠΟΙΗΣΗ ΑΠΟΣΤΟΛΗΣ

(Ονομασία Προγράμματος/ Έργου)

ΣΧΕΤΙΚΟ ΕΓΚΕΚΡΙΜΕΝΟ ΣΧΕΔΙΟ ΜΕΤΑΦΟΡΩΝ

Απαντήστε πριν την : (ημερομηνία)

1. Αποστολέας /παραλήπτης (..... όνομα, τηλέφωνο και διεύθυνση του ατόμου (α) υπεύθυνα για την αποστολή/ παράδοση και στους δύο τόπους).

2. Διοριζόμενοι Κυβερνητικοί Αντιπρόσωποι : (..... όνομα, τηλέφωνο και διευθύνσεις των εξουσιοδοτημένων αντιπροσώπων για αποστολή / παράδοση, αναλόγως).

3. Περιγραφή Αποστολής

α. Αριθμός συμβάσεως, διακήρυξη προσφοράς.

β. Άδεια εξαγωγής ή μνεία άλλης εξουσιοδοτημένης εισαγωγής.

γ. Περιγραφή αποστολής ..... (περιγράψτε τα αντικείμενα προς αποστολή και τη διαβάθμιση ασφαλείας τους).

δ. Περιγραφή Συσκευασίας.

(1) Τύπος συσκευασίας (ξύλο, χαρτόνι, μέταλλο κλπ).

(2) Αριθμός κιβωτίων.

(3) Αριθμός εσώκλειστων διαβαθμισμένων ειδών σε κάθε κιβώτιο.

(4) Διαστάσεις/ βάρος κιβωτίου : (μήκος, πλάτος, ύψος και βάρος).

ε. Αναφέρατε εάν το κιβώτιο περιέχει εύφλεκτα υλικά.

4. Δρομολόγιο Αποστολής/Παράδοσης:

α. Ημερομηνία/ώρα της αναχώρησης:

β. Ημερομηνία/πιθανή ώρα άφιξης:

γ. Διαδρομές που πρόκειται να χρησιμοποιηθούν μεταξύ σημείου προέλευσης, σημείο εξαγωγής, σημείο εισαγωγής και τελικός προορισμός: (Προσδιορίστε συγκεκριμένα σημεία μεταβιβάσεως, χρησιμοποιήστε τους κωδικούς που βρίσκονται στο σχέδιο μεταφορά, αναλόγως).

δ. Μέθοδοι μεταφοράς για κάθε μέρος της αποστολής (όνομα, τηλέφωνο, διευθύνσεις όλων των μεταφορέων και αριθμό πτήσης, τρένου ή πλοίου, αναλόγως).

ε. Πρακτορείο μεταφορών / αντιπρόσωποι (Όνομα, τηλέφωνο, διευθύνσεις εταιρειών εάν δεν προσδιορίζονται στο σχέδιο μεταφορών).

Σημείωση : Ο Αποστολέας εξακριβώνει εκ νέου την εξουσιοδότηση ασφαλείας και να βεβαιώνει για την ικανότητα των ανωτέρων πριν τους αναθέσει την αποστολή του υλικού.

στ. Τελωνεία ή σημεία ασφαλείας λιμένος (κατάσταση ονομάτων και τηλέφωνα εάν είναι διαφορετικά από τις εγκεκριμένες διαδικασίες του σχεδίου μεταφοράς).

5. Ονόματα και ταυτότητα του εξουσιοδοτημένου συνοδού.

Αντιπτέραρχος (Ι) Ιωάννης Γκοντικούλης
Επιτελάρχης

Ακριβές Αντίγραφο

Ασμχος (ΕΑ) Νικόλαος Ζήκος
Επιτελής ΓΕΕΘΑ/Ε3/1

ΓΕΝΙΚΟ ΕΠΙΤΕΛΕΙΟ ΕΘΝΙΚΗΣ ΑΜΥΝΑΣ
Ε’ ΚΛΑΔΟΣ
ΔΝΣΗ ΑΣΦΑΛΕΙΑΣ
07 Σεπ 20

ΠΑΡΑΡΤΗΜΑ «Γ» ΣΤΟΝ
ΕΚΒΑ

ΣΧΕΔΙΟ ΑΣΦΑΛΕΙΑΣ ΕΓΚΑΤΑΣΤΑΣΗΣ ΟΙΚΟΝΟΜΙΚΟΥ ΦΟΡΕΑ

Το σχέδιο ασφαλείας του οικονομικού φορέα συντάσσεται από τον υπεύθυνο ασφαλείας, σύμφωνα με τις διατάξεις του παρόντα Κανονισμού και περιλαμβάνει τα παρακάτω σημεία στα οποία αναγράφονται:

1. Σκοπός

Η οργάνωση και η εξασφάλιση της φυσικής ασφάλειας, της ασφάλειας προσωπικού, καθώς και της πυρασφάλειας των εγκαταστάσεων του οικονομικού φορέα, για την αποτροπή μη εξουσιοδοτημένης πρόσβασης, διαρροής και καταστροφής ΕΔΠΥ.

2. Κατάσταση

α. Παράγοντες Απειλών

Παράγοντας απειλής θεωρείται ο οποιοσδήποτε μη εξουσιοδοτημένος επιχειρεί να συλλέξει πληροφορίες ή να προκαλέσει δολιοφθορά με οποιοδήποτε τρόπο στις εγκαταστάσεις του οικονομικού φορέα. Οι ενέργειες από τις οποίες ιδίως προέρχεται κίνδυνος για την ασφάλεια των ΕΔΠΥ είναι οι ακόλουθες:

(1) Κατασκοπεία

(2) Ανατρεπτικές Ενέργειες

(3) Προπαγάνδα

(4) Δολιοφθορές

(5) Τρομοκρατία

(6) Ασύμμετρες Απειλές

(7) Οργανωμένο Έγκλημα

(8) Κυβερνοεπιθέσεις

β. Προσωπικό – Διατιθέμενα Μέσα Προστασίας

(1) Στοιχεία υπεύθυνου ασφαλείας και βοηθών του.

(2) Κατάσταση με τα στοιχεία του προσωπικού του οικονομικού φορέα που κατέχει εξουσιοδότηση ασφαλείας και του προσωπικού που εκτελεί χρέη φύλαξης ή προσωπικού της ΙΕΠΥΑ.

(3) Υπάρχοντα μέτρα ασφαλείας εγκαταστάσεων και σχεδιαγράμματα στα οποία απεικονίζονται.

(4) Υπάρχοντα μέτρα ασφαλείας υπαρχείου, χώρων ασφαλείας και σχεδιαγράμματα στα οποία απεικονίζονται.

(5) Υπάρχοντα συστήματα πυρασφαλείας, υλικά πυροσβέσεως και σχεδιαγράμματα στα οποία απεικονίζονται.

(6) Στοιχεία επικοινωνίας με Τμήματα της ΕΛ.ΑΣ, του ΛΣ-ΕΛ.ΑΚΤ και της Πυροσβεστικής Υπηρεσίας.

(7) Στοιχεία επικοινωνίας με άλλους συνεργαζόμενους αρμόδιους φορείς ή οικονομικούς φορείς, όπως ΔΑΑ, ΙΕΠΥΑ, υπεργολάβους.

(8) Περαιτέρω μέσα προστασίας που χρησιμοποιούνται.

3. Καθήκοντα

α. Καθήκοντα υπευθύνου ασφαλείας και των βοηθών του.

β. Καθήκοντα προσωπικού φύλαξης.

4. Εκτέλεση

α. Διαδικασίες ελέγχου εισόδου/εξόδου προσωπικού και οχημάτων στις εγκαταστάσεις του οικονομικού φορέα.

β. Διαδικασίες ελέγχου πρόσβασης προσωπικού σε χώρους ασφαλείας και στο υπαρχείο.

γ. Διαδικασίες προστασίας των ΕΔΠΥ σε έκτακτες ανάγκες, όπως πυρκαγιά και πλημμύρα.

δ. Διαδικασίες αντιμετώπισης εισβολέα.

ε. Ενέργειες σε περίπτωση διαρροής ΕΔΠΥ.

στ. Ενέργειες του προσωπικού για την προστασία των ΕΔΠΥ, κατά την αποχώρησή του από τους χώρους εργασίας.

ζ. Περαιτέρω διαδικασίες που ακολουθούνται για την προστασία ΕΔΠΥ.

5. Σχέδιο Εκκενώσεως Χώρων Ασφαλείας/Υπαρχείου

Σύμφωνα με την Προσθήκη «1» του Παραρτήματος «Γ».

Αντιναύαρχος Ιωάννης Δρυμούσης ΠΝ
Υπαρχηγός

Ακριβές Αντίγραφο

Ασμχος (ΕΑ) Νικόλαος Ζήκος
Επιτελής ΓΕΕΘΑ/Ε3/1

ΠΡΟΣΘΗΚΕΣ

«1» Σχέδιο Εκκενώσεως Χώρων Ασφαλείας/Υπαρχείου

ΓΕΝΙΚΟ ΕΠΙΤΕΛΕΙΟ ΕΘΝΙΚΗΣ ΑΜΥΝΑΣ
Ε’ ΚΛΑΔΟΣ
ΔΝΣΗ ΑΣΦΑΛΕΙΑΣ
07 Σεπ 20

ΠΡΟΣΘΗΚΗ «1» ΣΤΟ ΠΑΡΑΡΤΗΜΑ «Γ»
του ΕΚΒΑ

ΣΧΕΔΙΟ ΕΚΚΕΝΩΣΕΩΣ ΧΩΡΩΝ ΑΣΦΑΛΕΙΑΣ/ΥΠΑΡΧΕΙΟΥ

Το σχέδιο εκκενώσεως χώρων ασφαλείας/υπαρχείου ασφαλείας του οικονομικού φορέα συντάσσεται από τον υπεύθυνο ασφαλείας, σύμφωνα με τις διατάξεις του παρόντα Κανονισμού και περιλαμβάνει τα παρακάτω σημεία στα οποία αναγράφονται:

1. Σκοπός

Η διάσωση των ΕΔΠΥ που φυλάσσονται στους χώρους ασφαλείας/ υπαρχείο, ώστε να μην περιέλθουν στα χέρια αναρμόδιων προσώπων, σε περιπτώσεις έκτακτης ανάγκης, όπως πυρκαγιά και πλημμύρα. Το σχέδιο εφαρμόζεται παρουσία του υπευθύνου ασφαλείας ή βοηθού του.

2. Κατάσταση

α. Προσωπικό

Στοιχεία υπεύθυνου ασφαλείας και βοηθών του.

β. Υλικά - Μέσα

(1) Πυροσβεστήρας

(2) Πέλεκυς

(3) Φωτισμός ασφαλείας

(4) Σάκος/κιβώτιο μεταφοράς

(5) Οχήματα μεταφοράς

3. Εκτέλεση

α. Σειρά προτεραιότητας και μέσα απομάκρυνσης ΕΔΠΥ.

β. Διαδικασίες εκκένωσης/απογραφής και μεταφοράς ΕΔΠΥ σε χώρο φύλαξης.

γ. Καθορισμένοι χώροι φύλαξης ΕΔΠΥ μετά την εκκένωση, όπως Στρατιωτική Μονάδα, είτε Αστυνομικό Τμήμα ή σε άλλη διαβαθμισμένη εγκατάσταση του οικονομικού φορέα.

Αντιπτέραρχος (Ι) Ιωάννης Γκοντικούλης
Επιτελάρχης

Ακριβές Αντίγραφο

Ασμχος (ΕΑ) Νικόλαος Ζήκος
Επιτελής ΓΕΕΘΑ/Ε3/1

ΓΕΝΙΚΟ ΕΠΙΤΕΛΕΙΟ ΕΘΝΙΚΗΣ ΑΜΥΝΑΣ
Ε’ ΚΛΑΔΟΣ
ΔΝΣΗ ΑΣΦΑΛΕΙΑΣ
07 Σεπ 20

ΠΑΡΑΡΤΗΜΑ «Δ» ΣΤΟΝ
ΕΚΒΑ

ΠΡΟΔΙΑΓΡΑΦΕΣ ΑΣΦΑΛΕΙΑΣ ΕΓΚΑΤΑΣΤΑΣΕΩΝ - ΥΠΑΡΧΕΙΟΥ

1. Τα μέτρα φυσικής ασφάλειας εφαρμόζονται προκειμένου να εξασφαλιστεί η φυσική προστασία κατά του εκτιμώμενου κινδύνου. Κατά τη διαδικασία διαχείρισης κινδύνων συνεκτιμώνται οι παρακάτω παράγοντες:

α. Το επίπεδο διαβάθμισης της ΕΔΠΥ.

β. Η μορφή και η ποσότητα της ΕΔΠΥ.

γ. Ο περιβάλλων χώρος και η δομή των κτιρίων ή των χώρων στέγασης της ΕΔΠΥ.

δ. Η εκτιμώμενη απειλή δολιοφθοράς, τρομοκρατικών, ανατρεπτικών ή άλλων εγκληματικών δραστηριοτήτων.

2. Οι χώροι ασφαλείας πληρούν τις παρακάτω προϋποθέσεις:

α. Είναι σαφώς καθορισμένοι και προστατεύονται περιμετρικά, με τρόπο ώστε να ελέγχεται η είσοδος και έξοδος προσωπικού, υλικού και μέσων. Επίσης έχει καθοριστεί σαφώς το επίπεδο διαβάθμισης του κάθε χώρου, ανάλογα με την κατηγορία των ΕΔΠΥ και της εκτελούμενης εργασίας.

β. Υπάρχει κατάλληλη σήμανση, όπως γράμματα, αριθμοί, ή χρώματα και να διαθέτουν τα απαραίτητα μέσα ελέγχου προσωπικού, είτε ηλεκτρονικά είτε φύλακες ή συνδυασμός αυτών, ώστε να επιτρέπεται η είσοδος εργασίας μόνο σε αντίστοιχα εγκεκριμένο προσωπικό.

γ. Ασυνόδευτη πρόσβαση επιτρέπεται μόνο στα πρόσωπα, βάσει της αρχής «ανάγκη γνώσης», με προσήκουσα εξουσιοδότηση ασφαλείας και ειδική κάρτα εισόδου η οποία φέρει φωτογραφία και στοιχεία πιστοποίησης.

δ. Όλα τα άλλα άτομα συνοδεύονται διαρκώς ή υποβάλλονται σε ανάλογους ελέγχους.

ε. Στην περίπτωση που η είσοδος σε χώρο ασφαλείας συνεπάγεται άμεση πρόσβαση στις ΕΔΠΥ που φυλάσσονται στον οικείο χώρο, ισχύουν τα ακόλουθα:

(1) Αναφέρεται- αναγράφεται με σαφήνεια το επίπεδο ανώτατης διαβάθμισης ασφάλειας των ΕΔΠΥ που φυλάσσονται στο χώρο.

(2) Όλοι οι επισκέπτες έχουν ειδική άδεια εισόδου στο χώρο, συνοδεύονται διαρκώς και έχουν λάβει την προσήκουσα εξουσιοδότηση ασφαλείας, εκτός εάν ληφθούν μέτρα τα οποία καθιστούν αδύνατη την πρόσβαση σε ΕΔΠΥ.

στ. Οι εισερχόμενοι ελέγχονται ώστε να μη φέρουν οποιαδήποτε συσκευή λήψης φωτογραφιών [κινητό τηλέφωνο, φωτογραφική μηχανή ή μηχανή λήψεως (βιντεοκάμερα)], ή εξωτερική μονάδα αποθήκευσης Η/Υ.

ζ. Στην περίπτωση που απαιτείται η είσοδος φορητού Η/Υ ή εξωτερική μονάδα αποθήκευσης, για εργασίες / λόγους σύμβασης- έργου, ο υπεύθυνος ασφαλείας ελέγχει τα ανωτέρω συστήματα για τυχόν διαρροές ή τοποθέτησης κακόβουλου λογισμικού.

η. Να προβλέπεται διαδικασία επιθεώρησης των χώρων από ειδικά καθορισμένο προσωπικό, ώστε τόσο κατά τη διάρκεια όσο και με το πέρας της εργασίας, να διαπιστώνεται η εφαρμογή των προβλεπόμενων κανόνων ασφαλείας.

3. Οι οικονομικοί φορείς ανάλογα με τις εγκαταστάσεις τους κατατάσσονται στις παρακάτω κατηγορίες:

α. Συγκρότημα Κτιρίων (τα οποία ευρίσκονται στον αυτό περιφραγμένο χώρο) με περίβολο.

β. Μεμονωμένο κτίριο

(1) Με περίβολο

(2) Χωρίς περίβολο

γ. Σε όροφο κτιρίου.

4. Οι προδιαγραφές ασφαλείας των εγκαταστάσεων των οικονομικών φορέων προκειμένου να προστατευτούν οι χώροι ασφαλείας, εντός των οποίων πρόκειται να γίνει ο χειρισμός ΕΔΠΥ βαθμού ασφαλείας «ΕΜΠΙΣΤΕΥΤΙΚΟ» και άνω, ανά κατηγορία, είναι οι εξής:

α. Συγκρότημα κτιρίων / μεμονωμένο κτίριο με περίβολο

(1) Περιμετρική περίφραξη ύψους τουλάχιστον δύο (2) μέτρων.

(2) Επαρκής εσωτερικός και περιμετρικός φωτισμός.

(3) Συσκευές ανίχνευσης- παρείσφρησης εισβολών: Γίνεται χρήση ηλεκτρονικών συστημάτων συναγερμών, κλειστού κυκλώματος τηλεόρασης (control room) με αποθήκευση των δεδομένων που καταγράφονται σε σκληρό δίσκο ή καταγραφικό, για χρονικό διάστημα που καθορίζεται από τον οικονομικό φορέα (όχι λιγότερο από 15 ημέρες) καθώς και άλλων ηλεκτρονικών συσκευών, όπως είναι οι ανιχνευτές χώρου, τα αντικραδασμικά, οι μαγνητικές επαφές, τα «beams», τα οποία λειτουργούν με μόνιμη παροχή ηλεκτρικής ισχύος και με εφεδρική πηγή.

(4) Φύλακες: Επιλέγονται άτομα εκπαιδευμένα και κατάλληλα εξουσιοδοτημένα τα οποία εκτελούν αποκλειστικά την εργασία αυτή. Τις εργάσιμες ημέρες και ώρες χρέη φύλακα δύναται να εκτελεί και οποιοδήποτε κατάλληλα εκπαιδευμένο προσωπικό του οικονομικού φορέα. Εκδίδονται οδηγίες για τα καθήκοντα και το χώρο ευθύνης εκάστου φύλακα. Παρέχεται επαρκής επιτήρηση του χώρου καθ’ όλο το 24ώρο με ικανό αριθμό φυλάκων σε συνδυασμό με τα υπάρχοντα ηλεκτρονικά μέσα ανιχνεύσεως συναγερμού. Έκτος από τους φύλακες δύναται να χρησιμοποιηθούν και σκοποί, καθ’ όλο το 24ωρο.

(5) Περίπολοι: Οι περίπολοι στους χώρους εγκατάστασης του οικονομικού φορέα γίνονται εκτός του ωραρίου εργασίας καθημερινά σύμφωνα με καθορισμένο σχέδιο, που έχει εκπονηθεί από τον υπεύθυνο ασφαλείας του οικονομικού φορέα.

(6) Έλεγχος εισόδου:

(α) Για όλο το συγκρότημα υπάρχει μόνο μία κύρια πύλη εισό-

δου - εξόδου ελέγχου προσωπικού, οχημάτων και επισκεπτών.

(β) Ο έλεγχος διενεργείται από προσωπικό ασφαλείας ή από υπάλληλο υποδοχής.

(γ) Κάρτα ασφαλείας προσωπικού: Κάρτα η οποία φέρεται από το σύνολο του προσωπικού στην οποία περιέχεται φωτογραφία και στοιχεία για την πιστοποίηση του ώστε να εξασφαλίζεται η είσοδος μόνο στους επιτρεπόμενους γι’ αυτό χώρους.

(δ) Ειδοποιείται το τμήμα που ζητάει ο επισκέπτης και μετά την αποδοχή της επίσκεψης καταγράφονται τα στοιχεία του επισκέπτου στο βιβλίο επισκεπτών στο οποίο αναγράφονται τα στοιχεία ταυτότητας του επισκέπτη, η ιδιότητα του, η ώρα εισόδου - εξόδου και ο τόπος προορισμού.

(ε) Ο επισκέπτης επιδεικνύει κατά την είσοδό του την ταυτότητα, ή άλλο επίσημο έγγραφο πιστοποίησης των στοιχείων του, πχ. διαβατήριο, δίπλωμα οδήγησης.

(στ) Χορήγηση κάρτας επισκέπτη, αριθμημένης σύμφωνα με τα στοιχεία του στο βιβλίο επισκεπτών, με υπόδειξη την υποχρεωτική ανάρτησή της σε εμφανές σημείο καθ’ όλη τη διάρκεια της επίσκεψης.

(ζ) Εκτελείται έλεγχος των οχημάτων κατά την είσοδο-στάθμευση- έξοδο σύμφωνα με τις οδηγίες του υπευθύνου ασφαλείας.

(7) Άλλο φυσικό μέτρο: κάθε άλλο κατάλληλο μέτρο που συμβάλει στην ανίχνευση ή παρεμπόδιση της πρόσβασης μη εξουσιοδοτημένων ατόμων σε διαβαθμισμένο χώρο ή ακόμα και την αποτροπή απώλειας ή φθοράς της ΕΔΠΥ.

β. Μεμονωμένο κτίριο χωρίς περίβολο

(1) Μέτρα ασφαλείας ώστε να αποκλείεται με οιονδήποτε τρόπο πρόσβαση από τυχόν παράπλευρα κτίρια, (κιγκλιδώματα όπου είναι δυνατή η πρόσβαση στο κτίριο συμπεριλαμβανομένων ταρατσών και μπαλκονιών, εξωτερική πόρτα ασφαλείας κλπ).

(2) Επαρκής εσωτερικός και εξωτερικός φωτισμός.

(3) Συσκευές ανίχνευσης- παρείσφρησης εισβολών: Γίνεται χρήση ηλεκτρονικών συστημάτων συναγερμών, κλειστού κυκλώματος τηλεόρασης (control room) με αποθήκευση των δεδομένων που καταγράφονται σε σκληρό δίσκο ή καταγραφικό, για χρονικό διάστημα που καθορίζεται από τον οικονομικό φορέα (όχι λιγότερο από 15 ημέρες) καθώς και άλλων ηλεκτρονικών συσκευών, όπως είναι οι ανιχνευτές χώρου, τα αντικραδασμικά, οι μαγνητικές επαφές, τα «beams», τα οποία λειτουργούν με μόνιμη παροχή ηλεκτρικής ισχύος και με εφεδρική πηγή.

(4) Φύλακες: Επιλέγονται άτομα εκπαιδευμένα και κατάλληλα εξουσιοδοτημένα τα οποία εκτελούν αποκλειστικά την εργασία αυτή. Εκδίδονται οδηγίες για τα καθήκοντα και το χώρο ευθύνης εκάστου φύλακα. Παρέχεται επαρκής επιτήρηση του χώρου καθ’ όλο το 24ώρο με ικανό αριθμό φυλάκων σε συνδυασμό με τα υπάρχοντα ηλεκτρονικά μέσα ανιχνεύσεως συναγερμού.

(5) Έλεγχος εισόδου:

(α) Για το κτίριο υπάρχει μόνο μία κύρια πύλη εισόδου - εξόδου ελέγχου προσωπικού και επισκεπτών.

(β) Ο έλεγχος διενεργείται από προσωπικό ασφαλείας ή από υπάλληλο υποδοχής.

(γ) Κάρτα ασφαλείας προσωπικού: Κάρτα η οποία φέρεται από το σύνολο του προσωπικού στην οποία περιέχεται φωτογραφία και στοιχεία για την πιστοποίηση του ώστε να εξασφαλίζεται η είσοδος μόνο στους επιτρεπομένους γι’ αυτό χώρους.

(δ) Ειδοποιείται το τμήμα που ζητάει ο επισκέπτης και μετά την αποδοχή της επίσκεψης καταγράφονται τα στοιχεία του επισκέπτου στο βιβλίο επισκεπτών στο οποίο αναγράφονται τα στοιχεία ταυτότητας του επισκέπτη, η ιδιότητα του, η ώρα εισόδου - εξόδου και ο τόπος προορισμού.

(ε) Ο επισκέπτης επιδεικνύει κατά την είσοδό του την ταυτότητα, ή άλλο επίσημο έγγραφο πιστοποίησης των στοιχείων του, πχ. διαβατήριο, δίπλωμα οδήγησης.

(στ) Χορήγηση κάρτας επισκέπτη, αριθμημένης σύμφωνα με τα στοιχεία του στο βιβλίο επισκεπτών, με υπόδειξη την υποχρεωτική ανάρτησή της σε εμφανές σημείο καθ’ όλη τη διάρκεια της επίσκεψης.

(6) Άλλο φυσικό μέτρο: κάθε άλλο κατάλληλο μέτρο που συμβάλει στην ανίχνευση ή παρεμπόδιση της πρόσβασης μη εξουσιοδοτημένων ατόμων σε διαβαθμισμένο χώρο ή ακόμα και την αποτροπή απώλειας ή φθοράς της ΕΔΠΥ.

γ. Σε όροφο κτιρίου

(1) Μέτρα ασφαλείας ώστε να αποκλείεται με οιονδήποτε τρόπο πρόσβαση από τυχόν παράπλευρα κτίρια, (κιγκλιδώματα όπου είναι δυνατή η πρόσβαση στο κτίριο συμπεριλαμβανομένων ταρατσών και μπαλκονιών, εξωτερική πόρτα ασφαλείας κλπ).

(2) Επαρκής εσωτερικός και εξωτερικός φωτισμός.

(3) Συσκευές ανίχνευσης- παρείσφρησης εισβολών: Γίνεται χρήση ηλεκτρονικών συστημάτων συναγερμών, κλειστού κυκλώματος τηλεόρασης (control room) με αποθήκευση των δεδομένων που καταγράφονται σε σκληρό δίσκο ή καταγραφικό, για χρονικό διάστημα που καθορίζεται από τον οικονομικό φορέα (όχι λιγότερο από 15 ημέρες) καθώς και άλλων ηλεκτρονικών συσκευών, όπως είναι οι ανιχνευτές χώρου, τα αντικραδασμικά, οι μαγνητικές επαφές, τα «beams», τα οποία λειτουργούν με μόνιμη παροχή ηλεκτρικής ισχύος και με εφεδρική πηγή.

(4) Έλεγχος εισόδου:

(α) Υπάρχει μόνο μία κύρια πύλη εισόδου - εξόδου ελέγχου προσωπικού και επισκεπτών.

(β) Ο έλεγχος διενεργείται από προσωπικό ασφαλείας ή από υπάλληλο υποδοχής.

(γ) Κάρτα ασφαλείας προσωπικού: Κάρτα η οποία φέρεται από το σύνολο του προσωπικού στην οποία περιέχεται φωτογραφία και στοιχεία για την πιστοποίηση του ώστε να εξασφαλίζεται η είσοδος μόνο στους επιτρεπομένους γι’ αυτό χώρους.

(δ) Ειδοποιείται το τμήμα που ζητάει ο επισκέπτης και μετά την αποδοχή της επίσκεψης καταγράφονται τα στοιχεία του επισκέπτου στο βιβλίο επισκεπτών στο οποίο αναγράφονται τα στοιχεία ταυτότητας του επισκέπτη, η ιδιό-

τητα του, η ώρα εισόδου - εξόδου και ο τόπος προορισμού.

(ε) Ο επισκέπτης επιδεικνύει κατά την είσοδό του την ταυτότητα, ή άλλο επίσημο έγγραφο πιστοποίησης των στοιχείων του, πχ. διαβατήριο, δίπλωμα οδήγησης.

(στ) Χορήγηση κάρτας επισκέπτη, αριθμημένης σύμφωνα με τα στοιχεία του στο βιβλίο επισκεπτών, με υπόδειξη την υποχρεωτική ανάρτησή της σε εμφανές σημείο καθ’ όλη τη διάρκεια της επίσκεψης.

(5) Άλλο φυσικό μέτρο: κάθε άλλο κατάλληλο μέτρο που συμβάλει στην ανίχνευση ή παρεμπόδιση της πρόσβασης μη εξουσιοδοτημένων ατόμων σε διαβαθμισμένο χώρο ή ακόμα και την αποτροπή απώλειας ή φθοράς της ΕΔΠΥ.

5. Οι προδιαγραφές ασφαλείας του υπαρχείου είναι οι εξής:

α. Η θέση του Υπαρχείου εντός του οικονομικού φορέα είναι τέτοια ώστε να αποτρέπεται η εύκολη και χωρίς έλεγχο πρόσβαση σε αυτό. Ο χώρος του Υπαρχείου είναι κατασκευασμένος από στερεό συμπαγές και αδιαπέραστο υλικό. Στην περίπτωση που σε κάποια επιφάνεια υφίστανται μη συμπαγή υλικά (π.χ. παράγωγα ξύλου, γυψοσανίδα κλπ), αυτή απαιτείται να διαθέτει ενδιάμεσο ισχυρό μεταλλικό πλέγμα που να δύναται να ελεγχθεί.

β. Υπάρχει μία μόνο είσοδος με πόρτα ασφαλείας μεγάλης αντοχής η οποία ασφαλίζεται με κλειδαριά ασφαλείας και σύστημα εισόδου με μαγνητική κάρτα ή με πληκτρολόγιο (access control). Η είσοδος εποπτεύεται εξωτερικά του υπαρχείου από κλειστό κύκλωμα τηλεόρασης (control room) με αποθήκευση των δεδομένων που καταγράφονται σε σκληρό δίσκο ή καταγραφικό, για χρονικό διάστημα που καθορίζεται από τον οικονομικό φορέα (όχι λιγότερο από 15 ημέρες).

γ. Αν υπάρχει παράθυρο, φέρει απαραιτήτως εξωτερικό σιδερένιο κιγκλίδωμα από συμπαγές υλικό, εσωτερικά του οποίου να υπάρχει αδιαφανές παραπέτασμα όπως κουρτίνες, χαρτόνι ή άλλα καλύμματα, για να αποτρέπεται η οπτική παρατήρηση.

δ. Λειτουργεί σύστημα ηλεκτρονικού συναγερμού με αυτόνομη πηγή ενέργειας, για αντιμετώπιση διακοπής παροχής ηλεκτρικού ρεύματος. Επιπλέον, διαθέτει ηχητικό σήμα και συνδέεται με το χώρο διανυκτέρευσης του προσωπικού ασφαλείας. Σε περίπτωση που δεν υφίσταται προσωπικό ασφαλείας, απαιτείται να συνδέεται είτε με εξουσιοδοτημένη ΙΕΠΥΑ είτε με το πλησιέστερο Αστυνομικό Τμήμα.

ε. Η ηλεκτρική εγκατάσταση είναι μελετημένη για πρόληψη πυρκαγιάς από βραχυκύκλωμα.

στ. Υπάρχει εξωτερικά και εσωτερικά πυροσβεστήρας.

ζ. Υπάρχει πέλεκυς και καταστροφέας εγγράφων, αποκλειστικά τύπου cross/cut.

η. Υπάρχει αναρτημένο το σχέδιο εκκενώσεως υπαρχείου.

θ. Τοποθετείται χαλύβδινος/οι φωριαμός/οι (πακτωμένος/οι), τριπλού συστήματος ασφαλείας (κλειδαριά, συνδυασμός και μπάρα με λουκέτο) με τις παρακάτω προϋποθέσεις:

(1) Το ΕΔΠΥ «ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ» δεν συνυπάρχουν σε φωρια-

μούς με άλλο μικρότερου βαθμού ασφαλείας.

(2) Οι συνδυασμοί των φωριαμών είναι γνωστοί μόνο στον υπεύθυνο ασφαλείας και στους βοηθούς του.

(3) Οι συνδυασμοί αλλάζουν όταν γίνεται αντικατάσταση του υπεύθυνου ασφαλείας ή του βοηθού του, καθώς και κατά την κρίση τους ανάλογα με τις ειδικές συνθήκες που αντιμετωπίζονται. Κάθε αλλαγή, καθώς και οι λόγοι που την επιβάλλουν καταχωρείται (χωρίς την αναγραφή του συνδυασμού) σε βιβλίο και θεωρείται από τον υπεύθυνο ασφαλείας.

ι. Υπάρχει βιβλίο στο οποίο αναγράφονται τα πλήρη στοιχεία κάθε εισερχομένου στον χώρο (ονοματεπώνυμο, σκοπός εισόδου, ημερομηνία, ώρα εισόδου/εξόδου) και υπογράφεται από τον εισερχόμενο και τον υπεύθυνο ασφαλείας ή τον αναπληρωτή του.

ια. Η συντήρηση και καθαριότητα του χώρου γίνεται πάντα παρουσία του υπεύθυνου ασφαλείας ή των βοηθών του.

ιβ. Δεν επιτρέπεται η εισαγωγή εντός του υπαρχείου εξωτερική μονάδας αποθήκευσης Η/Υ, καθώς και οποιασδήποτε συσκευής λήψης φωτογραφιών, όπως κινητό τηλέφωνο, φωτογραφική μηχανή, μηχανή λήψεως.

Αντιναύαρχος Ιωάννης Δρυμούσης ΠΝ
Υπαρχηγός

Ακριβές Αντίγραφο

Ασμχος (ΕΑ) Νικόλαος Ζήκος
Επιτελής ΓΕΕΘΑ/Ε3/1

ΓΕΝΙΚΟ ΕΠΙΤΕΛΕΙΟ ΕΘΝΙΚΗΣ ΑΜΥΝΑΣ
Ε’ ΚΛΑΔΟΣ
ΔΝΣΗ ΑΣΦΑΛΕΙΑΣ
07 Σεπ 20

ΠΑΡΑΡΤΗΜΑ «Ε» ΣΤΟΝ
ΕΚΒΑ

ΔΙΑΔΙΚΑΣΙΑ ΕΠΙΛΟΓΗΣ ΚΑΙ ΕΞΟΥΣΙΟΔΟΤΗΣΗΣ ΑΣΦΑΛΕΙΑΣ ΠΡΟΣΩΠΙΚΟΥ

1. Το προσωπικό που πρόκειται να αποκτήσει πρόσβαση σε ΕΔΠΥ απαιτείται να εξουσιοδοτηθεί με διαβάθμιση αντίστοιχη του βαθμού ασφαλείας αυτών.

2. Για το ανωτέρω προσωπικό πραγματοποιείται από τον υπεύθυνο ασφαλείας και άλλα αρμόδια όργανα του οικονομικού φορέα μία αρχική εκτίμηση / έλεγχος για την καταλληλόλητά του να αποκτήσει πρόσβαση και να χειρίζεται ΕΔΠΥ.

3. Το προσωπικό υποβάλλει στον οικονομικό φορέα Αντίγραφο Ποινικού Μητρώου και Υπεύθυνη Δήλωση ότι δεν έχει υποπέσει σε κάποιο από τα αδικήματα που αποτελούν κωλύματα, σύμφωνα με το άρθρο 7 του παρόντος κανονισμού και στην περίπτωση εξουσιοδότησης ασφαλείας ΝΑΤΟ και ΕΕ να πληροί τα κριτήρια που προβλέπονται στα αντίστοιχα θεσμικά κείμενα.

4. Σε συνέχεια του ανωτέρω ελέγχου συμπληρώνονται μηχανογραφημένα, υπογράφονται και ελέγχονται ως προς την πληρότητα και την ορθότητα τα εξής:

α. Πίνακας προσωπικών στοιχείων (Υπόδειγμα 1) σε τρία αντίτυπα.

β. Υπεύθυνη δήλωση εξουσιοδότησης (Υπόδειγμα 2) σε ένα αντίτυπο.

γ. Δελτίο υποβολής στοιχείων καταλληλότητας (Υπόδειγμα 3) σε ένα αντίτυπο.

5. Τα ανωτέρω δικαιολογητικά υποβάλλονται στη ΔΑΑ, η οποία αφού τα ελέγξει ως προς την πληρότητα και την ορθότητα, τα διαβιβάζει στην ΕΑΑ για ενέργειες αρμοδιότητάς της.

6. Η ΕΑΑ διαβιβάζει τα απαραίτητα δικαιολογητικά σε αρμόδιες αρχές, προκειμένου να προβούν στον έλεγχο ασφαλείας του προσωπικού του οικονομικού φορέα, για την έκδοση της εξουσιοδότησης ασφαλείας.

7. Οι εξουσιοδοτήσεις ασφαλείας αποστέλλονται από την ΕΑΑ στη ΔΑΑ και εν συνεχεία στον υπεύθυνο ασφαλείας του οικονομικού φορέα, ο οποίος ενημερώνει αφενός το μητρώο καταχωρήσεως εξουσιοδοτημένου προσωπικού (Υπόδειγμα 4), και αφετέρου το προσωπικό που εξουσιοδοτείται, ενώ τοποθετεί το σχετικό έγγραφο στο φάκελο εξουσιοδοτήσεως ασφαλείας προσωπικού.

8. Η ισχύς των εξουσιοδοτήσεων δεν μπορεί να υπερβαίνει τα δέκα (10) έτη, ενώ η αντίστοιχη διάρκεια για βαθμό ΑΠ και άνω, δεν μπορεί να υπερβαίνει τα πέντε (5) έτη, με έναρξη την ημερομηνία έκδοσής τους. Για την ανανέωση των εξουσιοδοτήσεων εκδηλώνονται εγκαίρως (έξι μήνες προ της λήξεως ισχύος) οι ενέργειες των παραγράφων 2 έως 5 του παρόντος Παραρτήματος.

9. Όταν έχουν εκδηλωθεί εγκαίρως οι ενέργειες για την ανανέωση εξουσιοδότησης ασφαλείας προσωπικού από τον οικονομικό φορέα και η απαραίτητη έρευνα ασφαλείας δεν έχει ολοκληρωθεί, η ΕΑΑ δύναται να παρατείνει την ισχύ της τρέχουσας εξουσιοδότησης ασφαλείας για διάστημα έως δώδεκα (12) μηνών.

10. Σε περίπτωση παραβάσεων ασφαλείας ή απολύσεως ή παραιτήσεως εξουσιοδοτημένου προσωπικού εφαρμόζεται η διαδικασία άρσης εξουσιοδότησης, σύμφωνα με το άρθρο 7 του παρόντος.

11. Σε κάθε περίπτωση άρσης εξουσιοδότησης ο υπεύθυνος ασφαλείας ενημερώνει το εμπλεκόμενο προσωπικό επί των υποχρεώσεών του και ιδιαίτερα ότι συνεχίζει να διαφυλάττει το περιεχόμενο των ΕΔΠΥ που περιήλθε σε γνώση του από οποιαδήποτε διαρροή με υπαιτιότητα του.

Αντιναύαρχος Ιωάννης Δρυμούσης ΠΝ
Υπαρχηγός

Ακριβές Αντίγραφο

Ασμχος (ΕΑ) Νικόλαος Ζήκος
Επιτελής ΓΕΕΘΑ/Ε3/1

ΓΕΝΙΚΟ ΕΠΙΤΕΛΕΙΟ ΕΘΝΙΚΗΣ ΑΜΥΝΑΣ
Ε’ ΚΛΑΔΟΣ
ΔΝΣΗ ΑΣΦΑΛΕΙΑΣ
07 Σεπ 20

ΠΑΡΑΡΤΗΜΑ «ΣΤ» ΣΤΟΝ
ΕΚΒΑ

ΟΔΗΓΙΕΣ ΧΕΙΡΙΣΜΟΥ ΕΔΠΥ

1. Σκοπός

α. Η παροχή οδηγιών για:

(1) Τη σωστή και ασφαλή διακίνηση των ΕΔΠΥ, μέσα και έξω από τον οικονομικό φορέα.

(2) Τη διαφύλαξη, την αρχειοθέτηση, την αναπαραγωγή ή και την καταστροφή αυτών.

β. Η διατύπωση γενικών κανόνων ασφαλείας για τις ΕΔΠΥ.

2. Κατηγορίες ΕΔΠΥ

α. Κάθε πληροφορία η οποία απαιτείται να προστατεύεται από αποκάλυψη σε μη εξουσιοδοτημένα άτομα.

β. Κάθε μηχανολογικό αντικείμενο ή εξοπλισμός είτε κατασκευασμένο είτε στο στάδιο παρασκευής, που λόγω του περιεχομένου του απαιτεί προστασία ανάλογου βαθμού.

γ. Γραπτά κείμενα (χειρόγραφα, δακτυλογραφημένα ή τυπωμένα) μαγνητικές ταινίες ή δίσκους, φωτογραφίες, χάρτες, διαγράμματα, σχέδια, σκίτσα, σημειώσεις και όλα τα παράγωγά τους, άσχετα προς τον τόπο αναπαραγωγής τους), στα οποία φέρεται διαβάθμιση ασφαλείας.

δ. Κάθε ήχος, φωνή ή ηλεκτρονική ηχητική εγγραφή.

ε. Λογισμικό ηλεκτρονικού υπολογιστή ή δεδομένα, καθώς και τα μέσα αποθήκευσης, μεταφοράς και μετάδοσης αυτών, που περιέχουν διαβαθμισμένες πληροφορίες.

3. Βασικές Αρχές Ασφαλείας για την Προστασία των ΕΔΠΥ

α. Το προσωπικό το οποίο λόγω των καθηκόντων του λαμβάνει γνώση ΕΔΠΥ έχει την ανάλογη εξουσιοδότηση ασφαλείας.

β. Πριν επιτραπεί σε κάποιον από το προσωπικό του οικονομικού φορέα να διαχειριστεί ΕΔΠΥ, πρέπει, πλέον της εξουσιοδότησής του, να ενημερωθεί για τις διαδικασίες ασφαλείας καθώς και τους κινδύνους που ενδέχεται να προκύψουν από παραλείψεις.

γ. Κάθε άτομο που χειρίζεται ΕΔΠΥ φέρει προσωπική ευθύνη για τον τρόπο χρήσης – εκμετάλλευσης αυτής.

δ. Το προσωπικό του οικονομικού φορέα δεν γνωστοποιεί ΕΔΠΥ σε άλλα πρόσωπα, εφ’ όσον δεν απαιτείται, ακόμη και αν αυτά έχουν κατάλληλη εξουσιοδότηση ασφαλείας.

ε. Με βάση τη θεμελιώδη αρχή «ανάγκη γνώσης» ο χειρισμός και η γνώση ΕΔΠΥ περιορίζεται στο αποκλειστικά απαραίτητο να λάβει γνώση προσωπικό.

στ. Όταν μη εξουσιοδοτημένο προσωπικό είναι παρόν για οποιαδήποτε λόγο σε χώρο ασφαλείας απαιτείται να συνοδεύεται από εξουσιοδοτημένο προσωπικό για την προστασία των ΕΔΠΥ.

ζ. Η διαβίβαση του περιεχομένου των ΕΔΠΥ μέσω τηλεφώνου ή τηλεομοιοτυπίας (FAX) ή άλλη συσκευής χωρίς κρυπτοπροστασία δεν επιτρέπεται. Το Γραφείο ασφαλείας του οικονομικού φορέα λαμβάνει μέτρα για την αποφυγή διαβίβασης ΕΔΠΥ με μέσα χωρίς κρυπτοπροστασία αντίστοιχου βαθμού ασφαλείας.

θ. Κάθε ΕΔΠΥ διαβάθμισης «ΑΠΟΡΡΗΤΟ» και άνω, όταν δεν χρησιμοποιείται φυλάσσεται στο υπαρχείο του οικονομικού φορέα, σε μεταλλικούς φωριαμούς ασφαλείας, ειδικά κτισμένα σε τοίχο ή πάτωμα.

ι. Η απόθεση των κλειδιών των φωριαμών που περιέχουν ΕΔΠΥ πάνω σε γραφεία και γενικά όπου δεν υπάρχει συνεχής επίβλεψη αρμόδιου εξουσιοδοτημένου προσωπικού δεν επιτρέπεται.

4. Γενικές Αρχές Ασφαλείας για τη Διακίνηση ΕΔΠΥ

α. Όταν ΕΔΠΥ, ανεξάρτητα από το βαθμό ασφαλείας που φέρει, παραλαμβάνεται από τον οικονομικό φορέα, με οποιαδήποτε τρόπο και μέσο, ο υπεύθυνος ασφαλείας ελέγχει τα στοιχεία του συνοδευτικού εγγράφου, τα στοιχεία της σχετικής απόδειξης παραλαβής (αν υπάρχει), τον αριθμό των αντιτύπων και τα συνημμένα (αν υπάρχουν). Αν διαπιστώσει μη τήρηση των προβλεπόμενων διαδικασιών, ειδοποιεί άμεσα τη Διεύθυνση του οικονομικού φορέα και τον αποστολέα.

β. Η καταγραφή / καταχώρηση των συνοδευτικών εγγράφων των ΕΔΠΥ, γίνεται στα ανάλογα πρωτόκολλα που τηρούνται στον οικονομικό φορέα, ο οποίος τηρεί χωριστά πρωτόκολλα για κάθε βαθμό ασφαλείας.

γ. Η αποστολή των ΕΔΠΥ, εφόσον πρόκειται για διακίνηση έγγραφης πληροφορίας, γίνεται μέσα σε μη διαφανείς φακέλους, ενώ στην περίπτωση διακίνησης υλικού, αυτή λαμβάνει χώρα σε μη διαφανή συσκευασία αντίστοιχα.

δ. Οι ΕΔΠΥ που φέρουν έγγραφη μορφή και έχουν διαβάθμιση ασφαλείας από «ΑΠΟΡΡΗΤΟ» και άνω τοποθετούνται πάντοτε σε δύο (2) φακέλους. Ο εξωτερικός φάκελος δεν φέρει καμία ένδειξη βαθμού ασφαλείας, παρά μόνο τον αποστολέα, αριθμό φακέλου ή πρωτοκόλλου και τα στοιχεία του παραλήπτη. Ο εσωτερικός φάκελος έχει την ένδειξη ασφαλείας του εγγράφου και τα στοιχεία του παραλήπτη. Αν απευθύνεται ονομαστικά σε φυσικό πρόσωπο επιδίδεται σε αυτό μετά από καταγραφή των στοιχείων του φακέλου στο σχετικό πρωτόκολλο.

ε. Έγγραφα που αφορούν σε ΕΔΠΥ, με βαθμό ασφαλείας «ΑΠΟΡΡΗΤΟ» και άνω, χρεώνονται από τον υπεύθυνο ασφαλείας στα διάφορα τμήματα με σχετική απόδειξη (Υπόδειγμα 8). Η απόδειξη συντάσσεται σε τρία αντίτυπα, τα δύο εκ των οποίων συνοδεύουν το έγγραφο, ενώ το τρίτο παραμένει στο τμήμα που το αποστέλλει. Ο παραλήπτης υπογράφει και επιστρέφει την απόδειξη στον αποστολέα. Η διαδικασία αυτή εφαρμόζεται και στην περίπτωση που ΕΔΠΥ αποστέλλεται σε αποδέκτη εκτός του οικονομικού φορέα.

στ. Η ανωτέρω διαδικασία εφαρμόζεται από κάθε τμήμα, όταν λόγω του περιεχομένου του διαβαθμισμένου εγγράφου επιβάλλεται να το λάβουν και άλλα τμήματα ή πρόσωπα εντός του τμήματος ή του οικονομικού φορέα. Οι γραμματείες

των τμημάτων είναι υπεύθυνες για τη διακίνηση των διαβαθμισμένων εγγράφων προς τα άλλα τμήματα και την συμπλήρωση ξεχωριστής απόδειξης εσωτερικής διακίνησης (Υπόδειγμα 8), σημειώνοντας στο πρωτόκολλο τα ονόματα των χειριστών και την ημερομηνία παράδοσης/παραλαβής.

ζ. Η απόδειξη εσωτερικής διακίνησης είναι ανεξάρτητη από το βιβλίο χρέωσης αλληλογραφίας της γραμματείας του οικονομικού φορέα.

η. Η μεταφορά ΕΔΠΥ βαθμού ασφαλείας «ΑΠΟΡΡΗΤΟ» και άνω, από γραφείο σε γραφείο, γίνεται με εξουσιοδοτημένο προσωπικό και καλυμμένο με τέτοιο τρόπο, ώστε να αποκλείεται η παρατήρηση του περιεχομένου τους.

θ. Η αποστολή ΕΔΠΥ με απλό ταχυδρομείο δεν επιτρέπεται. Πάντα χρησιμοποιείται ειδικός αγγελιοφόρος – μεταφορέας με εξουσιοδότηση ασφαλείας ανάλογου βαθμού.

ι. Σε περίπτωση διαβαθμισμένου εγγράφου με την ένδειξη ΠΡΟΣΩΠΙΚΟ, το γραφείο διακίνησης αλληλογραφίας του οικονομικού φορέα συμπληρώνει στην απόδειξη διακίνησης τα στοιχεία του ταχυδρομικού φακέλου που περιέχει το έγγραφο.

ια. Μεταφορά ΕΔΠΥ εκτός του οικονομικού φορέα (σε επαγγελματικά ταξίδια, συναντήσεις κλπ) πραγματοποιείται κατόπιν έγκρισης του υπευθύνου ασφαλείας. Ο συνοδός των ΕΔΠΥ μεριμνά για την ασφαλή φύλαξη και προστασία αυτών.

ιβ. Η χρήση μέσων μαζικής μεταφοράς πρέπει, κατά το δυνατόν, να αποφεύγεται για την μεταφορά ΕΔΠΥ.

ιγ. Η μεταφορά ΕΔΠΥ εκτός του οικονομικού φορέα για εργασία στο σπίτι δεν επιτρέπεται.

ιδ. Τα βιβλία καταχώρησης και οι αποδείξεις διακίνησης ΕΔΠΥ, φυλάσσονται για δέκα (10) χρόνια, εκτός εάν αλλιώς ορίζεται, με την παρέλευση των οποίων καταστρέφονται με μέσο που δεν εμπεριέχει κίνδυνο διαρροής του περιεχομένου αυτών. Η καταστροφή των ΕΔΠΥ, βαθμού «ΑΠΟΡΡΗΤΟ» και άνω, συνοδεύεται από σχετικό πρωτόκολλο καταστροφής.

ιε. Σε περίπτωση αδυναμίας παράδοσης ΕΔΠΥ στον παραλήπτη αυτό επιστρέφεται στον οικονομικό φορέα που το απέστειλε.

5. Παραγωγή ΕΔΠΥ

α. Ο βαθμός ασφαλείας, στην περίπτωση ΕΔΠΥ σε μορφή εγγράφου ή στο συνοδευτικό έγγραφο, τίθεται δακτυλογραφημένος και υπογραμμισμένος σαν πρώτη ένδειξη, με κεφαλαία γράμματα στο πάνω αριστερό και στο κάτω δεξιό μέρος κάθε σελίδας.

β. Ο βαθμός ασφαλείας δίδεται από τον εκδότη και ανταποκρίνεται στην αξία και σπουδαιότητα του εγγράφου.

γ. ΕΔΠΥ βαθμού ασφαλείας «ΑΠΟΡΡΗΤΟ» και άνω, σφραγίζονται με σφραγίδα κεφαλαίων γραμμάτων και κόκκινο μελάνι στο άνω και κάτω περιθώριο της σελίδας.

δ. ΕΔΠΥ που φέρουν βαθμό ασφαλείας «ΕΜΠΙΣΤΕΥΤΙΚΟ» σφραγίζονται με σφραγίδα κεφαλαίων γραμμάτων και μπλε μελάνι στο άνω και κάτω περιθώριο της σελίδας.

ε. ΕΔΠΥ που φέρουν σφραγίδα ασφαλείας με χαρακτηρισμό «ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ» σφραγίζονται με μαύρο μελάνι.

στ. ΕΔΠΥ που φέρουν περισσότερους του ενός βαθμούς ασφαλείας, τα εξώφυλλα ή σημειώματα διανομής σφραγίζονται με το μεγαλύτερο βαθμό διαβάθμισης που περιλαμβάνουν.

ζ. Σχήματα και εικόνες μεγάλων διαστάσεων έχουν τις κατάλληλες σημάνσεις διαβάθμισης στο πάνω και κάτω μέρος τους και σε κάθε εξώφυλλο ή κάλυμμα. Η ακριβής τοποθέτηση των βασικών επιπρόσθετων σημάνσεων διαβάθμισης γίνεται έτσι ώστε να είναι απολύτως ορατές ανεξαρτήτως της μορφής ή συσκευασίας τους.

η. Εκτός από τον αριθμό φακέλου (ή αριθμό σχεδίου/ πρωτοκόλλου) και την ημερομηνία, κάθε έγγραφο έχει τον Αριθμό Εκδοθέντων Αντιτύπων (ΑΕΑ) και τον Αύξοντα Αριθμό Αντιτύπου (ΑΑΑ) (για τα έγγραφα με βαθμό ασφαλείας «ΑΠΟΡΡΗΤΟ» και πάνω). Και οι δυο αυτοί αριθμοί σημειώνονται στο πάνω δεξιό μέρος της σελίδας. Εάν κριθεί αναγκαίο, μερικοί ή όλοι οι αποδέκτες να λάβουν περισσότερα από ένα αντίγραφο του εγγράφου, τίθενται απέναντι σε κάθε ένα από αυτούς και μέσα σε παρένθεση, ο αριθμός των αποστελλομένων σε αυτούς αντιγράφων.

θ. Ο πίνακας αποδεκτών αναγράφεται στην τελευταία σελίδα.

ι. Κάθε σελίδα αριθμείται και αναγράφεται ο αριθμός σελίδας και το σύνολο των σελίδων (πχ. σελίδα 3 από σελίδες 5).

ια. Τα διαβιβαστικά έγγραφα, λαμβάνουν τον ανώτερο βαθμό ασφαλείας, σύμφωνα με τον βαθμό ασφαλείας των συνημμένων και των παραρτημάτων ή προσθηκών τους.

ιβ. Ο βαθμός ασφαλείας ενός εγγράφου μπορεί να αναβιβασθεί, υποβιβασθεί ή απαλειφθεί, όταν προκύψουν ή εκλείψουν οι λόγοι, που επέβαλαν την αρχική διαβάθμισή του. Δικαίωμα υποβιβασμού, αναβιβασμού του βαθμού ασφαλείας ενός εγγράφου ή της αποδιαβαθμίσεώς του έχει μόνο ο εκδότης.

ιγ. Όταν ένα (1) διαβιβαστικό έγγραφο έχει ανάλογη διαβάθμιση λόγω του υψηλού βαθμού ασφαλείας των συνημμένων του, τότε ο εκδότης του εγγράφου γράφει ως τελευταία παράγραφο του κειμένου την φράση «Όταν αποχωρισθούν τα συνημμένα, ο βαθμός ασφαλείας αυτού του εγγράφου υποβιβάζεται σε (γράφεται ο νέος βαθμός ασφαλείας)». Αυτό επιβάλλεται ιδιαίτερα στην περίπτωση, που το διαβιβαστικό έγγραφο κοινοποιείται σε μερικούς αποδέκτες χωρίς συνημμένα και επομένως δεν απαιτείται ιδιαίτερος χειρισμός του από αυτούς.

6. Αναπαραγωγή ΕΔΠΥ

α. Η αναπαραγωγή ΕΔΠΥ από το Βαθμό «ΑΠΟΡΡΗΤΟ» και άνω δεν επιτρέπεται χωρίς γραπτή άδεια του εκδότη.

β. Όλα τα αναπαραγόμενα αντίγραφα διαβαθμισμένων εγγράφων των ΕΔΠΥ, λαμβάνουν τον ίδιο βαθμό ασφαλείας με το πρωτότυπο και αριθμούνται.

γ. Η αναπαραγωγή ΕΔΠΥ βαθμού ασφαλείας έως «ΕΜΠΙΣΤΕΥΤΙΚΟ», επιτρέπεται μόνο κατόπιν εντολής και ευθύνης των Διευθυντών των τμημάτων τα οποία χρειάζονται τα αντίγραφα.

δ Υπεύθυνο και αρμόδιο τμήμα για την αναπαραγωγή διαβαθμισμένων εγγράφων των ΕΔΠΥ είναι η Γραμματεία, εκτός αν ορίζεται διαφορετικά από τον

οικονομικό φορέα και επιτρέπεται μόνο κατόπιν εντολής Διευθυντών των τμημάτων τα οποία πρόκειται να χειριστούν τα αντίγραφα.

ε. Η αναπαραγωγή πραγματοποιείται σε μηχανήματα που έχουν τοποθετηθεί σε χώρους ασφαλείας που έχουν εγκριθεί για αντιγραφή ή αναπαραγωγή ΕΔΠΥ. Όλα τα άλλα μηχανήματα αντιγραφής ή αναπαραγωγής φέρουν εμφανή ένδειξη στην οποία αναγράφεται ότι αντιγραφή υλικών σε επίπεδο διαβάθμισης από «ΕΜΠΙΣΤΕΥΤΙΚΟ» και άνω απαγορεύεται αυστηρά. Αναπαραγωγή εγγράφων έως βαθμού «ΕΜΠΙΣΤΕΥΤΙΚΟ» επιτρέπεται μόνο μετά από εντολή και ευθύνη των Διευθυντών των τμημάτων τα οποία χρειάζονται τα αντίγραφα.

στ. Η αναπαραγωγή γίνεται αποκλειστικά από εξουσιοδοτημένο προσωπικό ιδίου βαθμού ασφαλείας με την ΕΔΠΥ.

ζ. Όλα τα έγγραφα των ΕΔΠΥ είτε αυτά είναι αυθεντικά, είτε είναι αντίγραφα, είτε ελλιπή λόγω λανθασμένης αναπαραγωγής καθώς και όλα τα υλικά (καρμπόν, μελανοταινίες, φύλλα χαρτιού κλπ) που χρησιμοποιήθηκαν για την αναπαραγωγή, παραδίνονται στο γραφείο ασφαλείας προς φύλαξη ή καταστροφή.

η. Αρίθμηση και Χειρισμός Αναπαραγόμενων ΕΔΠΥ

(1) Η αρίθμηση και καταγραφή του αναπαραγομένου υλικού πραγματοποιείται αμέσως μετά την αναπαραγωγή και ακολουθεί τους γενικούς κανόνες των ΕΔΠΥ. Περαιτέρω αρίθμηση και καταγραφή χρησιμοποιείται για να διακρίνονται τα αυθεντικά από τα αντίγραφα.

(2) Οι αιτήσεις αντιγραφής ελέγχονται από το υπεύθυνο τμήμα για τη διακίνηση της αλληλογραφίας του οικονομικού φορέα (π,.χ. Γραμματεία, ή άλλο) και τηρούνται στο πρωτόκολλο καταγραφής.

(3) Όλα τα αντίγραφα εγγράφων των ΕΔΠΥ από βαθμό ασφαλείας «ΑΠΟΡΡΗΤΟ» και άνω έχουν τον βαθμό ασφαλείας τυπωμένο με σφραγίδα σε κόκκινο μελάνι στο πάνω και κάτω περιθώριο κάθε σελίδας.

7. Αποθήκευση και Φύλαξη ΕΔΠΥ

α. Τα ΕΔΠΥ βαθμού ασφαλείας «ΑΠΟΡΡΗΤΟ» και άνω φυλάσσονται στο υπαρχείο σε φωριαμούς ασφαλείας.

β. Όλα τα έγγραφα των ΕΔΠΥ βαθμού ασφαλείας ΕΤΝΑ, αρχειοθετούνται και φυλάσσονται στο υπαρχείο, όπου και γίνεται και ο χειρισμός τους.

γ. ΕΔΠΥ βαθμού ασφαλείας έως και «ΕΜΠΙΣΤΕΥΤΙΚΟ», τηρούνται από τον οικονομικό φορέα σε χώρους ανάλογης διαβάθμισης.

8. Καταστροφή ΕΔΠΥ

α. Η έννοια της καταστροφής σημαίνει ότι μετά από αυτήν τα ΕΔΠΥ λαμβάνουν τέτοια μορφή (τεμαχισμός, καταστροφή με φωτιά, τέλειος διαμελισμός) ώστε να είναι αδύνατη η αναπαραγωγή τους ή η εξαγωγή από αυτά οποιασδήποτε πληροφορίας. ΕΔΠΥ βαθμού ασφαλείας ΕΤΝΑ καταστρέφονται μόνο με φωτιά.

β. Η καταστροφή ΕΔΠΥ χωρίς γραπτή άδεια του εκδότη δεν επιτρέπεται.

γ. Η εκκαθάριση του Αρχείου από ΕΔΠΥ που δεν είναι πλέον σε ισχύ είναι επιβεβλημένη.

δ. Όταν ένα ΕΔΠΥ μεταφέρεται για καταστροφή, καταστρέφεται την ίδια μέρα της μεταφοράς του. ή τηλεομοιοτυπίας (FAX) ή άλλη συσκευής.

ε. Πλεονάζοντα αντίτυπα ΕΔΠΥ, υλικά που χρησιμοποιήθηκαν για την αναπαραγωγή τους, καθώς και πρόχειρα ή βοηθητικά έγγραφα που σχετίζονται με ΕΔΠΥ, όπως σχεδιαγράμματα, χειρόγραφες σημειώσεις και μοντέλα, καταστρέφονται με μέσο που δεν εμπεριέχει κίνδυνο διαρροής τους.

ζ. Η καταστροφή γίνεται παρουσία τριών (3) ατόμων του οικονομικού φορέα, ανάλογης εξουσιοδότησης, από τους οποίους ο ένας είναι ο αρμόδιος χειριστής των ΕΔΠΥ.

η. Κατά την καταστροφή των εγγράφων συντάσσεται πρωτόκολλο καταστροφής εις τριπλούν (Υπόδειγμα 9). Ένα αντίγραφο αποστέλλεται στον εκδότη, ένα τηρείται σε φάκελο πρωτοκόλλων καταστροφής διαβαθμισμένων εγγράφων και το τρίτο στο φάκελο (ή μέρος) από τον οποίο πάρθηκε το έγγραφο.

θ. Η καταστροφή των εγγράφων (εκκαθάριση του Αρχείου) γίνεται στο τέλος του έτους ή όταν απαιτείται.

9. Χειρισμός ΕΔΠΥ «ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ»

Για το χειρισμό ΕΔΠΥ βαθμού ασφαλείας «ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ» εφαρμόζονται τα ακόλουθα:

α. Μετά την πάροδο 30 ετών η διαβάθμιση ακυρώνεται, εκτός και αν αναφέρεται διαφορετικά στο κείμενο.

β. Δεν απαιτείται εξουσιοδότηση ασφάλειας προσωπικού για το χειρισμό τους, ενώ εφαρμόζεται η αρχή «ανάγκη γνώσης».

γ. Φυλάσσονται σε μέρη τα οποία ασφαλίζονται, ακόμα και με απλές κλειδαριές των συρταριών των γραφείων. Εφόσον δεν είναι δυνατόν να ασφαλιστούν, λόγω μεγέθους ή αριθμού, ασφαλίζεται ολόκληρος ο χώρος.

δ. Ο αριθμός των αντιγράφων, εφ’ όσον απαιτούνται, παραμένει στο ελάχιστο.

ε. Επιτρέπεται η χρήση των απλών μηχανών για αντιγραφή.

στ. Καταστρέφονται με τρόπο ώστε να μην υπάρχει κίνδυνος διαρροής τους.

10. Έλεγχος Παραβάσεων Ασφαλείας

α. Το προσωπικό του οικονομικού φορέα που καταλαμβάνεται να χειρίζεται ΕΔΠΥ χωρίς την προσήκουσα εξουσιοδότηση ή κατά παράβαση των οριζόμενων στον παρόντα Κανονισμό, τιμωρείται σύμφωνα με τις εκάστοτε εφαρμοζόμενες διατάξεις της ποινικής νομοθεσίας, ιδίως τα άρθρα 139, 146 έως 149 και 152 του Ποινικού Κώδικα.

β. Το προσωπικό του οικονομικού φορέα που έχει πρόσβαση σε ΕΔΠΥ υποχρεούται να ενημερώνει, αν έχει πληροφόρηση, τον υπεύθυνο ασφαλείας για κάθε διαρροή ή «προσπάθεια» διαρροής τους. Η πληροφόρηση αφορά σε συμβάντα που διαπιστώνονται ή ενδέχεται να πραγματοποιηθούν τόσο εντός όσο και εκτός του οικονομικού φορέα κατά τη διάρκεια ή μη του εργάσιμου ωραρίου.

Αντιναύαρχος Ιωάννης Δρυμούσης ΠΝ
Υπαρχηγός

Ακριβές Αντίγραφο

Ασμχος (ΕΑ) Νικόλαος Ζήκος
Επιτελής ΓΕΕΘΑ/Ε3/1

ΓΕΝΙΚΟ ΕΠΙΤΕΛΕΙΟ ΕΘΝΙΚΗΣ ΑΜΥΝΑΣ
Ε’ ΚΛΑΔΟΣ
ΔΝΣΗ ΑΣΦΑΛΕΙΑΣ
07 Σεπ 20

ΠΑΡΑΡΤΗΜΑ «Ζ» ΣΤΟΝ
ΕΚΒΑ

ΚΑΤΑΣΤΑΣΗ ΤΗΡΟΥΜΕΝΩΝ ΕΝΤΥΠΩΝ - ΒΙΒΛΙΩΝ

1. Βιβλίο Επισκεπτών Οικονομικού Φορέα
2. Βιβλίο Εισερχομένων Υπαρχείου
3. Βιβλίο Ενημερώσεων Διαβαθμισμένου Προσωπικού
4. Φάκελος Απορρήτων Εγγράφων
5. Πρωτόκολλο Εισερχομένων Εγγράφων
6. Φάκελος Αποδείξεων Διακίνησης Εγγράφων
7. Βιβλίο Ελέγχου Επιθεωρήσεων
8. Μητρώο Πυροσβεστήρων
9. Βιβλίο - Μητρώο Καταχώρησης Εξουσιοδοτημένου Προσωπικού
10. Φάκελος Πρωτοκόλλων Καταστροφής
11. Φάκελος Υπεύθυνων Δηλώσεων και Αντίγραφα Ποινικού Μητρώου Προσωπικού (παράγραφος 3, Παραρτήματος «Ε»), τα οποία τηρούνται σε φοριαμό ασφαλείας στο Υπαρχείο.
12. Φάκελος Εξουσιοδοτήσεων Ασφαλείας Προσωπικού

Αντιναύαρχος Ιωάννης Δρυμούσης ΠΝ
Υπαρχηγός

Ακριβές Αντίγραφο

Ασμχος (ΕΑ) Νικόλαος Ζήκος
Επιτελής ΓΕΕΘΑ/Ε3/1

ΓΕΝΙΚΟ ΕΠΙΤΕΛΕΙΟ ΕΘΝΙΚΗΣ ΑΜΥΝΑΣ
Ε’ ΚΛΑΔΟΣ
ΔΝΣΗ ΑΣΦΑΛΕΙΑΣ
07 Σεπ 20

ΠΑΡΑΡΤΗΜΑ «Η» ΣΤΟΝ
ΕΚΒΑ

ΗΛΕΚΤΡΟΜΑΓΝΗΤΙΚΗ ΠΡΟΣΤΑΣΙΑ

1. Όλα τα ηλεκτρονικά – ηλεκτρικά μέσα και συστήματα, εκπέμπουν ανεπιθύμητη ακτινοβολία, η οποία μπορεί να διαδοθεί δια μέσου του χώρου και κατά μήκος αγώγιμων επιφανειών που βρίσκονται πλησίον των λειτουργουσών συσκευών, καθώς και δια μέσου άλλων καναλιών εκπομπής (όπως τηλεφωνικές γραμμές, γραμμές μεταφοράς ηλεκτρικής ενέργειας, κάθοδοι κεραιών, συστήματα συναγερμού). Αυτή η ακτινοβολία μπορεί να υποκλαπεί από ένα ραδιοδέκτη ευρισκόμενο σε κάποια απόσταση μακριά από το μέσον.

2. Η διαδικασία ανάλυσης και μελέτης των ανεπιθύμητων και επικίνδυνων για την ασφάλεια διαφευγουσών ακτινοβολιών καλείται TEMPEST. Ο όρος TEMPEST, χρησιμοποιείται επίσης για να περιγράψει τα φαινόμενα αυτά, καθώς και τους μηχανισμούς καταστολής τους. Τα μέτρα και οι πολιτικές για τα θέματα TEMPEST καθορίζονται από την Εθνική Αρχή για θέματα TEMPEST (N.T.A) που είναι η ΕΥΠ. Βασίζονται δε στα ειδικά εγχειρίδια που έχει εκδώσει το ΝΑΤΟ και η Ευρωπαϊκή Ένωση. Ειδικότερα, το ΝΑΤΟ έχει εκδώσει ειδικά εγχειρίδια (SDIP-27, SDIP-28), με οδηγίες για τον τρόπο διεξαγωγής των μετρήσεων TEMPEST, τα οποία αναφέρουν επίσης και τα όρια εντός των οποίων οι μετρήσεις αυτές εμπίπτουν, ώστε οι αντίστοιχες συσκευές να είναι αποδεκτές από τα Κράτη – Μέλη, καθώς επίσης και εγχειρίδια που αφορούν στα κριτήρια σχεδιασμού και στις προδιαγραφές ασφαλούς εγκατάστασης εξοπλισμού που επεξεργάζεται διαβαθμισμένες πληροφορίες (SDIP-29). Η Ευρωπαϊκή Ένωση έχει εκδώσει τις οδηγίες IASG 07-01, IASG 07-02 και IASG 07-03.

3. Η δυνατότητα υποκλοπής διαφευγουσών ακτινοβολιών, οι αποστάσεις διαδόσεως τους, καθώς και η δυνατότητα αναλύσεώς τους, εξαρτάται από ποικίλους παράγοντες, όπως τη σχεδίαση λειτουργίας των συσκευών επεξεργασίας πληροφοριών, την εγκατάστασή τους, τις περιβαλλοντολογικές συνθήκες που σχετίζονται με τη φυσική τους ασφάλεια και τις συνθήκες ηλεκτρομαγνητικού θορύβου του χώρου. Για τους λόγους αυτούς, ένας αριθμός από τεχνικά μέτρα, λαμβάνεται για την καταστολή αυτών των ακτινοβολιών, οι οποίες αλλιώς είναι τρωτές σε υποκλοπή και άρα σε εκμετάλλευση.

4. Η ηλεκτρομαγνητική απειλή κατά των εγκαταστάσεων και μέσων επικοινωνιών, εξαρτάται από τους εξής παράγοντες:

α. Τις τεχνικές δυνατότητες του αντιπάλου.

β. Το βαθμό κινδύνου στον οποίο εκτίθεται ο αντίπαλος για να πετύχει τους στόχους του.

γ. Τη σημασία που αποδίδει ο αντίπαλος στις πληροφορίες που πρόκειται να συγκεντρώσει.

δ. Την εγγύτητα ή τη δυνατότητα που έχει ο αντίπαλος να προσεγγίσει τις εγκαταστάσεις και τα μέσα, για να πετύχει τους στόχους του.

5. Η δυνατότητα πρόσβασης ή η εγγύτητα που ο αντίπαλος έχει προς τους στόχους του, είναι καθοριστική για τον προσδιορισμό του βαθμού της ηλεκτρομαγνητικής απειλής που αντιμετωπίζουν οι εγκαταστάσεις και τα μέσα επικοινωνιών. Όπου οι εγκαταστάσεις ευρίσκονται σε απόσταση μικρότερη των 100μ. από άλλες «ύποπτες» εγκαταστάσεις, υπάρχουν ειδικές συνθήκες απειλής και λαμβάνονται τα πλέον αυστηρά μέτρα προστασίας.

6. Ελεγχόμενος Χώρος

Είναι ο χώρος τριών διαστάσεων ο οποίος περιβάλλει το υλικό που επεξεργάζεται διαβαθμισμένες πληροφορίες, μέσα στον οποίο η εκμετάλλευση ηλεκτρομαγνητικών ακτινοβολιών δε θεωρείται πρακτικά δυνατή ή υπάρχει αρμόδιο όργανο ασφαλείας για να αναγνωρίσει και να απαγορεύσει μια τέτοια εκμετάλλευση. Οι προδιαγραφές TEMPEST των υλικών, μπορούν να γίνονται ελαστικότερες όσο αυξάνεται ο ελεγχόμενος χώρος σε μία εγκατάσταση.

7. Συμβιβασμένη Ακτινοβολία (Compromising Emanation)

α. Αυτή οφείλεται, είτε σε απ’ ευθείας διασύζευξη στη ζώνη σημάτων, λόγω χωρητικής και επαγωγικής διασύζευξης, λόγω γαλβανισμού, είτε σε δευτερεύουσα διασύζευξη, λόγω διαμορφώσεως των αρμονικών, όπως οι ψηφιακά σταθεροποιημένες συχνότητες ρολογιού. Οι αρμονικές που εκπέμπονται από συσκευές για συχνότητες συγχρονισμού, είναι συνήθως οι στόχοι που προτιμούνται. Μόλις ανιχνευθεί η συχνότητα συγχρονισμού, το προς μέτρηση εύρος ζώνης εφαρμόζεται και ρυθμίζεται προς το σύνολο του εύρους ζώνης.

β. Εάν η αρμονική είναι διαμορφωμένη στη συνολική πληροφορία, είναι εύκολο να εξαχθεί η συμβιβασμένη πληροφορία.

8. Μέτρα Προστασίας

Υπάρχουν ορισμένα μέτρα που μπορούν να εφαρμοστούν εναντίον μίας ηλεκτρομαγνητικής απειλής. Οι παρακάτω παράγραφοι βοηθούν στην επιλογή των μέτρων αυτών:

α. Μέτρα κατά την Εγκατάσταση – Λειτουργία

Τα μέτρα ηλεκτρομαγνητικής προστασίας των χώρων και εγκαταστάσεων επεξεργασίας διαβαθμισμένων πληροφοριών, είναι σε γενικές γραμμές τα εξής:

(1) Σωστή και ασφαλής γείωση των συσκευών.

(2) Χρήση φίλτρων για τον περιορισμό ή αποφυγή εκπεμπόμενης ακτινοβολίας των επικοινωνιακών συσκευών και των γραμμών μεταφοράς.

(3) Διαχωρισμός των διαβαθμισμένων (red) από τα αδιαβάθμητα (black) κυκλώματα επεξεργασίας και διαβίβασης πληροφοριών.

(4) Ηλεκτρομαγνητική θωράκιση των διαβαθμισμένων χώρων και συσκευών.

(5) Αποφυγή τηλεφωνικής εγκατάστασης εντός των χώρων επεξεργασίας διαβαθμισμένων πληροφοριών.

(6) Μη τοποθέτηση των συσκευών και των οθονών πλησίον μεταλλικών επίπλων και παραθύρων.

β. Καθιέρωση Ζωνών Ασφαλείας (Zoning)

Η μέθοδος συνίσταται στην καθιέρωση ζωνών ασφαλείας με βάση την ολική εξασθένιση της ραδιοσυχνότητας που προξενείται στο χώρο μεταξύ της θέσεως που εγκαθίσταται μία συσκευή επικοινωνιών και της πιθανής θέσης εγκαταστάσεως μηχανημάτων υποκλοπής ηλεκτρομαγνητικών ακτινοβολιών, καθώς και στο διαθέσιμο ελεγχόμενο χώρο, ώστε να εξασφαλισθεί ο απαιτούμενος βαθμός προστασίας. Όταν εφαρμοστεί κατάλληλα η μέθοδος των ζωνών ασφάλειας (SDIP-28 και IASG 07-02), τότε αναμένεται ελάττωση του κόστους των εργασιών για τον έλεγχο των ηλεκτρομαγνητικών ακτινοβολιών και επιτρέπει μεγαλύτερη χρήση υλικών εμπορίου, αντί υλικών με στρατιωτικές προδιαγραφές και κατά συνέπεια μικρότερο κόστος συσκευών επικοινωνιών.

γ. Υπόγειες / Προστατευμένες Επικοινωνίες

Ορισμένα μέσα επικοινωνιών είναι εγκατεστημένα σε υπόγειες προστατευμένες εγκαταστάσεις, οι οποίες εκ φύσεως παρέχουν προστασία από τη διαφυγή των ηλεκτρομαγνητικών ακτινοβολιών. Σε τέτοιες εγκαταστάσεις που επιφέρουν ικανοποιητική εξασθένιση στις ηλεκτρομαγνητικές ακτινοβολίες, τα αντίμετρα μπορούν να ελαττωθούν σημαντικά, υπό την προϋπόθεση ότι εφαρμόζονται μέτρα εγκατάστασης σύμφωνα με τις SDIP-29, IASG 07-01 και IASG 07-03 σε γραμμές επικοινωνιών, γραμμές μεταφοράς ηλεκτρικής ισχύος και άλλους αγωγούς που οδηγούνται έξω από την προστατευμένη περιοχή. Πρέπει όμως πάντοτε να ελέγχονται οι χώροι αυτοί, ώστε να διαπιστωθεί ότι είναι κατάλληλοι για εφαρμογή περιορισμένων αντιμέτρων TEMPEST. Σε πολλές περιπτώσεις, οι προστατευμένες εγκαταστάσεις αποτελούν την οικονομικότερη εναλλακτική λύση, αντί της επιλογής υλικών με προδιαγραφές TEMPEST.

δ. Αντίμετρα TEMPEST για Τακτικά Υλικά και Συστήματα

Για συσκευές και υλικά που χρησιμοποιούνται σε ειδικό περιβάλλον, να εφαρμόζονται τα καθοριζόμενα στις SDIP-27, IASG 07-01 και IASG 07-03 ανάλογα με τη συγκεκριμένη περίπτωση. Η εφαρμογή των SDIP-27, IASG 07-01 και IASG 07-03 απαιτεί ιδιαίτερη προσοχή στην εγκατάσταση, ώστε να αποφευχθεί η παρενόχληση (από θόρυβο) του συστήματος ή επαγωγή ακτινοβολιών σε γραμμές επικοινωνιών και ισχύος που οδηγούν έξω από το χώρο των εγκαταστάσεων ή σε παραπλήσιους πομπούς.

Αντιναύαρχος Ιωάννης Δρυμούσης ΠΝ
Υπαρχηγός

Ακριβές Αντίγραφο

Ασμχος (ΕΑ) Νικόλαος Ζήκος
Επιτελής ΓΕΕΘΑ/Ε3/1

ΓΕΝΙΚΟ ΕΠΙΤΕΛΕΙΟ ΕΘΝΙΚΗΣ ΑΜΥΝΑΣ
Ε’ ΚΛΑΔΟΣ
ΔΝΣΗ ΑΣΦΑΛΕΙΑΣ
07 Σεπ 20

ΠΑΡΑΡΤΗΜΑ «Θ» ΣΤΟΝ
ΕΚΒΑ

ΠΙΝΑΚΑΣ ΚΑΘΑΡΙΣΜΟΥ ΚΑΙ ΕΞΥΓΙΑΝΣΗΣ ΜΕΣΩΝ

Τύπος Μέσου	Καθαρισμός (Downgrade)	Εξυγίανση (Sanitization)
Μαγνητική ταινία		
Type I	Α ή Β	Α ή Β ή ΙΓ
Type II	Α ή Β	Β ή ΙΓ
Type III	Α ή Β	ΙΓ
Μαγνητικός δίσκος		
Μπερνούλι	Α ή Β ή Γ	ΙΓ
Εύκαμπτος	Α ή Β ή Γ	ΙΓ
Σκληρός – μη αποσπώμενος	Γ	Α ή Β ή Δ ή ΙΓ
Σκληρός αποσπώμενος	Α ή Β ή Γ	Α ή Β ή Δ ή ΙΓ
Οπτικός δίσκος		
Επανεγγράψιμος	Γ	ΙΓ
Αναγνώσιμος	ΙΓ ή ΙΔ	ΙΓ
Εγγράψιμος	ΙΓ ή ΙΔ	ΙΓ
Μνήμες (ηλεκτρονικές)		
Δυναμική, τυχαίας προσπέλασης (DRAM)	Γ ή Ζ	Γ ή Ζ ή ΙΓ
Ηλεκτρικά επαναπρογραμματιζόμενη (EAPROM)	ΙΒ	Ι ή ΙΓ
Ηλεκτρικά διαγραφόμενη (EEPROM)	Θ	Η ή ΙΓ
Διαγραφόμενη (EPROM)	ΙΑ	(Ι και Γ) ή ΙΓ
Ανανεώσιμη (Flash PROM)	Θ	(Γ μετά Θ) ή ΙΓ
Προγραμματιζόμενη (PROM)	Γ	ΙΓ
Μαγνητικών φυσαλίδων	Γ	Α ή Β ή Γ ή ΙΓ
Μαγνητιζόμενων βρόχων	Γ	Α ή Β ή Ε ή ΙΓ
Μαγνητικά επενδυμένου σύρματος	Γ	(Γ και ΣΤ) ή ΙΓ
Μαγνητική εμπέδησης	Γ	ΙΓ
Αμετάβλητη (NOVRAM)	Γ ή Ζ	Γ ή Ζ ή ΙΓ
Αναγνώσιμη (ROM)	ΙΓ	
Στατική, τυχαίας προσπέλασης (SRAM)	Γ ή Ζ	(Γ και ΣΤ) ή Ζ ή ΙΓ
Συσκευές		
Καθοδική λυχνία	Ζ	ΙΖ

Τύπος Μέσου	Καθαρισμός (Downgrade)	Εξυγίανση (Sanitization)
Εκτυπωτές		
Λέιζερ	Ζ	ΙΕ μετά Ζ
Κρουστικοί	Ζ	ΙΣΤ μετά Ζ

ΜΕΘΟΔΟΙ ΚΑΘΑΡΙΣΜΟΥ ΚΑΙ ΕΞΥΓΙΑΝΣΗΣ

α. Απομαγνητισμός με απομαγνητιστή Type I.
β. Απομαγνητισμός με απομαγνητιστή Type II.
γ. Επανεγγραφή όλων των διευθυνσιοδοτούμενων θέσεων με ένα μόνο χαρακτήρα.
δ. Επανεγγραφή όλων των διευθυνσιοδοτούμενων θέσεων με ένα χαρακτήρα, το δυαδικό του συμπλήρωμα, μετά με έναν τυχαίο χαρακτήρα και τέλος εάν ο τυχαίος χαρακτήρας δεν επαληθεύεται ορθά, επανάληψη της διαδικασίας στη συγκεκριμένη θέση. Αυτή η μέθοδος δεν είναι κατάλληλη για την εξυγίανση «ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ» μέσων.
ε. Επανεγγραφή όλων των διευθυνσιοδοτούμενων θέσεων με ένα χαρακτήρα, μετά το δυαδικό του συμπλήρωμα και τέλος με έναν τυχαίο χαρακτήρα.
στ. Κάθε επανεγγραφή αποθηκεύεται στη μνήμη, για χρόνο μεγαλύτερο από το χρόνο αποθήκευσης διαβαθμισμένων δεδομένων.
ζ. Αφαίρεση κάθε πηγής ισχύος συμπεριλαμβανομένων μπαταριών ή πυκνωτών.
η. Επανεγγραφή όλων των θέσεων με τυχαίες σειρές δυαδικών ψηφίων, μετά με σειρά δυαδικών μηδέν και τέλος με σειρά δυαδικών άσσων.
θ. Εκτέλεση πλήρους διαγραφής του ολοκληρωμένου, όπως αυτή ορίζεται στα κατασκευαστικά φυλλάδια.
ι. Εκτέλεση οδηγίας (Θ) και μετά της οδηγίας (Γ), επανάληψη της διαδικασίας τρεις φορές.
ια. Διαγραφή με υπεριώδη ακτινοβολία, όπως αυτή ορίζεται στα κατασκευαστικά φυλλάδια.
ιβ. Διαγραφή με υπεριώδη ακτινοβολία, όπως αυτή ορίζεται στα κατασκευαστικά φυλλάδια και για χρόνο τριπλάσιο από τον οριζόμενο.
ιγ. Καταστροφή (κομμάτιασμα, αποτέφρωση, σύνθλιψη, κοπή ή τήξη).
ιδ. Απαιτείται καταστροφή, μόνο εάν περιέχονται διαβαθμισμένες πληροφορίες.
ιε. Απεικόνιση πέντε σελίδων τυχαίων πληροφοριών σε όλο το εύρος.
ιστ. Καταστροφή των μελανούμενων ταινιών. Καθαρισμός ακίδων.
ιζ. Επιθεώρηση και έλεγχος επιφανείας απεικόνισης για στοιχεία εναπομεινάντων πληροφοριών. Εάν υπάρχουν πληροφορίες, απαιτείται καταστροφή.

Αντιναύαρχος Ιωάννης Δρυμούσης ΠΝ
Υπαρχηγός

Ακριβές Αντίγραφο

Ασμχος (ΕΑ) Νικόλαος Ζήκος
Επιτελής ΓΕΕΘΑ/Ε3/1

ΓΕΝΙΚΟ ΕΠΙΤΕΛΕΙΟ ΕΘΝΙΚΗΣ ΑΜΥΝΑΣ
Ε’ ΚΛΑΔΟΣ
ΔΝΣΗ ΑΣΦΑΛΕΙΑΣ
07 Σεπ 20

ΠΑΡΑΡΤΗΜΑ «Ι» ΣΤΟΝ
ΕΚΒΑ

ΕΝΕΡΓΕΙΕΣ ΔΙΑΠΙΣΤΕΥΣΗΣ ΚΑΤΑ ΤΗ ΔΙΑΡΚΕΙΑ ΤΟΥ ΚΥΚΛΟΥ ΖΩΗΣ ΕΝΟΣ ΣΕΠ

1. Σχεδιασμός ΣΕΠ

Οι ακόλουθες ενέργειες και αντίστοιχα οι αρμόδιοι και οι εμπλεκόμενοι φορείς για την υλοποίηση αυτών, αφορούν στο στάδιο σχεδιασμού του ΣΕΠ:

Ενέργεια	Αρμόδιος Φορέας	Εμπλεκόμενοι Φορείς
α. Καθορισμός των λειτουργικών απαιτήσεων του ΣΕΠ από πλευράς ασφαλείας, καθώς και των πληροφοριακών δεδομένων που χειρίζεται.	ΑΕΛ	
β. Καθορισμός ημερομηνιών ολοκλήρωσης κάθε σταδίου της διαδικασίας διαπίστευσης.	ΑΕΛ	ΕΑΔΑ ή ΕΔΑ, εφόσον έχει καθοριστεί (στο εξής στο κείμενο αναφέρεται μόνο ΕΑΔΑ).
γ. Προσδιορισμός και αποτίμηση της αξίας των πληροφοριακών δεδομένων, σε ότι αφορά στο αντίκτυπο σε περίπτωση απώλειας διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας.	ΑΕΛ	ΕΑΑΕΠ
δ. Προσδιορισμός των απαιτήσεων ΑΚ. Τεκμηρίωση ακαταλληλότητας μεθόδου από την ΕΑΑΕΠ.	ΕΑΔΑ	ΕΑΑΕΠ
ε. Εκτέλεση Αρχικής ΑΚ.	ΑΕΛ	
στ. Έγκριση αποτελεσμάτων Αρχικής ΑΚ.	ΕΑΔΑ	
ζ Προσδιορισμός των μέτρων, για την υλοποίηση των απαιτήσεων, που προέκυψαν ως αποτέλεσμα της Αρχικής ΑΚ.	ΑΕΛ	ΕΑΑΕΠ, ΕΑΔΑ
η. Σύνταξη Αναφοράς Διαχείρισης Κινδύνου (ΑΔΚ).	ΑΕΛ	ΕΑΑΕΠ (κατόπιν αιτήσεως ΑΕΛ)
θ. Αποδοχή εναπομείναντος κινδύνου (για τον οποίο δεν έχουν ληφθεί μέτρα αντιμετώπισης).	ΑΕΛ, ΕΑΑΕΠ (κατόπιν αιτήσεως ΑΕΛ)	ΕΑΔΑ
ι. Καθορισμός των απαραίτητων κρυπτογραφικών προϊόντων και μηχανισμών.	ΑΕΛ	ΕΑΑΕΠ
ια. Ανάπτυξη αρχικής ΔΑΠΑΣ ή και των μορφών που αυτή απαιτείται να λάβει (ΔΑΠΑΚ, ΔΑΠΑΔ, ΔΑΤΑΣ).	ΑΕΛ ΕΑΑΕΠ (κατόπιν αιτήσεως ΑΕΛ)	ΕΑΔΑ

Ενέργεια	Αρμόδιος Φορέας	Εμπλεκόμενοι Φορείς
ιβ. Επεξεργασία της Αρχικής ΔΑΠΑΣ από την Ομάδα Εξέτασης ΔΑΠΑΣ (ΟΕΔ) η οποία αποτελείται από: (1) ΕΑΔΑ ή ΕΔΑ (πρόεδρος, επιτελής ασφαλείας πληροφορικής, επιτελής επί λοιπών θεμάτων ασφαλείας). (2) ΑΕΛ (υπεύθυνος ασφαλείας συστήματος, εκπρόσωπος τμήματος ανάπτυξης συστήματος, εκπρόσωπος τμήματος επιχειρησιακής εκμετάλλευσης συστήματος). (3) ΕΑΑΕΠ (εκπρόσωπος επί θεμάτων ασφαλείας επικοινωνιών και πληροφορικής, εκπρόσωπος επί θεμάτων κρυπτογράφησης).	ΕΑΔΑ, ΕΑΑΕΠ	ΑΕΛ
ιγ. Έγκριση αρχικής ΔΑΠΑΣ ή/και των μορφών που αυτή απαιτείται να λάβει (ΔΑΠΑΚ, ΔΑΠΑΔ, ΔΑΤΑΣ).	ΕΑΔΑ	

2. Ανάπτυξη και Προμήθεια Συστήματος

Οι ακόλουθες ενέργειες και αντίστοιχα οι αρμόδιοι / εμπλεκόμενοι φορείς για την υλοποίηση αυτών, αφορούν στο στάδιο αναπτύξεως και προμήθειας του συστήματος:

Ενέργεια	Αρμόδιος Φορέας	Εμπλεκόμενοι Φορείς
α. Εκτέλεση αναθεωρητικής ΑΚ.	ΑΕΛ	
β. Έγκριση αποτελεσμάτων αναθεωρητικής ΑΚ.	ΕΑΔΑ	
γ. Προσδιορισμός των μέτρων, για την υλοποίηση των απαιτήσεων, που προέκυψαν ως αποτέλεσμα της αναθεωρητικής ΑΚ.	ΕΑΔΑ	ΑΕΛ, ΕΑΑΕΠ
δ. Σύνταξη ΑΔΚ.	ΑΕΛ	ΕΑΑΕΠ
ε. Αποδοχή Εναπομεινάντων Κινδύνων (για τους οποίους δεν έχουν ληφθεί μέτρα αντιμετώπισης). Έγκριση αυτών από την ΕΑΔΑ.	ΑΕΛ	ΕΑΔΑ
στ. Περιγραφή της αρχιτεκτονικής ασφαλείας του συστήματος. Έγκριση αυτής από την ΕΑΔΑ.	ΑΕΛ	ΕΑΔΑ
ζ. Σύνταξη / καθορισμός των προδιαγραφών των μέτρων φυσικής ασφαλείας, ασφαλείας προσωπικού και ασφαλείας των πληροφοριών.	ΑΕΛ	ΕΑΔΑ
η. Σύνταξη των προδιαγραφών των μέτρων Ασφαλείας Επικοινωνιών και Πληροφορικής – ΑΕΠ (ασφαλείας υπολογιστών, επικοινωνιών, κρυπτογράφησης και ανεπιθύμητων εκπομπών) σε συνάρτηση με τις απαιτήσεις της ΕΑΔΑ, προκειμένου να επιτευχθεί λειτουργικότητα σε συνδυασμό με την ασφάλεια του συστήματος.	ΕΑΑΕΠ	ΑΕΛ, ΕΑΔΑ
θ. Σύνταξη καταλόγων προϊόντων πλην κρυπτογραφικών για την κάλυψη των απαιτήσεων επί των μέτρων ΑΕΠ. Επιλογή των πλέον κατάλληλων. Έγκριση αυτών από την ΕΑΔΑ.	ΕΑΑΕΠ	ΑΕΛ, ΕΑΔΑ
ι. Σύνταξη / καθορισμός, όπου απαιτείται, των λειτουργικών απαιτήσεων για κρυπτογραφικά προϊόντα και μηχανισμούς.	ΑΕΛ	ΕΑΑΕΠ
ια. Σύνταξη / καθορισμός των τεχνικών χαρακτηριστικών των κρυπτογραφικών προϊόντων και μηχανισμών	ΕΑΑΕΠ	ΑΕΛ

Ενέργεια	Αρμόδιος Φορέας	Εμπλεκόμενοι Φορείς
ιβ. Αξιολόγηση, και τελική επιλογή των κρυπτογραφικών προϊόντων και των μηχανισμών. Πιστοποίηση των κρυπτογραφικών προϊόντων και των μηχανισμών από την ΕΑΑΕΠ.	ΕΑΑΕΠ	ΑΕΛ
ιγ. Καθορισμός αντικειμένων και διαδικασιών Ελέγχου Ασφαλείας (ΕΑΣ) του ΣΕΠ και όπου απαιτείται των διασυνδέσεών του.	ΕΑΔΑ	ΕΑΑΕΠ, ΑΕΛ
ιδ. Σύνταξη τρέχουσας ΔΑΠΑΣ ή/και των μορφών που αυτή απαιτείται να λάβει (ΔΑΠΑΚ, ΔΑΠΑΔ, ΔΑΤΑΣ).	ΑΕΛ	
ιε. Επεξεργασία της Τρέχουσας ΔΑΠΑΣ ή/και των μορφών που αυτή απαιτείται να λάβει (ΔΑΠΑΚ, ΔΑΠΑΔ, ΔΑΤΑΣ) από την ΟΕΔ.	ΑΕΛ	ΕΑΔΑ, ΕΑΑΕΠ
ιστ. Έγκριση Τρέχουσας ΔΑΠΑΣ ή/και των μορφών που αυτή απαιτείται να λάβει (ΔΑΠΑΚ, ΔΑΠΑΔ, ΔΑΤΑΣ).	ΕΑΔΑ	

3. Υλοποίηση ΣΕΠ και Πιστοποίηση Ασφαλείας

Οι ακόλουθες ενέργειες και αντίστοιχα οι αρμόδιοι / εμπλεκόμενοι φορείς για την υλοποίηση αυτών, αφορούν είτε στο στάδιο υλοποίησης ενός ΣΕΠ υπό σχεδίαση, είτε στη φάση που ήδη λειτουργεί επιχειρησιακά (αλλά δεν έχει διαπιστευθεί) και της παροχής πιστοποίησης ασφαλείας αυτού:

Ενέργεια	Αρμόδιος Φορέας	Εμπλεκόμενοι Φορείς
α. Εκτέλεση ΕΑΣ του συστήματος ή όπου απαιτείται, της διασυνδέσεως των συστημάτων.	ΑΕΛ	ΕΑΔΑ, ΕΑΑΕΠ
β. Επεξεργασία των αποτελεσμάτων της ΕΑΣ.	ΑΕΛ	
γ. Συμπλήρωση της τελευταίας ΑΔΚ, σύμφωνα με τα αποτελέσματα της ΕΑΣ.	ΑΕΛ	ΕΑΑΕΠ
δ. Αποδοχή εναπομεινάντων κινδύνων (για τους οποίους δεν έχουν ληφθεί μέτρα αντιμετώπισης). Έγκριση αυτών από την ΕΑΔΑ.	ΑΕΛ	ΕΑΔΑ
ε. Προσδιορισμός των πρόσθετων μέτρων ασφαλείας τα οποία απαιτείται να εφαρμοσθούν, σύμφωνα με τα αποτελέσματα της ΕΑΣ.	ΑΕΛ	ΕΑΔΑ, ΕΑΑΕΠ
στ. Εφαρμογή των πρόσθετων μέτρων ασφαλείας σύμφωνα με τα αποτελέσματα της ΕΑΣ.	ΑΕΛ	
ζ. Σύνταξη τελικής ΔΑΠΑΣ ή/και των μορφών που αυτή απαιτείται να λάβει (ΔΑΠΑΚ, ΔΑΠΑΔ, ΔΑΤΑΣ).	ΑΕΛ	
η. Σύνταξη των Διαδικασιών Ασφαλούς Λειτουργίας (ΔΑΛ).	ΑΕΛ	
θ. Επεξεργασία της τελικής ΔΑΠΑΣ ή/και των μορφών που αυτή απαιτείται να λάβει (ΔΑΠΑΚ, ΔΑΠΑΔ, ΔΑΤΑΣ) και των ΔΑΛ από την ΟΕΔ.	ΑΕΛ	ΕΑΔΑ, ΕΑΑΕΠ
ι. Έγκριση της τελικής ΔΑΠΑΣ ή/και των μορφών που αυτή απαιτείται να λάβει (ΔΑΠΑΚ, ΔΑΠΑΔ, ΔΑΤΑΣ) και των ΔΑΛ (για ΣΕΠ με διαβάθμιση ασφαλείας «ΕΜΠΙΣΤΕΥΤΙΚΟ» και άνω).	ΕΑΔΑ	
ια. Διαπίστευση του συστήματος και όπου απαιτείται της διασύνδεσης των συστημάτων και γνωστοποίηση της διαπίστευσης.	ΕΑΔΑ	

Ενέργεια	Αρμόδιος Φορέας	Εμπλεκόμενοι Φορείς
ιβ. Σύνταξη των απαιτήσεων για παροχή επαναδιαπίστευσης και έγκριση αυτών από την ΕΑΔΑ.	ΑΕΛ	ΕΑΔΑ

4. Επιχειρησιακή Λειτουργία ΣΕΠ

Οι ακόλουθες ενέργειες και αντίστοιχα οι αρμόδιοι / εμπλεκόμενοι φορείς για την υλοποίηση αυτών, αφορούν στο στάδιο λειτουργίας του συστήματος:

Ενέργεια	Αρμόδιος Φορέας	Εμπλεκόμενοι Φορείς
α. Υλοποίηση των προβλεπομένων στις ΔΑΛ πριν τεθεί σε επιχειρησιακή λειτουργία το ΣΕΠ.	ΑΕΛ	
β. Εκτέλεση ΕΑΣ και έλεγχος αντίδρασης, σύμφωνα με τα προβλεπόμενα στις ΔΑΛ.	ΑΕΛ	
γ. Αναφορά των αποτελεσμάτων της ΕΑΣ στην ΕΑΔΑ. Σύνταξη πίνακα ευπαθειών του συστήματος.	ΑΕΛ	ΕΑΔΑ
δ. Εκτέλεση περιοδικών ΕΑΣ (ανά τρίμηνο και χωρίς προειδοποίηση των χρηστών) και αναθεώρηση του πίνακα ευπαθειών του συστήματος, σύμφωνα με τις απαιτήσεις της ΕΑΔΑ.	ΑΕΛ	
ε. Εκτέλεση περιοδικών επιθεωρήσεων ασφαλείας του συστήματος ή όπου απαιτείται, των διασυνδέσεων του συστήματος με άλλα συστήματα.	ΕΑΔΑ	

5. Τροποποίηση / Επέκταση Συστήματος και Διασύνδεση με Έτερα ΣΕΠ

Οι ακόλουθες ενέργειες και αντίστοιχα οι αρμόδιοι / εμπλεκόμενοι φορείς για την υλοποίηση αυτών, αφορούν στο στάδιο βελτιώσεως και επεκτάσεως ενός ΣΕΠ, καθώς και στη διασύνδεση του με έτερα ΣΕΠ:

Ενέργεια	Αρμόδιος Φορέας	Εμπλεκόμενοι Φορείς
α. Εκτέλεση αναθεωρητικής ΑΚ.	ΑΕΛ	
β. Έγκριση αποτελεσμάτων αναθεωρητικής ΑΚ.	ΕΑΔΑ	
γ. Σύνταξη ΑΔΚ.	ΑΕΛ	ΕΑΑΕΠ
δ. Προσδιορισμός των πρόσθετων μέτρων που απαιτείται να εφαρμοσθούν και ανάπτυξη, όπου απαιτείται, των νέων λειτουργικών απαιτήσεων για τα κρυπτογραφικά προϊόντα και μηχανισμούς.	ΑΕΛ	ΕΑΑΕΠ, ΕΑΔΑ
ε. Εκτέλεση ΕΑΣ σύμφωνα με τα νέα δεδομένα του ΣΕΠ, μετά την τροποποίηση / επέκταση του ή τη διασύνδεσή του με έτερα.	ΑΕΛ	ΕΑΔΑ, ΕΑΑΕΠ
στ. Επεξεργασία της ΕΑΣ σύμφωνα με τις απαιτήσεις της ΕΑΔΑ και εξαγωγή συμπερασμάτων.		ΕΑΔΑ, ΕΑΑΕΠ
ζ. Έγκριση των αποτελεσμάτων της ΕΑΣ.	ΕΑΔΑ	
η. Συμπλήρωση της τελευταίας ΑΔΚ, σύμφωνα με τα αποτελέσματα της ΕΑΣ.	ΑΕΛ	ΕΑΑΕΠ
θ. Αποδοχή εναπομεινάντων κινδύνων (για τους οποίους δεν έχουν ληφθεί μέτρα αντιμετώπισης). Έγκριση αυτών	ΑΕΛ	ΕΑΔΑ

από την ΕΑΔΑ.		
ι. Αναθεώρηση της ΔΑΠΑΣ ή/και των μορφών που αυτή απαιτείται να λάβει (ΔΑΠΑΚ, ΔΑΠΑΔ, ΔΑΤΑΣ).	ΑΕΛ	ΕΑΔΑ
ια. Αναθεώρηση των ΔΑΛ.	ΑΕΛ	
ιβ. Επεξεργασία της αναθεωρημένης ΔΑΠΑΣ ή/και των μορφών που αυτή απαιτείται να λάβει (ΔΑΠΑΚ, ΔΑΠΑΔ, ΔΑΤΑΣ) και των ΔΑΛ, από την ΟΕΔ.	ΑΕΛ	ΕΑΔΑ, ΕΑΑΕΠ
ιγ. Έγκριση της αναθεωρημένης ΔΑΠΑΣ ή/ και των μορφών που αυτή απαιτείται να λάβει (ΔΑΠΑΚ, ΔΑΠΑΔ, ΔΑΤΑΣ) και των αναθεωρημένων ΔΑΛ.	ΕΑΔΑ	
ιδ. Επαναδιαπίστευση του συστήματος και γνωστοποίηση της.	ΕΑΔΑ	
ιε. Σύνταξη των απαιτήσεων για παροχή επαναδιαπίστευσης και έγκριση αυτών από την ΕΑΔΑ.	ΑΕΛ	ΕΑΔΑ

6. Απόσυρση Συστημάτων και Διάθεση του Εξοπλισμού

Οι ακόλουθες ενέργειες και αντίστοιχα οι αρμόδιοι / εμπλεκόμενοι φορείς για την υλοποίηση αυτών, αφορούν στο στάδιο απόσυρσης συστημάτων από την υπηρεσία, και διάθεσης του εξοπλισμού:

Ενέργεια	Αρμόδιος Φορέας	Εμπλεκόμενοι Φορείς
α. Ανάληψη ενεργειών για την αρχειοθέτηση των δεδομένων σε ηλεκτρονική ή φυσική μορφή και αποδιαβάθμιση ή/και καταστροφή των σταθερών και αφαιρούμενων μέσων αποθήκευσης.	ΑΕΛ	
β. Εφαρμογή κατάλληλων διαδικασιών για τη διάθεση ή/και καταστροφή των κρυπτογραφημένων προϊόντων και των κρυπτογραφικών συστημάτων και του σχετικού υλικού τους.	ΑΕΛ	
γ. Αρχειοθέτηση ή καταστροφή των εκτυπωμένων εγγράφων που περιέχουν πληροφορίες του συστήματος.	ΑΕΛ	

Αντιναύαρχος Ιωάννης Δρυμούσης ΠΝ
Υπαρχηγός

Ακριβές Αντίγραφο

Ασμχος (ΕΑ) Νικόλαος Ζήκος
Επιτελής ΓΕΕΘΑ/Ε3/1

ΓΕΝΙΚΟ ΕΠΙΤΕΛΕΙΟ ΕΘΝΙΚΗΣ ΑΜΥΝΑΣ
Ε’ ΚΛΑΔΟΣ
ΔΝΣΗ ΑΣΦΑΛΕΙΑΣ
07 Σεπ 20

ΠΑΡΑΡΤΗΜΑ «ΙΑ» ΣΤΟΝ
ΕΚΒΑ

ΟΔΗΓΙΕΣ ΓΙΑ ΤΗ ΣΥΝΤΑΞΗ ΤΗΣ
ΔΗΛΩΣΗΣ ΑΠΑΙΤΗΣΕΩΝ ΑΣΦΑΛΕΙΑΣ ΣΥΣΤΗΜΑΤΟΣ (ΔΑΠΑΣ)

Στο Παράρτημα αυτό, παρέχονται οδηγίες για τη σύνταξη και τα περιεχόμενα της ΔΑΠΑΣ. Προκειμένου ο φορέας σύνταξης της ΔΑΠΑΣ, δηλαδή η ΑΕΛ, να αποκτήσει πληρέστερη εικόνα για τη μορφή και τη διαδικασία, χρησιμοποιεί τις οδηγίες του παρόντος Παραρτήματος σε συνδυασμό με τα αναφερόμενα στο Παράρτημα «ΙΒ».

1. Γενικά Στοιχεία ΣΕΠ

Απαιτείται να συμπληρωθούν τα παρακάτω στοιχεία:

α. Το όνομα του προγράμματος / συστήματος

Μέχρι την έναρξη ύπαρξης του ΣΕΠ, υφίσταται ως πρόγραμμα προς υλοποίηση.

β. Ο σκοπός του προγράμματος / συστήματος

Αναφέρεται η αναγκαιότητα δημιουργίας του, ο σκοπός λειτουργίας του, η αποστολή του.

γ. Η τοποθεσία ανάπτυξης του ΣΕΠ

Αναφέρεται το εύρος του ΣΕΠ, με βάση τη γεωγραφική κατανομή του και την ύπαρξη τυχόν τοπικών υποσυστημάτων. Στην περίπτωση αυτή, απαιτείται κατά περίπτωση ο καθορισμός από την ΑΕΛ των τοπικών ΑΕΛ.

δ. Οι χρήστες του ΣΕΠ

Αναφέρονται περιγραφικά οι χρήστες (ομάδες) του ΣΕΠ, οι λογαριασμοί και τα δικαιώματά τους.

ε. Το χρονικό πλαίσιο υλοποίησης βασικών ενεργειών

Ημερομηνίες υλοποίησης των προδιαγραφών ασφαλείας των χρηστών, αρχής και τέλους της φάσης ανάπτυξης, έναρξης λειτουργίας, έναρξης λειτουργίας με πλήρη ικανότητα, ολοκλήρωσης της διαδικασίας διαπίστευσης.

στ. Το είδος σχέσης / συνεργασίας / ανταλλαγής δεδομένων με έτερα ΣΕΠ

Συμπληρώνεται σε περίπτωση διασύνδεσης ή αποδέσμευσης πληροφοριών σε άλλους φορείς – οργανισμούς.

2. Περιγραφή ΣΕΠ

Περιγράφεται το ΣΕΠ, ως προς τα παρακάτω χαρακτηριστικά:

α. Ρόλος

Απαιτείται αναλυτική παρουσίαση επιχειρησιακής λειτουργίας του, ανάλογα με το χειρισμό δεδομένων, τα μέσα αποθήκευσης και τις διασυνδέσεις του.

β. Πληροφορίες

Ανάλυση του τύπου των πληροφοριών, του όγκου των, της διαβάθμισης, όπως επίσης και του ποσοστού αυτών ανά συγκεκριμένη διαβάθμιση (π.χ. 30% Εμπιστευτικά, 20% Απόρρητα).

γ. Χρήστες

Ο τύπος των χρηστών [απλοί χρήστες, χρήστες με ειδικά προνόμια, Διαχειριστές Λειτουργίας (ΔΙΑΛ), Υπεύθυνος Ασφαλείας Συστήματος (ΥΑΣ), Υπεύθυνος Ασφαλείας Δικτύου (ΥΑΔ), Υπεύθυνοι Ασφαλείας Τοποθεσίας (ΥΑΤ)] συμπεριλαμβανομένων των εξουσιοδοτήσεων ασφαλείας των, που είτε διασυνδέονται απευθείας με το σύστημα, είτε λαμβάνουν οποιασδήποτε μορφής δεδομένα από αυτό (π.χ εκτυπωμένα αντίγραφα).

δ. Αρχιτεκτονική Συστήματος

Περιγραφή, με επαρκείς λεπτομέρειες του υλικού (hardware), του λογισμικού συστήματος (firmware), του λογισμικού (software), των λειτουργικών στοιχείων, συμπεριλαμβανομένων των εξωτερικών διασυνδέσεων, πρωτοκόλλων επικοινωνίας και των τεχνικών προδιαγραφών του ΣΕΠ.

3. Προσδιορισμός των Απαιτήσεων Ασφαλείας

Περιγράφονται αναλυτικά, οι λόγοι που επιβάλλουν το επίπεδο ασφαλείας του ΣΕΠ, όπως και την έννοια της ασφαλείας, από την πλευρά:

α. Των απειλών

Αναφέροντας τους κινδύνους στην εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα των πληροφοριών, τη φύση των πιθανών επιθέσεων, την ελκυστικότητα του ΣΕΠ και τις πληροφορίες που το καθιστούν πιθανό στόχο.

β. Τη σπουδαιότητα των πληροφοριών που διαχειρίζεται, αναφέροντας την επίδραση στη λειτουργία του, στις περιπτώσεις απώλειας:

(1) Εμπιστευτικότητας (η μη εξουσιοδοτημένη αποκάλυψη πληροφοριών από μη εξουσιοδοτημένη πρόσβαση στο ΣΕΠ).

(2) Ακεραιότητας (η μη εξουσιοδοτημένη αλλαγή πληροφορίας και απώλειας της ορθής λειτουργίας των πηγών του ΣΕΠ).

(3) Διαθεσιμότητας (η άρνηση εξουσιοδοτημένης πρόσβασης ή καθυστέρηση στην εκτέλεση κρίσιμων λειτουργιών).

γ. Τις αδυναμίες του συστήματος, όπως για παράδειγμα:

(1) Σημαντικός αριθμός προσωπικού με δυνατότητα πρόσβασης στο ΣΕΠ και με δικαιώματα / γνώση διαχείρισης αυτού.

(2) Την ευκολία με την οποία μπορεί κάποιος, παράνομα να αποκτήσει πρόσβαση στις πληροφορίες.

(3) Την προσβασιμότητα σε πληροφορίες του ΣΕΠ, μέσω τηλεχειριζόμενων τερματικών ή θέσεων εργασίας ή άλλες εξωτερικές συνδέσεις.

(4) Την ευκαιρία για επιτηδευμένη πρόκληση ατερμόνων διαδικασιών ή ιών, στο λογισμικό (firmware, software).

(5) Την πιθανότητα δυσλειτουργίας του λογισμικού ή του υλικού, λόγω σχεδιαστικών ελαττωμάτων.

(6) Την ευπάθεια του συστήματος για εκμετάλλευση των μη ηθελημένων διαφυγουσών εκπομπών (compromising emanations).

(7) Τη διαβίβαση διαβαθμισμένων πληροφοριών μέσω μη προφυλαγμένων, ωστόσο εγκεκριμένων επικοινωνιακών διασυνδέσεων.

(8) Επιδιωκόμενο επίπεδο λειτουργικής ασφαλείας (dedicated / αποκλειστικός, system high / υψηλού, κατηγοριοποιημένου, ελεγχόμενου ή MLS / πολλαπλού επιπέδου).

4. Είδη Περιβάλλοντος Ασφαλείας

α. Στο τμήμα αυτό, περιγράφονται οι προδιαγραφές του ΣΕΠ, εντός των παρακάτω ειδών περιβάλλοντος ασφαλείας:

(1) Γενικό Περιβάλλον Ασφαλείας (ΓΠΑ), το οποίο ορίζεται ως το περιβάλλον εντός του οποίου βρίσκεται το ΣΕΠ, αλλά η ΑΕΛ δεν έχει δικαιοδοσία φυσικού ελέγχου.

(2) Τοπικό Περιβάλλον Ασφαλείας (ΤΠΑ), το οποίο ορίζεται ως το περιβάλλον εντός του οποίου βρίσκεται το ΣΕΠ και στο οποίο η ΑΕΛ έχει δικαιοδοσία άμεσου φυσικού ελέγχου.

(3) Ηλεκτρονικό Περιβάλλον Ασφαλείας (ΗΠΑ), στο οποίο λειτουργεί το ΣΕΠ, σε ό,τι αφορά τα ηλεκτρονικά όριά του και τις κάθε είδους διασυνδέσεις του (φυσικές ή και μέσω software) με έτερα συστήματα.

β. Εντός του ΓΠΑ συμπεριλαμβάνεται το ΤΠΑ, ενώ το ΗΠΑ υφίσταται εντός του ΤΠΑ.

5. Καθορισμός των Μέτρων Ασφαλείας

α. Αυτό αποτελεί το κυριότερο τμήμα της ΔΑΠΑΣ, στο οποίο περιγράφεται ο τρόπος εξασφάλισης του ΣΕΠ, ενώ επιπλέον καθορίζονται τα μέτρα ασφαλείας (φυσικής, προσωπικού, πληροφοριών, Η/Υ, κρυπτογράφησης, εκπομπών και επικοινωνιών), τα οποία λαμβάνονται σε κάθε ένα από τα περιβάλλοντα ασφαλείας, ώστε να επιτευχθεί ασφάλεια σε ό,τι αφορά:

(1) Τον έλεγχο πρόσβασης.

(2) Την ταυτοποίηση.

(3) Την καταγραφή ενεργειών προσωπικού.

(4) Τον εντοπισμό προσπαθειών παραβίασης ασφαλείας.

(5) Την επαναχρησιμοποίηση αντικειμένου.

(6) Την ακεραιότητα.

(7) Τη διαθεσιμότητα.

(8) Τις επικοινωνίες δεδομένων.

β. Η ΔΑΠΑΣ, αποτελεί μία δήλωση του κινδύνου ασφαλείας του ΣΕΠ, λαμβάνοντας υπόψη τις απειλές και τις αδυναμίες, η οποία είτε:

(1) Απλά επιβεβαιώνει την ύπαρξη γενικών κινδύνων και ότι δεν έχουν εξακριβωθεί ειδικού τύπου κίνδυνοι.

(2) Αναφέρει συγκεκριμένους κινδύνους με ειδική αναφορά στην ΑΚ και στις αποτιμήσεις που προέκυψαν από αυτή.

γ. Στη ΔΑΠΑΣ, καθορίζεται η μορφή του κινδύνου σε κάθε ένα από τα περιβάλλοντα ασφαλείας. Αυτό γίνεται, είτε προσδιορίζοντας ρητά τα μέτρα ασφαλείας τα οποία πρόκειται να εφαρμοστούν, είτε κάνοντας παραδοχές, ήτοι:

(1) Οι παραδοχές ασφαλείας, είναι απλές δηλώσεις σχετικά με τους παράγοντες που επηρεάζουν την ασφάλεια και οι οποίες εκτιμάται ότι ισχύουν. Είναι σημαντικό, αυτές οι δηλώσεις να αποτυπώνονται στη ΔΑΠΑΣ, ώστε να αποτελούν τη βάση, για τον καθορισμό των τομέων στους οποίους απαιτείται να ληφθούν μέτρα ασφαλείας.

(2) Οι παραδοχές ασφαλείας μπορεί να καθορίζουν, είτε:

(α) Ότι υφίστανται εναπομείναντες κίνδυνοι.

(β) Ότι τα γενικά μέτρα ασφαλείας, που καθορίζονται ρητά, αντιμετωπίζουν επαρκώς τους κινδύνους.

6. Έλεγχος Πρόσβασης

Ορίζεται η συγκεκριμένη αλληλεπίδραση μεταξύ του χρήστη και των δεδομένων μέσω του ΣΕΠ, η οποία έχει ως αποτέλεσμα τη ροή πληροφοριών από τον ένα στον άλλο.

α. Πολιτική Ασφαλείας

Η πρόσβαση σε διαβαθμισμένες πληροφορίες, περιορίζεται σε άτομα με την κατάλληλη εξουσιοδότηση και να εφαρμόζεται η αρχή «ανάγκη γνώσης».

β Κίνδυνοι

Άτομο χωρίς την κατάλληλη εξουσιοδότηση και την «ανάγκη γνώσης», μπορεί κατά λάθος ή εσκεμμένα να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε διαβαθμισμένη πληροφορία, υλικό, λογισμικό συστήματος και λογισμικό που προστατεύει διαβαθμισμένη πληροφορία.

(1) Γενικές Παραδοχές

(α) Όλοι οι εξουσιοδοτημένοι χρήστες έχουν πρόσβαση σε όλες τις πληροφορίες και διαχειρίζονται ορθά τις εξαγόμενες πληροφορίες.

(β) Οι διαχειριστές του ΣΕΠ, έχουν εξουσιοδοτηθεί για την πρόσβαση σε όλες τις πληροφορίες αρμοδιότητάς τους.

(γ) Το προσωπικό συντήρησης έχει εξουσιοδοτηθεί ανάλογα.

(δ) Οι έλεγχοι του ΓΠΑ, παρέχουν ικανό έλεγχο πρόσβασης στα τερματικά, περιφερειακά και στις θέσεις εργασίας.

(ε) Οι έλεγχοι του ΓΠΑ παρέχουν ικανή προστασία απέναντι σε μη εξουσιοδοτημένη πρόσβαση που πρόκειται να λάβει χώρα στο ΤΠΑ.

(στ) Όλες οι διαβαθμισμένες πληροφορίες που εισάγονται στο ΓΠΑ τυγχάνουν ανάλογου χειρισμού.

(ζ) Οι χρήστες με επιπλέον προνόμια έχουν τη δυνατότητα καθολικής πρόσβασης στο ΣΕΠ.

(η) Η ταυτοποίηση των χρηστών εντός του ΣΕΠ είναι μοναδική και αδιαμφισβήτητη.

(θ) Δεν υφίστανται επικοινωνίες του ΣΕΠ εκτός της περιμέτρου ΓΠΑ.

(ι) Το επίπεδο των απειλών εντός του ΣΕΠ, κατόπιν της ανάλυσης κινδύνου σύμφωνα με το Παράρτημα «ΙΔ», εγκρίνεται ως αποδεκτό.

(2) Σημεία Προσοχής στο ΓΠΑ

(α) Η ύπαρξη ανεπιθύμητων εκπομπών εκτός της περιμέτρου ασφαλείας.

(β) Οι επικοινωνίες του ΣΕΠ που διαπερνούν το ΓΠΑ.

(γ) Τα περιφερειακά του συστήματος / τερματικά / θέσεις εργασίας που βρίσκονται στο ΓΠΑ.

(δ) Τα ΣΕΠ που είναι διασυνδεδεμένα με το υπό εξέταση.

(3) Σημεία Προσοχής στο ΤΠΑ

(α) Η περίμετρος ασφαλείας ΤΠΑ (έλεγχοι πρόσβασης).

(β) Οι ειδικές περιοχές εντός της περιμέτρου ασφαλείας (όπως οι χώροι φύλαξης κρυπτοϋλικού).

(γ) Το εξουσιοδοτημένο προσωπικό (τακτικό ή έκτακτο).

(δ) Το μη εξουσιοδοτημένο προσωπικό (όπως επισκέπτες, προσωπικό καθαρισμού, προσωπικό συντήρησης κλπ).

(ε) Το υλικό που απαιτείται να προστατευθεί [αρχείο, μέσα αποθήκευσης δεδομένων, διαβαθμισμένες πληροφορίες, υλικό κρύπτο, κωδικοί πρόσβασης, λογισμικό, έγγραφα του συστήματος και σενάρια λειτουργίας].

(4) Προδιαγραφές των Μέτρων Ασφαλείας του ΓΠΑ και ΤΠΑ

(α) Διαβάθμιση του προσωπικού, με γνώμονα την αρχή «ανάγκη γνώσης».

(β) Επιτήρηση διαβαθμισμένου προσωπικού.

(γ) Επιτήρηση μη διαβαθμισμένου προσωπικού (όπως επισκέπτες, προσωπικό καθαρισμού, συντήρησης κτιρίων κλπ).

(δ) Έλεγχος πρόσβασης (υφίστανται κλειδαριές, κλειδιά, κάρτες ελέγχου πρόσβασης, προσωπικό φρούρησης, λίστες πρόσβασης κλπ).

(ε) Έλεγχος πρόσβασης σε διαβαθμισμένες περιοχές.

(στ) Αποτροπή μη επιτηρούμενης πρόσβασης στο ΤΠΑ.

(ζ) Φυσική προστασία των περιφερειακών / τερματικών / θέσεων εργασίας.

(η) Φυσική προστασία του υλικού του ΣΕΠ (όπως συστήματα κλιματισμού, σταθεροποιητές τάσης).

(θ) Εμφανής διαβάθμιση υλικού και χειρισμός του.

(ι) Έλεγχος των αρχείων στα οποία η πρόσβαση είναι περιορισμένη.

(ια) Έλεγχος της πρόσβασης στο ΣΕΠ και στις εφαρμογές του.

(ιβ) Έλεγχος των εξερχόμενων πληροφοριών σε εκτυπωμένη μορφή, πριν βγουν από το ΓΠΑ.

(ιγ) Διακοπή των εξωτερικών συνδέσεων του ΣΕΠ κατά τη διάρκεια διαβαθμισμένων διεργασιών (όπως αναβάθμιση, συντήρηση, επισκευή).

(ιδ) Κρυπτογράφηση – φυσική προστασία των επικοινωνιών.

(ιε) Έλεγχος των ανεπιθύμητων εκπομπών, με χρήση εγκεκριμένου εξοπλισμού (όπως συσκευές TEMPEST).

(5) Παραδοχές στο ΗΠΑ

(α) Έχουν καθοριστεί τα επίπεδα ασφαλείας πληροφοριών που χειρίζεται το ΣΕΠ.

(β) Υφίστανται διαβαθμισμένοι χρήστες του ΣΕΠ (με άμεση πρόσβαση σε αυτό).

(γ) Υφίστανται διαβαθμισμένοι χρήστες (χωρίς άμεση πρόσβαση στο ΣΕΠ, που όμως είναι αποδέκτες των πληροφοριών του).

(δ) Έχουν καθοριστεί οι απαιτήσεις για το συγκεκριμένο επίπεδο ασφαλείας, λαμβάνοντας υπόψη το συνολικό αριθμό και την εξουσιοδότηση των χρηστών, την κρισιμότητα των πληροφοριών, την απαίτηση διαχωρισμού ειδικού τύπου δεδομένων.

(6) Προδιαγραφές των Μέτρων Ασφαλείας του ΗΠΑ

(α) Υποχρεωτικός έλεγχος πρόσβασης.

(β) Διαδικασία πρόσβασης στο σύστημα.

(γ) Κρυπτογράφηση δεδομένων.

(δ) Προστασία του κωδικού πρόσβασης με χρήση κρυπτογράφησης.

(ε) Δυνατότητα ανάκτησης δεδομένων με χρήση των υφισταμένων αντιγράφων ασφαλείας.

(στ) Χαρακτηρισμός των δεδομένων.

(ζ) Ασφαλής και διαπιστευμένη διασύνδεση με άλλα συστήματα.

(η) Καθορισμός απαιτήσεων πρόσβασης για γενικό έλεγχο πρόσβασης ή για συγκεκριμένες ασφαλείς λειτουργίες.

7. Ταυτοποίηση

Ορίζεται ως η διαδικασία εξασφάλισης εγκυρότητας της δηλωθείσας ταυτότητας.

α. Πολιτική Ασφαλείας

Όλο το προσωπικό που έχει πρόσβαση σε διαβαθμισμένες πληροφορίες, ταυτοποιείται και η εξουσιοδότησή του αναγνωρίζεται. Όλες οι αυτοματοποιημένες διαδικασίες που λειτουργούν για την εξυπηρέτηση του χρήστη, συνδέονται απαρέγκλιτα με αυτόν.

β. Κίνδυνοι

Τα άτομα που μπορεί να μιμηθούν άλλους χρήστες, προκειμένου να εξασφαλίσουν πρόσβαση σε πληροφορίες μη συμβατές με την εξουσιοδότησή τους ή να κάνουν χρήση λογαριασμών που δεν τους ανήκουν.

(1) Γενικές Παραδοχές

(α) Η ταυτότητα του προσωπικού που εισέρχεται στο ΤΠΑ, αναγνωρίζεται από το ΓΠΑ.

(β) Η ταυτότητα του προσωπικού που εισέρχεται στο ΤΠΑ, αναγνωρίζεται από προσωπικό ασφαλείας του ΤΠΑ.

(γ) Όλες οι επικοινωνίες που περνούν από το ΓΠΑ, προστατεύονται από πιθανή υποκλοπή.

(δ) Συγκεκριμένα άτομα έχουν αναγνωριστεί κατά τη φυσική πρόσβαση σε συγκεκριμένα περιφερειακά / τερματικά / θέσεις εργασίας.

(2) Σημεία Προσοχής στο ΓΠΑ

(α) Τα τερματικά / θέσεις εργασίας.

(β) Οι γραμμές επικοινωνιών.

(γ) Οι συνδέσεις με άλλα συστήματα.

(δ) Τα τηλεχειριζόμενα διαγνωστικά προγράμματα.

(3) Σημεία Προσοχής στο ΤΠΑ

Μέσα ταυτοποίησης (καρτελάκια, σήματα, ταυτοποίηση στην είσοδο, συνεχή ταυτοποίηση).

(4) Προδιαγραφές των Μέτρων Ασφαλείας του ΓΠΑ και ΤΠΑ

(α) Μεταξύ του ΓΠΑ και του ΤΠΑ, να γίνεται η ταυτοποίηση μέσω χρήσης καρτών, σημάτων ή ειδικών διακριτικών.

(β) Μέσα υποστήριξης εντός του ΤΠΑ, με την εφαρμογή κανόνων για χρήση κωδικών πρόσβασης και συστημάτων αναγνώρισης προσωπικών στοιχείων.

(5) Σημεία Προσοχής στο ΗΠΑ

Ύπαρξη συσκευών ικανών για την υποκλοπή κωδικών πρόσβασης, μέσω προσπάθειας τυχαίας εύρεσης των κωδικών ή παραπλάνησης του συστήματος για την ταυτότητα του χρήστη.

(6) Προδιαγραφές των Μέτρων Ασφαλείας του ΗΠΑ

(α) Χρήση κωδικών πρόσβασης με αυξημένο εύρος χαρακτήρων.

(β) Χρήση συσκευών αναγνώρισης προσωπικών στοιχείων.

(γ) Αναγνώριση υλικού, μόνο μετά από ταυτόχρονη χρήση ελέγχου πρόσβασης σε αυτό.

(δ) Κρυπτογράφηση.

(ε) Συνεχής εφαρμογή αναγνώρισης.

(στ) Χρήση μη επαναλαμβανόμενων κωδικών πρόσβασης.

(ζ) Συστήματα αυτόματου αποκλεισμού του χρήστη, μετά την παρέλευση συγκεκριμένου χρόνου, εφόσον δεν υφίσταται δραστηριότητα από το τερματικό.

8. Καταγραφή Ενεργειών Προσωπικού

Ορίζεται ως ο καθορισμός των διαδικασιών καταγραφής της δημιουργίας, εκπομπής, τροποποίησης ή διαγραφής δεδομένων, όπως περιγράφεται στη ΔΑΠΑΣ.

α. Πολιτική Ασφαλείας

Η καταγραφή των ενεργειών του προσωπικού σε ό,τι αφορά το χειρισμό διαβαθμισμένων πληροφοριών, εφαρμόζεται προκειμένου να αποτραπεί η πρόσβαση σε πληροφορίες για τις οποίες δεν ισχύει η αρχή «ανάγκη γνώσης», καθώς και για να καταστεί δυνατή η έρευνα και η εξακρίβωση της ταυτότητας του προσωπικού που εμπλέκεται στην απώλεια διαβαθμισμένων πληροφοριών.

β. Κίνδυνοι

Το προσωπικό που έχει εξουσιοδότηση πρόσβασης σε συγκεκριμένες πληροφορίες στο πλαίσιο των καθηκόντων του, μπορεί να χρησιμοποιήσει με λάθος τρόπο τα δικαιώματα που έχει, προκειμένου, είτε να αποκτήσει πρόσβαση σε πληροφορίες για τις οποίες δεν ισχύει η «ανάγκη γνώσης», είτε να προβεί σε μη προβλεπόμενες από πλευράς ασφαλείας ενέργειες (όπως να πάρει εκτυπωμένα αντίγραφα εγγράφων για τα οποία δεν είναι εξουσιοδοτημένο).

(1) Γενικές Παραδοχές

(α) Η διαβάθμιση και η ποσότητα των πληροφοριών είναι τέτοια, που η καταγραφή είτε δε δικαιολογείται, είτε δεν αποτελεί πρωταρχικό στόχο.

(β) Όλο το προσωπικό δεν έχει απεριόριστη πρόσβαση σε όλο το υλικό.

(γ) Τα φυσικά ή τα άλλα μέτρα ασφαλείας εντός του ΓΠΑ, όπως ο έλεγχος νευραλγικών θέσεων ή η επιτήρηση ασφαλείας στο ΤΠΑ, είναι ικανά να εμποδίσουν μη εξουσιοδοτημένη εξαγωγή εκτυπωμένων αντιγράφων ή μαγνητικών μέσων αποθήκευσης.

(δ) Δεν εκτελείται καταγραφή των ενεργειών των χρηστών στο ΓΠΑ, που έχουν άμεση πρόσβαση στο ΣΕΠ.

(ε) Όλο το προσωπικό εντός του ΤΠΑ, θεωρείται έμπιστο.

(2) Σημεία Προσοχής στο ΓΠΑ

(α) Οι χρήστες των τερματικών / σταθμών εργασίας στο ΓΠΑ.

(β) Οι χρήστες των ΣΕΠ που έχουν διασυνδεθεί με το υπό εξέταση ΣΕΠ.

(γ) Οι έμμεσοι χρήστες που λαμβάνουν εκτυπωμένα δεδομένα από το ΤΠΑ.

(3) Σημεία Προσοχής στο ΤΠΑ

(α) Οι χρήστες στο ΤΠΑ και η ανάγκη για καταγραφή.

(β) Ο βαθμός στον οποίο ο διακριτικός έλεγχος πρόσβασης μπορεί να αποτελέσει το λόγο μη εκτέλεσης καταγραφής.

(γ) Η επιτήρηση ασφαλείας του προσωπικού.

(δ) Τα καθήκοντα των υπευθύνων ασφαλείας του ΣΕΠ.

(ε) Οι δραστηριότητες που επιδρούν στην ασφάλεια του ΣΕΠ [όπως η διαδικασία έκδοσης κωδικών πρόσβασης, η προσθήκη νέου λογισμικού, αλλαγές στα δικαιώματα χρηστών, δημιουργία αρχείων υποστήριξης (back up)].

(4) Προδιαγραφές των Μέτρων Ασφαλείας του ΓΠΑ και του ΤΠΑ

(α) Μεταφορά των στοιχείων της καταγραφής στους υπεύθυνους ασφαλείας για επαλήθευση.

(β) Τήρηση βιβλίων με δείγματα υπογραφών και των αρχείων ασφαλείας (logs), προκειμένου να καταγράφεται η πρόσβαση στο ΤΠΑ ή σε ειδικούς χώρους εντός αυτού, του προσωπικού συντήρησης, επισκεπτών και λοιπού προσωπικού.

(γ) Καθορισμός διαδικασίας καταγραφής των αρχείων που εξάγονται ή εισάγονται στο ΤΠΑ, σε οποιαδήποτε μορφή, όπως σε ηλεκτρονική, σε εκτυπωμένη, στις μνήμες του ΣΕΠ ή σε μορφή καταχώρισης.

(δ) Καταγραφή των αντιγράφων του λογισμικού του ΣΕΠ και των αρχείων των εφαρμογών (application software).

(ε) Έλεγχος της διαμόρφωσης νέου λογισμικού.

(στ) Καθορισμός περιόδου διατήρησης των στοιχείων της καταγραφής.

(5) Προδιαγραφές των Μέτρων Ασφαλείας του ΗΠΑ

(α) Συλλογή στοιχείων που χρειάζονται για συγκεκριμένες εργασίες καταγραφής (όπως ημερομηνία και ώρα, ταυτότητα χρήστη, επίπεδο διαβάθμισης, είδος εργασίας).

(β) Καταγραφή των δικαιωμάτων πρόσβασης (όπως δημιουργία αρχείου, ανάγνωση, διαβίβαση, εκτύπωση, διαγραφή και εκτέλεση).

(γ) Καταγραφή επιπέδων ασφαλείας (π.χ «ΕΜΠΙΣΤΕΥΤΙΚΟ» και άνω).

(δ) Καταγραφή ενεργειών χρηστών με ειδικά προνόμια (όπως η παραγωγή κωδικού πρόσβασης, η παραγωγή / αναβάθμιση νέου λογισμικού ασφαλείας).

(ε) Καταγραφή χαρακτηριστικών διαβαθμισμένων εξερχόμενων στοιχείων του συστήματος (όπως τι εκτυπώθηκε, σε ποιόν εκτυπωτή, πότε, πόσες σελίδες).

(στ) Σύνταξη προδιαγραφών ασφαλείας.

9. Εντοπισμός Προσπαθειών Παραβίασης Ασφαλείας

Έχει σκοπό την προειδοποίηση για δραστηριότητα στο ΣΕΠ, που μπορεί να επηρεάσει την ασφάλειά του.

α. Πολιτική Ασφαλείας

Όλες οι προσπάθειες παραβίασης της ασφαλείας του ΣΕΠ, απαιτείται να αποκαλύπτονται έγκαιρα.

β. Κίνδυνοι

Οι ενέργειες που δύνανται, είτε να προκαλέσουν, είτε να οδηγήσουν σε παραβίαση ασφαλείας, προσχεδιασμένη ή χωρίς πρόθεση, οι οποίες μπορεί να

μην αποκαλυφθούν, με αποτέλεσμα να μη ληφθούν μέτρα αποφυγής νέων παραβιάσεων ασφαλείας.

(1) Γενικές Παραδοχές

(α) Η πιθανή αφαίρεση υλικού, μέσων μεταφοράς δεδομένων και αρχείων που περιέχουν διαβαθμισμένες πληροφορίες, εντοπίζονται από τις διαδικασίες ασφαλείας που ισχύουν στο ΓΠΑ.

(β) Μη εξουσιοδοτημένη πρόσβαση στο υλικό, με σκοπό τη χρήση διαβαθμισμένων πληροφοριών, εντοπίζεται από τις διαδικασίες ασφαλείας που ισχύουν στο ΓΠΑ.

(γ) Το προσωπικό που έχει πρόσβαση στο ΣΕΠ και έχει εξουσιοδοτηθεί ανάλογα, θεωρείται έμπιστο.

(2) Σημεία Προσοχής στο ΓΠΑ

Ευκαιρίες για πρόσβαση στο σύστημα, από μη έμπιστο προσωπικό.

(3) Σημεία Προσοχής στο ΤΠΑ

Παροχή εμπιστοσύνης στο προσωπικό, ότι αυτό με τη σειρά του πρόκειται να σεβαστεί και να δείξει προσοχή σε θέματα ασφαλείας.

(4) Προδιαγραφές των Μέτρων Ασφαλείας του ΓΠΑ και του ΤΠΑ

(α) Εγκατάσταση συστήματος εντοπισμού παράνομα εισερχόμενου προσωπικού (π.χ συναγερμός).

(β) Συσκευές που αποκαλύπτουν παράνομη πρόσβαση ή προσπάθειες παράνομης πρόσβασης.

(γ) Εκτέλεση επιθεωρήσεων για εντοπισμό παρείσακτων.

(δ) Αναφορές για παραβιάσεις της φυσικής ασφαλείας στον υπεύθυνο ασφαλείας.

(ε) Αναφορές για παραβιάσεις της ηλεκτρονικής ασφαλείας στον υπεύθυνο ασφαλείας.

(στ) Ανάληψη ενεργειών στις περιπτώσεις συναγερμού του ΣΕΠ.

(ζ) Έρευνα για ίχνη ηλεκτρονικής ταυτότητας ή φυσικής επαλήθευσης.

(5) Προδιαγραφές των Μέτρων Ασφαλείας του ΗΠΑ

(α) Αναγνώριση ταυτότητας κατά τη διάρκεια ενεργειών όπως η δημιουργία, μετάδοση, τροποποίηση ή πρόσβαση στα τμήματα του συστήματος.

(β) Ενέργειες μετά τον εντοπισμό αποτυχημένων προσπαθειών για σύνδεση (log-in).

(γ) Ενέργειες μετά τον εντοπισμό αποκλεισμού (lock out) αρχείων.

(δ) Ενέργειες μετά τον εντοπισμό προσπαθειών για χρήση μη εξουσιοδοτημένων εντολών.

(ε) Ενέργειες σε διακοπές λειτουργίας τερματικών ή θέσεων

εργασίας.

(στ) Επιθεώρηση / ανάλυση σε ίχνη ταυτοποίησης.

(ζ) Παροχή προστασίας στα αρχεία εντοπισμού παρανόμων ενεργειών.

(η) Καθορισμός προδιαγραφών ασφαλείας.

10. Επαναχρησιμοποίηση Αντικειμένου

Αφορά στον καθορισμό προδιαγραφών, ώστε να εξασφαλιστεί ότι οι πόροι του συστήματος, όπως η κεντρική μνήμη και οι συσκευές αποθήκευσης δεδομένων, μπορούν να ξαναχρησιμοποιηθούν, ενώ δεν παραβιάζεται η ασφάλεια. Επιπλέον, στην ανάληψη ενεργειών για επανεκκίνηση ή εκκαθάριση δεδομένων που βρέθηκαν σε μη προβλεπόμενη θέση.

11. Ακεραιότητα

Αφορά στις ενέργειες για την προστασία των πληροφοριών από τροποποίηση, με οποιονδήποτε μη εξουσιοδοτημένο τρόπο. Συμπεριλαμβάνονται οι ενέργειες για την εγκαθίδρυση και διατήρηση της ακρίβειας των σχέσεων μεταξύ των δεδομένων. Επίσης, οι ενέργειες για να εξασφαλιστεί ότι όταν οι πληροφορίες κατά τη διάρκεια της επεξεργασίας διακινούνται μεταξύ των χρηστών και των τμημάτων του συστήματος, είναι δυνατός ο εντοπισμός και η αποφυγή απώλειας ή καθ' οιονδήποτε τρόπο τροποποίησης.

12. Διαθεσιμότητα

Αφορά στην εξασφάλιση ότι οι κρίσιμες ενέργειες πραγματοποιούνται χρονικά όταν απαιτείται, ότι η πρόσβαση είναι δυνατή όταν απαιτείται και ότι οι πηγές του συστήματος δε χρησιμοποιούνται άσκοπα. Επιπλέον, συμπεριλαμβάνονται οι ενέργειες για να εξασφαλιστεί ότι οι πηγές είναι διαθέσιμες και εύχρηστες από εξουσιοδοτημένα άτομα και ότι απαγορεύεται η επέμβαση σε κρίσιμες λειτουργίες του συστήματος. Στο πλαίσιο αυτό, αναλαμβάνονται οι ενέργειες δημιουργίας αντιγράφων των βάσεων δεδομένων, ως μέτρο διαθεσιμότητας. Τέλος, συμπεριλαμβάνονται οι ενέργειες εντοπισμού σφαλμάτων και επιδιόρθωσης αυτών, με στόχο τον περιορισμό της επίδρασης στη λειτουργία του ΣΕΠ.

13. Επικοινωνίες Δεδομένων

Καθορισμός των απαιτήσεων για την ασφάλεια των δεδομένων κατά τη διάρκεια μετάδοσης πληροφοριών. Τα μέτρα για την ασφάλεια των επικοινωνιών καλύπτουν τις απαιτήσεις:

α. Ελέγχου πρόσβασης.

β. Ταυτοποίησης.

γ. Εμπιστευτικότητα δεδομένων.

δ. Ακεραιότητα δεδομένων.

ε. Αποφυγή άρνησης λήψης.

14. Αποτελέσματα Ανάλυσης Κινδύνου – Εναπομείναντες Κίνδυνοι

Παρουσιάζονται τα αποτελέσματα της ΑΚ, μέσα από την Αναφορά Διαχείρισης Κινδύνου (ΑΔΚ), καθώς και ο πίνακας κινδύνων / αντίστοιχων αντιμέτρων, στον οποίο παρουσιάζονται οι εναπομείναντες κίνδυνοι, για τους οποίους δεν έ-

χουν ληφθεί μέτρα αντιμετώπισης. Αυτοί οι κίνδυνοι έχουν γίνει αποδεκτοί στο σύνολό τους από την ΑΕΛ και αποτελούν αντικείμενο της περιοδικής συνεχούς εκτέλεσης των Ελέγχων Ασφαλείας (ΕΑΣ). Επίσης, απαιτείται ο καθορισμός των συνθηκών που επιβάλλουν την εκ νέου εκτέλεση της ΕΑΣ.

15. Αρχές / Προσωπικό Διαχείρισης Ασφαλείας

Παρέχονται οι οδηγίες και οι υποχρεώσεις / καθήκοντα, τόσο των αρχών, όσο και του προσωπικού μεμονωμένα, που εμπλέκεται με την ασφάλεια του ΣΕΠ. Συνήθως, αναφέρονται οι παρακάτω:

α. ΑΕΛ (ο εκδότης της ΔΑΠΑΣ).

β. Αρχή Σχεδιασμού του Συστήματος, όπου απαιτείται.

γ. Διαχειριστές Λειτουργίας (ΔΙΑΛ) του ΣΕΠ.

δ. Υπεύθυνος Ασφαλείας Συστήματος (ΥΑΣ).

ε. Υπεύθυνος Ασφαλείας Δικτύου (ΥΑΔ), όπου απαιτείται.

στ. Υπεύθυνοι Ασφαλείας Τοποθεσίας (ΥΑΤ).

ζ. Υπεύθυνος Ασφαλείας του οικονομικού φορέα.

η. Οποιαδήποτε άλλο εμπλεκόμενο προσωπικό, κατά την κρίση της ΑΕΛ.

16. Διαδικασίες Ασφαλούς Λειτουργίας (ΔΑΛ)

Οι ΔΑΛ προκύπτουν από τη ΔΑΠΑΣ και αποτελούν τις οδηγίες προς τους χρήστες για την ασφαλή λειτουργία του ΣΕΠ. Αναλυτική περιγραφή των στοιχείων που συμπεριλαμβάνονται στις ΔΑΛ, ως Παράρτημα «ΙΒ».

17. Έλεγχος Διαμόρφωσης

Περιλαμβάνει πληροφορίες σχετικά με τις διαδικασίες για τον έλεγχο των αλλαγών της διαμόρφωσης σε ό,τι αφορά τα χαρακτηριστικά, τη σχεδίαση, τη λειτουργική ολοκλήρωση του υλικού και του λογισμικού, τις εγκαταστάσεις και τη βιβλιογραφία του ΣΕΠ. Επιπλέον, προσδιορίζονται οι διορθώσεις που είναι επιτρεπτές εντός των προδιαγραφών ασφαλείας, καθώς και οι αλλαγές που έχουν ως αποτέλεσμα την ακύρωση της διαπίστευσης ασφαλείας, που δόθηκε από την ΕΑΔΑ (ή την ΕΔΑ εφόσον έχει καθοριστεί).

18. Συντήρηση

Παρέχονται οι πληροφορίες σχετικά με τις οδηγίες για τη συνεργασία με το φορέα συντήρησης του υλικού και του λογισμικού, τις διαδικασίες εισόδου και παραμονής στους χώρους που είναι εγκατεστημένο το ΣΕΠ, καθώς και τις διαδικασίες για τη μεταφορά του υλικού (hardware) για επισκευή σε χώρο εκτός του ΓΠΑ.

19. Έγγραφα Ασφαλείας

Παρέχονται πληροφορίες και αντίγραφα των εγγράφων που σχετίζονται με την ασφάλεια, όπως τα έγγραφα ελέγχων και σχεδίασης του συστήματος, το εγχειρίδιο ασφαλείας του χρήστη, τα εγχειρίδιο των υπευθύνων ασφαλείας του ΣΕΠ κλπ.

20. Εκπαίδευση

Αφορά στις πληροφορίες σχετικά με τις προδιαγραφές εκπαίδευσης για κάθε κατηγορία εμπλεκόμενου προσωπικού ξεχωριστά (χρηστών, υπευθύνων

ασφαλείας κλπ), καθώς επίσης και το περιοδικό πρόγραμμα εκπαιδεύσεως του προσωπικού, με την ύλη προς διδασκαλία.

21. Διαπίστευση – Επαναδιαπίστευση

Αφορά στις οδηγίες για τα σχετικά με τη διαπίστευση έγγραφα, προκειμένου το ΣΕΠ να διαπιστευθεί από την ΕΑΔΑ (ή την ΕΔΑ εφόσον έχει καθοριστεί). Επίσης, παρέχονται οδηγίες για τον καθορισμό των συνθηκών (είδος εξοπλισμού, διαβάθμιση, εφαρμογές, αριθμός χρηστών και εξουσιοδοτήσεις), κάτω από τις οποίες απαιτείται επαναδιαπίστευση από την ΕΑΔΑ.

22. Απόσυρση από την Ενέργεια / Διάθεση του Εξοπλισμού για άλλες Χρήσεις

Παροχή οδηγιών για τις διαδικασίες που ακολουθούνται τόσο για την απόσυρση του ΣΕΠ από την ενέργεια, όσο και για την περαιτέρω διάθεση του εξοπλισμού.

Αντιναύαρχος Ιωάννης Δρυμούσης ΠΝ
Υπαρχηγός

Ακριβές Αντίγραφο

Ασμχος (ΕΑ) Νικόλαος Ζήκος
Επιτελής ΓΕΕΘΑ/Ε3/1

ΓΕΝΙΚΟ ΕΠΙΤΕΛΕΙΟ ΕΘΝΙΚΗΣ ΑΜΥΝΑΣ
Ε’ ΚΛΑΔΟΣ
ΔΝΣΗ ΑΣΦΑΛΕΙΑΣ
07 Σεπ 20

ΠΑΡΑΡΤΗΜΑ «ΙΒ» ΣΤΟΝ
ΕΚΒΑ

ΟΔΗΓΙΕΣ ΓΙΑ ΤΗ ΣΥΝΤΑΞΗ
ΤΩΝ ΔΙΑΔΙΚΑΣΙΩΝ ΑΣΦΑΛΟΥΣ ΛΕΙΤΟΥΡΓΙΑΣ (ΔΑΛ)

ΓΕΝΙΚΑ

1. Οι οδηγίες που παρέχονται παρακάτω, μπορούν να εφαρμοστούν σε οποιοδήποτε ΣΕΠ, που χειρίζεται (αποθηκεύει, επεξεργάζεται και διαβιβάζει) πληροφορίες διαβάθμισης «ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ», «ΕΜΠΙΣΤΕΥΤΙΚΟ» και «ΑΠΟΡΡΗΤΟ», όπως ορίζονται στον παρόντα Κανονισμό. Συγκεκριμένα, έχουν εφαρμογή σε όλα τα είδη ΣΕΠ, από τους μεμονωμένους (stand alone), τοπικά (LAN) και ευρεία δίκτυα (WAN) Η/Υ, μέχρι εκτεταμένα συστήματα επικοινωνιών και πληροφορικής (CIS), συμπεριλαμβανομένων όλων των φορητών υπολογιστικών συστημάτων (όπως laptops, notebooks, PDAs κλπ).

2. Οι Διαδικασίες Ασφαλούς Λειτουργίας (ΔΑΛ), συντάσσονται παράλληλα με την ανάπτυξη της ΔΑΠΑΣ και παίρνουν την οριστική μορφή τους μετά την έγκριση της ΔΑΠΑΣ, από την ΕΑΔΑ (ή την ΕΔΑ εφόσον έχει καθοριστεί). Η ΑΕΛ, είναι υπεύθυνη για τη σύνταξη και διαβάθμιση ασφαλείας των ΔΑΛ, οι οποίες ειδικά για τα ΣΕΠ με διαβάθμιση ασφαλείας «ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ», «ΕΜΠΙΣΤΕΥΤΙΚΟ» και «ΑΠΟΡΡΗΤΟ» (μόνο στις περιπτώσεις που διασυνδέονται με έτερα ή με δημόσια δίκτυα, όπως το διαδίκτυο), ελέγχονται και εγκρίνονται από την ΕΑΔΑ (ή την ΕΔΑ εφόσον έχει καθοριστεί).

3. Στο Παράρτημα αυτό, παρέχονται οι οδηγίες για το περιεχόμενο και τη σύνταξη των ΔΑΛ, οι οποίες αποτελούν την ακριβή περιγραφή:

α. Της εφαρμογής, των προηγουμένως καθορισμένων απαιτήσεων ασφαλείας, όπως αυτές προκύπτουν από τη ΔΑΠΑΣ.

β. Των λειτουργικών διαδικασιών που ακολουθούνται.

γ. Των ευθυνών του προσωπικού, που χρησιμοποιεί ένα συγκεκριμένο ΣΕΠ.

4. Διευκρινίζεται ότι οι ΔΑΛ, συσχετίζονται αποκλειστικά με τα ζητήματα ασφαλείας και κατά συνέπεια δεν αναφέρονται σε άλλες λειτουργικές διαδικασίες του ΣΕΠ. Οι ΔΑΛ, συντάσσονται με τέτοιο τρόπο, ώστε να λαμβάνουν ως έγγραφο, τη χαμηλότερη δυνατή διαβάθμιση ασφαλείας, μετά από αξιολόγηση των αναφερομένων σε αυτές. Σε περίπτωση που απαιτηθεί, γίνεται η έκδοση Παραρτήματος ή συμπληρωματικού εγγράφου υψηλότερης διαβάθμισης, για το οποίο περιορίζονται οι αποδέκτες.

ΠΕΡΙΕΧΟΜΕΝΑ ΤΩΝ ΔΑΛ

5. Οργάνωση του Συστήματος Ασφαλείας

Στην περιγραφή της οργάνωσης ασφαλείας ενός ΣΕΠ, περιλαμβάνονται τα ακόλουθα:

α. Η συνοπτική περιγραφή του ΣΕΠ και των συστημάτων που το αποτελούν, συμπεριλαμβανομένων των εξωτερικών διασυνδέσεων, καθώς και μια περίληψη των λειτουργικών του δυνατοτήτων.

β. Ο προσδιορισμός των αρχών ή του προσωπικού, των οποίων τα καθήκοντα σχετίζονται με την τήρηση της ασφάλειας του ΣΕΠ, όπως:

(1) Η ΑΕΛ.

(2) Το προσωπικό ασφαλείας της εγκατάστασης που βρίσκεται το ΣΕΠ, όπως ο Υπεύθυνος Ασφαλείας Συστήματος (ΥΑΣ), ο Υπεύθυνος Ασφαλείας Δικτύου (ΥΑΔ), οι Υπεύθυνοι Ασφαλείας Τοποθεσίας (ΥΑΤ), ο Υπεύθυνος Διαχείρισης Κρυπτοϋλικού, οι Διαχειριστές Λειτουργίας (ΔΙΑΛ) του συστήματος και το υπόλοιπο προσωπικό που είναι υπεύθυνο για τα καθημερινά θέματα ασφαλείας.

(3) Η Εθνική Αρχή Ασφαλείας Επικοινωνιών και Πληροφορικής (ΕΑΑΕΠ).

(4) Η Εθνική Αρχή Διαπίστευσης Ασφαλείας (ΕΑΔΑ).

(5) Η Επιτροπή Διαπίστευσης Ασφαλείας (ΕΔΑ), για το συγκεκριμένο ΣΕΠ.

γ. Οι ευθύνες όλου του προσωπικού επί της ασφάλειας και συγκεκριμένα του προσωπικού του φορέα που ασχολείται με τη λειτουργία του ΣΕΠ, συμπεριλαμβανομένου του προσωπικού ασφαλείας, όπως περιγράφεται στην προηγούμενη υποπαράγραφο, του προσωπικού της ΑΕΛ που ελέγχει την ομαλή λειτουργία και την ασφάλεια του ΣΕΠ, καθώς και των κάθε είδους χρηστών αυτού.

δ. Τα στοιχεία για τους τρόπους ασφαλούς λειτουργίας του ΣΕΠ, όπως αποκλειστικός (dedicated), υψηλού επιπέδου (system high) και τις αντίστοιχες διαβαθμίσεις ασφαλείας των δεδομένων.

ε. Οι διαδικασίες για την αναθεώρηση του καταλόγου των εξουσιοδοτημένων χρηστών και των δικαιωμάτων που αυτοί έχουν κατά την πρόσβασή τους στο ΣΕΠ.

στ. Ο τύπος αναφοράς γεγονότων παραβίασης ασφαλείας. Η αναφορά αυτή υποβάλλεται άμεσα στον ΥΑΣ, στην ΑΕΛ, και κατόπιν στην ΕΑΔΑ (στο εξής εννοείται και η ΕΔΑ, αλλά δεν αναφέρεται στο κείμενο), στην ΕΑΑΕΠ, χρησιμοποιώντας μια συγκεκριμένη φόρμα που είναι εγκεκριμένη από την ΕΑΔΑ.

ζ. Οι οδηγίες για την κυκλοφορία των ΔΑΛ σε όλο το εμπλεκόμενο προσωπικό. Απαιτείται επίσης η περιγραφή της διαδικασίας αναφοράς σχετικά με την παραλαβή και την κατανόηση των ΔΑΛ από το προσωπικό. Σε ένα περιβάλλον δικτύου και στο πλαίσιο ανάπτυξης της ανησυχίας του προσωπικού για θέματα ασφαλείας, οι ΔΑΛ και οι τυχόν τροποποιήσεις αυτών, καταχωρούνται σε έναν κεντρικό server, έτσι ώστε οι χρήστες να μπορούν να έχουν άμεση πρόσβαση σε αυτές, εφαρμόζοντας τις κατάλληλες διαδικασίες.

η. Οι τρόποι επικοινωνίας των απομακρυσμένων χρηστών με τους διαχειριστές ασφαλείας του ΣΕΠ και την ΑΕΛ, προκειμένου να είναι δυνατή η παροχή συμβουλευτικών οδηγιών και κατευθύνσεων, επί θεμάτων ασφαλείας.

θ. Οι εξειδικευμένες οδηγίες ασφαλείας επί των επικοινωνιών, όπως π.χ επιχειρησιακές οδηγίες για χρήση συσκευών επικοινωνιών, κρυπτοσυσκευών και αντίστοιχων μηχανισμών.

ι. Οι διαδικασίες ελέγχου του πάσης φύσεως προσωπικού υποστήριξης, εφόσον απαιτηθεί η πρόσβαση του σε έναν τομέα του ΣΕΠ ή σε απομακρυσμένα, εκτός του ΓΠΑ τερματικά.

ια. Οι διαδικασίες για τον έλεγχο των εγκεκριμένων από την ΑΕΛ, ιδιωτικών μετακινούμενων μέσων αποθήκευσης δεδομένων και του κάθε είδους ιδιωτικού λογισμικού και υλικού (hardware) που εισέρχεται στους χώρους που υφίστανται τμήματα του ΣΕΠ.

ιβ. Οι διαδικασίες για τον έλεγχο του εξοπλισμού που χρησιμοποιεί ο ανάδοχος του ΣΕΠ (υλικό και λογισμικό).

6. Φυσική Ασφάλεια

Τα μέτρα φυσικής ασφαλείας λαμβάνονται στο πλαίσιο της αποφυγής μη εξουσιοδοτημένης πρόσβασης σε διαβαθμισμένες πληροφορίες, μη εξουσιοδοτημένης λειτουργίας, άρνησης χρήσης των πόρων του συστήματος και προκειμένου να προστατευθεί ο πολύτιμος και ευαίσθητος εξοπλισμός του ΣΕΠ. Συγκεκριμένα, αναφέρονται τα ακόλουθα:

α. Οι χώροι πληροφορικής – επικοινωνιών που περιλαμβάνουν, ανάλογα με το είδος του ΣΕΠ, το κέντρο διαχείρισης δικτύου, το κέντρο κρυπτογράφησης, το χώρο που υφίστανται οι servers αποθήκευσης δεδομένων, τους χώρους τερματικών και θέσεων εργασίας, τα γραφεία, τους χώρους φύλαξης αντιγράφων ασφαλείας και τους χώρους δευτερεύοντος εξοπλισμού ανάγκης, συμπεριλαμβανομένης της θέσης και της φύσης όλου του συνδεδεμένου εξοπλισμού. Επίσης, υπάρχει περιγραφή των καλωδιώσεων με αναφορά στα κόκκινα και στα μαύρα καλώδια (μέσω των κόκκινων καλωδίων διαβιβάζονται διαβαθμισμένα δεδομένα χωρίς κρυπτογράφηση, ενώ μέσω των μαύρων καλωδίων κρυπτογραφημένα δεδομένα) και με αποτυπωμένο το διαχωρισμό των κόκκινων από τα μαύρα καλώδια. Επίσης, διευκρινίζονται οι διαδικασίες ασφαλείας που εφαρμόζονται για τη διασύνδεση απομακρυσμένων τερματικών του ΣΕΠ.

β. Τα χαρακτηριστικά των χώρων πληροφορικής / επικοινωνιών σε ό,τι αφορά τη φυσική ασφάλεια, συμπεριλαμβανομένων των στοιχείων που αφορούν στα κλειδιά ή/και τους συνδυασμούς κλειδαριών (η ταυτότητά τους, ο χώρος που φυλάσσονται τα αρχεία και το προσωπικό που έχει πρόσβαση σε αυτά). Επίσης, περιγράφονται οι διαδικασίες, ώστε να εξασφαλίζεται μετά το εργάσιμο ωράριο, η φυσική ασφάλεια των χώρων του ΣΕΠ.

γ. Τα μέτρα ελέγχου πρόσβασης προσωπικού / εξοπλισμού και συγκεκριμένα:

(1) Οι διαδικασίες και τα αρχεία που τηρούνται για τον έλεγχο των επισκεπτών, συμπεριλαμβανομένων των μέτρων που εφαρμόζονται για την απότροπή οπτικής επαφής με οθόνες και δεδομένα του ΣΕΠ, από μη εξουσιοδοτημένο προσωπικό.

(2) Οι κάρτες πρόσβασης. Οι τύποι καρτών πρόσβασης που χρησιμοποιούνται, οι λειτουργικές απαιτήσεις για τη χρήση αυτών (που φέρονται, πως επιδεικνύονται, σε ποια σημεία γίνεται ο έλεγχος αυτών), ποιο είναι το αρμόδιο προσωπικό για την έγκριση ή/και την έκδοση των καρτών πρόσβασης και τις λεπτομέρειες της διαδικασίας εφαρμογής του όλου μέτρου και της τήρησης και φύλαξης αρχείων που σχετίζονται με την έκδοση των καρτών πρόσβασης.

(3) Οι διαδικασίες ελέγχου εισόδου / εξόδου τμημάτων του εξοπλισμού του ΣΕΠ, που ισχύουν τόσο στο ΓΠΑ όσο και στο ΤΠΑ.

δ. Τα βασικά χαρακτηριστικά των συστημάτων εντοπισμού εισβολέων, που καλύπτουν το περιβάλλον στο οποίο έχει εγκατασταθεί το ΣΕΠ και συγκεκριμένα τους χώρους που είναι εγκατεστημένα, τις προδιαγραφές λειτουργίας, τις διαδικασίες δοκιμών, τη συχνότητα των δοκιμών, τις συνθήκες που ισχύουν για την ενεργοποίησή τους και τις διαδικασίες αντίδρασης του αρμόδιου προσωπικού σε κατάσταση συναγερμού.

7. Ασφάλεια Προσωπικού

α. Οποιοδήποτε πρόσωπο που μπορεί να αποκτήσει πρόσβαση (νόμιμη ή παράνομη) σε χώρο που υφίσταται εξοπλισμός του ΣΕΠ, θεωρείται ότι είναι σε θέση να εμπλακεί ή να κάνει ζημιά στον εξοπλισμό και στις διαβαθμισμένες πληροφορίες που είτε παρουσιάζονται στις οθόνες των τερματικών, είτε εκτυπώνονται για κάποια χρήση. Εννοείται ότι το προσωπικό που έχει νόμιμη πρόσβαση στις εγκαταστάσεις του ΣΕΠ, μπορεί είτε το ίδιο να επιτύχει μη εξουσιοδοτημένη και λαθραία κατοχή των πληροφοριών, είτε να επιτρέψει (εκούσια ή ακούσια) σε μη εξουσιοδοτημένα άτομα να αποκτήσουν πρόσβαση σε διαβαθμισμένες πληροφορίες. Επιπλέον, μπορεί να υπάρξει συγκεκριμένο προσωπικό (όπως για παράδειγμα προγραμματιστές συστήματος, αναλυτές συστήματος, μηχανικοί συστήματος, προσωπικό συντήρησης, εμπορικοί σύμβουλοι), με αποκλειστική γνώση των χαρακτηριστικών γνωρισμάτων ασφαλείας του ΣΕΠ και ως εκ τούτου να έχει τη δυνατότητα, είτε να παραβιάσει τα μέτρα ασφαλείας, είτε να τα παρακάμψει.

β. Στην παράγραφο αυτή, παρέχονται οι λεπτομέρειες, όπου απαιτείται, όλων των πτυχών της ασφάλειας προσωπικού, συμπεριλαμβάνοντας απαραιτήτως τα παρακάτω:

(1) Τα είδη εξουσιοδοτήσεων ασφαλείας και τον αναλυτικό κατάλογο του εξουσιοδοτημένου εμπλεκόμενου με το ΣΕΠ προσωπικού, όπου περιγράφονται:

(α) Οι προδιαγραφές έκδοσης εξουσιοδότησης ασφαλείας για το προσωπικό ασφαλείας της εγκατάστασης που βρίσκεται το ΣΕΠ, όπως ο ΥΑΣ, ο ΥΑΔ, οι ΥΑΤ, ο Υπεύθυνος Διαχείρισης Κρυπτοϋλικού, οι ΔΙΑΛ του συστήματος, το υπόλοιπο προσωπικό που είναι υπεύθυνο για τα καθημερινά θέματα ασφαλείας και τους κάθε είδους χρήστες του ΣΕΠ.

(β) Το απαιτούμενο προσωπικό ή αυτό που επιτρέπεται να βρίσκεται σε χώρους του ΣΕΠ, τόσο κατά τη διάρκεια της επεξεργασίας δεδομένων, όσο και εκτός ωρών λειτουργίας συμπεριλαμβανομένων των εξουσιοδοτήσεων ασφαλείας αυτού του προσωπικού.

(γ) Οι περιπτώσεις εφαρμογής της αρχής «των 2 ατόμων» στους χώρους του ΣΕΠ, σύμφωνα με την οποία απαιτείται η παρουσία 2 ατόμων τα οποία γνωρίζουν διαφορετικά τμήματα ή κωδικούς πρόσβασης, για τη διαδικασία ενεργοποίησης και τερματισμού μιας ιδιαίτερα σημαντικής λειτουργίας του συστήματος που αφορά στην ασφάλειά του.

(δ) Το απαιτούμενο προσωπικό ή αυτό που επιτρέπεται να βρίσκεται σε απομακρυσμένες θέσεις τερματικών / σταθμών εργασίας του ΣΕΠ κατά τη διάρκεια της επεξεργασίας δεδομένων, καθώς και εκτός ωρών λειτουργίας συμπεριλαμβανομένων των εξουσιοδοτήσεων ασφαλείας αυτού του προσωπικού.

(2) Περιγραφή του Βασικού Προσωπικού και συγκεκριμένα:

(α) Οποιαδήποτε στοιχεία σχετικά με το προσωπικό που θεωρείται βασικό, όπως σχεδιαστές / αναλυτές / προγραμματιστές συστημάτων, υπεύθυνο προσωπικό για τη λειτουργία, εμπορικοί σύμβουλοι, μηχανικοί συστημάτων και τεχνικό προσωπικό ή προσωπικό συντήρησης, συμπεριλαμβάνοντας τα ονόματα και τις θέσεις αυτού. Όλα αυτά τα στοιχεία αποτυπώνονται σε κατάλογο, που αποτελεί υποτμήμα των ΔΑΛ.

(β) Οποιεσδήποτε συγκεκριμένες λεπτομέρειες σχετικά με βοηθητικό προσωπικό, όπως συνεργεία καθαρισμού και συντήρησης κτιρίων.

(γ) Οποιεσδήποτε λεπτομέρειες σχετικά με το ποιος έχει την έγκριση πρόσβασης σε κάθε περιοχή, κτίριο ή γραφείο.

(3) Εκπαίδευση του προσωπικού στα θέματα ασφαλείας, όπου περιγράφονται οι προδιαγραφές εκπαίδευσης σε θέματα ασφαλείας για όλο το αρμόδιο προσωπικό, στην οποία συμπεριλαμβάνονται όλες οι πτυχές της ασφάλειας, όπως φυσική ασφάλεια, ασφάλεια προσωπικού, ασφάλεια πληροφοριών και ασφάλεια επικοινωνιών – πληροφορικής.

8. Ασφάλεια Διαβαθμισμένων Εγγράφων

Η ασφάλεια των πληροφοριών, συμπεριλαμβάνει όλους του τύπους των εγγράφων που χρησιμοποιούνται στο ΣΕΠ, καθώς και τα φορητά υπολογιστικά συστήματα (ΦΥΣ) όπως laptops, notebooks και PDA’s, τα οποία διαθέτουν σκληρό δίσκο ή μνήμη για την αποθήκευση πληροφοριών. Έτσι, παρέχονται οι λεπτομέρειες, όπου απαιτείται, για την ασφάλεια των πληροφοριών και συγκεκριμένα:

α. Οι χρησιμοποιούμενοι τύποι εγγράφων.

β. Τα χαρακτηριστικά διαβάθμισης που εφαρμόζονται για τους διάφορους τύπους εγγράφων.

γ. Οι διαδικασίες για την κατάλληλη διαβάθμιση και ταξινόμηση των εγγράφων.

δ. Οι προδιαγραφές αποθήκευσης των εν χρήση εγγράφων.

ε. Οι ευθύνες και οι διαδικασίες για την καταχώριση και τον έλεγχο των εγγράφων, για την επιθεώρηση των αρχείων συμπεριλαμβανομένης και της συχνότητας των επιθεωρήσεων.

στ. Οι διαδικασίες για την απόκτηση, την αποθήκευση, τον έλεγχο και την καταγραφή όλων των αποθηκευτικών μέσων, συμπεριλαμβανομένων των ΦΥΣ. Ειδικότερα, για τις βάσεις αποθήκευσης των δεδομένων αναφέρονται:

(1) Οι διαβαθμίσεις, οι προδιαγραφές σήμανσης και οι τοποθεσίες των βάσεων αποθήκευσης δεδομένων.

(2) Τα αρχεία που τηρούνται για κάθε έγγραφο, συμπεριλαμβανομένων εκείνων που τηρούνται σε άλλες θέσεις (όπως για παράδειγμα αντίγραφα ασφαλείας), τους καταλόγους ταξινόμησης εγγράφων ή το αυτοματοποιημένο σύστημα ταξινόμησης, τις φόρμες μετάδοσης και λήψης αρχείων και τον όγκο των ιστορικών αρχείων που τηρούνται.

(3) Οι διαδικασίες και οι αντίστοιχες φόρμες για την αίτηση λήψης δεδομένων.

(4) Τα καθήκοντα του προσωπικού φύλαξης των βιβλιοθηκών των αρχείων.

(5) Οι διαδικασίες για την αποθήκευση των εγγράφων ελέγχου.

ζ. Οι διαδικασίες για την παραλαβή, την ανταλλαγή και τη διάδοση των εγγράφων συμπεριλαμβανομένων των αρμοδιοτήτων του προσωπικού που είναι υπεύθυνο για την εισαγωγή / εξαγωγή αρχείων και τις διαδικασίες για τον έλεγχο όλων των εισερχομένων μέσων αποθήκευσης δεδομένων, για τον έλεγχο ιών υπολογιστών και άλλου κακόβουλου λογισμικού.

η. Οι ευθύνες και οι διαδικασίες για τον αποχαρακτηρισμό, την υποβάθμιση, την καταστροφή ή την απόσυρση των εγγράφων, καλύπτοντας τη χρήση των αποτεφρωτήρων, των συσκευών απομαγνητισμού του εξοπλισμού, τον εξοπλισμό διάλυσης του υλικού, καθώς και τον τόπο, τον τρόπο, το προσωπικό και τη συχνότητα που γίνεται η καταστροφή αυτή.

9. Ασφάλεια Η/Υ

Στην παράγραφο αυτή, αναλύονται οι μηχανισμοί ασφαλείας των Η/Υ, σε ό,τι αφορά το υλικό (hardware), στο λογισμικό λειτουργίας (firmware) και στο λογισμικό εφαρμογών (software), που μπορούν να συμβάλουν χωριστά, αλλά και σε συνδυασμό μεταξύ τους, στην ασφάλεια του ΣΕΠ. Συγκεκριμένα, αναφέρονται οι διαδικασίες:

α. Ταυτοποίησης των υπηρεσιών, των συσκευών, των μέσων και των χρηστών, που αποτελούν ξεχωριστά στοιχεία για τα συστήματα ελέγχου ασφαλείας.

β. Ελέγχου πρόσβασης, μέσω ειδικού λογισμικού, των χρηστών στα στοιχεία του συστήματος (υλικό, λογισμικό λειτουργίας και λογισμικό εφαρμογών). Επιπλέον, προσδιορίζονται εκείνα τα στοιχεία του συστήματος όπου απαγορεύεται η πρόσβαση, χωρίς ειδική εξουσιοδότηση.

γ. Εντοπισμού, μέσω μηχανισμών ελέγχου και αναφοράς της μη εξουσιοδοτημένης δραστηριότητας (π.χ προσπάθεια μη εξουσιοδοτημένης πρόσβασης), καθώς και των διαδικασιών αντίδρασης και αναφοράς τέτοιων γεγονότων.

δ. Ελέγχου εφαρμογής των τριών προαναφερθεισών διαδικασιών.

10. Ασφάλεια Υλικού (Hardware)

Σχετικά με τα προστατευτικά μέτρα ασφαλείας, που αφορούν στα φυσικά τμήματα του υλικού του ΣΕΠ, αναφέρονται τα παρακάτω:

α. Οι σχετικές με την ασφάλεια, διαδικασίες εκκίνησης του συστήματος και τα έγγραφα στα οποία αυτές προβλέπονται.

β. Οι σχετικές με την ασφάλεια, διαδικασίες τερματισμού λειτουργίας του συστήματος και τα έγγραφα στα οποία αυτές προβλέπονται.

γ. Οι σχετικές με την ασφάλεια, οδηγίες και διαδικασίες για τη σύνδεση και αποσύνδεση του εξοπλισμού και τα έγγραφα στα οποία αυτές προβλέπονται.

δ. Οι διαδικασίες για την εκτέλεση ελέγχων, για τον εντοπισμό ιχνών παράνομης επέμβασης στον εξοπλισμό του ΣΕΠ, όπως η παράνομη προσπάθεια τροποποίησης χαρακτηριστικών της κεντρικής μονάδας ενός Η/Υ ή της καλωδίωσης του.

ε. Η διαμόρφωση των Η/Υ, που εφαρμόζεται κατά τη διάρκεια συγκεκριμένων τύπων επεξεργασίας δεδομένων, όπως ποια τερματικά / θέσεις εργασίας αποσυνδέονται και ποιες περιφερειακές μονάδες τίθενται εκτός λειτουργίας, όταν εκτελείται κάθε διαφορετικός τύπος επεξεργασίας δεδομένων.

στ. Οι διαδικασίες για την εξασφάλιση συγκεκριμένης διαμόρφωσης των Η/Υ, στο πλαίσιο προετοιμασίας αυτών, για τη συντήρηση και την επισκευή τους, όπου συμπεριλαμβάνονται τα παρακάτω:

(1) Ο καθορισμός του επιπέδου της έγκρισης που απαιτήθηκε για την τροποποίηση εξοπλισμού, την εισαγωγή νέου υλικού και λογισμικού ή την απόσυρση οποιουδήποτε τμήματος του υλικού, (συμπεριλαμβανομένων των επεξεργαστών) που μπορούν να αποθηκεύσουν, να επεξεργαστούν ή να διαβιβάσουν διαβαθμισμένες πληροφορίες.

(2) Ο καθορισμός των περιορισμών που επιβάλλονται όταν εργασίες προγραμματισμένης συντήρησης επιτρέπεται ή όχι να εκτελεστούν.

(3) Τα στοιχεία των διαγνωστικών ρουτινών που ενεργοποιούνται, είτε στη συνήθη λειτουργία, είτε κατά τη διάρκεια προγραμματισμένης συντήρησης, είτε στο πλαίσιο τροποποίησης του υλικού.

(4) Οι προδιαγραφές όλων των τύπων προγραμματισμένων εργασιών συντήρησης συμπεριλαμβανομένων των οδηγιών για την εξακρίβωση οποιουδήποτε εκτυπωμένου διαγνωστικού εγγράφου που μπορεί να περιέχει διαβαθμισμένες πληροφορίες.

(5) Οι διαδικασίες για την αναγνώριση, την αποθήκευση και τον έλεγχο των ανταλλακτικών, του σχετικού με την ασφάλεια υλικού.

ζ. Οι διαδικασίες που ακολουθούνται σε περίπτωση αστοχίας υλικού, όπου περιγράφονται οι ενέργειες που απαιτείται να αναληφθούν, καθώς και το ποιος πρόκειται να τις εκτελέσει, ώστε να εξασφαλιστεί το υλικό σε περίπτωση που, αιφνίδια διακοπεί η λειτουργία του, όπως επίσης και τα σχετικά με αυτή τη διακοπή λειτουργίας, αρχεία που τηρούνται.

η. Οι διαδικασίες για την επανασύνδεση των απομακρυσμένων τερματικών ή θέσεων εργασίας, που έχουν αποσυνδεθεί για λόγους ασφαλείας.

11. Ασφάλεια Λογισμικού (Software)

Για τα προστατευτικά μέτρα ασφαλείας, που αφορούν στην ασφάλεια του λογισμικού, αναφέρονται τα παρακάτω:

α. Τα χαρακτηριστικά (τύπος – αναβαθμίσεις – πιστοποιητικό αυθεντικότητας) του λειτουργικού συστήματος ή συστημάτων που χρησιμοποιούνται.

β. Τα χαρακτηριστικά (τύπος – αναβαθμίσεις – πιστοποιητικό αυθεντικότητας) του λογισμικού υποστήριξης (utility programs) που υποστηρίζουν:

(1) Τις λειτουργίες αυτοματισμού γραφείου (office automation functions).

(2) Τα συστήματα διαχείρισης βάσεων δεδομένων.

(3) Την ταξινόμηση των αρχείων που περιέχουν δεδομένα.

γ. Τα χαρακτηριστικά (τύπος – αναβαθμίσεις – πιστοποιητικό αυθεντικότητας) των εφαρμογών που καλύπτουν συγκεκριμένες απαιτήσεις των χρηστών.

δ. Το έγγραφο έγκρισης από την ΕΑΑΕΠ, για τη χρήση παντός είδους λογισμικού που χρησιμοποιείται στο ΣΕΠ.

ε. Η πολιτική αναγνώρισης των λογαριασμών των απλών χρηστών, των ειδικών ομάδων χρηστών και η διαδικασία κατανομής του λογαριασμών αυτών. Επίσης, οι διαδικασίες για τη διαγραφή των λογαριασμών των χρηστών, κατά την περίπτωση μετάθεσής τους ή όταν διαπιστωθεί περιστατικό παραβίασης ασφαλείας.

στ. Η πολιτική επικύρωσης ταυτότητας των χρηστών, συμπεριλαμβανομένης της διαδικασίας επικύρωσης ταυτότητας [π.χ με χρήση κωδικών πρόσβασης, κλειδιών (tokens), βιομετρικών χαρακτηριστικών], των διαδικασιών ελέγχου και αλλαγής ταυτότητας των χρηστών που χρησιμοποιεί η εκδίδουσα αρχή, τη συχνότητα της αλλαγής αυτών των ταυτοτήτων, των αρχείων που αφορούν στους ελέγχους και το προσωπικό που τα τηρεί και τις διαδικασίες χρήσης των μηχανισμών επικύρωσης.

ζ. Οι μηχανισμοί ελέγχου πρόσβασης και συγκεκριμένα οι διαδικασίες για την εφαρμογή διακριτικού ή υποχρεωτικού ελέγχου της πρόσβασης στις πληροφορίες / υπηρεσίες / συσκευές (π.χ εκτυπωτές, σαρωτές κλπ), του συστήματος. Επίσης, οι διαδικασίες για την έκδοση των δικαιωμάτων των χρηστών και τις άδειες για τη χρησιμοποίηση των υπηρεσιών / πόρων του ΣΕΠ και τέλος τα στοιχεία για τις αρμόδιες αρχές και για την τήρηση των αρχείων ελέγχου πρόσβασης.

η. Οι εκδόσεις του λειτουργικού συστήματος, των αντίστοιχων προγραμμάτων υποστήριξης και των προγραμμάτων λογισμικού εφαρμογών που πρόκειται να χρησιμοποιηθούν σε ειδικές περιπτώσεις.

θ. Ο έλεγχος του εξοπλισμού για την αντιγραφή ή την τροποποίηση του λογισμικού λειτουργίας και τα στοιχεία της εμπλεκόμενης αρμόδιας αρχής και των εγγράφων που απαιτούνται προς τούτο.

ι. Τα μέτρα που λαμβάνονται για τον αποχαρακτηρισμό, την υποβάθμιση ή διαγραφή αντιγράφων ασφαλείας και τις διαδικασίες ώστε να εξασφαλιστεί ότι οι μνήμες (buffers) των περιφερειακών συσκευών δεν έχουν δεδομένα.

ια. Οι διαδικασίες λήψης και εισαγωγής δεδομένων, την έγκριση εξουσιοδότησης για αυτήν τη διεργασία και τα αντίστοιχα απαιτούμενα τυποποιημένα έγγραφα.

ιβ. Η διαβάθμιση των δεδομένων που χρησιμοποιούνται.

ιγ. Ο έλεγχος ενεργειών αντιγραφής δεδομένων.

ιδ. Η χρήση γλωσσών προγραμματισμού, των μεταγλωττιστών (compilers) και των μακροεντολών.

ιε. Οι διαδικασίες που ακολουθούνται σε περίπτωση βλάβης και τα σχετικά αρχεία που τηρούνται.

ιστ. Ο έλεγχος των εκτυπωμένων δεδομένων.

12. Προστασία από Κακόβουλο Λογισμικό

Σε ό,τι αφορά την αντιμετώπιση του κακόβουλου λογισμικού, συμπεριλαμβάνεται μία σύνοψη όλων των μηχανισμών και των διαδικασιών (αυτοματοποιημένων και χειροκίνητων) προστασίας του ΣΕΠ. Συγκεκριμένα, περιγράφονται:

α. Οι διαδικασίες για τον έλεγχο του εγκατεστημένου λογισμικού λειτουρ-

γίας, του αντίστοιχου λογισμικού υποστήριξης και του λογισμικού εφαρμογών, για την ύπαρξη κακόβουλου λογισμικού, συμπεριλαμβανομένων των διαδικασιών για τη διαγραφή του, σε περίπτωση που εντοπιστεί.

β. Οι διαδικασίες για τον έλεγχο των μέσων αποθήκευσης δεδομένων, τα οποία ελήφθησαν από εξωτερικές πηγές, συμπεριλαμβανομένων των διαδικασιών για την εξυγίανση όσων βρέθηκαν μολυσμένα.

γ. Οι διαδικασίες για τον έλεγχο των ηλεκτρονικών μηνυμάτων (e-mails) και των συνημμένων αυτών, εφόσον ελήφθησαν από εξωτερικές πηγές.

δ. Οι διαδικασίες εντοπισμού κακόβουλου λογισμικού που ακολουθούν οι χρήστες.

ε. Οι ευθύνες των χρηστών, εφόσον είτε ηθελημένα, είτε λόγω αμέλειάς τους, προκάλεσαν την εισαγωγή κακόβουλου λογισμικού στο ΣΕΠ.

στ. Οι διαδικασίες που ακολουθούνται από τον ΥΑΣ, τον ΥΑΔ και τους ΥΑΤ, όταν εντοπιστεί κακόβουλο λογισμικό, για την ενημέρωση και την υποβολή της αντίστοιχης αναφοράς, τόσο στο κέντρο διαχείρισης συμβάντων ασφαλείας του ΣΕΠ, όσο και στην ΑΕΛ, στην ΕΑΔΑ και στην ΕΑΑΕΠ.

13. Αυτοματοποιημένο Σύστημα Διαχείρισης και Αποτύπωσης Ενεργειών

Στην παράγραφο αυτή, περιγράφεται το σύστημα αυτοματοποιημένης διαχείρισης ασφαλείας, των διαδικασιών καταγραφής ενεργειών (αυτοματοποιημένων και μη), καθώς και των αντίστοιχων ευθυνών του προσωπικού που εμπλέκεται με αυτό. Συγκεκριμένα αναφέρονται:

α. Οι διαδικασίες για τη λειτουργία των αυτοματοποιημένων εργαλείων / προγραμμάτων διαχείρισης και λεπτομέρειες για τις εγκαταστάσεις όπου εκτελείται η καταγραφή ενεργειών.

β. Οι διαδικασίες καταγραφής ενεργειών και επιβεβαίωσης εξουσιοδότησης των χρηστών, καθώς και τα στοιχεία των σχετικών με την ασφάλεια γεγονότων που καταγράφονται (όπως ο τύπος του γεγονότος, οι πληροφορίες που συνδέονται με το κάθε γεγονός κλπ).

γ. Η διαδικασία χρήσης των αρχείων ασφαλείας (security journals), στο πλαίσιο της έρευνας προβληματικής λειτουργίας και της ανίχνευσης μη ομαλών λειτουργιών, συμπεριλαμβανομένων των στοιχείων των γεγονότων που ελέγχονται.

δ. Οι προδιαγραφές των συνηθισμένων επιθεωρήσεων για τον έλεγχο των ιχνών καταγραφής (audit trails), προκειμένου να αποτραπούν οι μη εξουσιοδοτημένες προσβάσεις, να αποκαλυφθούν άμεσα οι τυχόν προσπάθειες για κάτι τέτοιο και να ληφθούν τα απαραίτητα διορθωτικά μέτρα, εάν εντοπιστεί μη εξουσιοδοτημένη πρόσβαση.

ε. Οι ευθύνες του προσωπικού που ασχολείται με τη λειτουργία και επικύρωση της ακεραιότητας των αυτοματοποιημένων εργαλείων / προγραμμάτων διαχείρισης ασφαλείας, σε περίπτωση που εντοπιστούν ανωμαλίες στη λειτουργία αυτών.

στ. Οι διαδικασίες αντίδρασης σε συγκεκριμένες έκτακτες καταστάσεις, όπως η ενεργοποίηση συναγερμών.

ζ. Οι λεπτομέρειες της περιόδου διατήρησης των αρχείων καταγραφής

ενεργειών.

η. Οι ενέργειες που αναλαμβάνονται σε περίπτωση δυσλειτουργίας του συστήματος καταγραφής ενεργειών.

14. Ασφάλεια Κρυπτογράφησης

Στην παράγραφο αυτή, αναφέρονται τα παρακάτω που αφορούν στην ασφάλεια κρυπτογράφησης:

α. Τα στοιχεία του αρμόδιου προσωπικού (όπως όνομα, τίτλος εργασίας και ευθύνες) για την εφαρμογή και τον έλεγχο των διαδικασιών για την κρυπτογραφική ασφάλεια, καθώς και τις αντίστοιχες εξουσιοδοτήσεις που έχει το προσωπικό που ασχολείται με αυτή.

β. Οι διαδικασίες για τη χρήση του κρυπτογραφικού εξοπλισμού, όπως οι λεπτομέρειες για τη φύλαξη του κρυπτοϋλικού και οι ευθύνες του εμπλεκόμενου προσωπικού.

γ. Η συνοπτική περιγραφή των συσκευών κρυπτογράφησης που χρησιμοποιούνται στο ΣΕΠ.

15. Ασφάλεια Ηλεκτρομαγνητικών Εκπομπών

Σε ό,τι αφορά την ασφάλεια των ηλεκτρομαγνητικών (Η/Μ) εκπομπών, περιγράφονται τα παρακάτω:

α. Τα μέτρα προστασίας του ΣΕΠ επί θεμάτων TEMPEST (εκμετάλλευση ανεπιθύμητων ηλεκτρομαγνητικών εκπομπών του υλικού).

β. Οι διαδικασίες για τον καθορισμό των απαιτήσεων επί θεμάτων TEMPEST, που αφορούν τις εγκαταστάσεις του συστήματος, με τη συνεργασία της Εθνικής Αρχής TEMPEST.

γ. Οι διαδικασίες για τον έλεγχο των χώρων, όπου οι φορητοί Η/Υ και οι μεμονωμένοι Η/Υ (stand alone), μπορούν να λειτουργήσουν μέσα σε μια εγκατάσταση.

δ. Οι διαδικασίες για την εγκατάσταση του εξοπλισμού, σύμφωνα με τις οδηγίες του κατασκευαστή και του παρόντος Κανονισμού.

ε. Οι προδιαγραφές για τον έλεγχο του υλικού και το πρόγραμμα εκτέλεσης αυτού, που έχει συμφωνηθεί με την Εθνική Αρχή TEMPEST.

στ. Τα μέτρα για το φυσικό διαχωρισμό του εξοπλισμού που χειρίζεται τα διαβαθμισμένα δεδομένα, από τον αντίστοιχο που χειρίζεται αδιαβάθμητα δεδομένα.

16. Ασφάλεια Μετάδοσης Δεδομένων

Σε ό,τι αφορά τα χαρακτηριστικά της ασφάλειας μετάδοσης των δεδομένων, αναφέρονται τα ακόλουθα:

α. Ο προσδιορισμός του αρμόδιου προσωπικού, για την εφαρμογή και τον έλεγχο των διαδικασιών για την ασφάλεια μετάδοσης δεδομένων.

β. Οι διαδικασίες για τον περιορισμό των πληροφοριών που περιέχονται στα μη κρυπτογραφημένα τμήματα των δεδομένων που εκπέμπονται.

γ. Οι λειτουργικές διαδικασίες για τα συστήματα που ελέγχουν και ασφαλίζουν τη ροή των δεδομένων κατά τη μετάδοσή τους.

17. Σχέδιο Εκτάκτου Ανάγκης και Αντιμετώπισης Ειδικών Καταστάσεων

α. Σε ό,τι αφορά τις διαδικασίες εκτάκτου ανάγκης, αναφέρονται τα ακόλουθα:

(1) Οι λεπτομέρειες των διαδικασιών για τη δημιουργία αντιγράφων ασφαλείας των αρχείων, που αφορούν στην ασφάλεια.

(2) Τα χαρακτηριστικά των αντιγράφων ασφαλείας, τι και που φυλάσσεται, με ποια μορφή, με ποια συχνότητα δημιουργούνται, ποιος έχει εξουσιοδότηση για τη δημιουργία τους, ποιος έχει πρόσβαση σε αυτά, για πόσο χρόνο τηρούνται κλπ.

(3) Οι προδιαγραφές μετάδοσης και αποθήκευσης των αντιγράφων ασφαλείας.

(4) Οι διαδικασίες για την πρόσβαση και τη χρήση των αντιγράφων ασφαλείας.

β. Επιπλέον, παρέχονται οι διαδικασίες καταστροφής των δεδομένων, σε περίπτωση εκτάκτου ανάγκης, καθώς και οι διαδικασίες για την ανάκτηση των δεδομένων, στις περιπτώσεις:

(1) Αστοχίας του υλικού, του λογισμικού ή εισόδου στο ΣΕΠ κακόβολου λογισμικού.

(2) Διακοπής των ασύρματων συνδέσεων των επικοινωνιών του ΣΕΠ.

(3) Διακοπής της ηλεκτρικής παροχής ή σε διακυμάνσεις τάσεως.

(4) Περιβαλλοντικών φαινομένων (όπως καπνός, πυρκαγιά, έκρηξη, πλημμύρα, υγρή διαρροή, προβλήματα δομών κτιρίου, σεισμοί, τυφώνες και άλλες φυσικές καταστροφές).

(5) Γεγονότων που σχετίζονται με δολιοφθορά, τρομοκρατία, αστικές αναταραχές ή απειλές για βομβιστικές ενέργειες.

γ. Επίσης, περιγράφονται οι διαδικασίες καταστροφής του κρυπτογραφικού εξοπλισμού, σε περίπτωση έκτακτης ανάγκης.

δ. Τέλος, αναφέρεται η συχνότητα ασκήσεων, κατά τις οποίες εφαρμόζονται οι διαδικασίες εκτάκτου ανάγκης.

18. Διαχείριση Διαμόρφωσης

α. Η διαχείριση της διαμόρφωσης ενός ΣΕΠ περιλαμβάνει τον προσδιορισμό, τον έλεγχο και την καταγραφή όλων των αλλαγών που γίνονται σε ένα ΣΕΠ κατά τη διάρκεια όλων των σταδίων της διάρκειας ζωής του.

β. Σε ό,τι αφορά τα χαρακτηριστικά της διαχείρισης διαμόρφωσης του ΣΕΠ, αναφέρονται τα παρακάτω:

(1) Οι ευθύνες του προσωπικού για τον έλεγχο και την οργάνωση των αναβαθμίσεων της διαμόρφωσης.

(2) Τα έγγραφα στα οποία περιγράφεται η βασική διαμόρφωση του ΣΕΠ.

(3) Οι έλεγχοι που εφαρμόζονται, ώστε να εξασφαλιστεί ότι η εγκεκριμένη βασική διαμόρφωση του ΣΕΠ και το εγκεκριμένο λογισμικό του δεν μπορεί

να υποστούν αλλαγές.

(4) Οι διαδικασίες που εφαρμόζονται για τις τροποποιήσεις των εγγράφων στα οποία περιγράφονται οι προδιαγραφές και η βασική σχεδίαση του συστήματος.

(5) Οι έλεγχοι που εφαρμόζονται για τη διαπίστωση τυχόν αλλαγών στον πηγαίο κώδικα, καθώς και την τρέχουσα έκδοση αυτού.

(6) Οι έλεγχοι που εφαρμόζονται πριν την εγκατάσταση κάθε νέας έκδοσης του λειτουργικού συστήματος, του λογισμικού υποστήριξης και των εφαρμογών.

(7) Οι έλεγχοι που εφαρμόζονται μετά την εγκατάσταση εγκεκριμένων αναβαθμίσεων στο πάσης φύσεως λογισμικό του ΣΕΠ.

(8) Οι έλεγχοι που εφαρμόζονται για τη σύγκριση ενός πρόσφατα ενεργοποιημένου συστήματος, συμπεριλαμβανομένων του λογισμικού υποστήριξης και των πακέτων λογισμικού εφαρμογών, με την προηγούμενη έκδοσή του, προκειμένου να εξακριβωθεί ότι μόνο οι ηθελημένες αλλαγές έχουν γίνει.

(9) Οι έλεγχοι (τεχνικοί, φυσικοί και διαδικαστικοί) που εφαρμόζονται για την προστασία, από τη μη εξουσιοδοτημένη τροποποίηση ή την καταστροφή, του πρότυπου ή των αντιγράφων όλου του υλικού που χρησιμοποιείται για την ενεργοποίηση του συστήματος, συμπεριλαμβανομένων του λογισμικού υποστήριξης και των πακέτων λογισμικού εφαρμογών.

(10) Οι έλεγχοι των προδιαγραφών των συσκευών επικοινωνιών (π.χ routers) και των συσκευών προστασίας των εξωτερικών ορίων του συστήματος (BPD’s) όπως για παράδειγμα τα Firewall, IDS, IPS.

(11) Οι διαδικασίες για την αίτηση τροποποίησης διαμόρφωσης του υλικού, του λογισμικού λειτουργίας και του λογισμικού εφαρμογών.

(12) Οι διαδικασίες για την αίτηση τροποποίησης της διαμόρφωσης υλικού ή το σχετικό με το σύστημα περιβάλλον, όπου υπάρχει ανάγκη συμμόρφωσης με συγκεκριμένα πρότυπα TEMPEST και την καταγραφή των λειτουργιών του συστήματος, μετά την τροποποίηση της διαμόρφωσης.

(13) Οι διαδικασίες για την αναβάθμιση του λογισμικού κατά των ιών, καθώς και για την αναβάθμιση του λογισμικού λειτουργίας (service packs / security patches) των ΦΥΣ, που παραδίδονται για χρήση σε συγκεκριμένους χρήστες.

ΣΥΝΟΨΗ

19. Οι ΔΑΛ, αποτελούν απαραίτητο στοιχείο για τον τρόπο εφαρμογής της ασφάλειας σε ένα ΣΕΠ και περιλαμβάνει όλες τις πτυχές της ασφάλειας και όχι μόνο της ασφάλειας των Η/Υ. Οι ΔΑΛ συντάσσονται με μεγάλη προσοχή ως προς την κάθε λεπτομέρεια. Οι χρήστες συμμορφώνονται απόλυτα με τα οριζόμενα στις ΔΑΛ και κατανοούν ότι, αποτελούν το σημαντικότερο κρίκο για την επίτευξη της συνολικής ασφάλειας του ΣΕΠ.

Αντιναύαρχος Ιωάννης Δρυμούσης ΠΝ
Υπαρχηγός

Ακριβές Αντίγραφο

Ασμχος (ΕΑ) Νικόλαος Ζήκος
Επιτελής ΓΕΕΘΑ/Ε3/1

ΓΕΝΙΚΟ ΕΠΙΤΕΛΕΙΟ ΕΘΝΙΚΗΣ ΑΜΥΝΑΣ
Ε’ ΚΛΑΔΟΣ
ΔΝΣΗ ΑΣΦΑΛΕΙΑΣ
07 Σεπ 20

ΠΑΡΑΡΤΗΜΑ «ΙΓ» ΣΤΟΝ
ΕΚΒΑ

ΜΕΤΡΑ ΚΑΙ ΔΙΑΔΙΚΑΣΙΕΣ ΑΣΦΑΛΕΙΑΣ ΑΝΑ ΔΙΑΒΑΘΜΙΣΗ ΣΕΠ

1. Το παρόν Παράρτημα, παρέχει τις ελάχιστες αποδεκτές προδιαγραφές σε ότι αφορά στα μέτρα και τις διαδικασίες ασφαλείας που εφαρμόζονται σε ένα ΣΕΠ, προκειμένου να είναι δυνατή η διαπίστευσή του σε συγκεκριμένο βαθμό ασφαλείας.

2 Οι συντμήσεις Περιορισμένης Χρήσης (ΠΧ), Εμπιστευτικό (ΕΠ) και Απόρρητο (ΑΠ), αφορούν στη διαβάθμιση ασφαλείας των δεδομένων που χειρίζεται το, υπό εξέταση ΣΕΠ. Στα μέτρα που υφίσταται το σύμβολο «Χ» εκτελείται έλεγχος εφαρμογής κατά τη διάρκεια της διαδικασίας διαπίστευσης ή ελέγχου / επιθεώρησης.

3. Γενική Ασφάλεια

Α/Α	ΜΕΤΡΟ	ΔΙΑΒΑΘΜΙΣΗ ΣΕΠ			ΠΑΡ/ΣΕΙΣ
		ΠΧ	ΕΠ	ΑΠ	
	α. Βασικές Αρχές Ασφαλείας				
(1)	Τηρείται απαρέγκλιτα η αρχή «ανάγκη γνώσης» προκειμένου να δοθεί ανάλογη πρόσβαση στους χρήστες του ΣΕΠ; Υφίσταται πίνακας αιτιολόγησης παροχής πρόσβασης για κάθε χρήστη σύμφωνα με την εν λόγω αρχή;	Χ	Χ	Χ	
(2)	Τηρούνται οι προδιαγραφές φύλαξης των χώρων σύμφωνα με τον παρόντα Κανονισμό;	Χ	Χ	Χ	
(3)	Υφίσταται εκπαιδευμένος διαχειριστής δικτύου Η/Υ που ονομάζεται Διαχειριστής Λειτουργίας (ΔΙΑΛ) καθώς και βοηθός αυτού που να είναι υπεύθυνοι αποκλειστικά και μόνο για τη λειτουργία του συστήματος; Ο ΔΙΑΛ είναι υπεύθυνος για την ομαλή λειτουργία του συστήματος και την επίλυση των καθημερινών προβλημάτων πρόσβασης στα δεδομένα, τις ενημερώσεις (updates) και εγκαταστάσεις των λογισμικών λειτουργίας και εφαρμογών, την επισκευή τμημάτων του, την συντήρηση των SERVERS και την διαχείριση των κωδικών πρόσβασης του BIOS των SERVERS και των τερματικών.	Χ	Χ	Χ	
(4)	Υπάρχουν Σχέδια αντιμετώπισης πυρκαγιάς, εκκενώσεως και καταστροφής;	Χ	Χ	Χ	
(5)	Όλο το υλικό (hardware) του ΣΕΠ βρίσκεται μακριά από σωλήνες του νερού και εκτός χώρων με αυξημένη υγρασία;	Χ	Χ	Χ	

Α/Α	ΜΕΤΡΟ	ΔΙΑΒΑΘΜΙΣΗ ΣΕΠ			ΠΑΡ/ΣΕΙΣ
		ΠΧ	ΕΠ	ΑΠ	
(6)	Από τον τελευταίο έλεγχο μέχρι σήμερα υπήρξαν προβλήματα μη ασφαλούς λειτουργίας; Έχουν αναφερθεί αυτά στην ΕΑΔΑ (ή στην ΕΔΑ εφόσον έχει καθοριστεί);	X	X	X	
(7)	Έχουν αντιμετωπισθεί τα παραπάνω προβλήματα; Ποια είναι τα μέτρα που ελήφθησαν για την αποφυγή επανάληψης τους;	X	X	X	
	β. Προσωπικό Ασφαλείας				
(1)	Είναι ορισμένο και στελεχωμένο το προσωπικό ασφαλείας του φορέα όπως προβλέπεται από τον ΕΚΒΑ;	X	X	X	
(2)	Έχει ορισθεί ο Υπεύθυνος Ασφαλείας Συστήματος (ΥΑΣ); Γνωρίζει τα καθήκοντά του; Έχουν ορισθεί βοηθοί του ΥΑΣ που να διαθέτουν ειδικές γνώσεις σε θέματα ασφαλείας των ΣΕΠ;	X	X	X	
(3)	Εφόσον υφίσταται διασύνδεση μεταξύ δύο ή περισσότερων ΣΕΠ, έχει ορισθεί ο Υπεύθυνος Ασφαλείας Δικτύου (ΥΑΔ); Γνωρίζει τα καθήκοντά του; Έχουν ορισθεί βοηθοί του ΥΑΔ που να διαθέτουν ειδικές γνώσεις σε θέματα ασφαλείας των ΣΕΠ;	X	X	X	
(4)	Έχει ορισθεί ο Υπεύθυνος Ασφαλείας Τοποθεσίας (ΥΑΤ); Γνωρίζει τα καθήκοντά του; Έχουν ορισθεί βοηθοί του ΥΑΤ που να διαθέτουν ειδικές γνώσεις σε θέματα ασφαλείας των ΣΕΠ;	X	X	X	
(5)	Έχει ορισθεί ο Υπεύθυνος Κρυπτασφαλείας για το ΣΕΠ; Γνωρίζει τα καθήκοντά του;	X	X	X	
(6)	Είναι απόλυτα καθορισμένο ότι οι ΥΑΣ, ΥΑΔ, ΥΑΤ και οι βοηθοί τους έχουν απλά δικαιώματα χρήστη και δεν έχουν άλλη πρόσβαση στο ΣΕΠ, παρά μόνο μέσω ειδικού λογαριασμού που δίνει πρόσβαση μόνο στα αρχεία καταγραφής ενεργειών χρηστών ενώ προκειμένου να εκτελέσουν εργασίες που απαιτούν ανωτέρω δικαιώματα συνεργάζονται με τον ΔΙΑΛ;		X	X	
(7)	Κατά τις εργάσιμες ημέρες και ώρες, είναι παρόντες τουλάχιστον ένας ΥΑΣ και ένας ΔΙΑΛ; Κατά τις μη εργάσιμες ώρες είναι διαθέσιμοι τηλεφωνικά 24 ώρες το εικοσιτετράωρο;	X	X	X	
(8)	Έχει απαγορευτεί η ανάθεση έτερων καθηκόντων στους ΥΑΣ, ΥΑΔ και ΔΙΑΛ;	X	X	X	
	γ. Εκπαίδευση / Ενημέρωση Προσωπικού				
(1)	Υφίσταται εκπαιδευτικό πρόγραμμα σε θέματα ασφαλείας για όλο το προσωπικό;	X	X	X	
(2)	Συμμετέχει το προσωπικό ασφαλείας σε αντίστοιχα σεμινάρια / εκπαιδεύσεις για τη διαχείριση διαβαθμισμένων δεδομένων, την ασφάλεια Η/Υ και δικτύων κλπ, εσωτερικού ή εξωτερικού; Πότε ήταν η τελευταία συμμετοχή και επί ποιου αντι-	X	X	X	

Α/Α	ΜΕΤΡΟ	ΔΙΑΒΑΘΜΙΣΗ ΣΕΠ			ΠΑΡ/ΣΕΙΣ
		ΠΧ	ΕΠ	ΑΠ	
	κειμένου;				
(3)	Με ποιο τρόπο παρέχεται άμεση ενημέρωση του προσωπικού για την ύπαρξη πιθανότητας παραβίασης της ασφαλείας;	X	X	X	
(4)	Εκτελείται σε τακτά χρονικά διαστήματα, εκπαίδευση όλου του εμπλεκόμενου στο ΣΕΠ, προσωπικού για τις ποινικές ευθύνες σε περίπτωση απώλειας διαβαθμισμένων πληροφοριών; Πότε έγινε για τελευταία φορά; Υφίσταται αρχείο με τις υπογραφές όσων ενημερώθηκαν, το οποίο να τηρείται από τους ΥΑΤ;	X	X	X	
(5)	Εκτελείται ενημέρωση για τις ευθύνες του προσωπικού σε περίπτωση έκθεσης του συστήματος λόγω μη τήρησης των μέτρων ασφαλείας κατά την έξοδο από το γραφείο κατά τις εργάσιμες ώρες;	X	X	X	
(6)	Έχει γίνει, από όλους τους χρήστες του ΣΕΠ, η ενυπόγραφη αποδοχή των υποχρεώσεων τους σε ότι αφορά στα θέματα ασφαλείας και στις επιπτώσεις στην περίπτωση διαρροής διαβαθμισμένων πληροφοριών; Με ποια συχνότητα εκτελείται η υπενθύμιση αυτών των θεμάτων;	X	X	X	
	δ. Ανάλυση Κινδύνου (ΑΚ)				
(1)	Έχει εκτελεστεί η διαδικασία ΑΚ (Risk Assessment);	X	X	X	
(2)	Η ΑΕΛ διαθέτει αυτοματοποιημένο εργαλείο για την εκτέλεση ΑΚ; Αν ναι, να αναφερθούν τα στοιχεία αυτού.	X	X	X	
(3)	Έχουν καταρτιστεί πίνακες κινδύνων και αντίστοιχων μέτρων που προέκυψαν από την εκτέλεση ΑΚ; Σε ποιο βαθμό αντιμετωπίζεται κάθε ένας από τους κινδύνους που διαπιστώθηκαν;	X	X	X	
(4)	Έχουν αναγνωρισθεί και υποτυπωθεί οι εναπομείναντες κίνδυνοι, για τους οποίους δεν υφίστανται μέτρα;	X	X	X	
(5)	Υφίσταται η έγγραφη αποδοχή των εναπομεινάντων κινδύνων, από την ΑΕΛ του ΣΕΠ;	X	X	X	
(6)	Έχουν γίνει αποδεκτοί από την ΕΑΔΑ (ή την ΕΔΑ εφόσον έχει καθοριστεί), οι εναπομείναντες κίνδυνοι προηγούμενου μέτρου;	X	X	X	
	ε. Διαδικασίες Ασφαλούς Λειτουργίας (ΔΑΛ)				
(1)	Έχουν εκδοθεί οι ΔΑΛ του συστήματος; Έχουν ενημερωθεί ενυπογράφως όλοι οι χρήστες του συστήματος;	X	X	X	
(2)	Έχουν όλοι οι χρήστες πρόσβαση σε αντίγραφο των ΔΑΛ που ισχύουν για το ΣΕΠ; Αν ναι, που φυλάσσεται αυτό;	X	X	X	
(3)	Υφίσταται διαδικασία για περιοδική ενημέρωση και	X	X	X	

Α/Α	ΜΕΤΡΟ	ΔΙΑΒΑΘΜΙΣΗ ΣΕΠ			ΠΑΡ/ΣΕΙΣ
		ΠΧ	ΕΠ	ΑΠ	
	επανακυκλοφορία των ΔΑΛ στους χρήστες, με σκοπό τη συνεχή ενημέρωση όλου του προσωπικού;				
(4)	Οι ΔΑΛ καθορίζουν τις διαδικασίες που απαιτείται να ακολουθήσει ένας χρήστης ή οι ΥΑΣ, ΥΑΔ, ΥΑΤ και ΔΙΑΛ σε περίπτωση που διαπιστώσουν οποιαδήποτε κατάσταση μη ασφαλούς λειτουργίας του ΣΕΠ;	X	X	X	
(5)	Περιλαμβάνεται στις ΔΑΛ διαδικασία κλεισίματος του ΣΕΠ σε περίπτωση διακοπής ρεύματος, όπως και διαδικασία περιοδικού ελέγχου του UPS;	X	X	X	
(6)	Οι ΔΑΛ περιλαμβάνουν τα ηλεκτρολογικά σχέδια των εγκαταστάσεων και τα σχέδια δομημένης καλωδίωσης των δικτυακών υποδομών;	X	X	X	
	στ. Σχέδιο Ασφαλείας				
(1)	Υφίσταται συγκεκριμένο σχέδιο ασφαλείας για τη διασφάλιση των διαβαθμισμένων πληροφοριών; Έχουν καθορισθεί το σημαντικό Υλικό / Λογισμικό / Πληροφορίες, τα οποία εφόσον υποστούν οποιασδήποτε μορφής εξωτερική επέμβαση πρόκειται να επηρεάσουν αρνητικά τη λειτουργία του ΣΕΠ; Έχουν αποτυπωθεί οι πιθανοί τρόποι επίθεσης σε αυτά;	X	X	X	
(2)	Το υφιστάμενο εσωτερικό σχέδιο ασφαλείας περιλαμβάνει τα ακόλουθα: (α) Αποτελέσματα του πλέον πρόσφατου ελέγχου ασφαλείας; (β) Τα πάσης φύσεως υφιστάμενα μέτρα ασφαλείας; (γ) Σχέδιο αντίδρασης σε περίπτωση παραβίασης της ασφαλείας;	X	X	X	
(3)	Έχουν καθοριστεί οι περιοχές ασφαλείας της κάθε εγκατάστασης;	X	X	X	
(4)	Γίνεται έλεγχος των διαφόρων χώρων στους οποίους φυλάσσονται διαβαθμισμένα υλικά από το προσωπικό ασφαλείας μετά τις εργάσιμες ώρες και σε εικοσιτετράωρη βάση; Υφίσταται ειδικό ημερολόγιο ελέγχων;	X	X	X	
(5)	Υφίσταται λίστα των πλέον σημαντικών εγκαταστάσεων που απαιτείται να προστατευθούν ενώ παράλληλα έχουν υποτυπωθεί οι πιθανοί τρόποι επίθεσης σε αυτές;	X	X	X	
(6)	Εκτελείται έλεγχος χώρων από το προσωπικό ασφαλείας; Ορίζεται η διαδικασία ελέγχου – χώρων στο σχέδιο ασφαλείας; Πόσο συχνά εκτελούνται αυτοί οι έλεγχοι; Εντείνονται αυτοί σε μη εργάσιμες ώρες;	X	X	X	
(7)	Υφίσταται συγκεκριμένη διαδικασία για την έρευνα και αναφορά στις περιπτώσεις παραβίασης της ασφαλείας;	X	X	X	

4. Ασφάλεια Προσωπικού

Α/Α	ΜΕΤΡΟ	ΔΙΑΒΑΘΜΙΣΗ ΣΕΠ			ΠΑΡ/ΣΕΙΣ
		ΠΧ	ΕΠ	ΑΠ	
	Έλεγχος Προσωπικού				
(1)	Το προσωπικό που εισέρχεται στο Γενικό Περιβάλλον Ασφαλείας (ΓΠΑ) και στο Τοπικό Περιβάλλον Ασφαλείας (ΤΠΑ) ταυτοποιείται αξιόπιστα πριν την είσοδό του;	X	X	X	
(2)	Υπάρχει στο σημείου εισόδου του ΤΠΑ αναρτημένη λίστα εξουσιοδοτημένου για πρόσβαση προσωπικού;	X	X	X	
(3)	Τηρείται αρχείο για την ώρα εισόδου – εξόδου όλων από και προς το ΓΠΑ και ΤΠΑ το οποίο ελέγχεται τακτικά κάθε μήνα και διατηρείται επί εξάμηνο;	X	X	X	
(4)	Το προσωπικό, για το οποίο αιτείται η παροχή πρόσβασης στο δίκτυο, διαθέτει την κατάλληλη εξουσιοδότηση ασφαλείας;	X	X	X	
(5)	Τηρούνται σε συγκεκριμένο και ασφαλές σημείο τα πιστοποιητικά ασφαλείας όλου του προσωπικού που έχει πρόσβαση στο ΣΕΠ ανάλογα με τη διαβάθμιση των εγγράφων που διαχειρίζονται;	X	X	X	
(6)	Τηρείται πρόγραμμα ανανέωσης των πιστοποιητικών ασφαλείας τουλάχιστον 6 μήνες πριν από τη λήξη τους;	X	X	X	
(7)	Όλοι οι ΥΑΣ, ΥΑΔ, ΥΑΤ και οι ΔΙΑΛ έχουν εξουσιοδοτηθεί στην αμέσως ανώτερη διαβάθμιση ασφαλείας από αυτή του ΣΕΠ;	X	X	X	
(8)	Ειδικά για τα άτομα που διαχειρίζονται κρυπτοϋλικά και εισέρχονται στα κέντρα κρυπτογράφησης έχουν εκδοθεί αντίστοιχα πιστοποιητικά ασφαλείας (crypto);	X	X	X	
(9)	Κατά την είσοδο μη εξουσιοδοτημένου προσωπικού (προσωπικό καθαρισμού χώρων, προσωπικό συντήρησης κτιρίων κλπ) που εκτελεί συγκεκριμένες εργασίες, στους χώρους του συστήματος, με ποιο τρόπο εξασφαλίζεται η αποτροπή επαφής με το ΣΕΠ;	X	X	X	
(10)	Έχει εκδοθεί πιστοποιητικό βιομηχανικής ασφαλείας για τους πάσης φύσεως οικονομικούς φορείς που εμπλέκονται στο σχεδιασμό, ανάπτυξη, πιθανώς λειτουργία και συντήρηση του ΣΕΠ, προκειμένου να χειρίζονται διαβαθμισμένο υλικό σύμφωνα με τον ΕΚΒΑ;	X	X	X	
(11)	Το συγκεκριμένο προσωπικό των ανωτέρω οικονομικών φορέων, που πρόκειται να εμπλακεί στο σχεδιασμό, ανάπτυξη, πιθανώς λειτουργία και συντήρηση του ΣΕΠ, έχει εξουσιοδοτηθεί σύμφωνα με τον ΕΚΒΑ;	X	X	X	

5. Φυσική Ασφάλεια

Α/Α	ΜΕΤΡΟ	ΔΙΑΒΑΘΜΙΣΗ ΣΕΠ			ΠΑΡ/ΣΕΙΣ
		ΠΧ	ΕΠ	ΑΠ	
	α. Γενικά Μέτρα				
(1)	Προστατεύονται οι κρίσιμες εγκαταστάσεις από ένα συνδυασμό αλληλοκαλυπτόμενων μέτρων φυσικής ασφάλειας έτσι ώστε να επιτυγχάνεται «άμυνα σε βάθος»;	X	X	X	
(2)	Έχει θεσπιστεί διαδικασία για την παροχή κατευθύνσεων επί θεμάτων φυσικής ασφαλείας σε όλο το εμπλεκόμενο προσωπικό;	X	X	X	
(3)	Έχουν ληφθεί υπόψη τα οποιαδήποτε περιστατικά παραβίασης φυσικής ασφαλείας, ώστε να εξαχθούν συμπεράσματα και να γίνει κατάλληλη εκπαίδευση στο προσωπικό σύμφωνα με τα διδάγματα (lessons learned);	X	X	X	
(4)	Υφίσταται τυποποιημένο και εύχρηστο σύστημα αναφορών των παραβιάσεων φυσικής ασφαλείας στον ΥΑΣ; Πότε έγινε δοκιμή για τελευταία φορά και πότε σημειώθηκε το τελευταίο πραγματικό συμβάν;	X	X	X	
(5)	Το ΓΠΑ είναι όσο το δυνατό ασφαλισμένο από φυσικές καταστροφές (όπως σε απόσταση από αεροδρόμια και εργοστάσια χημικών, διαθέτει αλεξικέραυνο κλπ) ;		X	X	
(6)	Το ΓΠΑ έχει κεντρικά παρακολουθούμενους ανιχνευτές φωτιάς ενώ πλησίον αυτών, βρίσκονται συστήματα κατάσβεσης / πυροσβεστήρες;		X	X	
	β. Ασφάλεια Χώρων ΣΕΠ				
(1)	Το ΤΠΑ έχει συγκεκριμένη περίμετρο και καθορισμένα σημεία εισόδου, ώστε να είναι δυνατός ο έλεγχος σε προσωπικό και οχήματα;	X	X	X	
(2)	Τα παράθυρα είναι καλυμμένα ή προστατευμένα ώστε να εμποδίζεται η παρατήρηση, εξωτερικά του χώρου;	X	X	X	
(3)	Τα παράθυρα και οι πόρτες ασφαλίζουν;	X	X	X	
(4)	Τα παράθυρα εφόσον βρίσκονται σε ύψος μικρότερο των 6 μέτρων είναι εφοδιασμένα με εξωτερικές σιδεριές;		X	X	
(5)	Στους ευαίσθητους χώρους του συστήματος όπως κέντρα επικοινωνιών, τα γραφεία των ΥΑΣ, ΥΑΔ και ΔΙΑΛ κλπ υφίσταται ηλεκτρονικό σύστημα πρόσβασης, συναγερμός και οι πόρτες έχουν ειδικό μηχανισμό αυτόματου κλεισίματος;		X	X	
	γ. Ασφάλεια Διακομιστή (SERVER)				
(1)	Ο διακομιστής (server) έχει ταμπελάκι που να δείχνει το βαθμό ασφαλείας των εγγράφων που μπορεί να επεξεργαστεί;	X	X	X	

Α/Α	ΜΕΤΡΟ	ΔΙΑΒΑΘΜΙΣΗ ΣΕΠ			ΠΑΡ/ΣΕΙΣ
		ΠΧ	ΕΠ	ΑΠ	
(2)	Ο διακομιστής (SERVER) του δικτύου βρίσκεται σε ξεχωριστό δωμάτιο; Τα μέτρα ασφαλείας της εισόδου του διακομιστή περιλαμβάνουν πόρτα ασφαλείας καθώς και ηλεκτρονικό σύστημα πρόσβασης; Εάν υπάρχει συνδυασμός, αλλάζει κάθε 6 μήνες; Η είσοδος επιτρέπεται μόνο στο εξουσιοδοτημένο προσωπικό; Τηρείται κατάσταση αυτού του προσωπικού;	X	X	X	
(3)	Είναι αναρτημένος έξω από το διαμέρισμα του διακομιστή (SERVER), πίνακας με τις φωτογραφίες και τα ονόματα του προσωπικού που είναι εξουσιοδοτημένο για το χειρισμό και τη συντήρησή του;			X	
(4)	Είναι εγκατεστημένα στο δωμάτιο του διακομιστή (SERVER) τα παρακάτω: (α) Συναγερμός (β) Σύστημα πυρανίχνευσης (γ) Κλιματιστικό (αν απαιτείται) (δ) Σύστημα ελέγχου θερμοκρασίας, υγρασίας (ε) Σύστημα αδιάλειπτης και σταθερής παροχής ρεύματος (UPS)	X	X	X	
(5)	Όλα τα παραπάνω συστήματα ασφαλείας ελέγχονται σε περιοδική βάση για να ελεγχθεί η αξιοπιστία τους; Πότε έγινε ο τελευταίος έλεγχος;	X	X	X	
(6)	Τα διαμερίσματα στα οποία βρίσκονται διακομιστές και στα οποία εργάζονται διαχειριστές ελέγχονται σε τακτά διαστήματα για συστήματα παρακολούθησης (κάμερες, μικρόφωνα).		X	X	
(7)	Ο κλιματισμός του χώρου που βρίσκεται ο διακομιστής (SERVER), έχει αισθητήρα θερμοκρασίας συνδεδεμένο με συναγερμό για την περίπτωση βλάβης του;		X	X	
(8)	Σε περίπτωση βλάβης του κλιματιστικού αναλαμβάνεται η επισκευή του εντός μίας εργάσιμης μέρας; Υπάρχει κλιματισμός ανάγκης;		X	X	
(9)	Υπάρχει εναλλακτικός διακομιστής (SERVER) δια συνδεδεμένος στο δίκτυο ο οποίος σε περίπτωση βλάβης του κύριου διακομιστή αναλαμβάνει αυτόματα την λειτουργία του δικτύου. Βρίσκεται (αν είναι δυνατό) σε ξεχωριστό διαμέρισμα;		X	X	
δ. Ασφάλεια Σημείων Διασύνδεσης (Point of Presence-POP) Μεταξύ ΣΕΠ					
(1)	Το σημείο διασύνδεσης των δύο ΣΕΠ, βρίσκεται μέσα σε σαφώς καθορισμένο ΓΠΑ;	X			
(2)	Το σημείο διασύνδεσης των δύο ΣΕΠ, βρίσκεται μέσα σε σαφώς καθορισμένο ΓΠΑ, στις εισόδους του οποίου ελέγχεται η πρόσβαση και γίνεται αναγνώριση ταυτότητας με αξιόπιστο τρόπο; Οι επισκέπτες συνοδεύονται συνεχώς;		X	X	
(3)	Το σημείο διασύνδεσης των δύο ΣΕΠ, βρίσκεται μέσα σε σαφώς καθορισμένο ΤΠΑ;	X			

Α/Α	ΜΕΤΡΟ	ΔΙΑΒΑΘΜΙΣΗ ΣΕΠ			ΠΑΡ/ΣΕΙΣ
		ΠΧ	ΕΠ	ΑΠ	
(4)	Το σημείο διασύνδεσης των δύο ΣΕΠ, βρίσκεται μέσα σε σαφώς καθορισμένο ΤΠΑ το οποίο είναι διαβαθμισμένο και η είσοδος σε αυτό ισοδυναμεί με γνώση διαβαθμισμένων πληροφοριών;		X	X	
	ε. Έλεγχος Πρόσβασης				
(1)	Υφίσταται σύστημα ελέγχου πρόσβασης και βρίσκεται σε πλήρη λειτουργία; Είναι αποτελεσματικό;	X	X	X	
(2)	Εκτελείται έλεγχος φυσικής ταυτοποίησης του εισερχόμενου προσωπικού στο ΓΠΑ και στη συνέχεια νέος έλεγχος από το προσωπικό ασφαλείας του ΤΠΑ; Εφόσον δεν υπάρχει προσωπικό ασφαλείας στο ΤΠΑ, γίνεται ταυτοποίηση του προσωπικού με χρήση άλλων συστημάτων ελέγχου (βιομετρικά συστήματα πρόσβασης, ηλεκτρονικοί συνδυασμοί πρόσβασης, ηλεκτρονικές κάρτες κλπ); Έχει γίνει ενυπόγραφη ενημέρωση των χρηστών ότι η χρήση των καρτών πρόσβασης είναι αποκλειστικά και μόνο προσωπική και απαγορεύεται ο δανεισμός σε έτερα πρόσωπα;		X	X	
(3)	Οι έλεγχοι εκτός των χώρων του συστήματος παρέχουν ικανή προστασία απέναντι σε μη εξουσιοδοτημένη πρόσβαση στους χώρους αυτού;		X	X	
(4)	Οι επισκέπτες είναι εφοδιασμένοι με ειδικό δελτίο εισόδου και συνοδεύονται από εξουσιοδοτημένο προσωπικό στους χώρους στους οποίους υφίστανται τερματικά του ΣΕΠ;	X	X	X	
(5)	Ποια μέτρα λαμβάνονται από τους χρήστες κατά την είσοδο των επισκεπτών στους χώρους στους οποίους υφίστανται τερματικά του ΣΕΠ, ώστε αυτοί να μην έχουν οπτική πρόσβαση στις οθόνες των υπολογιστών, εφόσον δεν υπάρχει ανάγκη γνώσης;	X	X	X	
(6)	Οι χώροι στους οποίους έχουν εγκατασταθεί τερματικά του ΣΕΠ είναι εφοδιασμένοι με πόρτα που ασφαλίζεται; Η πόρτα αυτή κλειδώνεται εφόσον δεν υφίσταται χρήστης στο σύστημα (ακόμα και εντός ωραρίου εργασίας); Οι χώροι αυτοί ελέγχονται από το προσωπικό ασφαλείας κατά τις μη εργάσιμες ώρες; Με ποια συχνότητα;	X	X	X	
(7)	Εντός του κέντρου κρυπτογράφησης υπάρχει κατάσταση προσωπικού που έχει δικαίωμα εισόδου; Υπάρχει βιβλίο επισκεπτών; Ενημερώνεται σωστά; Στην είσοδό του υπάρχει κατάσταση με φωτογραφία του εξουσιοδοτημένου προσωπικού;		X	X	
(8)	Υφίστανται ιδιαίτερα μέτρα πρόσβασης στους χώρους από τους οποίους ελέγχονται οι λειτουργίες του ΣΕΠ, από τους ΔΙΑΛ;	X	X	X	

Α/Α	ΜΕΤΡΟ	ΔΙΑΒΑΘΜΙΣΗ ΣΕΠ			ΠΑΡ/ΣΕΙΣ
		ΠΧ	ΕΠ	ΑΠ	
(9)	Σε περίπτωση μη ύπαρξης αυτοματοποιημένου συστήματος ελέγχου πρόσβασης τοποθετείται σε εικοσιτετράωρη βάση προσωπικό φύλαξης; Έχει εκτελεστεί ενημέρωση στο προσωπικό αυτό και υφίσταται αρχείο με τις υπογραφές όσων έλαβαν μέρος στην εκπαίδευση; Υφίσταται μνημόνιο καθηκόντων και ενεργειών του εν λόγω προσωπικού ασφαλείας; Με ποια συχνότητα εκτελούνται έλεγχοι από τους υπευθύνους ασφαλείας στο εν λόγω προσωπικό φύλαξης; Υφίσταται αρχείο των ελέγχων αυτών;		Χ	Χ	
(10)	Εκτελούνται έλεγχοι για τον εντοπισμό παρείσακτων στους χώρους του συστήματος κατά της μη εργάσιμες ώρες;	Χ	Χ	Χ	
(11)	Έχουν καθοριστεί οι προβλεπόμενες ενέργειες στις οποίες προβαίνει ο χρήστης του ΣΕΠ στην περίπτωση που διαπιστωθεί πρόβλημα ασφαλείας του συστήματος;	Χ	Χ	Χ	
(12)	Έχουν τοποθετηθεί ταμπέλες σε εμφανή σημεία, για την απαγόρευση εισόδου σε μη εξουσιοδοτημένο προσωπικό, στους διαβαθμισμένους χώρους του ΣΕΠ ;	Χ	Χ	Χ	

6. Ασφάλεια Διαβαθμισμένου Υλικού

Α/Α	ΜΕΤΡΟ	ΔΙΑΒΑΘΜΙΣΗ ΣΕΠ			ΠΑΡ/ΣΕΙΣ
		ΠΧ	ΕΠ	ΑΠ	
	α. Γενικά Μέτρα				
(1)	Έχει εκτελεστεί εκπαίδευση σε όλους τους χρήστες σχετικά με τις διάφορες μορφές που μπορούν να έχουν τα διαβαθμισμένα έγγραφα (σε έντυπη μορφή, σε οποιουδήποτε τύπου μαγνητικό ή ηλεκτρονικό μέσο κλπ); Εκτελείται περιοδικά σε όλο το εμπλεκόμενο προσωπικό ενημέρωση σχετικά με τον τρόπο διαβάθμισης των εγγράφων; Αν ναι, πότε έγινε τελευταία φορά; Τηρείται βιβλίο των συμμετεχόντων με αντίστοιχη σελίδα των υπογραφών αυτών;	Χ	Χ	Χ	
(2)	Υφίστανται ειδικές αυτοκόλλητες ετικέτες σε όλους τους τύπους διαβαθμισμένων μέσων; (π.χ. δισκέτες, φορητοί σκληροί δίσκοι, αποσπώμενοι σκληροί δίσκοι κλπ) στις οποίες να περιγράφεται ο βαθμός ασφαλείας τους; Υφίστανται αντίστοιχες ετικέτες για όλα τα περιφερειακά του ΣΕΠ (εκτυπωτές, σαρωτές κλπ);	Χ	Χ	Χ	

Α/Α	ΜΕΤΡΟ	ΔΙΑΒΑΘΜΙΣΗ ΣΕΠ			ΠΑΡ/ΣΕΙΣ
		ΠΧ	ΕΠ	ΑΠ	
(3)	Εκτελείται έλεγχος των εξερχόμενων πληροφοριών σε εκτυπωμένη μορφή, πριν αυτά βγουν από το ΓΠΑ; Συγκεκριμένα, καταγράφεται το προσωπικό που παραλαμβάνει τα εκτυπωμένα δεδομένα καθώς και η θέση εργασίας / ο χρήστης από τον οποίο δόθηκε η εντολή εκτύπωσης;	X	X	X	
(4)	Όταν εισέρχεται προσωπικό, για το οποίο δεν ισχύει η αρχή «ανάγκη γνώσης», σε χώρο που υπάρχει τερματικό του συστήματος εφαρμόζονται τα παρακάτω; (α) Διακοπή Εκτύπωσης (β) Αποθήκευση των διαβαθμισμένων έγγραφων ώστε να μην είναι σε κοινή θέα. (γ) Κλείδωμα της οθόνης του τερματικού.	X	X	X	
(5)	Έχει διαπιστωθεί ότι οι εκτυπωτές που χρησιμοποιούνται στο ΣΕΠ δεν έχουν μόνιμη μνήμη (volatile memory), έτσι ώστε αμέσως μετά την απενεργοποίησή τους να διαγράφονται αυτόματα οποιεσδήποτε διαβαθμισμένες πληροφορίες;	X	X	X	
(6)	Υφίστανται τα κατάλληλα μέτρα ασφαλείας εντός του ΤΠΑ, με τα οποία αποτρέπεται η μη εξουσιοδοτημένη εξαγωγή τυπωμένων αντιγράφων ή μαγνητικών μέσων αποθήκευσης; Ποια είναι αυτά;	X	X	X	
	β. Χρήση Φοριαμών Ασφαλείας				
(1)	Εφαρμόζονται τα μέτρα ασφαλείας για τη φύλαξη συνδυασμών φοριαμών ασφαλείας και κλειδιών διαβαθμισμένων χώρων; Έχει γίνει εκπαίδευση στο εμπλεκόμενο προσωπικό; Υφίσταται αρχείο εκπαιδεύσεων επί του θέματος; Πότε έγινε για τελευταία φορά;		X	X	
(2)	Ποιοι από όλο το προσωπικό που έχει πρόσβαση στο ΣΕΠ, γνωρίζουν τους συνδυασμούς των φοριαμών ασφαλείας στους οποίους φυλάσσονται οι αφαιρούμενοι σκληροί δίσκοι και τα φορητά μέσα μεταφοράς δεδομένων;		X	X	
(3)	Αλλάζονται οι συνδυασμοί των φοριαμών ασφαλείας στους οποίους φυλάσσονται «ΑΠΟΡΡΗΤΑ» έγγραφα κάθε 6 μήνες; Πότε αλλάχθηκαν για τελευταία φορά; Τηρείται αρχείο αλλαγής συνδυασμών υπογεγραμμένο;			X	
(4)	Το κρυπτοϋλικό του ΣΕΠ, φυλάσσεται σε φοριαμό τριπλής ασφαλείας, ο οποίος βρίσκεται σε χώρο με προδιαγραφές κρυπτοκέντρου; Οι συνδυασμοί αλλάζουν τακτικά; Όταν απομακρύνεται προσωπικό που γνώριζε τον συνδυασμό, ο φορέας φροντίζει για την αλλαγή του;		X	X	
(5)	Οι κλείδες του λογισμικού κρυπτογράφησης (software) που χρησιμοποιεί το ΣΕΠ, φυλάσσονται σε φοριαμό ασφαλείας με συνδυασμό;	X			

Α/Α	ΜΕΤΡΟ	ΔΙΑΒΑΘΜΙΣΗ ΣΕΠ			ΠΑΡ/ΣΕΙΣ
		ΠΧ	ΕΠ	ΑΠ	
(6)	Ειδικά οι κωδικοί πρόσβασης των ΔΙΑΛ, των ΥΑΣ, ΥΑΔ και ΥΑΤ φυλάσσονται σε φοριαμό ασφαλείας με συνδυασμό σε συγκεκριμένο χώρο στον οποίο η πρόσβαση είναι περιορισμένη; Υπάρχει διαδικασία χρήσης τους σε περίπτωση ανάγκης; Εξασφαλίζεται ότι οι εν λόγω κωδικοί, εφόσον γνωστοποιηθούν, αλλάζουν άμεσα;	X	X	X	
(7)	Οι κωδικοί πρόσβασης των χρηστών έχουν διαβαθμιστεί με την διαβάθμιση ασφαλείας του ΣΕΠ; Φυλάσσονται σε φοριαμό ασφαλείας με συνδυασμό, σε συγκεκριμένο χώρο στον οποίο η πρόσβαση είναι περιορισμένη;	X	X	X	
γ. Χρήση Φωτοτυπικών Μηχανημάτων – FAX					
(1)	Υπάρχουν φωτοτυπικά μηχανήματα στους χώρους του ΣΕΠ, τα οποία δεν έχουν κωδικό αριθμό αναγνωρίσεως;	X	X	X	
(2)	Τα FAX, SCANNER και πολυμηχανήματα που χρησιμοποιούνται για την αναπαραγωγή των εγγράφων φέρουν σε εμφανές σημείο πινακίδα που να απαγορεύει τη χρήση τους ως φωτοτυπικά;	X	X	X	
(3)	Έχει εξασφαλιστεί η διαδικασία με την οποία ελέγχεται η πρόσβαση στα φωτοτυπικά και στις συσκευές FAX μόνο από εξουσιοδοτημένο προσωπικό και ότι τα παραγόμενα από αυτά αντίτυπα εγγράφων ελέγχονται και καταγράφονται;	X	X	X	
(4)	Έχει εξασφαλιστεί ότι τα φωτοτυπικά που χρησιμοποιούνται για το ΣΕΠ δε συνδέονται με άλλο δίκτυο;	X	X	X	
(5)	Έχει απαγορευτεί η χρήση φωτοτυπικών που διαθέτουν χαρακτηριστικά αντίστοιχα με Η/Υ (σκληρό δίσκο, εσωτερική μόνιμη μνήμη, δυνατότητα σάρωσης, θύρες USB κλπ) για διαβαθμισμένα έγγραφα ; Σε αντίθετη περίπτωση έχουν τοποθετηθεί σε χώρο με χαρακτηριστικά κλωβού FARADAY ή έχουν χαρακτηριστικά TEMPEST;	X	X	X	
(6)	Στις περιπτώσεις οποιασδήποτε, επιτόπου εργασίας συντήρησης στα φωτοτυπικά προηγούμενου μέτρου παρίσταται προσωπικό ασφαλείας του ΣΕΠ; Στις περιπτώσεις συντήρησης των φωτοτυπικών από προσωπικό, εκτός του ΣΕΠ, αποσυνδέεται η συσκευή από την ηλεκτρική παροχή η συσκευή πριν την έναρξη των εργασιών; Στις περιπτώσεις που απαιτείται να μεταφερθεί η συσκευή εκτός του ΤΠΑ, αντικαθίσταται ο σκληρός του δίσκος με άλλον κενό και να έχει καθαριστεί (reset) η μνήμη του;	X	X	X	
δ. Ασφάλεια Φορητών Υπολογιστικών Συστημάτων (ΦΥΣ) του Οικονομικού Φορέα [αφορά στους φορητούς Η/Υ, έξυπνα κινητά (smartphones), υπολογιστές ταμπλέτες (tablets), κλπ]					
(1)	Χρησιμοποιούνται τα ΦΥΣ εκτός του Γενικού Περιβάλλοντος Ασφαλείας, μόνο κατόπιν αδείας από την	X	X	X	

Α/Α	ΜΕΤΡΟ	ΔΙΑΒΑΘΜΙΣΗ ΣΕΠ			ΠΑΡ/ΣΕΙΣ
		ΠΧ	ΕΠ	ΑΠ	
	Αρχή Επιχειρησιακής Λειτουργίας (ΑΕΛ);				
(2)	Υφίσταται έγγραφη δήλωση του προσωπικού που παραλαμβάνει ένα ΦΥΣ σύμφωνα με την οποία γνωρίζει ότι απαγορεύεται να το παραδίδει ως αποσκευή ή να το τοποθετεί σε βαλίτσα;	X	X	X	
(3)	Έχει τονιστεί στο προσωπικό που μεταφέρει ένα ΦΥΣ ότι απαιτείται αυξημένη προσοχή για το ενδεχόμενο κλοπής του, ειδικά στα αεροδρόμια, λιμάνια και σιδηροδρομικούς σταθμούς;	X	X	X	
(4)	Γνωρίζει το προσωπικό που μεταφέρει ένα ΦΥΣ ότι η απώλεια αυτού, των παρελκομένων και των μέσων αποθήκευσης (media) αναφέρεται άμεσα στον ΥΑΣ και στη συνέχεια στην ΑΕΛ;	X	X	X	
(5)	Δίνεται στο εμπλεκόμενο προσωπικό αντίγραφο των οδηγιών ασφαλείας για τη χρήση ενός ΦΥΣ και συμπληρώνεται ενυπόγραφη δήλωση κατανόησης των ευθυνών που συνεπάγεται η μεταφορά ενός ΦΥΣ, πριν την εκτέλεση της αποστολής που του ανατέθηκε;	X	X	X	
ε. Υποβιβασμός / Καταστροφή Διαβαθμισμένου Υλικού					
(1)	Υπάρχει σχέδιο υποβιβασμού / αποχαρακτηρισμού διαβαθμισμένων πληροφοριών;	X	X	X	
(2)	Το άχρηστο διαβαθμισμένο υλικό φυλάσσεται εντός ειδικών σάκων και καταστρέφεται από κατάλληλο προσωπικό; Πριν την καταστροφή ελέγχεται αν πράγματι πρόκειται για άχρηστο υλικό που απαιτείται να καταστραφεί;	X	X	X	
(3)	Έχει καθοριστεί διαδικασία υποβίβασης βαθμού ασφαλείας για τα έγγραφα / αρχεία των οποίων η σημασία έχει περιοριστεί; Υφίσταται αρχείο καταγραφής αυτών;	X	X	X	
(4)	Όλα τα υλικά που προέρχονται από το σύστημα και πρόκειται να μην χρησιμοποιηθούν στο μέλλον (υπό απόσυρση) καταστρέφονται κατά τα προβλεπόμενα ανάλογα με τη διαβάθμιση του συστήματος; Εξασφαλίζει την προβλεπόμενη διαδικασία καταστροφής ο ΥΑΤ και με ποιο τρόπο;	X	X	X	
(5)	Με ποια διαδικασία καταστρέφονται τα μαγνητικά μέσα μεταφοράς δεδομένων, όταν αποφασισθεί η απόσυρσή τους; Εφαρμόζεται η διαδικασία που προβλέπεται στο Παράρτημα «Θ» πριν τη φυσική καταστροφή τους;	X	X	X	
(6)	Υπάρχει σχέδιο καταστροφής διαβαθμισμένου υλικού σε περίπτωση ανάγκης;	X	X	X	

(7)	Υφίσταται σε καθορισμένο χώρο υλικό καταστροφής διαβαθμισμένου υλικού όπως σφυριά για την καταστροφή των σκληρών δίσκων, γυαλόχαρτο για την καταστροφή των CD/DVD, όπως και πιστοποιημένος καταστροφέας εγγράφων, μαγνητικών μέσων κλπ;	X	X	X	
(8)	Υφίσταται Σχέδιο Εκκένωσης και Καταστροφής των τμημάτων του συστήματος σε περίπτωση κινδύνου αποκάλυψης των πληροφοριών που χειρίζεται; Γίνεται ενημέρωση στο εμπλεκόμενο προσωπικό σε τακτά χρονικά διαστήματα; Πότε έγινε για τελευταία φορά;	X	X	X	

7. Ασφάλεια Επικοινωνιών – Πληροφορικής

Α/Α	ΜΕΤΡΟ	ΔΙΑΒΑΘΜΙΣΗ ΣΕΠ			ΠΑΡ/ΣΕΙΣ
		ΠΧ	ΕΠ	ΑΠ	
	α. Γενικά Μέτρα				
(1)	Το ΣΕΠ (εφόσον δεν πρόκειται για stand alone) διαθέτει σύστημα IDS (Intrusion Detection System) για τον εντοπισμό των ηλεκτρονικών εισβολέων;		X	X	
(2)	Το ΣΕΠ (εφόσον δεν πρόκειται για stand alone) διαθέτει σύστημα IPS (Intrusion Prevention System) για την παρεμπόδιση των ηλεκτρονικών εισβολών;		X	X	
(3)	Είναι εφοδιασμένο το ΣΕΠ με ενημερωμένες εκδόσεις των παρακάτω ; (α) Λειτουργικό Συστήματος (β) Τείχους προστασίας (Firewall) (γ) Λογισμικού που να αντιλαμβάνεται την προσπάθεια παρακολούθησης ενεργειών (antispyware) (δ) Προγράμματος κατά κακόβουλου λογισμικού (anti-malware).	X	X	X	
(4)	Έχουν καθοριστεί οι προδιαγραφές και τα μέτρα ασφαλείας για τη χρήση Φορητών Υπολογιστικών Συσκευών (ΦΥΣ); Υπάρχει αναφορά σε αυτές τις συσκευές στη ΔΑΠΑΣ και στις ΔΑΛ;	X	X	X	
(5)	Το ΣΕΠ διαθέτει σύστημα κρυπτογράφησης μέσω πιστοποιημένου λογισμικού (software) κατά την επικοινωνία του εκτός του ΓΠΑ;	X			
(6)	Το ΣΕΠ διαθέτει σύστημα κρυπτογράφησης με χρήση πιστοποιημένων κρυπτοσυσκευών κατά την επικοινωνία του εκτός του ΓΠΑ;		X	X	
(7)	Πότε εκτελέστηκε ο τελευταίος Έλεγχος Ασφαλείας Συστήματος – ΕΑΣ (Security Test and Evaluation) και ο τελευταίος έλεγχος τρωτοτήτων (Vulnerability Test); Τα λογισμικά που χρησιμοποιήθηκαν είναι εγκεκριμένα από την ΕΑΑΕΠ;	X	X	X	

Α/Α	ΜΕΤΡΟ	ΔΙΑΒΑΘΜΙΣΗ ΣΕΠ			ΠΑΡ/ΣΕΙΣ
		ΠΧ	ΕΠ	ΑΠ	
(8)	Τηρείται η διαδικασία της έγγραφης παροχής αδείας από την ΑΕΛ στις περιπτώσεις που είναι απαραίτητη η αλλαγή του υλικού (hardware), πριν λάβει χώρα η αλλαγή αυτή; Τηρείται ειδικό αρχείο με όλες της τροποποιήσεις του υλικού που χρησιμοποιείται από το σύστημα; Πότε σημειώθηκε για τελευταία φορά και ποιος τηρεί το αρχείο της υπόθεσης;	X	X	X	
(9)	Τηρείται η διαδικασία της έγγραφης παροχής αδείας από την ΑΕΛ στις περιπτώσεις που είναι απαραίτητη η αλλαγή του λογισμικού (software) πριν λάβει χώρα η αλλαγή αυτή; Τηρείται ειδικό αρχείο με όλες τις τροποποιήσεις του λογισμικού που χρησιμοποιείται από το σύστημα; Πότε σημειώθηκε για τελευταία φορά και ποιος τηρεί το αρχείο της υπόθεσης;	X	X	X	
(10)	Έχει καθοριστεί το καθεστώς χρήσης κινητών τηλεφώνων;		X	X	
(11)	Επιτρέπεται η χρήση κινητών τηλεφώνων και των σχετιζόμενων συστημάτων επικοινωνίας (Bluetooth, GPRS κλπ) μόνο σε συγκεκριμένους χώρους που φέρουν κατάλληλη σήμανση;		X	X	
	β. Ακεραιότητα Δεδομένων				
(1)	Με ποιο τρόπο εξασφαλίζεται η προστασία των πληροφοριών από την τροποποίηση τους με μη εξουσιοδοτημένο τρόπο;	X	X	X	
(2)	Με ποιο τρόπο εξασφαλίζεται ότι κατά τη διάρκεια της επεξεργασίας και διακίνησης των πληροφοριών μεταξύ των χρηστών και των τμημάτων του ΣΕΠ είναι δυνατός ο εντοπισμός και η αποφυγή απώλειας ή καθ’ οιονδήποτε τρόπο τροποποίησής τους;	X	X	X	
	γ. Διαθεσιμότητα Δεδομένων				
(1)	Πως εξασφαλίζεται ότι οι κρίσιμες διεργασίες του συστήματος εκτελούνται χρονικά όταν απαιτείται από τους χρήστες (π.χ να μην υπάρχει καθυστέρηση εκτέλεσης εντολών λόγω αυξημένου αριθμού χρηστών);	X	X	X	
(2)	Με ποιο τρόπο εξασφαλίζεται η πρόσβαση των χρηστών στις πληροφορίες παράλληλα με την μη άσκοπη χρήση των πηγών του συστήματος (παροχή συγκεκριμένων δικαιωμάτων στους χρήστες για πρόσβαση στα προγράμματα που χρησιμοποιούν);	X	X	X	
(3)	Πως εξασφαλίζεται η απαγόρευση επέμβασης των χρηστών σε κρίσιμες λειτουργίες του συστήματος;	X	X	X	
(4)	Υφίσταται τυποποιημένη διαδικασία για την άμεση αναφορά στην ΑΕΛ αλλά και στην ΕΑΔΑ (ή στην ΕΔΑ εφόσον έχει καθοριστεί), των περιπτώσεων άρνησης πρόσβασης σε δεδομένα ή μη ικανοποιητικής λειτουργίας του υλικού (hardware);	X	X	X	

Α/Α	ΜΕΤΡΟ	ΔΙΑΒΑΘΜΙΣΗ ΣΕΠ			ΠΑΡ/ΣΕΙΣ
		ΠΧ	ΕΠ	ΑΠ	
	δ. Χρήση Διαδικτύου				
(1)	Έχει απαγορευτεί η σύνδεση του ΣΕΠ με το διαδίκτυο με προσωπικά μέσα; Εκτελείται έλεγχος καθώς και εκπαίδευση σε όλο το προσωπικό για τους κινδύνους που εγκυμονεί η παραβίαση αυτής της οδηγίας;	X	X	X	
(2)	Οι Η/Υ εκτός ΣΕΠ, αλλά εντός του ιδίου χώρου με τα τερματικά αυτού, οι οποίοι χρησιμοποιούνται για σύνδεση στο διαδίκτυο, έχει εξασφαλιστεί ότι δεν περιέχουν διαβαθμισμένα έγγραφα;	X	X	X	
(3)	Οι Η/Υ που χρησιμοποιούνται στο διαδίκτυο είναι συνδεδεμένοι σε οποιοδήποτε ΣΕΠ που περιέχει διαβαθμισμένες πληροφορίες;	X	X	X	
(4)	Τηρείται αρχείο όλων των πληροφοριών που προέρχονται από το διαδίκτυο και για τα οποία απαιτήθηκε η μεταφορά τους εντός του ΣΕΠ;	X	X	X	
(5)	Υφίσταται, σε συγκεκριμένο χώρο μεμονωμένος (stand alone) Η/Υ στον οποίο ο ΔΙΑΛ και μόνο έχει τη δυνατότητα εισαγωγής/εξαγωγής δεδομένων που προέρχονται από το διαδίκτυο προκειμένου να ελεγχθούν για κακόβουλο λογισμικό, ώστε στη συνέχεια και με έγκριση του ΥΑΣ, να καταστεί δυνατή η μεταφορά τους στο ΣΕΠ με φορητά μέσα μεταφοράς δεδομένων;	X	X	X	
	ε. Κωδικός Πρόσβασης				
(1)	Έχει εκτελεστεί εκπαίδευση για το χειρισμό και τη φύλαξη του κωδικού πρόσβασης (password); Κάθε πότε εκτελείται και πότε έγινε για τελευταία φορά;	X	X	X	
(2)	Κατά την αρχική πρόσβαση στο σύστημα υφίσταται η διαδικασία της υποχρεωτικής αλλαγής του κωδικού πρόσβασης (password) ;	X	X	X	
(3)	Οι κωδικοί πρόσβασης <u>των ΔΙΑΛ</u> αποτελούνται από <u>τουλάχιστον 12 χαρακτήρες</u> στους οποίους να περιλαμβάνονται κεφαλαία και μικρά γράμματα, αριθμοί και 2 σύμβολα; Απαιτείται η αλλαγή τους (με βάση τις ρυθμίσεις του συστήματος) <u>κάθε 90</u> ημέρες;	X	X	X	
(4)	Ο κωδικός πρόσβασης των χρηστών αποτελείται από <u>τουλάχιστον 10 χαρακτήρες</u> στους οποίους να περιλαμβάνονται κεφαλαία και μικρά γράμματα, αριθμοί και 2 σύμβολα; Απαιτείται η αλλαγή του (με βάση τις ρυθμίσεις του συστήματος) <u>κάθε 90</u> ημέρες;			X	
(5)	Ο κωδικός πρόσβασης των χρηστών αποτελείται από <u>τουλάχιστον 8 χαρακτήρες</u>; Απαιτείται η αλλαγή του (με βάση τις ρυθμίσεις του συστήματος) <u>κάθε 180</u> ημέρες ;	X	X		

Α/Α	ΜΕΤΡΟ	ΔΙΑΒΑΘΜΙΣΗ ΣΕΠ			ΠΑΡ/ΣΕΙΣ
		ΠΧ	ΕΠ	ΑΠ	
(6)	Έχει γίνει εκπαίδευση στο προσωπικό ότι οι κωδικοί πρόσβασης δεν έχουν καμία λογική σημασία ή να περιέχουν ονόματα χρηστών, ημερομηνίες γέννησης, ονόματα των παιδιών τους κλπ), διότι έτσι είναι εύκολο να βρεθούν και να παραβιαστούν;	X	X	X	
(7)	Έχει καθορισθεί διαδικασία κρυπτογράφησης των κωδικών πρόσβασης με σκοπό την αποφυγή αποκάλυψης και παράνομης χρήσης;	X	X	X	
(8)	Έχουν καθοριστεί συγκεκριμένοι παράμετροι στο σύστημα, που να ΜΗΝ επιτρέπουν την εκ νέου χρήση κωδικών πρόσβασης που είχαν χρησιμοποιηθεί στο παρελθόν, συνολικά μέχρι 5 φορές;		X	X	
(9)	Έχει καθοριστεί διαδικασία ειδοποίησης των χρηστών για άμεση αλλαγή του κωδικού πρόσβασης, στις περιπτώσεις που σημειώθηκε παραβίαση ασφαλείας;	X	X	X	
(10)	Φυλάσσονται οι ταυτότητες χρηστών και οι αντίστοιχοι κωδικοί πρόσβασης χρηστών με ιδιαίτερα προνόμια σε φοριαμούς ασφαλείας προκειμένου να χρησιμοποιηθούν σε έκτακτες περιπτώσεις; Καθορίζεται επακριβώς η εν λόγω διαδικασία στις ΔΑΛ;	X	X	X	
(11)	Έχει τεθεί ειδικός κωδικός πρόσβασης στο BIOS των τερματικών, προκειμένου να μην είναι δυνατή η πρόσβαση στο setup του Η/Υ; Ο κωδικός αυτός φυλάσσεται σε φοριαμό στον οποίο πρόσβαση έχουν μόνο οι ΔΙΑΛ;	X	X	X	
(12)	Έχει τεθεί ειδικός κωδικός πρόσβασης στον λογαριασμό του διαχειριστή (administrator) του κάθε τερματικού ώστε να μην είναι δυνατή η πρόσβαση του χρήστη στον Η/Υ του τοπικά; Ο κωδικός αυτός φυλάσσεται σε φοριαμό από τους ΔΙΑΛ;	X	X	X	
(13)	Οι SERVER's του συστήματος διαθέτουν μηχανισμό προστασίας των κωδικών πρόσβασης και της δομής δεδομένων τους από απώλεια, παραβίαση ή προσπάθεια μη εξουσιοδοτημένης πρόσβασης; Στο ίδιο πλαίσιο έχουν δυνατότητα εκτέλεσης αυτοελέγχων κατά την έναρξη λειτουργίας τους, επαναλειτουργίας τους (μετά από απότομη διακοπή) και μετά από εντολή του ΔΙΑΛ;		X	X	
στ. Έλεγχος Πρόσβασης					
(1)	Τηρείται η διαδικασία αρχικού καθημερινού ελέγχου των ταινιών ασφαλείας του κάθε τερματικού εργασίας, από τον πρώτο χρήστη προκειμένου να διαπιστωθούν ίχνη προσπάθειας μη εξουσιοδοτημένης πρόσβασης στο ΣΕΠ ή προσπάθειας παραβίασης του υλικού (hardware); Η διαδικασία αυτή περιγράφεται στις ΔΑΛ;	X	X	X	

Α/Α	ΜΕΤΡΟ	ΔΙΑΒΑΘΜΙΣΗ ΣΕΠ			ΠΑΡ/ΣΕΙΣ
		ΠΧ	ΕΠ	ΑΠ	
(2)	Έχει εξασφαλιστεί ότι η διαδικασία ταυτοποίησης και αυθεντικότητας των στοιχείων του χρήστη προηγείται οποιασδήποτε δυνατότητας πρόσβασης στο σύστημα;	X	X	X	
(3)	Έχει εξασφαλιστεί ότι πρόσβαση στις πληροφορίες που αφορούν την διαδικασία ταυτοποίησης και αυθεντικότητας των στοιχείων του χρήστη κατά την αρχική πρόσβαση στο ΣΕΠ, έχουν μόνο οι ΔΙΑΛ, ο ΥΑΣ και οι βοηθοί του; Επιπλέον έχει καθοριστεί η διαδικασία τροποποίησης των στοιχείων αυτών από τα προαναφερθέντα και μόνο πρόσωπα; Τηρείται η αρχή ταυτόχρονης παρουσίας 2 ατόμων για να καταστεί δυνατή η τροποποίηση των στοιχείων αυτών;	X	X	X	
(4)	Έχει εξασφαλιστεί ότι σε περίπτωση που η σύνδεση ενός τερματικού με τον διακομιστή (server) δεν είναι εφικτή, δεν είναι δυνατή ούτε η πρόσβαση στον Η/Υ τοπικά;		X	X	
(5)	Στην περίπτωση πέντε αποτυχημένων προσπαθειών εισόδου στο σύστημα, έχει καθοριστεί λειτουργία αυτόματου κλειδώματος του λογαριασμού του χρήστη καθώς και δυνατότητα ξεκλειδώματος μόνο από το ΔΙΑΛ;	X	X	X	
(6)	Έχουν καθοριστεί, εκείνα τα γεγονότα, που εφόσον συμβούν απαιτείται ο εκ νέου έλεγχος αυθεντικότητας του χρήστη;		X	X	
(7)	Υφίστανται μηχανισμοί απαγόρευσης πρόσβασης του χρήστη σε δεδομένα για τα οποία ισχύει η αρχή «ανάγκη γνώσης»;	X	X	X	
(8)	Πριν την έγκριση πρόσβασης ενός χρήστη στο ΣΕΠ, εμφανίζεται στην οθόνη μήνυμα με το οποίο να ενημερώνεται ότι στο σύστημα εκτελείται έλεγχος των προσπαθειών πρόσβασης σε δεδομένα για τα οποία ο χρήστης δεν έχει «ανάγκη γνώσης»;	X	X	X	
(9)	Έχουν τεθεί οι κατάλληλοι ρυθμίσεις ώστε να μην εμφανίζεται το όνομα του τελευταίου χρήστη (user name) που απέκτησε πρόσβαση στο σύστημα, από το συγκεκριμένο τερματικό;	X	X	X	
(10)	Οι λογαριασμοί χρηστών που δεν χρησιμοποιούνται πλέον, έχουν κλειδωθεί ή διαγραφεί;	X	X	X	
(11)	Εφαρμόζεται ο έλεγχος των IP addresses σε συνδυασμό με τις MAC addresses για το κάθε τερματικό ξεχωριστά, ώστε να μην είναι δυνατή η σύνδεση έτερου μη εγκεκριμένου Η/Υ στο ΣΕΠ;	X	X	X	
	ζ. Εκπαίδευση Προσωπικού				
(1)	Υπάρχει πρόγραμμα εκπαιδεύσεως του ανατοποθετημένου προσωπικού στα θέματα ασφαλείας πληροφορικής;	X	X	X	

Α/Α	ΜΕΤΡΟ	ΔΙΑΒΑΘΜΙΣΗ ΣΕΠ			ΠΑΡ/ΣΕΙΣ
		ΠΧ	ΕΠ	ΑΠ	
(2)	Έχει εκτελεστεί εκπαίδευση περί της απαγόρευσης χρήσης του ΣΕΠ για ιδιωτικούς σκοπούς και περί της απαγόρευσης χρήσης μη εγκεκριμένου λογισμικού (προγράμματα) και δεδομένων εκτός του προβλεπόμενου; Έχει τονιστεί ότι εάν επιχειρηθεί κάτι τέτοιο αυξάνεται η πιθανότητα κακόβουλου λογισμικού στο σύστημα; Πότε έγινε για τελευταία φορά; Με ποια διαδικασία επιτυγχάνεται ο έλεγχος για την εφαρμογή αυτών;	X	X	X	
(3)	Εκτελείται εκπαίδευση για τις ευθύνες του προσωπικού σε περίπτωση έκθεσης του συστήματος λόγω μη τήρησης των μέτρων ασφαλείας κατά την έξοδο από το γραφείο κατά τις εργάσιμες ώρες;	X	X	X	
(4)	Έχουν εκπονηθεί εγχειρίδια ασφαλείας για τους υπεύθυνους ασφαλείας (ΥΑΣ, ΥΑΔ και ΥΑΤ) του συστήματος, τους ΔΙΑΛ και τους κάθε είδους χρήστες;	X	X	X	
	η. Ασφάλεια Τερματικών				
(1)	Τα τερματικά του ΣΕΠ, έχουν σήμανση του ανώτατου βαθμού ασφαλείας των εγγράφων που μπορούν να επεξεργαστούν;	X	X	X	
(2)	Τα τερματικά του ΣΕΠ είναι εφοδιασμένα με αφαιρούμενο σκληρό δίσκο, ο οποίος αφαιρείται μετά το πέρας του ωραρίου και φυλάσσεται σε φοριαμό ασφαλείας; Σε περίπτωση που αυτό δεν είναι εφικτό, έχουν γίνει όλες οι απαραίτητες ενέργειες ώστε τα δεδομένα να αποθηκεύονται <u>αποκλειστικά και μόνο</u> στον κεντρικό SERVER του δικτύου και όχι στο κάθε τερματικό;		X	X	
(3)	Εφαρμόζεται η διαδικασία αυτόματης ενεργοποίησης ασφάλισης πρόσβασης (lock computer) για τις θέσεις εργασίας, στις περιπτώσεις που δεν υφίσταται δραστηριότητα στον υπολογιστή για περισσότερο από 15 λεπτά;	X	X	X	
(4)	Οι θύρες επικοινωνίας (εισόδου – εξόδου) των Η/Υ, που είναι συνδεδεμένοι στο ΣΕΠ έχουν απενεργοποιηθεί;	X	X	X	
(5)	Είναι κλειδωμένο (μη δυνατότητα επέμβασης) το BIOS των τερματικών των χρηστών;	X	X	X	
(6)	Γίνονται τακτικοί έλεγχοι στους Η/Υ από τους ΥΑΤ ώστε να διαπιστωθεί ότι δεν έχουν προστεθεί σ’ αυτούς μη εγκεκριμένα περιφερειακά ή λογισμικό;	X	X	X	
(7)	Υφίστανται σε όλα τα τερματικά ειδικές ταινίες ασφαλείας (security seals) προκειμένου να διαπιστώνεται εάν έχει επιχειρηθεί επέμβαση στο εσωτερικό του υλικού (hardware); Ελέγχονται σε εβδομαδιαία βάση από τους ΥΑΤ οι οποίοι τηρούν και σχετικό βιβλίο ελέγχων; Τυχόν ευρήματα έχουν αναφερθεί ΑΜΕΣΑ στον ΥΑΣ;	X	X	X	

Α/Α	ΜΕΤΡΟ	ΔΙΑΒΑΘΜΙΣΗ ΣΕΠ			ΠΑΡ/ΣΕΙΣ
		ΠΧ	ΕΠ	ΑΠ	
(8)	Έχει απαγορευτεί η χρήση συσκευών KVM switches που είτε επιδέχονται προγραμματισμού είτε διαθέτουν ενσωματωμένη μνήμη;	X	X	X	
	θ. Σχεδιαστικά Χαρακτηριστικά του ΣΕΠ				
(1)	Υπάρχουν διαγράμματα του ΣΕΠ; Είναι ενημερωμένα;	X	X	X	
(2)	Υφίστανται τοπογραφικά και σχεδιαστικά διαγράμματα που να καταδεικνύουν τα προς εφαρμογή μέτρα ασφαλείας (zoning, firewalls, black/red lines κλπ);	X	X	X	
(3)	Υφίστανται διαγράμματα διασυνδέσεως του συστήματος στα οποία να αποτυπώνονται οι διακομιστές (SERVER's), οι κρυπτοσυσκευές, οι δρομολογητές (routers), το τείχος ασφαλείας (firewall), τα τερματικά κλπ;	X	X	X	
	ι. Χρήση Περιφερειακών – Μαγνητικών Μέσων				
(1)	Έχει απαγορευτεί η δυνατότητα εκκίνησης (BOOT) από τις εξωτερικές θύρες (USB κτλ) και τους οδηγούς (floppy disk, zip drive, CD, DVD κτλ) του τερματικού, από το χρήστη;	X	X	X	
(2)	Χρησιμοποιούνται αποκλειστικά δικτυακοί εκτυπωτές σε φυλασσόμενους χώρους; Ελέγχονται και υποτυπώνονται τα αντίγραφα των εγγράφων που εκτυπώνονται καθώς και ο χρήστης που τα χρησιμοποιεί;	X	X	X	
(3)	Έχουν απενεργοποιηθεί όλες οι εξωτερικές θύρες επικοινωνίας και οι συσκευές εισαγωγής δεδομένων (οδηγοί δισκετών, CD, DVD's, zip drives κλπ) των τερματικών του ΣΕΠ; Εκτελούνται έλεγχοι από τους ΥΑΤ, για να διαπιστωθεί η πλήρης εφαρμογή του μέτρου;	X	X	X	
(4)	Στη συνέχεια του προηγούμενου μέτρου, έχουν καθοριστεί συγκεκριμένα τερματικά στα οποία να είναι ενεργοποιημένη μία θύρα USB ώστε να επιτρέπεται η εισαγωγή και εξαγωγή δεδομένων με χρήση αποκλειστικά και μόνο εγκεκριμένων (όχι ιδιωτικών) μαγνητικών / ηλεκτρονικών φορητών μέσων μεταφοράς. Έχει γίνει εκπαίδευση του προσωπικού που χρησιμοποιεί αυτό το τερματικό; Εκτελούνται τακτικοί έλεγχοι στα τερματικά αυτά από τους ΥΑΤ και ΥΑΣ για να διαπιστωθεί ο τρόπος χρήσης τους;	X	X	X	
(5)	Εξασφαλίζεται ότι στα μαγνητικά / ηλεκτρονικά φορητά μέσα μεταφοράς δεδομένων που χρησιμοποιούνται για τη μεταφορά διαβαθμισμένων εγγράφων δεν αποθηκεύονται άλλου τύπου αρχεία (πχ προγράμματα ή άλλες εφαρμογές);	X	X	X	

Α/Α	ΜΕΤΡΟ	ΔΙΑΒΑΘΜΙΣΗ ΣΕΠ			ΠΑΡ/ΣΕΙΣ
		ΠΧ	ΕΠ	ΑΠ	
(6)	Τα μαγνητικά / ηλεκτρονικά φορητά μέσα μεταφοράς δεδομένων είναι εγκεκριμένα και φέρουν ετικέτες που αναγράφεται ειδικός αριθμός αναγνώρισης και ο βαθμός ασφαλείας τους;	X	X	X	
(7)	Φυλάσσονται σε ασφαλές χώρο από τους ΥΑΤ τα φορητά μέσα μεταφοράς δεδομένων που χρησιμοποιούνται στο ΣΕΠ;	X			
(8)	Φυλάσσονται σε ειδικό φοριαμό ασφαλείας τα φορητά μέσα μεταφοράς δεδομένων που χρησιμοποιούνται στο ΣΕΠ;		X	X	
(9)	Εκτελείται έλεγχος και καταγραφή όλων των εγκεκριμένων μαγνητικών / ηλεκτρονικών φορητών μέσων μεταφοράς δεδομένων από τον ΥΑΤ ανά δίμηνο;			X	
(10)	Εκτελείται έλεγχος και καταγραφή όλων των εγκεκριμένων μαγνητικών / ηλεκτρονικών φορητών μέσων μεταφοράς δεδομένων από τον ΥΑΤ ανά τετράμηνο;	X	X		
(11)	Εφαρμόζεται η διαδικασία απαγόρευσης της χρήσης των μαγνητικών / ηλεκτρονικών φορητών μέσων μεταφοράς δεδομένων που χρησιμοποιούνται για μεταφορά εγγράφων χαμηλότερης διαβάθμισης από ΣΕΠ με υψηλότερη διαβάθμιση (π.χ. εφόσον κάποια δισκέτα έχει χαρακτηρισθεί ως «ΕΜΠΙΣΤΕΥΤΙΚΟ» να μη χρησιμοποιείται για τη μεταφορά «ΑΠΟΡΡΗΤΩΝ» εγγράφων);	X	X	X	
(12)	Στις περιπτώσεις που αλλάξει η διαβάθμιση των μαγνητικών μέσων που χρησιμοποιούνται στο ΣΕΠ, τηρούνται οι διαδικασίες φύλαξης αυτών, σύμφωνα με τα νέα δεδομένα;	X	X	X	
(13)	Στις περιπτώσεις που τα μαγνητικά / ηλεκτρονικά φορητά μέσα μεταφοράς δεδομένων μεταφερθούν σε χώρους που δεν έχουν εξουσιοδότηση για χρήση αυτής της διαβάθμισης εγγράφων, έχει προηγηθεί έγγραφη άδεια από τον ΥΑΤ;	X	X	X	
(14)	Χρησιμοποιούνται, πιστοποιημένοι από την ΕΑΑΕΠ, μηχανισμοί και λογισμικό για τη διαγραφή δεδομένων από τα φορητά μέσα μεταφοράς και αποθήκευσης (φορητοί σκληροί δίσκοι κλπ) δεδομένων;	X	X	X	
(15)	Χρησιμοποιούνται, πιστοποιημένοι από την ΕΑΑΕΠ, μηχανισμοί και λογισμικό για την καταστροφή των φορητών μέσων μεταφοράς και αποθήκευσης (φορητοί σκληροί δίσκοι κλπ) δεδομένων;	X	X	X	
(16)	Τηρείται η διαδικασία διακοπής λειτουργίας των εκτυπωτών και η διαγραφή της μνήμης τους μετά το πέρας του ωραρίου;	X	X	X	

Α/Α	ΜΕΤΡΟ	ΔΙΑΒΑΘΜΙΣΗ ΣΕΠ			ΠΑΡ/ΣΕΙΣ
		ΠΧ	ΕΠ	ΑΠ	
(17)	Έχει απαγορευτεί η χρήση συσκευών KVM switches που είτε επιδέχεται προγραμματισμού είτε διαθέτει ενσωματωμένη μνήμη και χρησιμοποιείται για την ταυτόχρονη διασύνδεση ενός περιφερειακού (π.χ. scanner, printer κλπ) με δύο ή περισσότερα ΣΕΠ διαφορετικής διαβάθμισης μεταξύ τους;	X	X	X	
(18)	Υφίσταται συγκεκριμένος Η/Υ ο οποίος δεν είναι συνδεδεμένος με το δίκτυο και χρησιμοποιείται για τον έλεγχο και «καθαρισμό» φορητών μέσων αποθήκευσης από την ύπαρξη κακόβουλου λογισμικού πριν τα δεδομένα που μεταφέρουν εισαχθούν στο ΣΕΠ; Είναι ενεργοποιημένη η λειτουργία του λογισμικού κατά κακόβουλου λογισμικού, για αυτόματο έλεγχο αρχείων προερχόμενων από οπτικά η μαγνητικά μέσα πριν εκτελεστούν; Πότε εντοπίστηκε για τελευταία φορά κακόβουλο λογισμικό;	X	X	X	
	ια. Αντίγραφα Ασφαλείας				
(1)	Τηρείται η διαδικασία δημιουργίας αντιγράφων (back up) των αρχείων που διαχειρίζεται το σύστημα δύο φορές την εβδομάδα; Φυλάσσονται τα αντίγραφα αυτά, εκτός ΣΕΠ και ανάλογα με την διαβάθμιση ασφαλείας τους;		X	X	
(2)	Τηρείται η διαδικασία δημιουργίας αντιγράφων (back up) των αρχείων που διαχειρίζεται το σύστημα μία φορά την εβδομάδα; Φυλάσσονται τα αντίγραφα αυτά, εκτός ΣΕΠ και ανάλογα με την διαβάθμιση ασφαλείας τους;	X			
	Ιβ. Υποτύπωση Ενεργειών Χρηστών				
(1)	Με χρήση ειδικού λογισμικού, τηρούνται αρχεία καταγραφής (audit records) όλων των ενεργειών των χρηστών που χρησιμοποιούν το ΣΕΠ; Γίνεται έλεγχος σε εβδομαδιαία βάση από την ΥΑΣ;	X	X	X	
(2)	Τα εν λόγω αρχεία περιλαμβάνουν στοιχεία όπως τον ακριβή χρόνο των ενεργειών, τον τύπο ενέργειας (π.χ. ανάγνωση, τροποποίηση, εκτύπωση κλπ) και την ταυτότητα του χρήστη;	X	X	X	
(3)	Τα αρχεία καταγραφής των ενεργειών των χρηστών προστατεύονται με ειδικό λογισμικό και διαδικασίες για την απαγόρευση πρόσβασης αλλά και τροποποίησής τους;	X	X	X	
(4)	Υφίσταται λογισμικό για την άμεση ανάλυση των στοιχείων των αρχείων καταγραφής προκειμένου να διαπιστωθούν πιθανές παραβιάσεις ασφαλείας;	X	X	X	
(5)	Τηρούνται τα προαναφερθέντα αρχεία καταγραφής των ενεργειών των χρηστών για διάστημα ***6 μηνών*** τουλάχιστον εντός του ΣΕΠ; Τηρούνται σε μορφή backup για διάστημα τουλάχιστον ***5 ετών***;		X	X	

Α/Α	ΜΕΤΡΟ	ΔΙΑΒΑΘΜΙΣΗ ΣΕΠ			ΠΑΡ/ΣΕΙΣ
		ΠΧ	ΕΠ	ΑΠ	
(6)	Τηρούνται τα προαναφερθέντα αρχεία καταγραφής των ενεργειών των χρηστών για διάστημα ***3 μηνών*** τουλάχιστον εντός του ΣΕΠ; Τηρούνται σε μορφή backup για διάστημα τουλάχιστον ***3 ετών***;	X			
(7)	Τα αρχεία καταγραφής των ενεργειών τροποποιούνται σε αρχεία μόνο για ανάγνωση (read only) αμέσως μετά τη δημιουργία τους, ώστε να μην είναι δυνατή η τροποποίησή τους από μη εξουσιοδοτημένο προσωπικό;	X	X	X	
(8)	Εκτελείται σε τακτικά χρονικά διαστήματα συγχρονισμός των ρολογιών του συστήματος και των τερματικών, δεδομένου ότι αν υπάρχει χρονική διαφοροποίηση τα στοιχεία των αρχείων καταγραφής των ενεργειών αλλάζουν;	X	X	X	
(9)	Έχουν ενημερωθεί ενυπόγραφα όλοι οι χρήστες του ΣΕΠ ότι εκτελείται υποτύπωση των ενεργειών τους, κατά την οποιαδήποτε χρήση του ΣΕΠ;	X	X	X	
(10)	Ειδικά για τα «ΑΠΟΡΡΗΤΑ» ΣΕΠ αποστέλλεται σε μηνιαία βάση, στους χρήστες αρχείο που περιέχει όλες τις ενέργειες τους (πρόσβαση σε αρχεία, ανάγνωση, τροποποίηση κλπ);			X	
	ιγ. Διασύνδεση με Έτερα ΣΕΠ				
(1)	Έχει απαγορευτεί η οποιαδήποτε διασύνδεση ενός ΣΕΠ με έτερο σύστημα το οποίο δεν έχει διαπιστευτεί;	X	X	X	
(2)	Έχει απαγορευτεί η διασύνδεση με το διαδίκτυο ή δημόσια δίκτυα για τα ΣΕΠ με διαβάθμιση ασφαλείας «ΕΜΠΙΣΤΕΥΤΙΚΟ» και άνω;		X	X	
(3)	Για ΣΕΠ με διαβάθμιση «ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ» έχει επιτραπεί η διασύνδεση με δημόσια δίκτυα ή το διαδίκτυο μόνο εφόσον χρησιμοποιούνται εγκεκριμένα από την ΕΑΔΑ και την ΕΑΑΕΠ συστήματα ασφάλειας εξωτερικών ορίων (Boundary Protection Devices – BPD's) όπως είναι τα Firewalls, IDS, IPS, Proxy SERVER's, συσκευές Κρυπτογράφησης, Routers, Gateways, Antivirus Services κλπ;	X			
(4)	Τα BPD's που χρησιμοποιούνται έχουν τη δυνατότητα καταγραφής όλων των γεγονότων (είδος, χρόνος, διάρκεια, σημεία του συστήματος που επηρεάστηκαν κλπ) που σχετίζονται με την ασφάλεια προκειμένου να διευκολύνουν τις έρευνες που πρόκειται να ακολουθήσουν ένα περιστατικό διάσπασης ή προσπάθειας διάσπασης της ασφαλείας του ΣΕΠ;		X	X	
(5)	Όλα τα ΣΕΠ που πρόκειται να διασυνδεθούν μεταξύ τους χρησιμοποιούν αυτόνομα συστήματα ασφάλειας εξωτερικών ορίων (BPD's);	X	X	X	
(6)	Ειδικά για «ΑΠΟΡΡΗΤΑ» ΣΕΠ τα συστήματα ασφάλειας εξωτερικών ορίων (BPD's) έχουν λάβει πιστοποίηση από την ΕΑΑΕΠ κατηγορίας τουλάχι-			X	

Α/Α	ΜΕΤΡΟ	ΔΙΑΒΑΘΜΙΣΗ ΣΕΠ			ΠΑΡ/ΣΕΙΣ
		ΠΧ	ΕΠ	ΑΠ	
	στον EAL 3+				
(7)	Τηρείται η αρχή ότι η διασύνδεση ενός ΣΕΠ διαβάθμισης «ΕΜΠΙΣΤΕΥΤΙΚΟ» και άνω με «ΑΔΙΑΒΑΘΜΗΤΟ» ή «ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ» ΣΕΠ που διασυνδέεται με το διαδίκτυο ισοδυναμεί με άμεση διασύνδεση του με το διαδίκτυο και κατά συνέπεια απαγορεύεται	X	X	X	
(8)	Έχουν ελεγχθεί από την ΕΑΔΑ και την ΕΑΑΕΠ οι κάθε είδους διασυνδέσεις (back–end connections) των ΣΕΠ που πρόκειται να διασυνδεθούν μεταξύ τους;	X	X	X	
(9)	Στην περίπτωση διασύνδεσης δύο ΣΕΠ με διαφορετική διαβάθμιση ασφαλείας χρησιμοποιείται υποχρεωτικά, εγκεκριμένη από την ΕΑΑΕΠ, συσκευή μονόδρομης μετάδοσης δεδομένων (one way flow regulator) από το χαμηλότερης διαβάθμισης προς το υψηλότερης διαβάθμισης ΣΕΠ;	X	X	X	
(10)	Έχουν καθοριστεί τα απολύτως απαραίτητα και μόνο πρωτόκολλα επικοινωνίας και τα δεδομένα για τη μετάδοση των οποίων, προέκυψε η ανάγκη διασύνδεσης των δύο ή περισσότερων ΣΕΠ;	X	X	X	
(11)	Έχει εγκριθεί από την ΕΑΔΑ η Δήλωση Απαιτήσεων Ασφαλείας Διασύνδεσης (ΔΑΠΑΔ) που αφορά αποκλειστικά στη διασύνδεση δύο ή περισσότερων ΣΕΠ;	X	X	X	
(12)	Εφαρμόζεται η αρχή απαγόρευσης διασύνδεσης δύο ήδη διαπιστευμένων ΣΕΠ, στην περίπτωση που δεν έχει διαπιστευτεί η διασύνδεσή τους;	X	X	X	
	ιδ. Καθήκοντα Διαχειριστών Λειτουργίας (ΔΙΑΛ)				
(1)	Εκτελείται απαρέγκλιτα έλεγχος από τον ΔΙΑΛ για την ύπαρξη κακόβουλου λογισμικού σε οποιοδήποτε φορητό μέσο που δεν ανήκει στο ΣΕΠ και από το οποίο πρόκειται να εισαχθούν πληροφορίες σ' αυτό;	X	X	X	
(2)	Προστατεύεται ολόκληρο το ΣΕΠ από ένα εγκεκριμένο πρόγραμμα εναντίων των ιών; Ενημερώνεται αυτό σε καθημερινή βάση; Ελέγχει αυτομάτως οποιοδήποτε μαγνητικό ή ηλεκτρονικό μέσο από / προς το οποίο λαμβάνονται / αποστέλλονται δεδομένα;	X	X	X	
(3)	Έχει καθορισθεί από τον ΥΑΣ πολιτική παροχής δικαιωμάτων προς τους χρήστες; Να γίνει συνοπτική περιγραφή.	X	X	X	
(4)	Εξασφαλίζεται ότι τα έγγραφα που προέρχονται από κάποιο σύστημα (πηγή) υψηλότερης διαβάθμισης και τα οποία πρόκειται να χρησιμοποιηθούν σε άλλο σύστημα (προορισμός) χαμηλότερης διαβάθμισης, έχουν ίδια ή χαμηλότερη διαβάθμιση από	X	X	X	

Α/Α	ΜΕΤΡΟ	ΔΙΑΒΑΘΜΙΣΗ ΣΕΠ			ΠΑΡ/ΣΕΙΣ
		ΠΧ	ΕΠ	ΑΠ	
	το σύστημα προορισμού;				
(5)	Έχουν καθοριστεί οι πληροφορίες που χρειάζονται για συγκεκριμένες εργασίες καταγραφής (π.χ ημερομηνία και ώρα, ταυτότητα χρήστη, επίπεδο διαβάθμισης, είδος εργασίας κλπ);	X	X	X	
(6)	Ποιες ενέργειες αναλήφθηκαν από τον ΔΙΑΛ και το προσωπικό ασφαλείας του συστήματος στις περιπτώσεις αποτυχημένων προσπαθειών για σύνδεση (log–on) και κλειδώματος του λογαριασμού χρήστη από το ΣΕΠ;	X	X	X	
(7)	Υφίσταται τυποποιημένο και εύχρηστο σύστημα αναφορών των παραβιάσεων ηλεκτρονικής ασφάλειας; Πότε έγινε δοκιμή για τελευταία φορά και πότε σημειώθηκε το τελευταίο πραγματικό συμβάν;	X	X	X	
(8)	Εκτελείται έλεγχος από το αρμόδιο προσωπικό ασφαλείας για την τήρηση της ανώτατης διαβάθμισης, που μπορούν να φέρουν οι διαχειριζόμενες πληροφορίες από το ΣΕΠ (απαγόρευση εισαγωγής δεδομένων με υψηλότερη της ανώτερης επιτρεπόμενης διαβάθμισης);	X	X	X	
	ιε. Θέματα TEMPEST – ZONING				
(1)	Χρησιμοποιούνται αποκλειστικά οπτικές ίνες, προκειμένου να αντιμετωπιστεί ο κίνδυνος υποκλοπής, με εκμετάλλευση της ανεπιθύμητης ακτινοβολίας (compromising emanations) των καλωδίων διασύνδεσης;			X	
(2)	Το προσωπικό γνωρίζει τον κίνδυνο από τις ανεπιθύμητες ακτινοβολίες;		X	X	
(3)	Έχει καθοριστεί, από την Εθνική Αρχή TEMPEST (ΕΥΠ), ο προβλεπόμενος, σύμφωνα με τους ισχύοντες κανονισμούς ΝΑΤΟ και ΕΕ, εξοπλισμός που απαιτείται να χρησιμοποιηθεί για το συγκεκριμένο ΣΕΠ ανάλογα με τη διαβάθμισή ασφαλείας του και την απόσταση κάθε τμήματός του από τη εξωτερική περίμετρο της εγκατάστασης; Υφίσταται σχετικό έγγραφο;		X	X	
(4)	Εφόσον έχει κριθεί απαραίτητη η χρήση υλικού TEMPEST στο ΣΕΠ, το υλικό αυτό διαθέτει ταινίες ασφαλείας από τον κατασκευαστή ώστε να εξασφαλίζεται ότι δεν έχει υποστεί οποιαδήποτε «επέμβαση» και κατά συνέπεια τροποποίηση των χαρακτηριστικών του;		X	X	

Α/Α	ΜΕΤΡΟ	ΔΙΑΒΑΘΜΙΣΗ ΣΕΠ			ΠΑΡ/ΣΕΙΣ
		ΠΧ	ΕΠ	ΑΠ	
(5)	Σε περίπτωση που χρησιμοποιούνται ερμάρια με χαρακτηριστικά TEMPEST για την προστασία συνηθισμένου υλικού (SERVER's, απλά τερματικά κλπ), αυτά κατά τη λειτουργία τους τηρούν τα παρακάτω; (α) Κατά την επεξεργασία των δεδομένων είναι πάντα κλειστά. (β) Εφόσον δεν υφίσταται εξουσιοδοτημένο προσωπικό στο χώρο, είναι κλειδωμένα. (γ) Ανοίγονται για εργασίες συντήρησης/ επισκευής μόνο παρουσία του ΥΑΣ και όταν συμβαίνει αυτό δεν επεξεργάζονται διαβαθμισμένα δεδομένα.		X	X	
(6)	Έχει απαγορευτεί η χρήση πομπών (κινητών τηλεφώνων, ασύρματων σταθερών τηλεφώνων, WiFi κλπ) σε απόσταση μικρότερη των 2 μέτρων από οποιαδήποτε οθόνη ή μονάδα τερματικού του ΣΕΠ;		X	X	
	ιστ. Κρυπτογράφηση				
(1)	Υφίσταται προσωπικό ασφαλείας το οποίο έχει εκπαιδευτεί σε θέματα CRYPTO;		X	X	
(2)	Υφίσταται πρόγραμμα εκπαιδεύσεως του προσωπικού κρυπτογράφησης;		X	X	
(3)	Έχει ορισθεί υπεύθυνος κρυπτασφαλείας; Έχει εξουσιοδοτηθεί; Γνωρίζει τα καθήκοντα του;		X	X	
(4)	Χρησιμοποιούνται μόνο πιστοποιημένα (από την ΕΑΑΕΠ) κρυπτοσυστήματα για την ανταλλαγή δεδομένων τόσο εντός του ίδιου ΣΕΠ όσο και μεταξύ διαπιστευμένων ΣΕΠ;		X	X	
(5)	Υπάρχει αυστηρή εφαρμογή των χρονικών περιόδων ισχύος των κλείδων κάθε κώδικα;		X	X	
(6)	Τα υλικά εντός του κρυπτοκέντρου φυλάσσονται σύμφωνα με τα προβλεπόμενα;		X	X	
(7)	Πραγματοποιούνται έκτακτοι απογραφικοί έλεγχοι του υλικού κρυπτογράφησης;		X	X	
(8)	Ποιο πιστοποιημένο λογισμικό (software) διαθέτει το ΣΕΠ για την κρυπτογράφηση των δεδομένων που διακινούνται εκτός του ΓΠΑ;	X			
	ιζ. Ασφάλεια Επικοινωνιών				
(1)	Λαμβάνονται όλα τα μέτρα ασφάλειας ασύρματων εκπομπών;	X	X	X	
(2)	Τα υλικά ασφαλείας επικοινωνιών έχουν καταγραφεί σωστά και παρακολουθούνται διαχειριστικά;	X	X	X	

Α/Α	ΜΕΤΡΟ	ΔΙΑΒΑΘΜΙΣΗ ΣΕΠ			ΠΑΡ/ΣΕΙΣ
		ΠΧ	ΕΠ	ΑΠ	
(3)	Εφαρμόζεται η οδηγία ότι τα αποκρυπτογραφημένα δεδομένα μέσα σε ελεγχόμενο περιβάλλον διακινούνται μέσω των παρακάτω; (α) Με καλώδιο οπτικής ίνας ορατό από άκρο σε άκρο ή (β) Με καλώδιο οπτικής ίνας μέσα σε σωλήνα κενού συνδεδεμένου με συναγερμό πτώσης πίεσης ή (γ) Με κρυπτογράφηση από άκρο σε άκρο χρησιμοποιώντας κατάλληλες κρυπτομηχανές.		Χ	Χ	
(4)	Υφίστανται επικοινωνίες του ΣΕΠ εκτός της περιμέτρου του ΓΠΑ;	Χ	Χ	Χ	
(5)	Προστατεύονται από πιθανή υποκλοπή οι επικοινωνίες που περνούν από το ΓΠΑ; Αν ναι με ποιο τρόπο (συνοπτική περιγραφή);	Χ	Χ	Χ	
(6)	Οι μεταγωγείς (switches) που χρησιμοποιούνται για την διασύνδεση των τμημάτων του συστήματος (servers, τερματικά, περιφερειακά κλπ) έχουν τα παρακάτω χαρακτηριστικά; (α) Στατική αναγνώριση των MAC addresses (β) Στατική αναγνώριση των IP addresses (γ) Δυνατότητα τροποποίησης παραμέτρων μόνο με χρήση ειδικών κωδικών πρόσβασης και μόνο τοπικά (χωρίς τη δυνατότητα τηλεχειρισμού)	Χ	Χ	Χ	
(7)	Οι δρομολογητές (routers) του συστήματος επιτρέπουν μόνο τοπικό χειρισμό (χωρίς τη δυνατότητα τηλεχειρισμού) και η πρόσβαση στο λογισμικό τους επιτυγχάνεται μόνο μέσω χρήσης ειδικών κωδικών πρόσβασης;	Χ	Χ	Χ	
(8)	Γίνεται μηνιαίος έλεγχος των κυκλωμάτων για παροχετεύσεις ή παραλληλισμούς;		Χ	Χ	
(9)	Οι κρυπτοσυσκευές και τα συστήματα ασφάλειας εξωτερικών ορίων (BPD's) που βρίσκονται εκτός κρυπτοκέντρου, είναι τοποθετημένες σε ικριώματα που κλειδώνονται, ανάλογων προδιαγραφών με τη διαβάθμιση ασφαλείας τους;		Χ	Χ	
(10)	Εφόσον υφίστανται κρυπτοσυσκευές και BPD's έτερων συστημάτων από το ΣΕΠ αυτά είναι εγκατεστημένα σε ξεχωριστά ικριώματα που κλειδώνουν;	Χ	Χ	Χ	
ιη. Ασφάλεια Φορητών Υπολογιστικών Συστημάτων (ΦΥΣ) του Οικονομικού Φορέα [αφορά στους φορητούς Η/Υ, έξυπνα κινητά (smartphones), υπολογιστές ταμπλέτες (tablets), κλπ]					
(1)	Γίνεται έλεγχος των ΦΥΣ από προσωπικό της ΑΕΛ πριν την παράδοσή τους στο εξουσιοδοτημένο προσωπικό που πρόκειται να τα χρησιμοποιήσει;	Χ	Χ	Χ	
(2)	Έχουν οριστεί οι διαχειριστές για τη διαμόρφωση των ΦΥΣ και την εγκατάσταση του λογισμικού που απαιτείται σε αυτά, μετά από έγκριση του ΥΑΣ; Έχει οριστεί κωδικός εισόδου στο BIOS;	Χ	Χ	Χ	
(3)	Δίνονται δικαιώματα απλού χρήστη (user) και μόνο στα άτομα που παραλαμβάνουν τα ΦΥΣ;	Χ	Χ	Χ	

Α/Α	ΜΕΤΡΟ	ΔΙΑΒΑΘΜΙΣΗ ΣΕΠ			ΠΑΡ/ΣΕΙΣ
		ΠΧ	ΕΠ	ΑΠ	
(4)	Είναι εφοδιασμένα τα ΦΥΣ με ενημερωμένες εκδόσεις των παρακάτω: (α) Λειτουργικού Συστήματος (β) Τείχους προστασίας (firewall) (γ) Λογισμικού που να αντιλαμβάνεται την προσπάθεια παρακολούθησης ενεργειών (antispyware) (δ) Προγράμματος κατά κακόβουλου λογισμικού (anti-malware).	X	X	X	
(5)	Έχει διευκρινιστεί στους χρήστες ότι ο σκληρός δίσκος του ΦΥΣ δεν χρησιμοποιείται για την αποθήκευση των δεδομένων; Αποθηκεύονται τα δεδομένα σε εγκεκριμένο φορητό μέσο αποθήκευσης (π.χ USB flash disk) που έχει σύστημα κρυπτασφάλισης, φέρει κατάλληλη σήμανση και το οποίο, μετά την ολοκλήρωση της εργασίας, φυλάσσεται από το προσωπικό που εκτέλεσε την εργασία σε κατάλληλο χώρο και σίγουρα όχι μαζί με το ΦΥΣ;	X	X	X	
(6)	Έχει απαγορευτεί η χρήση των ΦΥΣ για πρόσβαση στο Διαδίκτυο (Internet) είτε ενσύρματη είτε ασύρματη, εφόσον περιέχει οποιοδήποτε διαβαθμισμένο έγγραφο, μέσω της απενεργοποίησης των διαδικτυακών δυνατοτήτων αυτού;	X	X	X	
(7)	Προστατεύεται το υλικό στο σύνολό του (φορητός Η/Υ και τυχόν παρελκόμενα) σύμφωνα με τις οδηγίες ασφαλείας που ισχύουν για τα δεδομένα της υψηλότερης διαβάθμισης που χειρίζεται το ΦΥΣ;	X	X	X	
(8)	Για τη μεταφορά ενός ΦΥΣ χρησιμοποιείται τσάντα η οποία να διαθέτει κατάλληλη κλειδαριά και να έχει τέτοιο μέγεθος και βάρος ώστε να μπορεί να ελέγχεται ανά πάσα στιγμή από το άτομο που τη μεταφέρει;	X	X	X	
(9)	Ελέγχονται όλα τα δεδομένα και τα μέσα αποθήκευσης που συνδέονται στο ΦΥΣ για την ύπαρξη κακόβουλου λογισμικού (ιών, δούρειων ίππων κλπ) με χρήση πρόσφατα ενημερωμένου λογισμικού;	X	X	X	
(10)	Εφόσον το ΦΥΣ πρόκειται να διασυνδεθεί με δίκτυο της ΕΕ ή του ΝΑΤΟ έχει εκτελεστεί έλεγχος από την ΑΕΛ, πριν την παράδοση του, ότι δεν περιέχει οποιοδήποτε Εθνικό διαβαθμισμένο δεδομένο;	X	X	X	
ιθ. Χρήση Μη Εγκεκριμένων ΦΥΣ (επισκεπτών, προσωπικών κλπ)					
(1)	Εξασφαλίζεται ότι μη εγκεκριμένα ΦΥΣ μπορούν να χρησιμοποιούνται μόνο εφόσον έχουν ειδική έγκριση από τον ΥΑΣ ή τον βοηθό του;	X	X	X	
(2)	Έχει απαγορευτεί η διασύνδεση μη εγκεκριμένων ΦΥΣ με οποιοδήποτε ΣΕΠ της εγκατάστασης;	X	X	X	
(3)	Στις εξαιρετικές περιπτώσεις που είναι απαραίτητη η ανταλλαγή δεδομένων μεταξύ μη εγκεκριμένου ΦΥΣ και του ΣΕΠ, εξασφαλίζεται ότι αυτή εκτελείται αποκλειστικά και μόνο από τον ΥΑΣ του ΣΕΠ και σε	X	X	X	

Α/Α	ΜΕΤΡΟ	ΔΙΑΒΑΘΜΙΣΗ ΣΕΠ			ΠΑΡ/ΣΕΙΣ
		ΠΧ	ΕΠ	ΑΠ	
	καμία περίπτωση από έναν απλό χρήστη;				
(4)	Εφόσον απαιτηθεί η χρήση μη εγκεκριμένων ΦΥΣ εντός μιας εγκατάστασης που διαθέτει διαβαθμισμένο ΣΕΠ, υφίσταται γραπτή έγκριση από τον ΥΑΣ της εγκατάστασης στην οποία να αναφέρεται ότι το προσωπικό που προσκάλεσε τον επισκέπτη έχει την πλήρη ευθύνη για την χρήση των μη εγκεκριμένων ΦΥΣ καθ’ όλη τη διάρκεια της επίσκεψης;	X	X	X	

8. Συντήρηση – Απόσυρση Εξοπλισμού

Α/Α	ΜΕΤΡΟ	ΔΙΑΒΑΘΜΙΣΗ ΣΕΠ			ΠΑΡ/ΣΕΙΣ
		ΠΧ	ΕΠ	ΑΠ	
	α. Γενικά Μέτρα				
(1)	Αναφέρονται όλες οι εργασίες συντήρησης των SERVER’s στους ΥΑΣ, ΥΑΔ και ΥΑΤ, πριν την έναρξή τους; Τηρείται ειδικό αρχείο;	X	X	X	
(2)	Αναφέρονται όλες οι εργασίες συντήρησης των τερματικών των θέσεων εργασίας στον ΥΑΤ, πριν την έναρξη τους; Τηρείται ειδικό αρχείο;	X	X	X	
(3)	Εξασφαλίζει ο ΥΑΤ, πριν την έναρξη εργασιών συντήρησης ότι όλα τα εκτυπωμένα αντίγραφα και τα μέσα αποθήκευσης αποθηκεύονται ασφαλώς και εκτελείται διακοπή της ισχύος, του προς επισκευή τμήματος του ΣΕΠ, ώστε να επιτευχθεί η διαγραφή οποιασδήποτε εργασίας από τη μνήμη του συστήματος;	X	X	X	
(4)	Εξασφαλίζει ο ΥΑΤ, πριν την έναρξη εργασιών συντήρησης ότι όλο το προσωπικό συντήρησης βρίσκεται υπό στενή παρακολούθηση από αρμόδιο προσωπικό ασφαλείας, ώστε όλες οι εργασίες να τίθενται υπό έλεγχο και ότι δεν υφίσταται δυνατότητα εμφύτευσης παρανόμων συσκευών εντός του υλικού;	X	X	X	
(5)	Εξασφαλίζει ο ΥΑΣ ότι δεν μετακινούνται οι SERVER's εκτός του ΤΠΑ χωρίς την άδεια του, στο πλαίσιο συντήρησής τους;	X	X	X	
(6)	Πριν την μεταφορά των SERVER's για εργασίες επισκευής, δημιουργείται αντίγραφο των υφισταμένων αρχείων με χρήση εξωτερικού σκληρού δίσκου που φέρει την ίδια ακριβώς διαβάθμιση με τη διαβάθμιση του συστήματος; Έχουν αφαιρεθεί οι σκληροί δίσκοι του SERVER πριν τη μεταφορά του για επισκευή;	X	X	X	
(7)	Έχει απαγορευτεί η μεταφορά σκληρών δίσκων του συστήματος για επισκευή εκτός του ΤΠΑ;	X	X	X	

Α/Α	ΜΕΤΡΟ	ΔΙΑΒΑΘΜΙΣΗ ΣΕΠ			ΠΑΡ/ΣΕΙΣ
		ΠΧ	ΕΠ	ΑΠ	
(8)	Εξασφαλίζεται από τον ΥΑΣ η απαγόρευση εκτέλεσης διαγνωστικών προγραμμάτων στους SERVER's με χρήση δισκετών ή φορητών μαγνητικών μέσων, από τους τεχνικούς συντήρησης καθώς και η απομάκρυνση των μέσων αυτών από τους χώρους του ΣΕΠ;	X	X	X	
(9)	Τηρείται ειδικό βιβλίο συντήρησης των SERVER's του ΣΕΠ, στο οποίο να περιγράφεται η ημερομηνία επίσκεψης, τα στοιχεία του προσωπικού συντήρησης, ο λόγος της επίσκεψης και οι εργασίες που εκτελέστηκαν;	X	X	X	
(10)	Τηρείται ειδικό βιβλίο συντήρησης των τμημάτων του ΣΕΠ στο οποίο να περιγράφεται η ημερομηνία επίσκεψης, τα στοιχεία του προσωπικού συντήρησης, ο λόγος της επίσκεψης και οι ενέργειες που εκτελέστηκαν, καθώς επίσης και η αναλυτική περιγραφή των τμημάτων του συστήματος που εγκαταστάθηκε, αντικαταστάθηκε, επισκευάστηκε ή αποσύρθηκε;	X	X	X	
(11)	Το προσωπικό που εκτελεί συντήρηση στο ΣΕΠ έχει εξουσιοδοτηθεί κατάλληλα;	X	X	X	
(12)	Ακολουθείται η διαδικασία της διακοπής εξωτερικών συνδέσεων του συστήματος κατά τη διάρκεια διαβαθμισμένων διεργασιών αναβάθμιση, συντήρηση, επισκευή κλπ);	X	X	X	
(13)	Έχουν καθοριστεί οι διαδικασίες για την απόσυρση του εξοπλισμού του ΣΕΠ και την περαιτέρω επαναδιάθεση του υλικού (hardware);	X	X	X	
(14)	Εφόσον τα τμήματα (hardware) ενός ΣΕΠ προς απόσυρση από την επιχειρησιακή λειτουργία, πρόκειται να χρησιμοποιηθούν σε άλλο ΣΕΠ, εκτελείται ηλεκτρονική διαγραφή των μέσων αποθήκευσης με πιστοποιημένο από την ΕΑΑΕΠ λογισμικό;	X	X	X	

Αντιναύαρχος Ιωάννης Δρυμούσης ΠΝ
Υπαρχηγός

Ακριβές Αντίγραφο

Ασμχος (ΕΑ) Νικόλαος Ζήκος
Επιτελής ΓΕΕΘΑ/Ε3/1

ΓΕΝΙΚΟ ΕΠΙΤΕΛΕΙΟ ΕΘΝΙΚΗΣ ΑΜΥΝΑΣ
Ε’ ΚΛΑΔΟΣ
ΔΝΣΗ ΑΣΦΑΛΕΙΑΣ
07 Σεπ 20

ΠΑΡΑΡΤΗΜΑ «ΙΔ» ΣΤΟΝ
ΕΚΒΑ

ΔΙΑΔΙΚΑΣΙΑ ΑΝΑΛΥΣΗΣ ΚΙΝΔΥΝΟΥ ΑΣΦΑΛΕΙΑΣ

1. Γενικά

α. Η ασφάλεια είναι ένα δυναμικό ζήτημα, το οποίο διερευνάται, σε περιοδική βάση, καθ’ όλη τη διάρκεια του κύκλου ζωής των ΣΕΠ και όποτε κρίνεται απαραίτητο, να αναθεωρούνται τα μέτρα ασφαλείας.

β. Υπεύθυνος φορέας για την αξιοποίηση των οδηγιών, του παρόντος Παραρτήματος, είναι η ΑΕΛ του ΣΕΠ.

γ. Προκειμένου να αντιμετωπισθούν οι απειλές και να μειωθούν ή να εξαλειφθούν οι ευπάθειες ενός ΣΕΠ, οι ενέργειες για την επίτευξη του επιθυμητού επιπέδου ασφαλείας ξεκινούν από τη φάση της σχεδίασής του. Τα αντίμετρα που εισάγονται, όταν το ΣΕΠ βρίσκεται σε προχωρημένο στάδιο ενεργοποίησης ή λειτουργίας, είναι αναπόφευκτα πολύ πιο δαπανηρά, ενώ ενδέχεται να μην είναι και τόσο αποτελεσματικά.

δ. Ως κίνδυνος ασφαλείας, ορίζεται η πιθανότητα που έχει ένα ΣΕΠ, να υποστεί εκμετάλλευση από τις κάθε είδους απειλές, λόγω των αδυναμιών που παρουσιάζει.

ε. Η αξιολόγηση του κινδύνου ασφαλείας, ενσωματώνεται στη διαδικασία σχεδιασμού, ανάπτυξης και λειτουργίας του συστήματος και τα αποτελέσματά της αποτελούν αναπόσπαστο τμήμα της ΔΑΠΑΣ, η οποία διατυπώνεται για το ΣΕΠ, στο πλαίσιο της διαδικασίας διαπίστευσής του.

2. Ανάλυση Κινδύνου (ΑΚ)

α. Η ΑΚ αποτελεί τη διαδικασία αναγνώρισης και καταγραφής των κινδύνων ασφαλείας, δηλαδή των απειλών και των τρωτοτήτων ενός ΣΕΠ, με την οποία καθορίζεται το μέγεθος αυτών, καθώς και τα μέτρα προστασίας που εφαρμόζονται, ώστε αυτό να είναι ασφαλές.

β. Ο σκοπός της ΑΚ, είναι ο καθορισμός του βέλτιστου συστήματος ασφαλείας του ΣΕΠ, προκειμένου να αντιμετωπιστούν οι υφιστάμενοι κίνδυνοι σε περίπτωση που υλοποιηθούν. Κατά συνέπεια, τα αποτελέσματα της ΑΚ, έχουν άμεση επίπτωση τόσο στον αρχικό προϋπολογισμό, όσο και στο τελικό κόστος του ΣΕΠ.

3. Χαρακτηριστικά της ΑΚ

α. Υφίστανται οι παρακάτω τύποι ΑΚ:

(1) Αρχική.

(2) Αναθεωρητική, η οποία πραγματοποιείται είτε σε προχωρημένο στάδιο σχεδίασης του ΣΕΠ, είτε σε περίπτωση τροποποίησης / επέκτασής του.

(3) Έκτακτη, στην περίπτωση εμφάνισης νέων κινδύνων που εκτιμάται ότι επηρεάζουν την ασφάλεια του ΣΕΠ.

β. Η ΑΚ, δεν αποτελεί διαδικασία η οποία γίνεται για μια και μόνο φορά, αλλά εκτελείται σε συγκεκριμένα στάδια της διαδικασίας διαπίστευσης. Μόνο έτσι μπορεί να αντιμετωπίσει τις όποιες αλλαγές στους κινδύνους και τις αδυναμίες του ΣΕΠ, στο πλαίσιο εκπλήρωσης της αποστολής του και λαμβανομένων υπόψη των δεδομένων, των εγκαταστάσεων και του εξοπλισμού που αυτό χρησιμοποιεί. Εξάλλου, η βάση των δεδομένων που προκύπτει από την αρχική ΑΚ, χρησιμοποιείται και κατά την εκτέλεση των άλλων 2 τύπων ΑΚ.

γ. Ο διατιθέμενος χρόνος για την ολοκλήρωση της ΑΚ, αντιστοιχεί τόσο στους στόχους, που έχουν τεθεί, όσο και στο μέγεθος του κάθε ΣΕΠ.

δ. Η επιτυχία της ΑΚ, εξαρτάται σε μεγάλο βαθμό από:

(1) Τη συμμετοχή και την υποστήριξη της διεύθυνσης του φορέα, η οποία έχει κατανοήσει το στόχο και το αντικείμενο της ΑΚ. Αυτή είναι υπεύθυνη για την ενεργή συμμετοχή όλου του προσωπικού στη διαδικασία αυτή.

(2) Την επιλογή εξειδικευμένου προσωπικού που πρόκειται να εκτελέσει την αρχική ΑΚ, την αναθεωρητική ΑΚ, την έκτακτη ΑΚ (όποτε απαιτηθεί) και να συντάξει την Αναφορά Διαχείρισης Εναπομείναντος Κινδύνου (ΑΔΕΚ).

4. Ομάδα ΑΚ (ΟΑΚ)

α. Η συγκρότηση της ΟΑΚ, η οποία καθορίζεται από την ΑΕΛ του ΣΕΠ, αποτελεί ιδιαίτερης σημασίας παράγοντα για το επιτυχές αποτέλεσμα της διαδικασίας. Στην ΟΑΚ συμμετέχει προσωπικό από:

(1) Την ομάδα σχεδιασμού.

(2) Την ομάδα ελέγχου επιχειρησιακής λειτουργίας του.

(3) Την ασφάλεια προσωπικού.

(4) Τον υπεύθυνο ασφαλείας.

(5) Το προσωπικό ασφαλείας επικοινωνιών και πληροφορικής (εφόσον υφίσταται).

β. Τα καθήκοντα της ΟΑΚ, είναι σαφώς καθορισμένα, ενώ καθ’ όλη τη διάρκεια της διαδικασίας, η οποία μπορεί να αποβεί χρονοβόρα, το προσωπικό που την απαρτίζει, απασχολείται κυρίως με αυτή, προκειμένου να επιτύχει στην αποστολή της.

5. Διαδικασία ΑΚ

α. Τα στάδια της διαδικασίας ΑΚ, είναι τα παρακάτω:

(1) Προσδιορισμός του πλαισίου και του στόχου αξιολογήσεως του κινδύνου.

(2) Προσδιορισμός των φυσικών στοιχείων και των στοιχείων πληροφοριών, τα οποία συμβάλλουν στην εκπλήρωση της αποστολής του συστήματος.

(3) Προσδιορισμός της αξίας των φυσικών στοιχείων, τα οποία περιλαμβάνουν το υλικό (hardware), το λογισμικό (software), το πάσης φύσεως υλικό του περιβάλλοντος του ΣΕΠ, τα σχετικά έγγραφα και την αντίστοιχη βιβλιογραφία.

(4) Προσδιορισμός της αξίας των στοιχείων πληροφοριών απέναντι στις εξής απειλές:

(α) Αποκάλυψη σε μη εξουσιοδοτημένα πρόσωπα.

(β) Τροποποίηση.

(γ) Μη διαθεσιμότητα.

(δ) Καταστροφή.

(5) Προσδιορισμός των απειλών και των αδυναμιών, στο περιβάλλον κινδύνου και του επιπέδου αυτών.

(6) Εξακρίβωση των υπαρχόντων μέτρων ασφαλείας.

(7) Προσδιορισμός των απαραίτητων μέτρων που απαιτείται να ληφθούν και σύγκριση αυτών με τα υφιστάμενα.

(8) Εξέταση των κινδύνων και των προτεινομένων αντιμέτρων, σε συνάρτηση με τα παρακάτω που αφορούν στην ασφάλεια διαβαθμισμένων πληροφοριών:

(α) Εξάλειψη του κινδύνου, που στόχο έχει την πλήρη εξάλειψη των αληθινών ή πιθανών αδυναμιών με την πλήρη εφαρμογή των αντιμέτρων.

(β) Πρόληψη απώλειας φυσικών στοιχείων και στοιχείων πληροφοριών, της οποίας στόχος είναι η εφαρμογή των μέτρων για την αποφυγή της απώλειας, όσο είναι δυνατό, γνωρίζοντας ότι ορισμένοι κίνδυνοι δεν είναι δυνατό να εξαλειφθούν λόγω τεχνικών ή λειτουργικών αιτιών.

(γ) Περιορισμός απώλειας φυσικών στοιχείων και στοιχείων πληροφοριών, της οποίας στόχος είναι η εφαρμογή των μέτρων, ώστε η πιθανή απώλεια να διατηρείται σε αποδεκτό επίπεδο.

(δ) Αποδοχή του κινδύνου απώλειας φυσικών στοιχείων και στοιχείων πληροφοριών, όπου πλέον καθίσταται παραδεκτό ότι είτε ο αντίκτυπος της απώλειας δεν είναι σημαντικός, είτε η πιθανότητα της απώλειας είναι περιορισμένη, είτε το κόστος των μέτρων είναι πολύ υψηλό σε σχέση με τη σημασία της απώλειας των δεδομένων.

(9) Ανάπτυξη και υποβολή της Αναφοράς Διαχείρισης Κινδύνου (ΑΔΚ), η οποία να περιλαμβάνει μια περιγραφή των μέτρων που απαιτείται να εφαρμοστούν όπως και την περιγραφή του εναπομείναντος κινδύνου.

6. Διαχείριση Κινδύνου (ΔΚ)

α. Ως εναπομένων κίνδυνος, ορίζεται ο κίνδυνος ο οποίος συνεχίζει να υφίσταται και μετά την εφαρμογή των μέτρων ασφαλείας σε ένα ΣΕΠ, δεδομένου ότι δεν είναι δυνατό να αντιμετωπισθούν, με την εφαρμογή κατάλληλων μέτρων, όλες οι πιθανές απειλές και παράλληλα δεν είναι δυνατό να εξαλειφθούν όλες οι αδυναμίες και οι τρωτότητες του ΣΕΠ. Επιπλέον, τόσο οι απειλές όσο και οι αδυναμίες είναι δυναμικές, με αποτέλεσμα ο εναπομένων κίνδυνος να διαφοροποιείται κατά καιρούς και κατά συνέπεια να απαιτείται η αντιμετώπισή του σε ολόκληρο τον κύκλο ζωής των ΣΕΠ.

β. Με δεδομένα τα αναφερόμενα στην προηγούμενη υποπαράγραφο, η ΔΚ είναι η συνολική διαδικασία αναγνώρισης, ελέγχου και προσπάθειας απομείωσης των πιθανών γεγονότων, τα οποία μπορεί να επηρεάσουν την ασφαλή λει-

τουργία του ΣΕΠ. Κατά τη διαδικασία αυτή, εξετάζονται οι επιλογές για τη διαχείριση του κινδύνου, συμπεριλαμβανομένης της μειώσεως, της μεταβιβάσεως, της εξαλείψεως, της αποφυγής όπως και της αποδοχής αυτού.

γ. Με τη ΔΚ, επιδιώκεται να εξασφαλιστεί ότι ο κίνδυνος που προκύπτει, μετά την εφαρμογή των μέτρων ασφαλείας, βρίσκεται εντός αποδεκτών ορίων. Επίσης, μέσα από τη διαδικασία αυτή, επιδιώκεται η ανάπτυξη μιας κοινής αντίληψης των διαφόρων ομάδων προσωπικού που εμπλέκονται με το ΣΕΠ (όπως διαχειριστών, χρηστών, προσωπικού ασφαλείας), επί των απαιτήσεων και των επιλογών σε ό,τι αφορά τα μέτρα ασφαλείας. Αυτό έχει ως αποτέλεσμα, τη βελτίωση της αντίληψης περί της ασφαλείας και την ενσυνείδητη αποδοχή αλλά και εφαρμογή των αντίστοιχων μέτρων, από την πλευρά των χρηστών.

7. Χαρακτηριστικά της ΔΚ

α. Η ΔΚ ενέχει για το ΣΕΠ, κάποιες ιδιαίτερες δυσκολίες, οι οποίες προκύπτουν από τη δυναμική φύση των κινδύνων και την ταχύτατη εξέλιξη της τεχνολογίας. Η τυχόν αποτυχία στη θεώρηση των παραγόντων του κινδύνου με ένα συγκεκριμένο και ακριβή τρόπο, μπορεί να οδηγήσει σε μη αποτελεσματικά και ιδιαίτερα υψηλού κόστους μέτρα ασφαλείας. Για αυτό, θεωρείται ως τμήμα ολόκληρου του κύκλου ζωής του ΣΕΠ.

β. Τα αποτελέσματα της ΔΚ, παρέχουν τα στοιχεία, σε ό,τι αφορά τους κινδύνους που εξακολουθούν να υφίστανται, τα οποία συμπεριλαμβάνονται απαραιτήτως στα έγγραφα ασφαλείας που απαιτούνται για την παροχή διαπίστευσης ασφαλείας του ΣΕΠ.

Αντιναύαρχος Ιωάννης Δρυμούσης ΠΝ
Υπαρχηγός

Ακριβές Αντίγραφο

Ασμχος (ΕΑ) Νικόλαος Ζήκος
Επιτελής ΓΕΕΘΑ/Ε3/1

ΠΡΟΣΘΗΚΕΣ

«1» Ανάλυση Σταδίων της Διαδικασίας Ανάλυσης Κινδύνου (ΑΚ)
«2» Διαδικασία Επιλογής Αυτοματοποιημένων Εργαλείων Ανάλυσης Κινδύνου (ΑΚ)

ΓΕΝΙΚΟ ΕΠΙΤΕΛΕΙΟ ΕΘΝΙΚΗΣ ΑΜΥΝΑΣ
Ε’ ΚΛΑΔΟΣ
ΔΝΣΗ ΑΣΦΑΛΕΙΑΣ
07 Σεπ 20

ΠΡΟΣΘΗΚΗ «1» ΣΤΟ ΠΑΡΑΡΤΗΜΑ «ΙΔ»
του ΕΚΒΑ

ΑΝΑΛΥΣΗ ΣΤΑΔΙΩΝ ΤΗΣ ΔΙΑΔΙΚΑΣΙΑΣ ΑΝΑΛΥΣΗΣ ΚΙΝΔΥΝΟΥ (ΑΚ)

1. Καθορισμός του Περιβάλλοντος Κινδύνου

α. Ο πρώτος στόχος της εξακρίβωσης του περιβάλλοντος κινδύνου, είναι να εξασφαλιστεί η ακριβής απεικόνιση των φυσικών ορίων των εγκαταστάσεων του οικονομικού φορέα, τα οποία συμπεριλαμβάνουν:

(1) Τις εγκαταστάσεις των Η/Υ.

(2) Τις εγκαταστάσεις και τα μέσα αποθήκευσης δεδομένων.

(3) Τους χώρους ελέγχου εισόδου / εξόδου του προσωπικού που χρησιμοποιεί το σύστημα.

(4) Τους χώρους των τερματικών σταθμών και των θέσεων εργασίας καθώς και τις εγκαταστάσεις τηλεχειρισμού.

(5) Τους χώρους των χρηστών.

(6) Τους χώρους προγραμματισμού.

(7) Τις εγκαταστάσεις επικοινωνιών του συστήματος.

(8) Τους χώρους της διεύθυνσης και των γραφείων γενικά.

β. Επίσης, υποβάλλονται τα σχέδια του εξοπλισμού υποστήριξης, όπως για παράδειγμα παροχές ηλεκτρικής ενέργειας, θέρμανσης, εξαερισμού και κλιματισμού.

γ. Πολλά από τα στοιχεία που αναφέρθηκαν και απαιτούνται για την αρχική ΑΚ, χρησιμοποιούνται ξανά, κατά την εκτέλεση της αναθεωρητικής ΑΚ ή της έκτακτης ΑΚ, αφού προηγουμένως υποστούν μικρής εκτάσεως τροποποιήσεις ή βελτιώσεις.

2. Αξιολόγηση των Φυσικών και Πληροφοριακών Στοιχείων του Συστήματος

α. Για τα φυσικά στοιχεία του συστήματος, στα οποία συμπεριλαμβάνονται το υλικό (hardware), το λογισμικό (software), ο εξοπλισμός γραφείου και το σχετικό αρχείο εγγράφων, η αξιολόγηση έγκειται στον καθορισμό του κόστους αντικατάστασης και αναδόμησης του κάθε στοιχείου του συστήματος, σε περίπτωση απώλειας ή μη λειτουργικής διαθεσιμότητας.

β. Για τα πληροφοριακά στοιχεία, η αξιολόγηση γίνεται είτε από τους κατόχους / συντάκτες τους ή από έτερο προσωπικό, που δύναται να αναφερθεί επίσημα σε αυτά, προκειμένου να καθοριστεί ο αντίκτυπος στο ΣΕΠ συνολικά στις περιπτώσεις, όπου αυτά υποστούν:

(1) Καταστροφή.

(2) Μη διαθεσιμότητα.

(3) Αποκάλυψη σε μη εξουσιοδοτημένα άτομα.

(4) Τροποποίηση από μη εξουσιοδοτημένα άτομα.

3. Αξιολόγηση Απειλών και Πιθανών Αδυναμιών του Συστήματος

α. Ο κίνδυνος έχει τρεις παραμέτρους, την αδυναμία, την απειλή και την επίδραση. Η αδυναμία, είναι μια τρωτότητα ανοιχτή για εκμετάλλευση. Η απειλή, είναι η πιθανότητα κάποιος να εκμεταλλευτεί την αδυναμία ή σε περιπτώσεις περιβαλλοντολογικών απειλών (όπως καταιγίδες, σεισμός), είναι η πιθανότητα το γεγονός να συμβεί. Η επίδραση, είναι οι συνέπειες όταν πραγματοποιείται μια απειλή. Στο στάδιο αυτό, απαιτείται η κατάρτιση ενημερωμένης λίστας των απειλών και των πιθανών αδυναμιών του ΣΕΠ. Η λίστα συντάσσεται από την ΟΑΚ, αφού προηγουμένως συμβουλευτεί την ΕΑΑΕΠ και την ΕΑΔΑ (ή την ΕΔΑ εφόσον έχει καθοριστεί). Η μεθοδολογία που ακολουθείται είναι η παρακάτω:

(1) Καθορισμός και ανάλυση του μεγέθους κάθε απειλής. Αυτό μπορεί να εξεταστεί από την άποψη της πιθανότητας (τυχαίες απειλές) ή της δυνατότητας (σκόπιμες απειλές) μιας απειλής, να εκμεταλλευτεί μία τρωτότητα και με αυτόν τον τρόπο να προξενήσει έναν αντίκτυπο στην ασφάλεια του ΣΕΠ.

(2) Καθορισμός των αδυναμιών του ΣΕΠ.

β. Στις απειλές, συμπεριλαμβάνονται καταστάσεις όπως η πυρκαγιά, η πλημμύρα, το ηλεκτρικό βραχυκύκλωμα, η περίπτωση απώλειας ηλεκτρικής ισχύος (black out), καθώς και τα φυσικά φαινόμενα, όπως καταιγίδες, σεισμοί κλπ

γ. Κάθε πιθανή αδυναμία από τη λίστα, προσδιορίζεται σε συνάρτηση με το υφιστάμενο περιβάλλον κινδύνου και συνοδεύεται από μια εκτίμηση της πιθανότητας πραγματοποίησης των απειλών, που την αξιοποιήσουν (την αδυναμία), προκειμένου να πλήξουν το ΣΕΠ. Στο πλαίσιο αυτό, απαιτείται η επιθεώρηση των εγκαταστάσεων από την ΟΑΚ και η συνεργασία με το αρμόδιο προσωπικό αυτών.

δ. Στο τέλος της αξιολόγησης, συντάσσεται ένας κατάλογος στον οποίο παρουσιάζονται συγκεκριμένοι κίνδυνοι που ενδέχεται να εμφανιστούν στο ΣΕΠ. Ο κατάλογος αυτός, ελέγχεται από την ΕΑΑΕΠ και στη συνέχεια να εγκρίνεται από την ΕΑΔΑ.

4. Αξιολόγηση των Υφιστάμενων Μέτρων

Το στάδιο αυτό, αφορά μόνο στα συστήματα, στα οποία η ΑΚ δεν έχει εκτελεστεί από τη φάση της σχεδίασης και για την υλοποίησή του, απαιτείται η ανάλυση των υφισταμένων μέτρων σε ό,τι αφορά:

α. Τη φυσική ασφάλεια.

β. Την ασφάλεια προσωπικού.

γ. Την ασφάλεια πληροφοριών.

δ. Την ασφάλεια επικοινωνιών και πληροφορικής (ασφάλεια Η/Υ, ανεπιθύμητων εκπομπών, κρυπτογράφησης και επικοινωνιών).

5. Προσδιορισμός Προτεινομένων Μέτρων

α. Αφού έχουν αναγνωριστεί όλα τα φυσικά και πληροφοριακά στοιχεία, έχει καθοριστεί η σημασία του καθενός στο περιβάλλον κινδύνου, παράλληλα με τις απειλές και τις αδυναμίες, καθορίζονται τα προτεινόμενα μέτρα. Η επιλογή των μέτρων από ένα συμβιβασμό μεταξύ των λειτουργικών περιορισμών, των τεχνικών

απαιτήσεων, των νομικών απαιτήσεων, των οικονομικών περιορισμών και του διαθέσιμου προσωπικού.

β. Αυτό επιτυγχάνεται:

(1) Είτε με τη μελέτη των κινδύνων και των αδυναμιών κάθε φυσικού ή πληροφοριακού στοιχείου ξεχωριστά ή ως ομάδα στοιχείων και στη συνέχεια την καταγραφή καταλόγου των τεχνικών ή μη μέτρων.

(2) Είτε με την αντιστοίχιση κάθε επιβεβαιωμένης απειλής και αδυναμίας στο αντίστοιχο φυσικό και πληροφοριακό στοιχείο που επηρεάζεται, ενώ στη συνέχεια επιλέγεται το κατάλληλο μέτρο (ενδέχεται να απαιτηθεί συνδυασμός μέτρων για την αντιμετώπιση μιας απειλής).

γ. Ωστόσο, λαμβάνεται υπόψη ότι, η απειλή έχει σημασία μόνο εφόσον υπάρχει αδύνατο σημείο το οποίο μπορεί να τύχει εκμετάλλευσης. Κατά αντιστοιχία ένα αδύνατο σημείο γίνεται σημαντικό, μόνο εφόσον υπάρχει μια απειλή για να το εκμεταλλευτεί.

δ. Η αναγνώριση των μέτρων γίνεται υπό το πρίσμα:

(1) Των πλέον απαραίτητων μέτρων για τη συνολική ασφάλεια των διαβαθμισμένων πληροφοριών.

(2) Των απαιτήσεων των ΑΕΛ και ΕΑΔΑ.

ε. Στο τέλος της διαδικασίας, καταρτίζεται μια λίστα απαιτούμενων μέτρων ασφαλείας, τα οποία συγκρίνονται με τα ήδη υφιστάμενα, προκειμένου να εξαχθεί η λίστα των προτεινομένων μέτρων.

στ. Η επόμενη ενέργεια, αφορά στην εξέταση των κινδύνων σε σχέση με τα προτεινόμενα μέτρα, η οποία καταλήγει στη συμφωνία επί του αριθμού και του είδους των μέτρων. Γι' αυτή την εργασία, απαιτείται η συνεργασία της ΑΕΛ με την ΕΑΑΕΠ και την ΕΑΔΑ.

ζ. Η διαδικασία καθορισμού των μέτρων, μπορεί να μην παρέχει ένα τέλειο αποτέλεσμα για τους παρακάτω λόγους:

(1) Έλλειψη της κατάλληλης τεχνολογίας για την αντιμετώπιση ενός κινδύνου.

(2) Αδυναμία πρακτικής εφαρμογής των μέτρων (μη ρεαλιστικά μέτρα).

(3) Περιορισμοί στην υλοποίηση, οι οποίοι μπορούν να καταστήσουν αδύνατο να αντιμετωπιστεί, είτε μερικώς, είτε πλήρως ένας κίνδυνος.

6. Περιγραφή του Εναπομείναντος Κινδύνου

α. Εάν θεωρείται ότι τα προτεινόμενα μέτρα δεν μπορούν να αντιμετωπίσουν πλήρως τους θεωρητικούς κινδύνους, τότε συντάσσεται πίνακας με τους εναπομείναντες κινδύνους. Για τη σύνταξη του εν λόγω πίνακα απαιτείται η συνεργασία της ΟΑΚ με την ΕΑΑΕΠ.

β. Τον πίνακα με τους εναπομείναντες κινδύνους, απαιτείται να τον εγκρίνει η ΕΑΔΑ, ενώ σε αντίθετη περίπτωση απαιτείται η εκ νέου μελέτη των δεδομένων και η προσθήκη κατάλληλων μέτρων, καθόσον διαφορετικά διακυβεύεται σοβαρά η ασφάλεια του ΣΕΠ.

7. Υποβολή Αναφοράς Διαχείρισης Κινδύνου (ΑΔΚ)

Η ΑΔΚ, περιλαμβάνει τα παρακάτω:

α. Το σκοπό και το στόχο της ΑΚ.

β. Τη μεθοδολογία που ακολουθήθηκε με τον αντίστοιχο σχεδιασμό.

γ. Τη διακρίβωση των στοιχείων, των κινδύνων, των απειλών και των αδυναμιών του ΣΕΠ.

δ. Τη συμμόρφωση με τις προδιαγραφές που ισχύουν.

ε. Τα προτεινόμενα μέτρα.

στ. Τον εναπομείναντα αποδεκτό κίνδυνο.

ζ. Την ισχύουσα διαδικασία ΔΚ.

Αντιπτέραρχος (Ι) Ιωάννης Γκοντικούλης
Επιτελάρχης

Ακριβές Αντίγραφο

Ασμχος (ΕΑ) Νικόλαος Ζήκος
Επιτελής ΓΕΕΘΑ/Ε3/1

ΓΕΝΙΚΟ ΕΠΙΤΕΛΕΙΟ ΕΘΝΙΚΗΣ ΑΜΥΝΑΣ
Ε’ ΚΛΑΔΟΣ
ΔΝΣΗ ΑΣΦΑΛΕΙΑΣ
07 Σεπ 20

ΠΡΟΣΘΗΚΗ «2» ΣΤΟ ΠΑΡΑΡΤΗΜΑ «ΙΔ»
του ΕΚΒΑ

ΔΙΑΔΙΚΑΣΙΑ ΕΠΙΛΟΓΗΣ ΑΥΤΟΠΟΙΗΜΕΝΩΝ ΕΡΓΑΛΕΙΩΝ
ΑΝΑΛΥΣΗΣ ΚΙΝΔΥΝΟΥ (ΑΚ)

1. Εκτέλεση ΑΚ με χρήση Αυτοματοποιημένων Εργαλείων

Η ΑΕΛ ενός ΣΕΠ, στο πλαίσιο υποβοήθησης της ΟΑΚ, στην εκτέλεση της ΑΚ, μπορεί να προβεί στην προμήθεια Αυτοματοποιημένου Εργαλείου Ανάλυσης Κινδύνου (ΑΕΡΓΑΚ). Το ΑΕΡΓΑΚ έχει τη μορφή λογισμικού (software) και μέσω των αναβαθμίσεων που επιδέχεται, τηρείται πάντα ενημερωμένο για τους υφιστάμενους κινδύνους που μπορούν να απειλήσουν ένα ΣΕΠ, αλλά και για τα αντίμετρα που απαιτείται να ληφθούν στο πλαίσιο αντιμετώπισης αυτών. Με την απόκτηση ενός ΑΕΡΓΑΚ, η ΑΕΛ σε οποιαδήποτε περίπτωση σχεδιάζει την τροποποίηση / βελτίωση / διαφοροποίηση ενός ΣΕΠ, έχει τη δυνατότητα για άμεση εκτέλεση ΑΚ, τα αποτελέσματα της οποίας την κατευθύνουν στις επόμενες ενέργειές της.

2. Η Σημασία του ΑΕΡΓΑΚ στο έργο της ΟΑΚ

Η ΟΑΚ, εξασφαλίζει ότι το αποτέλεσμα της όλης διεργασίας είναι μια εμπεριστατωμένη ΑΚ και όχι απλή απαρίθμηση των αδυναμιών του συστήματος (όπως τις εκτίμησε το προσωπικό που την αποτελεί), μαζί με την παράθεση κάποιων λύσεων για την αντιμετώπιση αυτών. Στο έργο της αυτό, η χρήση ενός σύγχρονου και ενημερωμένου ΑΕΡΓΑΚ κρίνεται ως καταλυτικής σημασίας.

3. Πλεονεκτήματα της χρήσης ΑΕΡΓΑΚ στην ΑΚ

Τα πλεονεκτήματα της χρήσης ενός ΑΕΡΓΑΚ είναι:

α. Η ευκολία στο χειρισμό και η πρόσβαση σε βάσεις δεδομένων που περιέχουν επεξεργασμένα στοιχεία εκτίμησης κινδύνου.

β. Η δυνατότητα αποτύπωσης των αποτελεσμάτων από την απώλεια φυσικών και πληροφοριακών πόρων από το συνδυασμό των μέτρων.

γ. Η δυνατότητα γρήγορης εισαγωγής αλλαγών στο περιβάλλον κινδύνου και η παρακολούθηση των αλλαγών που επιτελούνται στο περιβάλλον ασφαλείας του οργανισμού/υπηρεσίας.

4. Διαδικασία Ελέγχου Επάρκειας του ΑΕΡΓΑΚ

Προκειμένου να ελεγχθεί η επάρκεια του ΑΕΡΓΑΚ που πρόκειται να χρησιμοποιηθεί στην ΑΚ, απαιτείται να:

α. Καθοριστούν οι προδιαγραφές του, σύμφωνα με τα στάδια της ΑΚ.

β. Καθοριστεί το αρμόδιο προσωπικό για την αξιολόγησή του.

γ. Γίνει η προετοιμασία του αναλυτικού πίνακα των στοιχείων επιλογής.

δ. Αιτηθεί στην προμηθεύτρια εταιρεία την εκτέλεση δοκιμής του.

ε. Γίνει η αξιολόγηση και επιλογή των κατάλληλων εναλλακτικών ΑΕΡΓΑΚ.

5. Προδιαγραφές του ΑΕΡΓΑΚ

Το ΑΕΡΓΑΚ που επιλέγεται να χρησιμοποιηθεί στην ΑΚ, απαιτείται να μπορεί να εκτελέσει τις παρακάτω ουσιώδεις διαδικασίες:

α. Συλλογή δεδομένων για το ΣΕΠ, είτε σε μορφή κειμένου είτε σε γραφικό περιβάλλον. Στη φάση αυτή, προκύπτει η περιγραφή των στοιχείων (φυσικών και πληροφοριακών) του συστήματος και η σημασία τους, είτε σε ποσοτικούς, είτε σε ποιοτικούς όρους. Επίσης, γίνεται συλλογή στοιχείων για τις απειλές, τις αδυναμίες και τα μέτρα.

β. Αξιολόγηση των δεδομένων, μέσω ανάλυσης των σχέσεων μεταξύ των στοιχείων, των απειλών, των αδυναμιών και των μέτρων, ώστε να καθορίσει τις πιθανές απώλειες. Για την αξιολόγηση των δεδομένων μπορεί να χρησιμοποιούνται οι παρακάτω μέθοδοι:

(1) Ποσοτική προσέγγιση, με τη χρήση της οποίας επιτυγχάνονται:

(α) Η προσέγγιση της απώλειας μέσω της εκτίμησης, για κάθε πληροφορία, αρχείο ή εφαρμογή.

(β) Ο υπολογισμός της συχνότητας πραγματοποίησης των γεγονότων που επιδρούν στην εμπιστευτικότητα, στην ακεραιότητα και στη διαθεσιμότητα.

(γ) Η ποσοτική μέτρηση της βλάβης, που πρόκειται να υποστεί το ΣΕΠ από την απώλεια αυτή.

(2) Ποιοτική προσέγγιση, η οποία αποδέχεται το γεγονός ότι πολλές πιθανές απώλειες είναι ασαφείς και για αυτό το λόγο οι κίνδυνοι δεν μπορούν εύκολα να προσδιοριστούν ποσοτικά. Τα αποτελέσματα των κινδύνων απεικονίζονται κατά τρόπο περιγραφικό (πχ. «κανένας κίνδυνος» έως «πολύ μεγάλος κίνδυνος»). Κάποιες ποιοτικές προσεγγίσεις παρουσιάζουν το αποτέλεσμα των κινδύνων με μαθηματικό τρόπο με χρήση κλιμάκων διαβάθμισης από το 1 έως το 10, με περιγραφική ορολογία για κάθε σημείο της κλίμακας.

γ. Απεικόνιση της Επίδρασης σε Περίπτωση Αλλαγής των Παραμέτρων του ΣΕΠ. Δίνονται αποτελέσματα σε σενάρια διαφοροποίησης βασικών χαρακτηριστικών του συστήματος, όπως η αλλαγή των πόρων, η αύξηση των χρηστών, η αλλαγή τροποποίηση περιβάλλοντος λειτουργίας κλπ

δ. Παροχή Αποτελεσμάτων της Αξιολόγησης των Δεδομένων. Ώστε να εντοπιστούν τα σημεία στα οποία απαιτείται να εφαρμοστούν μέτρα, για την προστασία των ζωτικών στοιχείων του ΣΕΠ.

6. Κριτήρια Επιλογής του ΑΕΡΓΑΚ

Κατά τη διαδικασία επιλογής ενός ΑΕΡΓΑΚ, λαμβάνονται υπόψη και εξετάζονται τα παρακάτω χαρακτηριστικά αυτού:

α. Απαιτήσεις Υλικού και Λογισμικού. Το ΑΕΡΓΑΚ, στο πλαίσιο περιορισμού του κόστους, είναι χρήσιμο, να έχει τη δυνατότητα λειτουργίας σε κοινούς υπολογιστές που βρίσκονται εντός της ΑΕΛ και να μην απαιτεί ειδικού τύπου Η/Υ. Επίσης, οι απαιτήσεις σε περιφερειακό υλικό (οθόνες, εκτυπωτές, σαρωτές κλπ), προσδιορίζονται εκ των προτέρων. Ο πηγαίος κώδικας, συνήθως δεν είναι διαθέ-

σιμος, ωστόσο κάποιες εταιρείες μπορούν να προσαρμόσουν το προϊόν στις ανάγκες του φορέα. Η αδυναμία προσαρμογής του ΑΕΡΓΑΚ, στις απαιτήσεις υλικού και λογισμικού, οδηγεί σε επανέλεγχο για την πιθανότητα επιλογής του.

β. Μεθοδολογία. Εξετάζεται η λειτουργική μέθοδος που χρησιμοποιεί για την περιγραφή των απωλειών που προκύπτουν, από ανεπιθύμητα γεγονότα. Οι απώλειες προκύπτουν είτε από μαθηματικά, είτε από περιγραφικά μοντέλα. Ένα ΑΕΡΓΑΚ, δεν αξιολογείται αποκλειστικά με βάση την ταχύτητα εξαγωγής αποτελεσμάτων. Αντιθέτως, η αξία του έγκειται στη δυνατότητά του για την παραγωγή ορθών αποτελεσμάτων. Το ΑΕΡΓΑΚ επιτρέπει στο χρήστη την ανάπτυξη μιας μεθόδου κατανόησης του τρόπου εξαγωγής των αποτελεσμάτων και του τρόπου αποτελεσματικής εφαρμογής τους.

γ. Απαιτήσεις επί των Αναφορών της ΑΚ

(1) Η λήψη ορθών αποφάσεων για την επιλογή και την εφαρμογή αποτελεσματικών μέτρων, εξαρτάται από την πληρότητα των αναφορών της ΑΚ. Οι αναφορές συνοψίζουν τις απειλές ή τις αδυναμίες και προσδιορίζουν τα πιθανά μέτρα. Στη συνέχεια, αυτά αξιολογούνται βάση των ελάχιστων απαιτήσεων ασφαλείας που καθορίζονται στον παρόντα Κανονισμό.

(2) Η ποιότητα των αναφορών μπορεί να διαφέρει ανάλογα, με το υπό χρήση ΑΕΡΓΑΚ. Οι τύποι των αναφορών που συνήθως παράγουν τα ΑΕΡΓΑΚ είναι οι παρακάτω:

(α) Αναφορές χρήσιμες στη Διεύθυνση του φορέα του ΣΕΠ.

(β) Αναφορές που χρησιμοποιούνται ως βοηθητική βιβλιογραφία.

(γ) Αναφορές καταλόγων απειλών και αδυναμιών καθώς και λίστες μέτρων.

(δ) Αναφορές που αποτυπώνουν τα αποτελέσματα των κινδύνου σε γραφικές παραστάσεις επιτρέποντας έτσι στο χρήστη να μπορεί να συγκρίνει τον κίνδυνο ανάλογα με την απειλή.

δ. Βιβλιογραφία

Αποτελεί απαραίτητο στοιχείο για την αποτελεσματική χρήση του ΑΕΡΓΑΚ. Η βιβλιογραφία, παρέχει πληροφορίες, οι οποίες λεπτομερώς επεξηγούν τα παρακάτω:

(1) Τη λειτουργία του.

(2) Τις οδηγίες για τη φόρτωσή του.

(3) Τις επεξηγήσεις των μηνυμάτων λάθους (error messages).

(4) Τις οδηγίες για την επαναλειτουργία του.

(5) Τα είδη και τις διαμορφώσεις (format) των αναφορών που μπορούν να παραχθούν.

ε. Χαρακτηριστικά Ασφαλείας και Ιστορικών Στοιχείων

(1) Από τη στιγμή που οι πληροφορίες που έχουν συλλεχθεί για ένα ΣΕΠ, μπορεί να είναι διαβαθμισμένες, καθορίζονται οι απαιτήσεις για ελέγχους ασφαλείας (εξακρίβωση και αυθεντικότητα, έλεγχος πρόσβασης και επαλήθευση). Έτσι, η δυνατότητα να διατηρείται ιστορικό αρχείο των πληροφοριών που έχουν

συλλεχθεί, πρόκειται να αποβεί χρήσιμη στις μελλοντικές ΑΚ του συγκεκριμένου συστήματος.

(2) Εάν οι έλεγχοι ασφαλείας δεν αποτελούν χαρακτηριστικό του ΑΕΡΓΑΚ που έχει επιλεγεί, τότε είναι απαραίτητο να τηρηθούν διαδικασίες οι οποίες εξασφαλίζουν την προστασία διαβαθμισμένων πληροφοριών που έχουν συλλεχθεί για το φορέα και οι οποίες επιβάλουν ελέγχους σχετικά με το προσωπικό (εκτός του φορέα), που έχει πρόσβαση σε αυτές τις πληροφορίες.

στ. Ευκολία στη Χρήση. Η δυνατότητα για αποτελεσματική και παράλληλα ευχερή χρήση ενός ΑΕΡΓΑΚ αποτελεί σημαντικό παράγοντα για την επιλογή, καθόσον εάν είναι δύσκολο στη χρήση ή δυσλειτουργικό, τελικά καθίσταται άχρηστο. Έτσι, πριν την τελική επιλογή ενός ΑΕΡΓΑΚ, όλες οι προδιαγραφές καθορίζονται και διαβιβάζονται στους υποψήφιους προμηθευτές. Η επίδειξη του ΑΕΡΓΑΚ, εξασφαλίζει ότι οι προδιαγραφές πληρούνται. Επιπλέον, οι αξιολογήσεις από έτερους χρήστες που ήδη χρησιμοποιούν το συγκεκριμένο ΑΕΡΓΑΚ, ζητούνται προκειμένου να επιβεβαιώνονται οι δυνατότητες του προϊόντος.

ζ. Εκπαίδευση και Τεχνική Υποστήριξη. Η αποτελεσματική χρήση οποιουδήποτε ΑΕΡΓΑΚ, εξαρτάται από την εκπαίδευση του προσωπικού, που το χρησιμοποιεί. Ως εκ τούτου, οι λεπτομερείς οδηγίες χρήσεως και η ολοκληρωμένη εκπαίδευση αποτελούν βασικό κριτήριο επιλογής.

η. Κόστος Πρόσκτησης. Το οποίο λαμβάνεται υπόψη, αλλά δεν αποτελεί πρωταρχικό παράγοντα για την επιλογή του. Επιπλέον, το κόστος αξιολογείται σε συνδυασμό με όλους του προαναφερθέντες παράγοντες, ώστε να γίνει συνολική εκτίμηση του ΑΕΡΓΑΚ.

Αντιπτέραρχος (Ι) Ιωάννης Γκοντικούλης
Επιτελάρχης

Ακριβές Αντίγραφο

Ασμχος (ΕΑ) Νικόλαος Ζήκος
Επιτελής ΓΕΕΘΑ/Ε3/1

ΓΕΝΙΚΟ ΕΠΙΤΕΛΕΙΟ ΕΘΝΙΚΗΣ ΑΜΥΝΑΣ
Ε’ ΚΛΑΔΟΣ
ΔΝΣΗ ΑΣΦΑΛΕΙΑΣ
07 Σεπ 20

ΠΑΡΑΡΤΗΜΑ «ΙΕ» ΣΤΟΝ
ΕΚΒΑ

ΑΡΜΟΔΙΟΤΗΤΕΣ ΚΑΙ ΚΑΘΗΚΟΝΤΑ ΑΡΧΩΝ ΚΑΙ ΠΡΟΣΩΠΙΚΟΥ ΑΣΦΑΛΕΙΑΣ

1. Στο παρόν Παράρτημα αναφέρονται οι γενικές αρμοδιότητες, ευθύνες και καθήκοντα των εμπλεκόμενων, με τη διαδικασία διαπίστευσης ασφαλείας των ΣΕΠ, αρχών και προσωπικού.

2. Εθνική Αρχή Διαπίστευσης Ασφαλείας (ΕΑΔΑ)

Η ΕΑΔΑ, έχει θεσμοθετηθεί σύμφωνα με το άρθρο 21 του παρόντος Κανονισμού και τα καθήκοντά της έχουν ανατεθεί στο ΓΕΕΘΑ/Ε' ΚΛΑΔΟΣ και είναι υπεύθυνη για τα παρακάτω:

α. Εκτέλεση της διαδικασίας διαπίστευσης, με τη συμμετοχή κατά περίπτωση της Εθνικής Αρχής Ασφαλείας Επικοινωνιών και Πληροφορικής (ΕΑΑΕΠ) και των εμπλεκομένων φορέων.

β. Μεταβίβαση της αρμοδιότητας διεξαγωγής διαδικασίας διαπίστευσης ασφαλείας σε κατάλληλους φορείς οι οποίοι σε συνεργασία με την ΕΑΑΕΠ, υλοποιούν για συγκεκριμένα και μόνο ΣΕΠ, τη διαδικασία της διαπίστευσης ασφαλείας και φέρουν τον τίτλο Επιτροπή Διαπίστευσης Ασφαλείας (ΕΔΑ). Ωστόσο, την τελική ευθύνη για τη διαπίστευση ασφαλείας και τη δικαιοδοσία για την επιβολή προτύπων ασφαλείας, τη διατηρεί στο ακέραιο η ΕΑΔΑ.

γ. Παροχή συμβουλών και οδηγιών σχετικά με την πολιτική ασφαλείας των διαβαθμισμένων ΣΕΠ, [εκτός των θεμάτων για τα οποία είναι υπεύθυνη η ΕΑΑΕΠ (άρθρο 20), τα καθήκοντα της οποίας έχουν ανατεθεί στην ΕΥΠ/Ε' ΔΝΣΗ]:

(1) Στον εμπλεκόμενο οικονομικό φορέα.

(2) Στο προσωπικό διαχειρίσεως ασφαλείας των ΣΕΠ του εμπλεκόμενου οικονομικού φορέα.

(3) Στο προσωπικό σχεδιασμού των δικτύων Η/Υ του εμπλεκόμενου οικονομικού φορέα.

δ. Έλεγχο και έγκριση της διασύνδεσης δύο ή περισσοτέρων ΣΕΠ, σύμφωνα με τις συμφωνηθείσες Δηλώσεις Απαιτήσεως Ασφαλείας Διασυνδέσεως συστημάτων (ΔΑΠΑΔ).

ε. Παροχή Συμβουλών για τη Διασύνδεση των ΣΕΠ με:

(1) ΣΕΠ της ΕΕ σε διαφορετικές περιοχές ασφαλείας ή διοικήσεως.

(2) ΣΕΠ του ΝΑΤΟ σε διαφορετικές περιοχές ασφαλείας ή διοικήσεως.

(3) Εθνικά ΣΕΠ.

στ. Συντονισμό και συνεργασία με τις αρμόδιες Αρχές / Υπηρεσίες της ΕΕ

και του ΝΑΤΟ, για τις διαδικασίες διαπίστευσης των εθνικών ΣΕΠ που πρόκειται να διασυνδεθούν με ΣΕΠ των οργανισμών αυτών.

3. Επιτροπή Διαπίστευσης Ασφαλείας (ΕΔΑ)

α. Η ΕΔΑ υλοποιεί τη διαδικασία διαπίστευσης για συγκεκριμένα και μόνο ΣΕΠ, με αρμοδιότητες και καθήκοντα τα οποία, κατά περίπτωση, της παραχωρούνται από την ΕΑΔΑ. Ωστόσο την τελική ευθύνη για τη διαπίστευση ασφαλείας των εν λόγω ΣΕΠ, τη διατηρεί η ΕΑΔΑ η οποία έχει και τη δυνατότητα ανά πάσα στιγμή να ελέγξει την πορεία της διαδικασίας διαπίστευσης.

β. Η ΕΔΑ είναι υπεύθυνη για τα παρακάτω:

(1) Εφαρμογή της υφιστάμενης διαδικασίας διαπίστευσης σε συνεργασία με την ΕΑΑΕΠ.

(2) Έγκριση και εφόσον απαιτείται αναθεώρηση, των σχετικών με την ασφάλεια εγγράφων όπως οι εκθέσεις Ανάλυσης Κινδύνου (ΑΚ), η Δήλωση Απαιτήσεων Ασφαλείας (ΔΑΠΑΣ), οι Διαδικασίες Ασφαλούς Λειτουργίας (ΔΑΛ), οι εκθέσεις ελέγχου ασφαλείας, οι εκθέσεις διαχείρισης κινδύνων, που εκπονούνται από την ΑΕΛ.

(3) Παροχή της δήλωσης συμμόρφωσης (Statement of Compliance - SoC), η οποία δηλώνει το χρονικό διάστημα για το οποίο, υπό την υφιστάμενη διαμόρφωση, το ΣΕΠ θεωρείται ότι λειτουργεί ασφαλώς, ενώ καθορίζονται οι συνθήκες κάτω από τις οποίες απαιτείται η εκ νέου διαπίστευση του συστήματος. Στις περιπτώσεις που παρέχεται η δήλωση Προσωρινής Εγκρίσεως για Λειτουργία (ΠΕΛ), προσδιορίζονται σε αυτή οι όροι προσωρινής λειτουργίας του ΣΕΠ και οι δραστηριότητες οι οποίες απαιτούνται για να δοθεί η πλήρης πιστοποίηση ασφαλούς λειτουργίας.

(4) Έλεγχο για την εφαρμογή των μέτρων ασφαλείας, όπως αναφέρονται στα εγκεκριμένα έγγραφα ασφαλείας, για τα ΣΕΠ τα οποία έχει ήδη διαπιστεύσει, κυρίως με την εκτέλεση περιοδικών επιθεωρήσεων ή εκτάκτων περιορισμένης κλίμακας ελέγχων. Επιπλέον, έχει δικαίωμα απροειδοποίητων ελέγχων στα ήδη διαπιστευμένα από αυτή ΣΕΠ.

(5) Έλεγχο της ΑΕΛ σε ό,τι αφορά τη μεθοδολογία και τα αποτελέσματα της ΑΚ, των ενεργειών για τη, σε συνεχή βάση, διαχείριση κινδύνου και την αποδοχή των εναπομεινάντων κινδύνων.

(6) Παροχή οδηγιών σε συνεργασία με την ΕΑΑΕΠ, στις ΑΕΛ των ΣΕΠ και το προσωπικό ασφαλείας/διαχειρίσεως συστημάτων στην έρευνα οποιασδήποτε παραβιάσεως ή πιθανής παραβιάσεως, την αξιολόγηση της προκαλούμενης ζημίας, την παροχή συμβουλών / συστάσεων σχετικά με τα μέτρα αποκαταστάσεως.

(7) Παροχή συμβουλών προς τις ΑΕΛ των ΣΕΠ για τον κίνδυνο ασφαλείας και τις αντίστοιχες επιπτώσεις, στις περιπτώσεις των τυχών προτεινόμενων αλλαγών στα ΣΕΠ.

(8) Έγγραφη ενημέρωση της ΕΑΔΑ, κάθε μήνα αλλά και εκτάκτως εάν απαιτείται επί της εξέλιξης της διαδικασίας διαπίστευσης για τα ΣΕΠ αρμοδιότητάς της.

4. Εθνική Αρχή Ασφαλείας Επικοινωνιών και Πληροφορικής (ΕΑΑΕΠ)

Η ΕΑΑΕΠ (άρθρο 20), που τα καθήκοντα της έχουν ανατεθεί στην ΕΥΠ/Ε' ΔΝΣΗ, είναι υπεύθυνη για τα παρακάτω:

α. Συμμετοχή στις διαπιστεύσεις των ΣΕΠ, με προσωπικό που ελέγχει τα μέτρα και τις διαδικασίες που αφορούν στην Ασφάλεια Επικοινωνιών – Πληροφορικής (ΑΕΠ).

β. Παροχή τεχνικής συνδρομής, καθώς και υποστήριξη στην ΕΑΔΑ (και στην ΕΔΑ εφόσον έχει καθοριστεί), επί των θεμάτων ΑΕΠ στα ΣΕΠ.

γ. Καθορισμό των τεχνικών προδιαγραφών και των πτυχών εφαρμογής της ΑΕΠ για τα ΣΕΠ, σε συνεργασία με τις εκάστοτε ΑΕΛ.

δ. Παροχή συμβουλών προς την ΑΕΛ, επί των θεμάτων ΑΕΠ ενός ΣΕΠ, που προκύπτουν από προτεινόμενες αλλαγές του, όπως τροποποιήσεις / επεκτάσεις του ή αλλαγών στη διαβάθμιση ασφαλείας των δεδομένων τα οποία αυτό χειρίζεται.

ε. Παροχή οδηγιών επί θεμάτων ΑΕΠ, όπως οι απαιτήσεις ασφαλείας δικτύων και λειτουργικών συστημάτων, απαιτήσεων συσκευών προστασίας εξωτερικών ορίων, απαιτήσεων σε υλικό και λογισμικό στην προσπάθεια πρόληψης και αντιμετώπισης κακόβουλου λογισμικού, απαιτήσεων σε θέματα κρυπτογράφησης και συστημάτων ελέγχου καταγραφής ενεργειών.

στ. Καθορισμός των απαιτήσεων των πόρων ΑΕΠ, όπως του προσωπικού που ασχολείται με θέματα ΑΕΠ, του κυρίου υλικού (hardware) και περιφερειακού (εκτυπωτές, αντιγραφικά κλπ), του ενσωματωμένου σε αυτά λογισμικού λειτουργίας (firmware), του λογισμικού υποστήριξης (utilities) και του λογισμικού εφαρμογών (software), ανάλογα με τις λειτουργικές απαιτήσεις για τα υπό εξέταση ΣΕΠ.

ζ. Περιοδική έκδοση πινάκων με πιστοποιημένα υλικά (hardware), λογισμικά λειτουργίας (firmware), λογισμικά υποστήριξης (utilities) και λογισμικά εφαρμογών (software), τα οποία έχουν πιστοποιηθεί από την ΕΑΑΕΠ ή την ΕΕ ή το ΝΑΤΟ.

η. Παροχή οδηγιών αλλά και εκτέλεση ελέγχων σε θέματα TEMPEST.

5. Αρχή Επιχειρησιακής Λειτουργίας (ΑΕΛ) των ΣΕΠ

Η ΑΕΛ ενός ΣΕΠ, στο πλαίσιο εκμετάλλευσης και ασφαλούς λειτουργίας του διαβαθμισμένου ΣΕΠ, που η ίδια δημιούργησε ή πρόκειται να υλοποιήσει, προκειμένου να καλύψει τις λειτουργικές της ανάγκες, είναι υπεύθυνη για τα ακόλουθα:

α. Συγκρότηση επιτροπής σχεδιασμού του ΣΕΠ, στην οποία συμμετέχει τόσο προσωπικό ανάλυσης και σχεδίασης δικτύων, όσο και εξειδικευμένο προσωπικό ασφαλείας δικτύων, προκειμένου το κάθε στάδιο σχεδίασης και υλοποίησης του ΣΕΠ, να συμβαδίζει με την εφαρμογή αντίστοιχων μέτρων ασφαλείας. Αυτό είναι ιδιαίτερα σημαντικό καθόσον, εάν τα μέτρα ασφαλείας προστεθούν μετά το τέλος της σχεδίασης, τότε όχι μόνο δε καλύπτουν τις απαιτήσεις, αλλά αυξάνουν σε μεγάλο βαθμό το κόστος του όλου προγράμματος.

β. Συνεργασία με την ΕΑΔΑ (ή την ΕΔΑ εφόσον έχει καθοριστεί) και την ΕΑΑΕΠ, στο πλαίσιο καθορισμού των προτύπων που πρόκειται να χρησιμοποιήσει ο προμηθευτής του συστήματος, των μέτρων ΑΕΠ και των πόρων (προσωπι-

κό, υλικό και πάσης φύσεως λογισμικό), που απαιτούνται για την εκπλήρωση των καθημερινών λειτουργικών απαιτήσεων διαχείρισης του ΣΕΠ.

γ. Καθορισμό και υλοποίηση του προγράμματος εκπαίδευσης τόσο του αρμόδιου προσωπικού για την ασφάλεια (των ΥΑΣ, ΥΑΔ και ΥΑΤ που περιγράφονται παρακάτω) και τη διαχείριση [Διαχειριστών Λειτουργίας (ΔΙΑΛ)] του ΣΕΠ, όσο και των πάσης φύσεως χρηστών αυτού. Ειδικά ο/οι ΔΙΑΛ, δεν ανήκουν στο προσωπικό ασφαλείας του ΣΕΠ, με το οποίο ωστόσο συνεργάζονται, αλλά αποτελούν το προσωπικό που ασχολείται με την ομαλή λειτουργία του συστήματος και την επίλυση των καθημερινών προβλημάτων πρόσβασης στα δεδομένα, τις ενημερώσεις (updates) και εγκαταστάσεις του λογισμικού λειτουργίας, την επισκευή τμημάτων του, τη δημιουργία των αντιγράφων ασφαλείας του συστήματος τα οποία παραδίδει στον ΥΑΣ, τη συντήρηση των servers και τη διαχείριση των κωδικών πρόσβασης του BIOS των servers και των τερματικών. Επίσης, μετά από εντολή του ΥΑΣ, προβαίνει σε ενεργοποίηση κλειδωμένων λογαριασμών και διαγραφή παλαιότερων που δε χρησιμοποιούνται πλέον.

δ. Διατύπωση, αναθεώρηση, εφόσον απαιτείται και υποβολή των σχετικών με την ασφάλεια εγγράφων, όπως είναι οι εκθέσεις ΑΚ, η ΔΑΠΑΣ, οι ΔΑΛ, οι εκθέσεις ελέγχου ασφαλείας και οι εκθέσεις διαχείρισης κινδύνων, στην ΕΑΔΑ (ή στην ΕΔΑ εφόσον έχει καθοριστεί) μέσω της ΔΑΑ, προκειμένου αυτή να εκτελέσει τη διαδικασία διαπίστευσης. Αυτά ισχύουν για τα διαβαθμισμένα Εθνικά ΣΕΠ, για τις διασυνδέσεις αυτών μεταξύ τους και για τις διασυνδέσεις Εθνικών ΣΕΠ με ΣΕΠ της ΕΕ ή ΝΑΤΟ. Στις περιπτώσεις λήξης της διάρκειας της διαπίστευσης ή τροποποίησης του ΣΕΠ, η ΑΕΛ προβαίνει στην έγκαιρη υποβολή των προαναφερθέντων εγγράφων στην ΕΑΔΑ (ή ΕΔΑ εφόσον έχει καθοριστεί) μέσω της ΔΑΑ, ώστε να ακολουθήσει η εκ νέου διαπίστευσή του.

ε. Συνεχή έλεγχο και υποστήριξη των εφαρμοζόμενων μέτρων ΑΕΠ, ώστε να διασφαλίζεται ότι το επίπεδο ασφαλείας του ΣΕΠ είναι σύμφωνο με τις απαιτήσεις της διαπίστευσης που αυτό έχει λάβει. Επίσης, διατηρεί μέσω συνεχών ενημερώσεων την ανησυχία και το ενδιαφέρον τόσο των ΥΑΣ, ΥΑΔ, ΥΑΤ και ΔΙΑΛ του δικτύου όσο και των πάσης φύσεως χρηστών, για την ασφάλεια του ΣΕΠ.

στ. Έρευνα, από κοινού με το προσωπικό διαχειρίσεως ασφαλείας, των παραβιάσεων ή προσπαθειών παραβίασης της ασφαλείας του ΣΕΠ, αξιολογώντας την τυχόν προκληθείσα ζημία και υποβολή έκθεσης συμπερασμάτων στην ΕΑΑΕΠ και την ΕΑΔΑ (ή την ΕΔΑ εφόσον έχει καθοριστεί), με τη βοήθεια των οποίων, καθορίζονται οι περαιτέρω ενέργειες ασφάλισης του συστήματος και αποκατάστασης των προβλημάτων που τυχόν δημιουργήθηκαν.

ζ. Εξέταση και έγκριση του προσωπικού διαχειρίσεως ασφαλείας των εγκαταστάσεων, οι οποίες πρόκειται είτε μέσω τοπικού δικτύου, είτε μέσω μεμονωμένων τερματικών, να διασυνδεθούν στο ΣΕΠ για το οποίο είναι υπεύθυνη. Η διασύνδεση δύναται να αναβληθεί κατά περίπτωση, εάν κριθεί ότι το προτεινόμενο προσωπικό διαχείρισης ασφαλείας δεν καλύπτει τις προϋποθέσεις που έχει θέσει η ΑΕΛ.

6. Προσωπικό Διαχειρίσεως Ασφαλείας

Το προσωπικό διαχειρίσεως ασφαλείας μιας υπηρεσίας ή εγκατάστασης, η οποία διαθέτει ΣΕΠ, ανεξάρτητα από το μέγεθος του (είτε τοπικό δίκτυο είτε μεμονωμένα τερματικά που διασυνδέονται με ένα ευρύτερο ΣΕΠ), αφού εγκριθεί από την αντίστοιχη ΑΕΛ, αποτελείται από τους παρακάτω:

α. Υπεύθυνος Ασφαλείας Συστήματος (ΥΑΣ)

Ο ΥΑΣ ορίζεται από την ΑΕΛ με τη σύμφωνη γνώμη της ΕΑΔΑ (ή της ΕΔΑ εφόσον έχει καθοριστεί) και ευθύνεται για την ανάπτυξη, υλοποίηση και τήρηση των μέτρων ασφαλείας του συστήματος. Τα καθήκοντα του είναι τα παρακάτω:

(1) Συμμετέχει στον καθορισμό των προδιαγραφών ασφαλείας που απαιτούνται για το ΣΕΠ κατά τη φάση της σχεδίασής του.

(2) Συμμετέχει ενεργά στον καθορισμό της πολιτικής ασφαλείας του ΣΕΠ και στη σύνταξη των ΔΑΠΑΣ και ΔΑΛ.

(3) Είναι υπεύθυνος για την εφαρμογή και τον έλεγχο των τεχνικών χαρακτηριστικών ασφαλείας και συγκεκριμένα:

(α) Τηρεί ενημερωμένο πίνακα με όλο το προσωπικό για το οποίο έχει εγκριθεί η πρόσβαση και η χρήση οποιουδήποτε τμήματος του ΣΕΠ. Στον ίδιο πίνακα περιγράφεται η εξουσιοδότηση ασφαλείας του κάθε χρήστη, η διάρκεια ισχύος της έγκρισης πρόσβασης και τα καθήκοντα του με βάση τα οποία προκύπτει η «ανάγκη γνώσης», για τα συγκεκριμένα δεδομένα στα οποία έχει πρόσβαση.

(β) Τηρεί ενημερωμένο διάγραμμα όλων των τμημάτων του συστήματος, στο οποίο περιγράφονται οι καλωδιώσεις κρυπτογραφημένων δεδομένων (black), καθώς και των μη κρυπτογραφημένων (red), οι servers, οι δρομολογητές (routers), τα τερματικά και οι κρυπτοσυσκευές, καθώς και οι συσκευές εξωτερικής προστασίας (Firewalls, Proxies, IPS, IDS κλπ).

(γ) Εγκρίνει την πρόσβαση στο ΣΕΠ σε χρήστες, ανάλογα με την αρχή «ανάγκη γνώσης» και προσδιορίζει τους λογαριασμούς χρηστών που απαιτείται να διαγραφούν, για τα οποία ενεργεί ο ΔΙΑΛ. Επίσης, εκδίδει τους κωδικούς πρόσβασης των συστημάτων ελέγχου και πρόσβασης στους χώρους του ΣΕΠ, μεριμνώντας για την αλλαγή τους κάθε 90 ημέρες ή όποτε απαιτηθεί για λόγους ασφαλείας.

(δ) Διασφαλίζει ότι τα μέσα αποθηκεύσεως δεδομένων, τα οποία πρόκειται να υποβαθμιστούν, σε ό,τι αφορά τη διαβάθμιση ασφαλείας τους, περιέχουν μόνο αντίστοιχα δεδομένα.

(ε) Ελέγχει σε εβδομαδιαία βάση τα αρχεία καταγραφής ενεργειών για τη διερεύνηση περιπτώσεων προβληματικής λειτουργίας / διαδικασιών και των περιπτώσεων μη εξουσιοδοτημένης δραστηριότητας χρηστών σε τμήματα του ΣΕΠ.

(στ) Τηρεί σε ασφαλές χώρο και ανάλογα με την διαβάθμιση τους τα αντίγραφα ασφαλείας του συστήματος, τα οποία του παραδίδει/ουν ο/οι ΔΙΑΛ του συστήματος.

(ζ) Διασφαλίζει την ορθή εφαρμογή των διαδικασιών διαβιβάσεως και κρυπτογράφησης των εκπομπών του ΣΕΠ, συμπεριλαμβανομένου του χειρισμού, της συντηρήσεως και της προστασίας του κρυπτογραφικού υλικού.

(η) Διασφαλίζει ότι οι προμηθευτές του συστήματος, το τεχνικό ή άλλο προσωπικό του αναδόχου του συστήματος ή έτερα πρόσωπα που δεν ανήκουν στον οικονομικό φορέα οι οποίοι ενδέχεται να αποκτήσουν πρόσβαση σε διαβαθμισμένα δεδομένα του ΣΕΠ, έχουν κατάλληλη εξουσιοδότηση ασφαλείας,

σύμφωνα με τα καθοριζόμενα στον ΕΚΒΑ και στον ΕΚΑ.

(4) Προετοιμάζει το ΣΕΠ, για έλεγχο στο πλαίσιο της διαπίστευσής του.

(5) Ενημερώνει άμεσα (αρχικά τηλεφωνικά και στη συνέχεια με υποβολή αναφοράς) τον υπεύθυνο ασφάλειας της ΑΕΛ, για οποιαδήποτε αδυναμία, ευπάθεια ή παραβίαση ασφαλείας που εντοπίστηκε κατά τη λειτουργία του ΣΕΠ.

(6) Επιπλέον, οι αρμοδιότητές του συμπεριλαμβάνουν και τα καθήκοντα του διαχειριστή ασφαλείας, κατά τις περιπτώσεις διασύνδεσης εθνικών ΣΕΠ, με ΣΕΠ της ΕΕ.

(7) Απαγορεύεται να εκτελεί παράλληλα και άλλα καθήκοντα, ενώ σε καμία περίπτωση δεν αποτελεί το ΔΙΑΛ του ΣΕΠ.

β. Υπεύθυνος Ασφαλείας Δικτύου (ΥΑΔ)

Ο ΥΑΔ είναι υπεύθυνος για το συντονισμό των μέτρων ασφαλείας που έχουν καθοριστεί, είτε στην περίπτωση ενός μεγάλου ενιαίου συστήματος (WAN), είτε στην περίπτωση διασύνδεσης δύο ή περισσοτέρων ΣΕΠ. Ο ΥΑΔ συντονίζεται με τους ΥΑΣ των ΣΕΠ που διασυνδέονται και αποτελεί πρόσωπο κοινής αποδοχής των ΑΕΛ των συστημάτων. Επιπλέον, συμμετέχει ενεργά στη σύνταξη της Δήλωσης Απαιτήσεων Ασφαλείας Διασύνδεσης (ΔΑΠΑΔ) των ΣΕΠ που πρόκειται να διασυνδεθούν.

γ. Υπεύθυνος Ασφαλείας Τοποθεσίας (ΥΑΤ)

Ο ΥΑΤ ορίζεται από τον οικονομικό φορέα, ως υπεύθυνος για την εφαρμογή και τη διατήρηση των μέτρων ασφαλείας που μπορούν να εφαρμοσθούν σε συγκεκριμένη τοποθεσία. Η τοποθεσία μπορεί να είναι μια ευρύτερη περιοχή ή σύνολο αυτών, που περιλαμβάνουν χώρους στους οποίους υφίστανται σταθμοί εργασίας / τερματικά από ένα ή περισσότερα ΣΕΠ. Τα καθήκοντά του είναι τα παρακάτω:

(1) Προετοιμάζει και υποβάλλει στον ΥΑΣ, τις ΔΑΛ για την τοποθεσία που είναι υπεύθυνος. Μετά την έγκρισή τους, είναι υπεύθυνος την πλήρη εφαρμογή αυτών.

(2) Προετοιμάζει την τοποθεσία για τη διαδικασία διαπίστευσης και συμμετέχει στην ομάδα διαπίστευσης.

(3) Ελέγχει και ενημερώνει όποτε απαιτείται τη λίστα με τους εξουσιοδοτημένους χρήστες της τοποθεσίας ενημερώνοντας παράλληλα τον ΥΑΣ. Επίσης, εξασφαλίζει ότι όλο το προσωπικό που έχει πρόσβαση στο σύστημα είναι εξοικειωμένο με τις ΔΑΛ που ισχύουν για τη τοποθεσία ευθύνης του.

(4) Τηρεί πλήρως ενημερωμένο διάγραμμα των τερματικών για τα οποία είναι υπεύθυνος, ενώ σε περιπτώσεις αλλαγών ενημερώνει άμεσα τον ΥΑΣ.

(5) Εκτελεί έλεγχο σε εβδομαδιαία βάση στις ειδικές ταινίες ασφαλείας (security shields) των τερματικών της τοποθεσίας. Σε περίπτωση που διαπιστώσει ίχνη προσπάθειας παραβίασης, αναφέρει άμεσα στον ΥΑΣ.

(6) Εκτελεί έλεγχο των διαβαθμισμένων φορητών μέσων αποθήκευσης δεδομένων καθώς και των εκτυπωμένων εγγράφων με δεδομένα του ΣΕΠ, με την πραγματοποίηση αιφνιδιαστικών ελέγχων, τηρεί αρχεία για τους ελέγχους αυτούς, όπως προβλέπονται στις ΔΑΛ, ενώ ελέγχει την αντιστοιχία διαβάθμισης των

φορητών μέσων αποθήκευσης, σε σχέση με τη διαβάθμιση των δεδομένων που περιέχουν.

(7) Παρέχει συμβουλές επί θεμάτων ασφαλείας στους χρήστες του συστήματος που ανήκουν στην τοποθεσία για την οποία είναι υπεύθυνος.

(8) Τηρεί αρχείο με τις υπογεγραμμένες δηλώσεις όλων των χρηστών ότι διάβασαν, κατανόησαν και πρόκειται να συμμορφωθούν με τα προβλεπόμενα στις ΔΑΛ.

(9) Ενημερώνει άμεσα τον ΥΑΣ για οποιαδήποτε συσκευή, υλικό ή λογισμικό που εντοπιστεί και δεν προβλέπεται στη διαμόρφωση του συστήματος.

(10) Τηρεί αρχείο όλων των εργασιών συντήρησης που έγιναν στο υλικό και υποβάλλει αντίστοιχη αναφορά στον ΥΑΣ, κάθε φορά που γίνεται συντήρηση.

(11) Αναφέρει στον ΥΑΣ οποιαδήποτε συμβάντα πιθανής παράβασης – παραβίασης ασφαλείας, καθώς και αδυναμίες που ενδέχεται να επηρεάσουν την ασφάλεια.

(12) Εξασφαλίζει ότι η καταστροφή του τυχόν διαβαθμισμένου υλικού του ΣΕΠ, που βρίσκεται στην τοποθεσία ευθύνης του, γίνεται ανά τακτά χρονικά διαστήματα, τηρουμένων των προβλεπόμενων διαδικασιών.

Αντιναύαρχος Ιωάννης Δρυμούσης ΠΝ
Υπαρχηγός

Ακριβές Αντίγραφο

Ασμχος (ΕΑ) Νικόλαος Ζήκος
Επιτελής ΓΕΕΘΑ/Ε3/1

ΥΠΟΔΕΙΓΜΑΤΑ 1 - 14

ΥΠΟΔΕΙΓΜΑ 1

ΠΙΝΑΚΑΣ ΠΡΟΣΩΠΙΚΩΝ ΣΤΟΙΧΕΙΩΝ
PERSONALPARTICULARS FORM

(Τα στοιχεία συμπληρώνονται μηχανογραφημένα με κεφαλαία γράμματα)
(Complete the form computerized using capital letters)

Φωτογραφία
Photo

1. ΣΤΟΙΧΕΙΑ ΤΑΥΤΟΤΗΤΟΣ
ID DETAILS

ΕΠΩΝΥΜΟ: SURNAME:
ΟΝΟΜΑ: NAMES:
ΟΝΟΜΑ ΠΑΤΕΡΑ: FATHER’S NAME:
ΟΝΟΜΑ ΜΗΤΕΡΑΣ: MOTHER’S NAME:
ΗΜΕΡΟΜΗΝΙΑ ΓΕΝΝΗΣΗΣ: DATE OF BIRTH:
ΤΟΠΟΣ ΓΕΝΝΗΣΕΩΣ: PLACE OF BIRTH:
ΑΡ. ΤΑΥΤΟΤΗΤΑΣ Ή ΔΒΡΙΟΥ: ΤΟΠΟΣ & ΗΜΕΡΟΜΗΝΙΑ ΕΚΔΟΣΗΣ: I.D. No OR PASSPORT No.: ISSUED AT DATE OF ISSUE:
ΠΑΡΟΥΣΑ ΕΘΝΙΚΟΤΗΤΑ (ΚΑΙ ΔΙΠΛΗ ΕΦΟΣΟΝ ΥΦΙΣΤΑΤΑΙ): PRESENT NATIONALITY (INCLUDING ANY DUAL NATIONALITY):
ΠΡΟΗΓΟΥΜΕΝΗ ΕΘΝΙΚΟΤΗΤΑ (ΕΑΝ ΥΠΗΡΧΕ): FORMER NATIONALITY (IF ANY):
ΤΗΛΕΦΩΝΟ ΕΠΙΚΟΙΝΩΝΙΑΣ: PHONE:
ΔΙΕΥΘΥΝΣΗ ΗΛ. ΤΑΧΥΔΡΟΜΕΙΟΥ: EMAIL ADDRESS

2. ΣΤΟΙΧΕΙΑ ΓΟΝΕΩΝ
DETAILS ABOUT PARENTS

ΠΑΤΕΡΑΣ FATHER	ΜΗΤΕΡΑ MOTHER
ΕΠΙΘΕΤΟ: SURNAME:	ΕΠΙΘΕΤΟ: SURNAME(NOW):
ΟΝΟΜΑ: NAME:	ΟΝΟΜΑ: NAME:
ΟΝ. ΠΑΤΕΡΑ: FATHER’S NAME:	ΤΟ ΓΕΝΟΣ: SURNAME AT BIRTH:
ΟΝ. ΜΗΤΕΡΑΣ: MOTHER’S NAME:	ΟΝ. ΠΑΤΕΡΑ: FATHER’S NAME:
ΗΜ. ΓΕΝΝΗΣΗΣ: DATE OF BIRTH:	ΟΝ. ΜΗΤΕΡΑΣ: MOTHER’S NAME:
ΤΟΠΟΣ ΓΕΝΝΗΣΗΣ: PLACE OF BIRTH:	ΗΜ. ΓΕΝΝΗΣΗΣ: DATE OF BIRTH:
ΕΘΝΙΚΟΤΗΤΑ: NATIONALITY	ΤΟΠΟΣ ΓΕΝΝΗΣΗΣ: PLACE OF BIRTH:
	ΕΘΝΙΚΟΤΗΤΑ: NATIONALITY:

3. ΣΤΟΙΧΕΙΑ ΣΥΖΥΓΟΥ
(Αφορά επίσης σύντροφο, με τον/την οποίο/α συζείτε ως ζεύγος)
DETAILS ABOUT YOUR SPOUSE
(OR THE PARTNER YOU LIVE WITH, AS A COUPLE)

ΕΠΙΘΕΤΟ (ΤΩΡΑ): SURNAME (NOW):
ΟΝΟΜΑ: NAME:
ΤΟ ΓΕΝΟΣ: (προκειμένου για γυναίκα) SURNAME AT BIRTH: (concerning women)
ΗΜ. ΓΕΝΝΗΣΗΣ: DATE OF BIRTH:
ΤΟΠΟΣ ΓΕΝΝΗΣΗΣ: PLACE OF BIRTH:
ΕΘΝΙΚΟΤΗΤΑ: NATIONALITY
ΕΠΑΓΓΕΛΜΑ: OCCUPATION:

4. ΣΤΟΙΧΕΙΑ ΤΕΚΝΩΝ
DETAILS ABOUT YOUR CHILDREN

ΟΝΟΜΑΤΕΠΩΝΥΜΟ FULL NAME	ΗΜ. ΓΕΝΝΗΣΗΣ DATE OF BIRTH	ΤΟΠΟΣ ΓΕΝΝΗΣΗΣ PLACE OF BIRTH

5. ΣΤΟΙΧΕΙΑ ΑΤΟΜΩΝ ΑΠΟ ΑΛΛΗ ΧΩΡΑ ΜΕ ΤΑ ΟΠΟΙΑ ΕΧΕΤΕ ΕΠΑΦΕΣ
DETAILS ABOUT PERSONS OF OTHER COUNTRY WHO HAVE CONNECTIONS WITH

ΟΝΟΜΑΤΕΠΩΝΥΜΟ FULL NAME	ΧΩΡΑ COUNTRY	ΑΙΤΙΟΛΟΓΗΣΗ ΕΠΑΦΩΝ REASONS	ΑΠΟ FROM	ΕΩΣ ΤΟ

6. ΕΠΑΓΓΕΛΜΑΤΙΚΗ ΑΠΑΣΧΟΛΗΣΗ ΚΑΤΑ ΤΑ ΤΕΛΕΥΤΑΙΑ ΔΕΚΑ ΧΡΟΝΙΑ
EMPLOYMENT DETAILS FOR THE LAST TEN YEARS

ΟΝΟΜΑΣΙΑ ΥΠΗΡΕΣΙΑΣ, ΟΙΚΟΝΟΜΙΚΟΥ ΦΟΡΕΑ Κ.Λ.Π. NAME OF AGENCY, FIRM E.T.C.	ΚΑΘΗΚΟΝΤΑ OCCUPATION	ΔΝΣΗ ΕΡΓΑΣΙΑΣ WORK ADDRESS	ΑΠΟ FROM	ΕΩΣ ΤΟ

7. ΔΙΑΜΟΝΗ ΚΑΤΑ ΤΑ ΤΕΛΕΥΤΑΙΑ ΔΕΚΑ ΧΡΟΝΙΑ
HOME ADDRESS DURING THE LAST TEN YEARS

ΧΩΡΑ COUNTRY	ΑΚΡΙΒΗΣ ΔΝΣΗ FULL ADDRESS	ΑΠΟ FROM	ΕΩΣ ΤΟ

8. ΛΟΙΠΑ ΣΤΟΙΧΕΙΑ
OTHER DETAILS

*** Residence abroad regardless paragraph 7 in full detail**
*** Διαμονή στο εξωτερικό ανεξαρτήτως παραγράφου 7 με ακριβή στοιχεία**

Συμπλήρωσα τα παραπάνω προσωπικά στοιχεία με γνώση της νομοθεσίας περί ψευδούς δηλώσεως και βεβαιώνω ότι είναι αληθή και σωστά.
I have completed the above personal particulars in the knowledge of relevant laws and I confirm that they are true and correct

ΘΕΩΡΗΘΗΚΕ
Για το γνήσιο της υπογραφής
Από αρμόδια κρατική αρχή- φορέα

Τόπος – Ημερομηνία
Place - Date

(Υπογραφή)
(Signature)

ΣΗΜΕΙΩΣΗ: 1. Συντάσσεται ιδιοχείρως από το προς εξουσιοδότηση πρόσωπο.

2. Η ημερομηνία του γνήσιου της υπογραφής να είναι εντός διμήνου από την υποβολή.

REMARK: 1. The form is personally completed.

2. The date of the signature of authenticity must be within two months before the submission of the form.

ΥΠΟΔΕΙΓΜΑ 2

(Τα στοιχεία συμπληρώνονται μηχανογραφημένα)
(Complete the form computerized)

ΕΜΠΙΣΤΕΥΤΙΚΟ
(ΟΤΑΝ ΣΥΜΠΛΗΡΩΘΕΙ)

ΥΠΕΥΘΥΝΗ ΔΗΛΩΣΗ ΕΞΟΥΣΙΟΔΟΤΗΣΗΣ

Ο (Η)……..…(ονοματεπώνυμο),
του .....(όνομα πατρός) και της…….(όνομα μητρός),
με Αριθμό Δελτίου Ταυτότητας…….. …… ,
υπάλληλος του .....(όνομα οικονομικού φορέα),
με καθήκοντα .....(καθήκοντα που εκτελεί).
ή με την ιδιότητα……(εξ. Συνεργάτης, φύλακας κλπ)
δηλώνω υπεύθυνα και εν γνώσει του Νόμου για ψευδή δήλωση ότι:

α. Ενημερώθηκα πλήρως από τον ..... υπεύθυνο ασφαλείας επί των:

(1) Άρθρων του Ποινικού Κώδικα 139, 146 έως 149 και 152 και των άρθρων του ΣΠΚ 141,142,143,144 και 145.

(2) Κανόνων ασφαλείας διαβαθμισμένου υλικού, των οποίων την απόλυτη τήρηση αναλαμβάνω με την παρούσα.

(3) Διαδικασιών εξουσιοδότησης του Εθνικού Κανονισμού Βιομηχανικής Ασφαλείας

β. Επιθυμώ εφ’ όσον κριθώ κατάλληλος να εξουσιοδοτηθώ για χειρισμό διαβαθμισμένου υλικού και δεν θα αφήσω να περιέλθει σε γνώση τρίτου μη εξουσιοδοτημένου και αναρμόδιου.

γ. Ενημερώθηκα ότι η επεξεργασία των προσωπικών μου δεδομένων γίνεται σύμφωνα με το άρθρο 6 παρ. 1 στοιχ. γ’ και ε’ και το άρθρο 9 παρ. 2 στοιχ. ζ’ του Γενικού Κανονισμού για την Προστασία Δεδομένων (ΓΚΠΔ – Κανονισμός ΕΕ 2016/679 της 27 Απρ 16), προκειμένου να ασκηθεί ο αναγκαίος έλεγχος ασφαλείας, ώστε να μου χορηγηθεί εξουσιοδότηση χειρισμού διαβαθμισμένου υλικού – πληροφοριών.

ΘΕΩΡΗΘΗΚΕ
Για το γνήσιο της υπογραφής
Από αρμόδια κρατική αρχή- φορέα

Ο Δηλών

ΠΡΟΣ ΔΙΕΥΚΟΛΥΝΣΗ ΕΠΙΣΥΝΑΠΤΟΝΤΑΙ
ΤΑ ΑΝΑΦΕΡΟΜΕΝΑ ΑΡΘΡΑ ΤΟΥ Π.Κ. ΚΑΙ ΤΟΥ Σ.Π.Κ.
(δεν υποβάλλονται με το Υπόδειγμα 2)

ΑΡΘΡΑ Π.Κ.

Άρθρο 139
Νόθευση αποδεικτικών

Όποιος νοθεύει, καταστρέφει ή κρύβει έγγραφα ή άλλα αντικείμενα που χρησιμεύουν για την απόδειξη των εδαφικών δικαιωμάτων του ελληνικού κράτους ή την υποστήριξη συμφερόντων του τιμωρείται με κάθειρξη έως δέκα έτη.

Άρθρο 146
Παραβίαση μυστικών της Πολιτείας

1. Όποιος παραδίδει ή αφήνει να περιέλθει στην κατοχή ή τη γνώση άλλου κρατικό απόρρητο τιμωρείται με κάθειρξη έως δέκα έτη.

2. Αν η πράξη τελείται σε καιρό πολέμου, επιβάλλεται κάθειρξη ισόβια ή πρόσκαιρη τουλάχιστον δέκα ετών.

3. Με τις ποινές των προηγούμενων παραγράφων τιμωρείται και όποιος δημόσια με οποιονδήποτε τρόπο ή μέσω διαδικτύου ανακοινώνει ή διαδίδει κρατικό απόρρητο.

Άρθρο 147
Παραβίαση μυστικών της Πολιτείας από αμέλεια

Όποιος τελεί τις πράξεις του προηγούμενου άρθρου από αμέλεια, εφόσον τα απόρρητα ήταν υπηρεσιακώς εμπιστευμένα σε αυτόν ή του ήταν προσιτά λόγω της δημόσιας υπηρεσίας του ή με εντολή κάποιας αρχής, τιμωρείται με φυλάκιση έως τρία έτη ή χρηματική ποινή και σε καιρό πολέμου, με φυλάκιση τουλάχιστον τριών ετών και χρηματική ποινή.

Άρθρο 148
Κατασκοπεία

1. Όποιος παράνομα πετυχαίνει να περιέλθει στην κατοχή ή στη γνώση του κρατικό απόρρητο τιμωρείται με φυλάκιση τουλάχιστον ενός έτους και χρηματική ποινή.

2. Αν όμως ο υπαίτιος ενήργησε με σκοπό να χρησιμοποιήσει το κρατικό απόρρητο για να το διαβιβάσει σε άλλον ή να το ανακοινώσει δημόσια, με τρόπο που μπορεί να προκαλέσει κίνδυνο στα συμφέροντα του κράτους, επιβάλλεται κάθειρξη έως δέκα έτη και αν η πράξη έγινε σε καιρό πολέμου, κάθειρξη.

Άρθρο 149
Έννοια κρατικού απορρήτου

Κρατικό απόρρητο κατά την έννοια των άρθρων 146 έως 148 είναι ένα γεγονός, αντικείμενο ή πληροφορία, η πρόσβαση στα οποία είναι δυνατή σε ένα προσδιορισμένο κύκλο προσώπων και που χαρακτηρίζονται ως μυστικά για να αποφευχθεί ο κίνδυνος προσβολής της εδαφικής ακεραιότητας, της αμυντικής ικανότητας, των διεθνών σχέσεων ή των οικονομικών συμφερόντων του ελληνικού κράτους και

της διεθνούς ειρήνης.

Άρθρο 152
Παρεπόμενες ποινές

Στα εγκλήματα αυτού του κεφαλαίου, το δικαστήριο, μαζί με την ποινή, επιβάλλει αποστέρηση θέσεων και αξιωμάτων.

ΑΡΘΡΑ ΣΤΡΑΤΙΩΤΙΚΟΥ ΠΟΙΝΙΚΟΥ ΚΩΔΙΚΑ

Άρθρο 141
Απώλεια απορρήτων

1. Όποιος από αμέλεια γίνεται πρόξενος απώλειας ή καταστροφής εγγράφων, βιβλίων ή άλλων αντικειμένων οποιασδήποτε στρατιωτικής υπηρεσίας, τα οποία χαρακτηρίσθηκαν νομίμως ως απόρρητα και παραδόθηκαν σ΄ αυτόν για μεταφορά φύλαξη, ή διαχείριση, τιμωρείται:

α. Σε ειρηνική περίοδο, με φυλάκιση μέχρι έξι μηνών.

β. Σε πολεμική περίοδο, με φυλάκιση δύο ετών.

2. Με τις ίδιες ποινές τιμωρείται και ο στρατιωτικός που τελεί την πράξη της προηγούμενης παραγράφου, σε σχέση με έγγραφα ή άλλα αντικείμενα διπλωματικής υπηρεσίας.

Άρθρο 142
Παράλειψη διασφάλισης απορρήτων

Όποιος σε πολεμική περίοδο και ενώ βρίσκεται σε κίνδυνο να αιχμαλωτιστεί ή να πέσει στα χέρια του εχθρού, δεν προσπαθεί με κάθε τρόπο να αποκρύψει ή να εξαφανίσει τα έγγραφα ή άλλα αντικείμενα οποιασδήποτε στρατιωτικής υπηρεσίας, τα οποία χαρακτηρίσθηκαν νομίμως ως απόρρητα και του παραδόθηκαν για χρήση, φύλαξη ή μεταφορά τιμωρείται: με κάθειρξη μέχρι δέκα ετών ή φυλάκιση τουλάχιστον δύο ετών.

Άρθρο 143
Μυστικές πληροφορίες στρατιωτικής σημασίας

Ως μυστικές πληροφορίες στρατιωτικής σημασίας θεωρούνται οι αναφερόμενες:

α. Στην κατάσταση γενικά του στρατού και του πολεμικού υλικού, στα έργα οχύρωσης, στα κρυπτογραφικά μέσα συνεννόησης, στο δίκτυο των στρατιωτικών συγκοινωνιών, στις θέσεις του στρατού, στους τόπους ανεφοδιασμού και την κατάσταση προμηθειών σε όπλα, πολεμοφόδια, καύσιμα, τρόφιμα ή χρήματα.

β. Στο σχέδιο οργάνωσης ή σύνθεσης του στρατού, στο σχέδιο και τα προπαρασκευαστικά μέτρα επιστράτευσης ή κινητοποίησης του στρατού και στα σχέδια στρατιωτικής επιχείρησης.

γ. Σε στρατιωτικές μετακινήσεις ή μεταφορές που εκτελούνται ή σχεδιάζονται.

δ. Στην κατάσταση υγείας ή του φρονήματος και πειθαρχίας του στρατού ή στον αριθμό των τραυματιών, νεκρών ή αιχμαλώτων.

ε. Σε κάθε αντικείμενο που χαρακτηρίστηκε νομίμως ως απόρρητο.

Άρθρο 144
Μετάδοση στρατιωτικών μυστικών

1. Στρατιωτικός και όποιος ανήκει στην υπηρεσία του στρατού που παράνομα και με πρόθεση παραδίνει ή ανακοινώνει σε άλλον ή αφήνει με οποιοδήποτε τρόπο να περιέλθουν στην κατοχή ή στη γνώση άλλου μυστικές πληροφορίες στρατιωτικής σημασίας, τιμωρείται με κάθειρξη.

2. Αν πρόκειται για πληροφορίες μικρής σημασίας, ο υπαίτιος τιμωρείται με φυλάκιση τουλάχιστον έξι μηνών.

3. Αν η πράξη τελέστηκε σε πολεμική περίοδο για να ωφελήσει ξένο κράτος ή για να βλάψει το ελληνικό κράτος, επιβάλλεται θάνατος ή ισόβια κάθειρξη.

4. Αν οι πράξεις των παραγράφων 1 και 2 έγιναν από αμέλεια, ο υπαίτιος τιμωρείται:

α. Με φυλάκιση τουλάχιστον έξι μηνών, αν οι πληροφορίες της παραγράφου ή τα αντικείμενα που τις περιέχουν είναι εμπιστευμένα ή προσιτά σ΄ αυτόν λόγω της υπηρεσίας του ή μετά από εντολή της αρχής και με φυλάκιση τουλάχιστον ενός έτους, αν ανακοινώθηκαν ή παραδόθηκαν σε ξένο κράτος ή σε κατάσκοπό του.

β. Με φυλάκιση μέχρι ενός έτους, σε κάθε άλλη περίπτωση.

5. Ο υπαίτιος τιμωρείται, κατά τις παραπάνω διατάξεις και αν το έγκλημα τελέστηκε μετά την έξοδό του από την υπηρεσία, εφόσον οι πληροφορίες ή τα αντικείμενα της παραγράφου 1 είχαν περιέλθει σε κατοχή ή γνώση του λόγω της υπηρεσίας του.

6. Αν ο αποδέκτης των μυστικών ήταν κατάσκοπος, μπορεί ο υπαίτιος να απαλλαγεί από την ποινή, εφόσον κατάγγειλε την πράξη στις αρχές, με αποτέλεσμα να συλληφθεί έγκαιρα ο κατάσκοπος ή να προληφθεί ο κίνδυνος.

7. Η απόπειρα και η προσφορά για την τέλεση των πράξεων αυτών τιμωρούνται με την ποινή του τετελεσμένου εγκλήματος.

Άρθρο 145
Ανακοίνωση στρατιωτικών πληροφοριών

Στρατιωτικός και όποιος ανήκει στην υπηρεσία του στρατού που χωρίς έγκριση της στρατιωτικής αρχής ανακοινώνει ή δημοσιεύει με οποιοδήποτε μέσο πληροφορίες σχετικές με το στρατό, άλλες από τις αναφερόμενες στο άρθρο 143 ικανές να κλονίσουν την εμπιστοσύνη του κοινού σ΄ αυτόν, τιμωρείται με φυλάκιση μέχρι έξι μηνών.

ΥΠΟΔΕΙΓΜΑ 3
(Τα στοιχεία συμπληρώνονται μηχανογραφημένα)
(Complete the form computerized)

ΔΕΛΤΙΟ
ΥΠΟΒΟΛΗΣ ΣΤΟΙΧΕΙΩΝ ΚΑΤΑΛΛΗΛΟΤΗΤΑΣ

……(α)
του/της……(β)
Αριθμός Δελτίου Ταυτότητος .....(γ)
Ο/Η υπογεγραμμένος/η.....(δ)

ΠΙΣΤΟΠΟΙΩ
ότι από τα συλλεγμένα στοιχεία και από την καθημερινή επαφή και συνεργασία με το ανωτέρω πρόσωπο, προέκυψαν οι παρακάτω διαπιστώσεις:

1. Χαρακτήρας: αξιοπρεπής, σοβαρός, εχέμυθος, εκτελεί τα καθήκοντά του καλώς και έχει συνειδητή πίστη προς την πατρίδα.
2. Δεν διαπιστώθηκαν:

α. Πάθη, ελαττώματα ή άλλα στοιχεία που να επηρεάζουν την αξιοπιστία του και να εγκυμονούν κινδύνους ασφαλείας των ΕΔΠΥ.

β. Παραβάσεις της ποινικής νομοθεσίας (ΠΚ, ειδικών ποινικών νόμων αφορούσες στα αδικήματα που αναφέρονται στο άρθρο 7 του ΕΚΒΑ), καθώς και λαμβάνοντας υπόψη τα κριτήρια του Κανονισμού Ασφαλείας του ΝΑΤΟ [CM 2002(49) του 2002] και της απόφασης του Συμβουλίου της Ευρωπαϊκής Ένωσης (ΕΕ) της 23 Σεπ 2013 (2013/488/ΕΕ), σε περιπτώσεις εξουσιοδότησης ασφαλείας ΝΑΤΟ και ΕΕ αντίστοιχα.

ΓΕΝΙΚΑ
Από τις γενόμενες διαπιστώσεις και αφού δεν υπάρχουν αντίθετες πληροφορίες και ενδείξεις
ΘΕΩΡΩ
ότι ο/η .....(β)
δύναται να χειρισθεί διαβαθμισμένες πληροφορίες και υλικό βαθμού ασφαλείας
…….....…….... (ε)

Τόπος – Ημερομηνία……
Ο
Διευθύνων Σύμβουλος
Τίθεται Σφραγίδα - Υπογραφή

ΟΔΗΓΙΕΣ ΣΥΜΠΛΗΡΩΣΗΣ
α. Οικονομικός φορέας.
β. Ονοματεπώνυμο του προς εξουσιοδότηση προσώπου.
γ. Αριθμός ταυτότητας του προς εξουσιοδότηση προσώπου.
δ. Ονοματεπώνυμο και η ιδιότητα του ασκούντος τη διαχείριση/διοίκηση του οικονομικού φορέα (π.χ. διευθύνων σύμβουλος)
ε. Τίθεται η κατηγορία εξουσιοδότησης, σύμφωνα με την παράγραφο 2 του άρθρου 7, ενώ για εξουσιοδοτήσεις ΝΑΤΟ και ΕΕ με βάση, σύμφωνα με τον πίνακα της παραγράφου 6 του άρθρου 5 παρόντος.

ΥΠΟΔΕΙΓΜΑ 4

ΜΗΤΡΩΟ
ΚΑΤΑΧΩΡΗΣΕΩΣ ΕΞΟΥΣΙΟΔΟΤΗΜΕΝΟΥ ΠΡΟΣΩΠΙΚΟΥ

ΟΝΟΜΑ ΕΠΩΝΥΜΟ	ΧΡΟΝΟΛΟΓΙΑ ΕΞΟΥΣ/ΤΗΣΗΣ	ΧΡΟΝΟΛΟΓΙΑ ΛΗΞΗΣ ΕΞΟΥΣ/ΤΗΣΗΣ	ΣΧΕΤΙΚΗ ΔΙΑΤΑΓΗ	ΕΝΕΡΓΕΙΑ ΓΙΑ ΑΡΣΗ ΕΞΟΥΣ/ΣΗΣ

Ο Συντάξας

Ο Υπεύθυνος Ασφαλείας

ΥΠΟΔΕΙΓΜΑ 5
(Τα στοιχεία συμπληρώνονται μηχανογραφημένα)
(Complete the form computerized)

ΥΠΕΥΘΥΝΗ ΔΗΛΩΣΗ ΓΙΑ ΑΡΣΗ ΕΞΟΥΣΙΟΔΟΤΗΣΗΣ

ΕΜΠΙΣΤΕΥΤΙΚΟ (όταν συμπληρωθεί)

Ονοματεπώνυμο.....

Όνομα Πατρός.....

Αριθμός Ταυτότητας.....

Τόπος διαμονής (λεπτομερής).....

Οικονομικός φορέας.....

Καθήκοντα που εκτελούσα.....

Ο υπογεγραμμένος .....

Αφού ανέγνωσα και κατανόησα πλήρως τα παρακάτω άρθρα του Στρατ. Ποινικού Κώδικα

ΔΗΛΩΝΩ ΥΠΕΥΘΥΝΑ

Ότι μετά τη λήξη της υπηρεσίας μου κατά την οποία είχα τύχει εξουσιοδότησης σύμφωνα με το έγγραφο ΓΔΑΕΕ/ΔΑΕΤΕ..... και αριθμό διαβάθμισης..... και είχα χειρισθεί διαβαθμισμένες πληροφορίες και υλικά, έχω πλήρη αντίληψη των υποχρεώσεων μου και της ποινικής ευθύνης την οποία φέρω για την τήρηση απόλυτου εχεμύθειας και ότι δεν θα ανακοινώσω ουδέποτε και σε κανένα πρόσωπο, οποιαδήποτε διαβαθμισμένη πληροφορία την οποία γνώρισα κατά την εκτέλεση των καθηκόντων μου.

ΑΡΘΡΑ ΤΟΥ ΠΟΝΙΚΟΥ ΚΩΔΙΚΑ

Άρθρο 139
Νόθευση αποδεικτικών

Όποιος νοθεύει, καταστρέφει ή κρύβει έγγραφα ή άλλα αντικείμενα που χρησιμεύουν για την απόδειξη των εδαφικών δικαιωμάτων του ελληνικού κράτους ή την υποστήριξη συμφερόντων του τιμωρείται με κάθειρξη έως δέκα έτη.

Άρθρο 146
Παραβίαση μυστικών της Πολιτείας

1. Όποιος παραδίδει ή αφήνει να περιέλθει στην κατοχή ή τη γνώση άλλου κρατικό απόρρητο τιμωρείται με κάθειρξη έως δέκα έτη.

2. Αν η πράξη τελείται σε καιρό πολέμου, επιβάλλεται κάθειρξη ισόβια ή πρόσκαιρη τουλάχιστον δέκα ετών.

3. Με τις ποινές των προηγούμενων παραγράφων τιμωρείται και όποιος δημόσια με οποιονδήποτε τρόπο ή μέσω διαδικτύου ανακοινώνει ή διαδίδει κρατικό απόρρητο.

Άρθρο 147
Παραβίαση μυστικών της Πολιτείας από αμέλεια

Όποιος τελεί τις πράξεις του προηγούμενου άρθρου από αμέλεια, εφόσον τα απόρρητα ήταν υπηρεσιακώς εμπιστευμένα σε αυτόν ή του ήταν προσιτά λόγω της δημόσιας υπηρεσίας του ή με εντολή κάποιας αρχής, τιμωρείται με φυλάκιση έως τρία έτη ή χρηματική ποινή και σε καιρό πολέμου, με φυλάκιση τουλάχιστον τριών ετών και χρηματική ποινή.

Άρθρο 148
Κατασκοπεία

1. Όποιος παράνομα πετυχαίνει να περιέλθει στην κατοχή ή στη γνώση του κρατικό απόρρητο τιμωρείται με φυλάκιση τουλάχιστον ενός έτους και χρηματική ποινή.

2. Αν όμως ο υπαίτιος ενήργησε με σκοπό να χρησιμοποιήσει το κρατικό απόρρητο για να το διαβιβάσει σε άλλον ή να το ανακοινώσει δημόσια, με τρόπο που μπορεί να προκαλέσει κίνδυνο στα συμφέροντα του κράτους, επιβάλλεται κάθειρξη έως δέκα έτη και αν η πράξη έγινε σε καιρό πολέμου, κάθειρξη.

Άρθρο 149
Έννοια κρατικού απορρήτου

Κρατικό απόρρητο κατά την έννοια των άρθρων 146 έως 148 είναι ένα γεγονός, αντικείμενο ή πληροφορία, η πρόσβαση στα οποία είναι δυνατή σε ένα προσδιορισμένο κύκλο προσώπων και που χαρακτηρίζονται ως μυστικά για να αποφευχθεί ο κίνδυνος προσβολής της εδαφικής ακεραιότητας, της αμυντικής ικανότητας, των διεθνών σχέσεων ή των οικονομικών συμφερόντων του ελληνικού κράτους και της διεθνούς ειρήνης.

Άρθρο 152
Παρεπόμενες ποινές

Στα εγκλήματα αυτού του κεφαλαίου, το δικαστήριο, μαζί με την ποινή, επιβάλλει αποστέρηση θέσεων και αξιωμάτων.

ΑΡΘΡΑ ΣΤΡΑΤΙΩΤΙΚΟΥ ΠΟΙΝΙΚΟΥ ΚΩΔΙΚΑ

Άρθρο 141
Απώλεια απορρήτων

1. Όποιος από αμέλεια γίνεται πρόξενος απώλειας ή καταστροφής εγγράφων, βιβλίων ή άλλων αντικειμένων οποιασδήποτε στρατιωτικής υπηρεσίας, τα οποία χαρακτηρίσθηκαν νομίμως ως απόρρητα και παραδόθηκαν σ΄ αυτόν για μεταφορά φύλαξη, ή διαχείριση, τιμωρείται:

α. Σε ειρηνική περίοδο, με φυλάκιση μέχρι έξι μηνών.

β. Σε πολεμική περίοδο, με φυλάκιση δύο ετών.

2. Με τις ίδιες ποινές τιμωρείται και ο στρατιωτικός που τελεί την πράξη της προηγούμενης παραγράφου, σε σχέση με έγγραφα ή άλλα αντικείμενα διπλωματικής υπηρεσίας.

Άρθρο 142
Παράλειψη διασφάλισης απορρήτων

Όποιος σε πολεμική περίοδο και ενώ βρίσκεται σε κίνδυνο να αιχμαλωτιστεί ή να πέσει στα χέρια του εχθρού, δεν προσπαθεί με κάθε τρόπο να αποκρύψει ή να εξαφανίσει τα έγγραφα ή άλλα αντικείμενα οποιασδήποτε στρατιωτικής υπηρεσίας, τα οποία χαρακτηρίσθηκαν νομίμως ως απόρρητα και του παραδόθηκαν για χρήση, φύλαξη ή μεταφορά τιμωρείται: με κάθειρξη μέχρι δέκα ετών ή φυλάκιση τουλάχιστον δύο ετών.

Άρθρο 143
Μυστικές πληροφορίες στρατιωτικής σημασίας

Ως μυστικές πληροφορίες στρατιωτικής σημασίας θεωρούνται οι αναφερόμενες:

α. Στην κατάσταση γενικά του στρατού και του πολεμικού υλικού, στα έργα οχύρωσης, στα κρυπτογραφικά μέσα συνεννόησης, στο δίκτυο των στρατιωτικών συγκοινωνιών, στις θέσεις του στρατού, στους τόπους ανεφοδιασμού και την κατάσταση προμηθειών σε όπλα, πολεμοφόδια, καύσιμα, τρόφιμα ή χρήματα.

β. Στο σχέδιο οργάνωσης ή σύνθεσης του στρατού, στο σχέδιο και τα προπαρασκευαστικά μέτρα επιστράτευσης ή κινητοποίησης του στρατού και στα σχέδια στρατιωτικής επιχείρησης.

γ. Σε στρατιωτικές μετακινήσεις ή μεταφορές που εκτελούνται ή σχεδιάζονται.

δ. Στην κατάσταση υγείας ή του φρονήματος και πειθαρχίας του στρατού ή στον αριθμό των τραυματιών, νεκρών ή αιχμαλώτων.

ε. Σε κάθε αντικείμενο που χαρακτηρίστηκε νομίμως ως απόρρητο.

Άρθρο 144
Μετάδοση στρατιωτικών μυστικών

1. Στρατιωτικός και όποιος ανήκει στην υπηρεσία του στρατού που παράνομα και με πρόθεση παραδίνει ή ανακοινώνει σε άλλον ή αφήνει με οποιοδήποτε τρόπο να περιέλθουν στην κατοχή ή στη γνώση άλλου μυστικές πληροφορίες στρατιωτικής σημασίας, τιμωρείται με κάθειρξη.
2. Αν πρόκειται για πληροφορίες μικρής σημασίας, ο υπαίτιος τιμωρείται με φυλάκιση τουλάχιστον έξι μηνών.

3. Αν η πράξη τελέστηκε σε πολεμική περίοδο για να ωφελήσει ξένο κράτος ή για να βλάψει το ελληνικό κράτος, επιβάλλεται θάνατος ή ισόβια κάθειρξη.

4. Αν οι πράξεις των παραγράφων 1 και 2 έγιναν από αμέλεια, ο υπαίτιος τιμωρείται:

α. Με φυλάκιση τουλάχιστον έξι μηνών, αν οι πληροφορίες της παραγράφου ή τα αντικείμενα που τις περιέχουν είναι εμπιστευμένα ή προσιτά σ΄ αυτόν λόγω της υπηρεσίας του ή μετά από εντολή της αρχής και με φυλάκιση τουλάχιστον ενός έτους, αν ανακοινώθηκαν ή παραδόθηκαν σε ξένο κράτος ή σε κατάσκοπό του.

β. Με φυλάκιση μέχρι ενός έτους, σε κάθε άλλη περίπτωση.

5. Ο υπαίτιος τιμωρείται, κατά τις παραπάνω διατάξεις και αν το έγκλημα τελέστηκε μετά την έξοδό του από την υπηρεσία, εφόσον οι πληροφορίες ή τα αντικείμενα της παραγράφου 1 είχαν περιέλθει σε κατοχή ή γνώση του λόγω της υπηρεσίας του.

6. Αν ο αποδέκτης των μυστικών ήταν κατάσκοπος, μπορεί ο υπαίτιος να απαλλαγεί από την ποινή, εφόσον κατάγγειλε την πράξη στις αρχές, με αποτέλεσμα να συλληφθεί έγκαιρα ο κατάσκοπος ή να προληφθεί ο κίνδυνος.

7. Η απόπειρα και η προσφορά για την τέλεση των πράξεων αυτών τιμωρούνται με την ποινή του τετελεσμένου εγκλήματος.

Άρθρο 145
Ανακοίνωση στρατιωτικών πληροφοριών

Στρατιωτικός και όποιος ανήκει στην υπηρεσία του στρατού που χωρίς έγκριση της στρατιωτικής αρχής ανακοινώνει ή δημοσιεύει με οποιοδήποτε μέσο πληροφορίες σχετικές με το στρατό, άλλες από τις αναφερόμενες στο άρθρο 143 ικανές να κλονίσουν την εμπιστοσύνη του κοινού σ΄ αυτόν, τιμωρείται με φυλάκιση μέχρι έξι μηνών.

Τόπος, ...

Ο ΥΠΕΥΘΥΝΑ ΔΗΛΩΝ

Υπογραφή

Ο
Υπεύθυνος Ασφαλείας

Υπογραφή

Ο
Διευθύνων Σύμβουλος

Υπογραφή

ΥΠΟΔΕΙΓΜΑ 6

ΒΙΒΛΙΟ ΕΝΗΜΕΡΩΣΕΩΣ ΠΡΟΣΩΠΙΚΟΥ

Α/Α	ΗΜΝΙΑ ΕΝΗΜΕΡΩΣΗΣ	ΑΝΤΙΚΕΙΜΕΝΑ ΕΝΗΜΕΡΩΣΗΣ	ΟΝΟΜΑΤΕΠΩΝΥΜΑ ΣΥΜΜΕΤΕΧΟΝΤΟΣ ΠΡΟΣΩΠΙΚΟΥ	ΥΠΟΓΡΑΦΕΣ ΣΥΜΜΕΤΕΧΟΝΤΟΣ ΠΡΟΣΩΠΙΚΟΥ
		1.		
		2.		
		3.		
		4.		
		5.		
		6.		
		1.		
		2.		
		3.		
		4.		
		5.		
		6.		
		1.		
		2.		
		3.		
		4.		
		5.		
		6.		

Ο Υπεύθυνος Ασφαλείας

ΥΠΟΔΕΙΓΜΑ 7

ΒΙΒΛΙΟ ΕΠΙΣΚΕΠΤΩΝ

Α/Α	ΗΜ/ΝΙΑ	ΟΝΟΜ/ΜΟ ΕΠΙΣΚΕΠΤΗ	ΑΡ. ΟΧΗΜ. ΕΠΙΣΚΕΠΤΗ	ΩΡΑ ΕΙΣΟΔ.	ΩΡΑ ΕΞΟΔ.	ΠΡΟΟΡΙΣΜΟΣ - ΠΑΡΑΤΗΡΗΣΕΙΣ	ΥΠΟΓΡΑΦΗ ΓΡΑΜ/ΤΕΙΑΣ

Ο Συντάξας

Ο Υπεύθυνος Ασφαλείας

ΥΠΟΔΕΙΓΜΑ 8

ΑΠΟΔΕΙΞΗ
ΠΑΡΑΛΑΒΗΣ ΔΙΑΒΑΘΜΙΣΜΕΝΟΥ ΕΓΓΡΑΦΟΥ

ΟΙΚΟΝΟΜΙΚΟΣ ΦΟΡΕΑΣ:
ΑΠΟΔΕΙΞΗ ΠΑΡΑΛΑΒΗΣ ΔΙΑΒΑΘΜΙΣΜΕΝΟΥ ΕΓΓΡΑΦΟΥ……
ΒΑΘΜΟΣ ΑΣΦΑΛΕΙΑΣ
ΠΡΟΣ: ……..

ΑΡΙΘ. ΠΡΩΤΟΚΟΛΛΟΥ	ΘΕΜΑ	ΣΥΝΗΜΜΕΝΑ	ΗΜΕΡΟΜΗΝΙΑ
ΥΠΟΓΡΑΦΗ ΠΑΡΑΛΗΠΤΟΥ		ΗΜΕΡΟΜΗΝΙΑ	

Παράκληση για την επιστροφή το ταχύτερο

Ο Υπεύθυνος Ασφαλείας

ΥΠΟΔΕΙΓΜΑ 9

ΠΡΩΤΟΚΟΛΛΟ ΚΑΤΑΣΤΡΟΦΗΣ ΕΔΠΥ ΤΟΥ ΟΙΚΟΝΟΜΙΚΟΥ ΦΟΡΕΑ

ΟΙΚΟΜΟΜΙΚΟΣ ΦΟΡΕΑΣ:

ΕΝΤΟΛΗ ΚΑΤΑΣΤΡΟΦΗΣ ΕΔΠΥ

Α/Α	ΣΤΟΙΧΕΙΑ ΕΓΓΡΑΦΟΥ	ΘΕΜΑ	ΒΑΘΜΟΣ

Βεβαιώνεται ότι τα ανωτέρω έγγραφα καταστράφηκαν παρουσία μας σήμερα με φωτιά/πολτοποίηση

Η ΕΠΙΤΡΟΠΗ

	ΟΝΟΜΑΤΕΠΩΝΥΜΟ	ΥΠΟΓΡΑΦΗ	ΗΜΕΡΟΜΗΝΙΑ
α.	.....		.....
β.	.....		.....
γ.	.....		.....

Ο

Υπεύθυνος Ασφαλείας

ΥΠΟΔΕΙΓΜΑ 10

ΜΗΤΡΩΟ ΠΥΡΟΣΒΕΣΤΗΡΩΝ

Α/Α	Α/Α ΠΥΡΟΣΒ/ΡΑ	ΤΥΠΟΣ ΠΥΡΟΣΒ/ΡΑ	ΘΕΣΗ ΠΥΡΟΣΒ/ΡΑ	ΧΡΟΝΟΣ ΠΡΟΜΗΘΕΙΑΣ	ΗΜΕΡ/ΝΙΑ ΕΛΕΓΧΟΥ	ΗΜΕΡ/ΝΙΑ ΑΝΑΓΟΜ.

Ο Υπεύθυνος Ασφαλείας

ΥΠΟΔΕΙΓΜΑ 11

ΒΙΒΛΙΟΥ
ΕΛΕΓΧΟΥ ΚΑΙ ΕΠΙΘΕΩΡΗΣΕΩΝ

Ημερομηνία .....

Χώρος που επιθεωρήθηκε .....

Διαπιστώσεις – Ελλείψεις – Παραλήψεις .....

.....
.....
.....
.....
.....
.....
.....

Προτάσεις:

.....
.....
.....
.....
.....
.....

Ο
Επιθεωρών

Ο
Υπεύθυνος Ασφαλείας

ΥΠΟΔΕΙΓΜΑ 12

ΕΝΔΕΙΚΤΕΣ ΕΠΙΘΕΩΡΗΣΕΩΣ ΑΣΦΑΛΕΙΑΣ - ΜΕΤΡΑ ΒΙΟΜΗΧΑΝΙΚΗΣ ΑΣΦΑΛΕΙΑΣ

1. Μέτρα Φυσικής Ασφάλειας

α. Μέτρα προστασίας χώρων από μη εξουσιοδοτημένη είσοδο.

Υπεύθυνος Ασφαλείας Εγκαταστάσεων.

Φρουρές/Σκοπιές (ενημέρωση, αποστολή, δύναμη, ενδοεπικοινωνία, ωράρια).

Συστήματα εντοπισμού εισβολέων (είδος συστήματος, αδυναμίες, ολοκλήρωση, δύναμη ασφάλειας) .

Περιφράξεις (φράκτες, ορύγματα, πλέγματα).

β. Ορισμός χώρων ασφαλείας.

γ. Πρόσβαση στους χώρους ασφαλείας, παρασυνθήματα, σημεία ελέγχου, ηλεκτρονικές συσκευές.

δ. Συνθήκες αποθήκευσης (φοριαμοί ασφαλείας, ασφάλιση θυρών και παραθύρων, κλειδαριές ασφαλείας και μη, έλεγχος κλειδιών, συστήματα συναγερμού και υποστήριξή τους).

ε. Καθαρισμός και συντήρηση χώρων υλικού.

στ. Διαδικασίες εκτάκτου ανάγκης.

ζ. Διαδικασίες ελέγχου επισκεπτών.

η. Πυρασφάλεια.

2. Ασφάλεια Προσωπικού

α. Εξουσιοδοτήσεις ασφαλείας προσωπικού.

β. Συνεχής ενημέρωση προσωπικού σε ότι αφορά τα θέματα ασφαλείας από το αρμόδιο προσωπικό, με ιδιαίτερη έμφαση στη σημασία διατήρησης εχεμύθειας, αξιοπιστίας, αφοσίωσης στο υπηρεσιακό καθήκον. Ενημέρωση πάνω στη σχετική νομοθεσία και τους ειδικότερους κανονισμούς ασφάλειας της επιχείρησης.

γ. Παραβιάσεις μέτρων ασφαλείας, εντοπισμός παραβατών και προβλεπόμενες συνέπειες.

δ. Ασφάλεια κατά τις μετακινήσεις στο εσωτερικό και εξωτερικό.

3. Ασφάλεια ΕΔΠΥ

α. Διαχείριση Διαβαθμισμένων εγγράφων (1).

Διαβαθμίσεις ασφαλείας.

Αρχειοθέτηση/Καταγραφή.

Υπεύθυνος χειριστής/Πρόσβαση Αρχείων.

Διακίνηση στο εσωτερικό και εξωτερικό.

Χώροι εργασίας, μελέτης και παραγωγής.

Εσωτερική Διανομή.

Καταστροφή.

Αναπαραγωγή.

β. Εσωτερικός κανονισμός προστασίας διαβαθμισμένου υλικού.

γ. Ηλεκτρονική Αλληλογραφία.

δ. Ύπαρξη διαβαθμισμένου ΣΕΠ με διαπίστευση εν ισχύ ή μεμονωμένου Η/Υ για διαχείριση ΕΔΠΥ.

4. Στοιχεία Οικονομικού Φορέα

1. ΚΩΔΙΚΟΣ ΑΡΙΘΜΟΣ – ΑΜ	
2. ΕΠΩΝΥΜΙΑ ΟΙΚΟΝΟΜΙΚΟΥ ΦΟΡΕΑ	
3. ΔΝΣΗ ΓΡΑΦΕΙΟΥ α. ΝΟΜΟΣ-ΕΠΑΡΧΙΑ β. ΔΗΜΟΣ/ΚΟΙΝΟΤΗΤΑ γ. ΟΔΟΣ-ΑΡΙΘΜΟΣ δ. ΣΥΝΟΙΚΙΑ ε. ΤΗΛΕΦΩΝΑ στ. ΤΑΧ. ΚΩΔΙΚΑΣ	
4. ΔΝΣΗ ΕΡΓΟΣΤΑΣΙΟΥ α. ΝΟΜΟΣ-ΕΠΑΡΧΙΑ β. ΔΗΜΟΣ/ΚΟΙΝΟΤΗΤΑ γ. ΟΔΟΣ-ΑΡΙΘΜΟΣ δ. ΣΥΝΟΙΚΙΑ ε. ΤΗΛΕΦΩΝΑ στ. ΤΑΧ. ΚΩΔΙΚΑΣ	
5. ΠΑΡΑΓΩΜΕΝΟ ΠΡΟΪΟΝ ή ΕΡΓΟ	
6. ΑΡΜΟΔΙΟ ΥΠΟΥΡΓΕΙΟ ΣΤΗΝ ΕΙΡΗΝΗ	
7. ΥΠΟΥΡΓΕΙΟ ή ΕΠΙΤΕΛΕΙΟ ΣΤΟ ΟΠΟΙΟ ΕΚΧΩΡΕΙΤΑΙ ΣΕ ΠΟΛΕΜΟ ΚΑΙ ΠΟΣΟΣΤΟ ΕΚΧΩΡΗΣΗΣ	

8. ΙΔΙΟΚΤΗΣΙΑΚΟ ΚΑΘΕΣΤΩΣ α. ΣΥΝΘΕΣΗ ΔΙΟΙΚ. ΣΥΜΒΟΥΛΙΟΥ β. ΜΕΤΟΧΙΚΟ ΚΕΦΑΛΑΙΟ γ. ΝΟΜΙΚΗ ΜΟΡΦΗ ΟΙΚΟΝΟΜΙΚΟΥ ΦΟΡΕΑ δ. ΦΕΚ ή ΑΛΛΟ ΕΓΓΡΑΦΟ ΠΟΥ ΑΠΟΡΡΕΕΙ ΑΠΟ ΤΑ ΑΝΩΤΕΡΩ	
9. ΣΥΝΕΡΓΑΖΟΜΕΝΟΙ ΟΙΚΟΝΟΜΙΚΟΙ ΦΟΡΕΙΣ ή ΘΥΓΑΤΡΙΚΕΣ, ΕΘΝΙΚΟΤΗΤΑ	
10. ΥΠΟΚΑΤΑΣΚΕΥΑΣΤΕΣ – ΣΥΝΕΡΓΑΤΕΣ, ΕΘΝΙΚΟΤΗΤΑ	

Τα αναφερόμενα μέτρα είναι ενδεικτικά και μπορούν να συμπληρωθούν ή να τροποποιηθούν κατά περίπτωση. Αποτελούν τις ελάχιστες απαιτούμενες προϋποθέσεις για το χαρακτηρισμό ασφαλείας/προμηθευτών αμυντικού υλικού.

ΣΗΜΕΙΩΣΕΙΣ

ΕΠΙΘΕΩΡΟΥΜΕΝΟΣ:

.....

.....

.....

.....

1 .....

ΥΠΟΔΕΙΓΜΑ 13

ΠΙΣΤΟΠΟΙΗΤΙΚΟ
ΗΛΕΚΤΡΟΝΙΚΗΣ ΑΣΦΑΛΕΙΑΣ ΕΓΚΑΤΑΣΤΑΣΗΣ

1. Λαμβάνοντας υπόψη τις διατάξεις του Εθνικού Κανονισμού Βιομηχανικής Ασφαλείας (ΕΚΒΑ 201...), της πολιτικής ασφαλείας του NATO C-M(2002)49 – Enclosure “G”/17 June 2002, καθώς και της απόφασης του EUROPEAN COUNCIL 2013/488/EC, το ΓΕΕΘΑ/Ε΄ Κλάδος, ως Εθνική Αρχή Διαπίστευσης Ασφαλείας,

Χ Ο Ρ Η Γ Ε Ι

στην επιχείρηση **(……)** Πιστοποιητικό βαθμού ασφαλείας **«……»,** για το Σύστημα Επικοινωνιών – Πληροφορικής (ΣΕΠ) όπως αυτό περιγράφεται στην Δήλωση Απαιτήσεων Ασφαλείας (ΔΑΠΑΣ) …….. και την Δήλωση Ασφαλούς Λειτουργίας (ΔΑΛ) ……..
Το παρόν ισχύει μέχρι ……..

2. Η Εθνική Αρχή Διαπίστευσης Ασφαλείας, βεβαιώνει ότι η αναγραφόμενη εγκατάσταση, που βρίσκεται στ……..
……, διαθέτει σύστημα Ηλεκτρονικών Υπολογιστών, όπως παρουσιάζεται στις (ΔΑΠΑΣ) ……
και (ΔΑΛ) ……, για ασφαλή φύλαξη και επεξεργασία διαβαθμισμένων πληροφοριών, μέχρι βαθμού ασφαλείας **«……»** .

Ο
Διευθυντής Ε΄ Κλάδου

ΥΠΟΔΕΙΓΜΑ 14

ΠΙΣΤΟΠΟΙΗΤΙΚΟ
ΑΣΦΑΛΕΙΑΣ ΕΓΚΑΤΑΣΤΑΣΗΣ

1. Λαμβάνοντας υπόψη τις διατάξεις του Εθνικού Κανονισμού Βιομηχανικής Ασφαλείας (ΕΚΒΑ 201...), της πολιτικής ασφαλείας του NATO C-M(2002)49 – Enclosure “G”/17 June 2002, καθώς και της απόφασης του EUROPEAN COUNCIL 2013/488/EC, το ΓΕΕΘΑ/Ε΄ ΚΛΑΔΟΣ, ως Εθνική Αρχή Ασφαλείας,

Χ Ο Ρ Η Γ Ε Ι

στην επιχείρηση **(.....)** Πιστοποιητικό Ασφάλειας Εγκαταστάσεως, βαθμού ασφαλείας **«.....»,** για τις εγκαταστάσεις που διαθέτει ..... Το παρόν ισχύει μέχρι **.....**

2. Η Εθνική Αρχή Ασφαλείας, βεβαιώνει ότι η αναγραφόμενη εγκατάσταση:

α. Διαθέτει/ Δεν διαθέτει υπαρχείο για την προστασία ΕΔΠΥ βαθμού ασφαλείας **«.....»**.

β. Διαθέτει/ Δεν διαθέτει χώρους ασφαλείας για την προστασία ΕΔΠΥ βαθμού ασφαλείας **«.....»**.

γ. Διαθέτει/ Δεν διαθέτει πιστοποιημένο Σύστημα Επικοινωνιών – Πληροφορικής (ΣΕΠ) για ασφαλή φύλαξη και επεξεργασία διαβαθμισμένων πληροφοριών, μέχρι βαθμού ασφαλείας **«.....»**.

Ο
Διευθυντής Ε΄ Κλάδου

ΥΠΟΔΕΙΓΜΑ 15

ΑΙΤΗΣΗ ΕΠΙΣΚΕΨΗΣ
(REQUEST FOR VISIT)

1.	ΑΙΤΩΝ ΤΗΝ ΕΠΙΣΚΕΨΗ: (REQUESTOR) ΠΡΟΣ : (TO)	ΗΜΕΡΟΜΗΝΙΑ: (DATE) ΤΟΠΟΣ ΕΠΙΣΚΕΨΗΣ: (INDUSTRIAL FACILITIES TO BE VISITED)
2.	ΣΤΟΙΧΕΙΑ ΑΙΤΟΥΣΑΣ ΕΠΙΧΕΙΡΗΣΗΣ (REQUESTING INDUSTRIAL FACILITY) ΟΝΟΜΑ (NAME): ΔΙΕΥΘΥΝΣΗ (POSTAL ADDRESS): FAX NO: ΤΗΛΕΦΩΝΟ (TELEPHONE NO): EMAIL ADDRESS:	
3.	ΣΤΟΙΧΕΙΑ ΠΡΟΣ ΕΠΙΣΚΕΨΗ ΕΠΙΧΕΙΡΗΣΗΣ (INDUSTRIAL FACILITY TO BE VISITED) ΟΝΟΜΑ (NAME): ΔΙΕΥΘΥΝΣΗ (POSTAL ADDRESS): FAX NO: ΤΗΛΕΦΩΝΟ (TELEPHONE NO): EMAIL ADDRESS: ΥΠΕΥΘΥΝΟΣ ΑΣΦΑΛΕΙΑΣ (FACILITY SECURITY OFFICER):	
4.	ΗΜΕΡΟΜΗΝΙΕΣ ΕΠΙΣΚΕΨΗΣ: (DATE OF VISIT)	ΑΠΟ ----/----/---- (FROM) ΕΩΣ ----/----/---- (TO)
5.	ΤΥΠΟΣ ΕΠΙΣΚΕΨΗΣ (επιλέξτε ένα από κάθε στήλη) (TYPE OF INITIATIVE – SELECT ON FROM EACH COLUMN) ( ) ΚΥΒΕΡΝΗΤΙΚΗ (GOVERNMENT INITIATIVE) ( ) ΕΜΠΟΡΙΚΗ (COMMERCIAL INITIATIVE)	( ) ΑΠΟ ΤΟΝ ΑΙΤΟΥΝΤΑ (INITIATED BY REQUESTING FACILITY) ( ) ΑΠΟ ΤΟΝ ΕΠΙΣΚΕΠΤΟΜΕΝΟ (BY INVITATION OF FACILITY TO BE VISITED)
6.	ΘΕΜΑΤΑ ΠΡΟΣ ΣΥΖΗΤΗΣΗ (SUBJECT TO BE DISCUSSED):	
7.	ΕΚΤΙΜΩΜΕΝΟ ΕΠΙΠΕΔΟ ΔΙΑΒΑΘΜΙΣΗΣ ΠΛΗΡΟΦΟΡΙΩΝ: (ANTICIPATED HIGHEST LEVEL OF INFORMATION)	
8.	Η ΕΠΙΣΚΕΨΗ ΣΧΕΤΙΖΕΤΑΙ ΜΕ : (THE VISIT IS PERTINENT TO) Συγκεκριμένο εξοπλισμό ή οπλικό σύστημα (SPECIFIC EQUIPEMENT OR WEAPON SYSTEN) Στρατιωτικές πωλήσεις ή άδεια εξαγωγής (MILITARY SALES OR EXPORT LICENSE) Πρόγραμμα ή Συμφωνία (PROGRAMME OR AGREEMENT) Απόκτηση αμυντικού προγράμματος (DEFENSE ACQUISITION PROCESS) Άλλο (OTHER)	ΕΞΗΓΗΣΗ: (SPECIFICATION OF SELECTED) ( ) ( ) ( ) ( ) ( )
9.	ΣΤΟΙΧΕΙΑ ΕΠΙΣΚΕΠΤΩΝ: (PARTICULARS OF VISITORS) ΟΝΟΜΑ (NAME): ΗΜ/ΝΙΑ ΓΕΝΝΗΣΗΣ (DATE OF BIRTH): ΤΟΠΟΣ ΓΕΝΝΗΣΗΣ (PLACE OF BIRTH): ΒΑΘΜΟΣ ΑΣΦΑΛΕΙΑΣ (SECURITY CLEARANCE LEVEL) ΑΡ. ΤΑΥΤ (PP/ID NO): ΕΘΝΙΚΟΤΗΤΑ (NATIONALITY): ΘΕΣΗ – ΒΑΘΜΟΣ (RANK - POSITION) : ΕΤΑΙΡΕΙΑ (COMPANY):	

ΕΑΝ ΥΠΑΡΧΟΥΝ ΠΕΡΑΝ ΤΟΥ ΕΝΟΣ ΕΠΙΣΚΕΠΤΕΣ, ΝΑ ΧΡΗΣΙΜΟΠΟΙΗΘΕΙ Η ΑΝΤΙΣΤΟΙΧΗ ΦΟΡΜΑ (COMPLETE THE SAME FORM FOR EACH VISITOR)
10. ΑΞΙΩΜΑΤΙΚΟΣ ΑΣΦΑΛΕΙΑΣ ΑΙΤΟΥΝΤΟΣ ΓΡΑΦΕΙΟΥ ‘Η ΕΤΑΙΡΕΙΑΣ (REQUESTING FACILITY SECURITY OFFICER) ΟΝΟΜΑ (NAME): ΤΗΛΕΦΩΝΟ (TELEPHONE NO): ΥΠΟΓΡΑΦΗ (SIGNATURE – STAMP):
11. ΒΕΒΑΙΩΣΗ ΕΠΙΠΕΔΟΥ ΒΑΘΜΟΥ ΑΣΦΑΛΕΙΑΣ (CERTIFICATION OF SECURITY CLEARANCE LEVEL) ΟΝΟΜΑ (NAME): ΔΙΕΥΘΥΝΣΗ (ADDRESS): ΤΗΛΕΦΩΝΟ (TELEPHONE NO): ΥΠΟΓΡΑΦΗ (SIGNATURE – STAMP):
12 ΑΙΤΟΥΣΑ ΕΘΝΙΚΗ ΑΡΧΗ ΑΣΦΑΛΕΙΑΣ / ΔΙΟΡΙΣΜΕΝΗ ΑΡΧΗ ΑΣΦΑΛΕΙΑΣ (REQUESTING NATIONAL SECURITY AUTHORITY / DESIGNATED SECURITY AUTHORITY) ΔΙΕΥΘΥΝΣΗ (ADDRESS): ΤΗΛΕΦΩΝΟ (TELEPHONE NO): FAX NO: ΟΝΟΜΑ (NAME): ΥΠΟΓΡΑΦΗ (SIGNATURE – STAMP):
13. ΠΑΡΑΤΗΡΗΣΕΙΣ (REMARKS):

Αντιναύαρχος Ιωάννης Δρυμούσης ΠΝ
Υπαρχηγός

Ακριβές Αντίγραφο

Ασμχος (ΕΑ) Νικόλαος Ζήκος
Επιτελής ΓΕΕΘΑ/Ε3/1

Άρθρο 3
Έναρξη ισχύος

Η ισχύς της παρούσας αρχίζει από τη δημοσίευσή της στην Εφημερίδα της Κυβερνήσεως.
Η παρούσα και ο ΕΚΒΑ να δημοσιευθούν στην Εφημερίδα της Κυβερνήσεως.

Αθήνα, 7 Σεπτεμβρίου 2020

Ο Υπουργός

ΝΙΚΟΛΑΟΣ ΠΑΝΑΓΙΩΤΟΠΟΥΛΟΣ

ΕΘΝΙΚΟ ΤΥΠΟΓΡΑΦΕΙΟ

Το Εθνικό Τυπογραφείο αποτελεί δημόσια υπηρεσία υπαγόμενη στην Προεδρία της Κυβέρνησης και έχει την ευθύνη τόσο για τη σύνταξη, διαχείριση, εκτύπωση και κυκλοφορία των Φύλλων της Εφημερίδας της Κυβερνήσεως (ΦΕΚ), όσο και για την κάλυψη των εκτυπωτικών - εκδοτικών αναγκών του δημοσίου και του ευρύτερου δημόσιου τομέα (ν. 3469/2006/Α΄ 131 και π.δ. 29/2018/Α΄58).

1. ΦΥΛΛΟ ΤΗΣ ΕΦΗΜΕΡΙΔΑΣ ΤΗΣ ΚΥΒΕΡΝΗΣΕΩΣ (ΦΕΚ)

• Τα **ΦΕΚ σε ηλεκτρονική μορφή** διατίθενται δωρεάν στο **www.et.gr**, την επίσημη ιστοσελίδα του Εθνικού Τυπογραφείου. Όσα ΦΕΚ δεν έχουν ψηφιοποιηθεί και καταχωριστεί στην ανωτέρω ιστοσελίδα, ψηφιοποιούνται και αποστέλλονται επίσης δωρεάν με την υποβολή αίτησης, για την οποία αρκεί η συμπλήρωση των αναγκαίων στοιχείων σε ειδική φόρμα στον ιστότοπο www.et.gr.

• Τα **ΦΕΚ σε έντυπη μορφή** διατίθενται σε μεμονωμένα φύλλα είτε απευθείας από το Τμήμα Πωλήσεων και Συνδρομητών, είτε ταχυδρομικά με την αποστολή αιτήματος παραγγελίας μέσω των ΚΕΠ, είτε με ετήσια συνδρομή μέσω του Τμήματος Πωλήσεων και Συνδρομητών. Το κόστος ενός ασπρόμαυρου ΦΕΚ από 1 έως 16 σελίδες είναι 1,00 €, αλλά για κάθε επιπλέον οκτασέλιδο (ή μέρος αυτού) προσαυξάνεται κατά 0,20 €. Το κόστος ενός έγχρωμου ΦΕΚ από 1 έως 16 σελίδες είναι 1,50 €, αλλά για κάθε επιπλέον οκτασέλιδο (ή μέρος αυτού) προσαυξάνεται κατά 0,30 €. Το τεύχος Α.Σ.Ε.Π. διατίθεται δωρεάν.

• **Τρόποι αποστολής κειμένων προς δημοσίευση:**

Α. Τα κείμενα προς δημοσίευση στο ΦΕΚ, από τις υπηρεσίες και τους φορείς του δημοσίου, αποστέλλονται ηλεκτρονικά στη διεύθυνση **webmaster.et@et.gr** με χρήση προηγμένης ψηφιακής υπογραφής και χρονοσήμανσης.

Β. Κατ’ εξαίρεση, όσοι πολίτες δεν διαθέτουν προηγμένη ψηφιακή υπογραφή μπορούν είτε να αποστέλλουν ταχυδρομικά, είτε να καταθέτουν με εκπρόσωπό τους κείμενα προς δημοσίευση εκτυπωμένα σε χαρτί στο Τμήμα Παραλαβής και Καταχώρισης Δημοσιευμάτων.

• Πληροφορίες, σχετικά με την αποστολή/κατάθεση εγγράφων προς δημοσίευση, την ημερήσια κυκλοφορία των Φ.Ε.Κ., με την πώληση των τευχών και με τους ισχύοντες τιμοκαταλόγους για όλες τις υπηρεσίες μας, περιλαμβάνονται στον ιστότοπο (www.et.gr). Επίσης μέσω του ιστότοπου δίδονται πληροφορίες σχετικά με την πορεία δημοσίευσης των εγγράφων, με βάση τον Κωδικό Αριθμό Δημοσιεύματος (ΚΑΔ). Πρόκειται για τον αριθμό που εκδίδει το Εθνικό Τυπογραφείο για όλα τα κείμενα που πληρούν τις προϋποθέσεις δημοσίευσης.

2. ΕΚΤΥΠΩΤΙΚΕΣ - ΕΚΔΟΤΙΚΕΣ ΑΝΑΓΚΕΣ ΤΟΥ ΔΗΜΟΣΙΟΥ

Το Εθνικό Τυπογραφείο ανταποκρινόμενο σε αιτήματα υπηρεσιών και φορέων του δημοσίου αναλαμβάνει να σχεδιάσει και να εκτυπώσει έντυπα, φυλλάδια, βιβλία, αφίσες, μπλοκ, μηχανογραφικά έντυπα, φακέλους για κάθε χρήση, κ.ά.

Επίσης σχεδιάζει ψηφιακές εκδόσεις, λογότυπα και παράγει οπτικοακουστικό υλικό.

Ταχυδρομική Διεύθυνση: Καποδιστρίου 34, τ.κ. 10432, Αθήνα	Ιστότοπος: **www.et.gr**
ΤΗΛΕΦΩΝΙΚΟ ΚΕΝΤΡΟ: 210 5279000 - fax: 210 5279054	Πληροφορίες σχετικά με την λειτουργία του ιστότοπου: **helpdesk.et@et.gr**
ΕΞΥΠΗΡΕΤΗΣΗ ΚΟΙΝΟΥ **Πωλήσεις - Συνδρομές:** (Ισόγειο, τηλ. 210 5279178 - 180) **Πληροφορίες:** (Ισόγειο, Γρ. 3 και τηλεφ. κέντρο 210 5279000) **Παραλαβή Δημ. Ύλης:** (Ισόγειο, τηλ. 210 5279167, 210 5279139)	Αποστολή ψηφιακά υπογεγραμμένων εγγράφων προς δημοσίευση στο ΦΕΚ: **webmaster.et@et.gr**
Ωράριο για το κοινό: Δευτέρα ως Παρασκευή: 8:00 - 13:30	Πληροφορίες για γενικό πρωτόκολλο και αλληλογραφία: **grammateia@et.gr**

Πείτε μας τη γνώμη σας,

για να βελτιώσουμε τις υπηρεσίες μας, συμπληρώνοντας την ειδική φόρμα στον ιστότοπό μας.

02040712209200192