II

(Μη νομοθετικές πράξεις)

ΑΠΟΦΑΣΕΙΣ

ΑΠΟΦΑΣΗ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ

της 23ης Σεπτεμβρίου 2013

σχετικά με τους κανόνες ασφαλείας για την προστασία των διαβαθμισμένων πληροφοριών της ΕΕ

(2013/488/ΕΕ)

ΤΟ ΣΥΜΒΟΥΛΙΟ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ,

Έχοντας υπόψη τη Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης, και ιδίως το άρθρο 240 παράγραφος 3,

Έχοντας υπόψη την απόφαση 2009/937/ΕΕ του Συμβουλίου, της 1ης Δεκεμβρίου 2009, για την έγκριση του εσωτερικού του κανονισμού [1], και ιδίως το άρθρο 24,

Εκτιμώντας τα ακόλουθα:

(1) Προκειμένου να αναπτυχθούν οι δραστηριότητες του Συμβουλίου σε όλους τους τομείς όπου απαιτείται χειρισμός διαβαθμισμένων πληροφοριών, είναι σκόπιμο να θεσπισθεί ολοκληρωμένο σύστημα ασφαλείας για την προστασία των διαβαθμισμένων πληροφοριών το οποίο θα καλύπτει το Συμβούλιο, τη Γενική Γραμματεία του και τα κράτη μέλη.

(2) Η παρούσα απόφαση δέον να εφαρμόζεται οσάκις το Συμβούλιο, τα προπαρασκευαστικά όργανά του και η Γενική Γραμματεία του Συμβουλίου (ΓΓΣ) χειρίζονται διαβαθμισμένες πληροφορίες της ΕΕ (ΔΠΕΕ).

(3) Σύμφωνα με τις εθνικές νομοθετικές και κανονιστικές διατάξεις και στο βαθμό που απαιτείται για τη λειτουργία του Συμβουλίου, τα κράτη μέλη πρέπει να τηρούν την παρούσα απόφαση όταν οι αρμόδιες αρχές, το προσωπικό ή οι εργολάβοι τους χειρίζονται ΔΠΕΕ, προκειμένου να έχουν τη βεβαιότητα ότι εξασφαλίζεται ισοδύναμο επίπεδο προστασίας για τις ΔΠΕΕ.

(4) Το Συμβούλιο, η Επιτροπή και η Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης (ΕΥΕΔ) έχουν δεσμευθεί να εφαρμόζουν ισοδύναμες προδιαγραφές ασφαλείας για την προστασία των ΔΠΕΕ.

(5) Το Συμβούλιο υπογραμμίζει τη σημασία της συμμετοχής του Ευρωπαϊκού Κοινοβουλίου και άλλων θεσμικών και λοιπών οργάνων ή οργανισμών της Ένωσης, όπου ενδείκνυται, στην εφαρμογή των αρχών, προδιαγραφών και κανόνων προστασίας των διαβαθμισμένων πληροφοριών που απαιτούνται για την προστασία των συμφερόντων της Ένωσης και των κρατών μελών.

(6) Το Συμβούλιο θα πρέπει να καθορίσει το κατάλληλο πλαίσιο ώστε οι διαβαθμισμένες πληροφορίες ΕΕ τις οποίες το Συμβούλιο έχει την κατοχή του να κοινοποιούνται, κατά περίπτωση, σε άλλα θεσμικά και λοιπά όργανα ή οργανισμούς της Ένωσης, σύμφωνα με την παρούσα απόφαση και τις ισχύουσες διοργανικές ρυθμίσεις.

(7) Τα λοιπά όργανα και οι οργανισμοί της Ένωσης που έχουν ιδρυθεί δυνάμει του τίτλου V κεφάλαιο 2 της Συνθήκης για την Ευρωπαϊκή Ένωση (ΣΕΕ), η Ευρωπόλ και η Eurojust θα πρέπει να εφαρμόζουν, στο πλαίσιο της εσωτερικής τους οργάνωσης, τις βασικές αρχές και τις ελάχιστες προδιαγραφές της παρούσας απόφασης για την προστασία των ΔΠΕΕ, όταν αυτό προβλέπεται στις πράξεις για την ίδρυσή τους.

(8) Στις επιχειρήσεις διαχείρισης κρίσεων που συστήνονται δυνάμει του τίτλου V κεφάλαιο 2 της ΣΕΕ και στο προσωπικό τους θα πρέπει να εφαρμόζονται οι κανόνες ασφαλείας που θεσπίζει το Συμβούλιο για την προστασία των ΔΠΕΕ όταν αυτό προβλέπεται στην πράξη του Συμβουλίου για τη σύστασή τους.

(9) Οι ειδικοί εντεταλμένοι της ΕΕ και τα μέλη των ομάδων τους θα πρέπει να εφαρμόζουν τους κανόνες ασφαλείας που θεσπίζει το Συμβούλιο για την προστασία των ΔΠΕΕ όταν αυτό προβλέπεται στην αντίστοιχη πράξη του Συμβουλίου.

(10) Η παρούσα απόφαση λαμβάνεται με την επιφύλαξη των άρθρων 15 και 16 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης (ΣΛΕΕ) και των πράξεων εφαρμογής τους.

(11) Η παρούσα απόφαση λαμβάνεται με την επιφύλαξη της πρακτικής των κρατών μελών όσον αφορά την ενημέρωση των εθνικών κοινοβουλίων τους για τις δραστηριότητες της Ένωσης.

[1] ΕΕ L 325 της 11.12.2009, σ. 35.

(12) Προκειμένου να εξασφαλιστεί εγκαίρως η εφαρμογή των κανόνων ασφαλείας για την προστασία των ΔΠΕΕ όσον αφορά την προσχώρηση της Δημοκρατίας της Κροατίας στην Ευρωπαϊκή Ένωση, η παρούσα απόφαση θα πρέπει να αρχίσει να ισχύει από την ημερομηνία δημοσίευσής της,

ΕΞΕΔΩΣΕ ΤΗΝ ΠΑΡΟΥΣΑ ΑΠΟΦΑΣΗ:

Άρθρο 1

Σκοπός, πεδίο εφαρμογής και ορισμοί

1. Η παρούσα απόφαση καθορίζει τις βασικές αρχές και τις ελάχιστες προδιαγραφές ασφαλείας για την προστασία των ΔΠΕΕ.

2. Οι εν λόγω βασικές αρχές και ελάχιστες προδιαγραφές θα ισχύουν για το Συμβούλιο και τη ΓΓΣ και θα τηρούνται από τα κράτη μέλη, σύμφωνα με τις αντίστοιχες εθνικές νομοθετικές και κανονιστικές τους διατάξεις, προκειμένου τα κράτη να έχουν τη βεβαιότητα ότι παρέχεται ισοδύναμο επίπεδο προστασίας στις ΔΠΕΕ.

3. Για τους σκοπούς της παρούσας οδηγίας, ισχύουν οι ορισμοί του προσαρτήματος Α.

Άρθρο 2

Ορισμός των ΔΠΕΕ, διαβαθμίσεις και σημάνσεις ασφαλείας

1. «Διαβαθμισμένες πληροφορίες της ΕΕ» (ΔΠΕΕ): κάθε πληροφορία ή υλικό που έχει χαρακτηρισθεί με διαβάθμιση ασφαλείας ΕΕ και των οποίων η άνευ αδείας κοινολόγηση μπορεί να βλάψει ποικιλοτρόπως τα συμφέροντα της Ευρωπαϊκής Ένωσης ή ενός ή περισσοτέρων κρατών μελών.

2. Οι ΔΠΕΕ διαβαθμίζονται σε ένα από τα παρακάτω επίπεδα:

α) TRÈS SECRET UE/EU TOP SECRET: πληροφορίες και υλικό των οποίων η άνευ αδείας κοινολόγηση μπορεί να προξενήσει εξαιρετικά σοβαρή ζημία στα ζωτικά συμφέροντα της Ευρωπαϊκής Ένωσης ή ενός ή περισσοτέρων κρατών μελών·

β) SECRET UE/EU SECRET: πληροφορίες και υλικό των οποίων η άνευ αδείας κοινολόγηση μπορεί να βλάψει σοβαρά τα ζωτικά συμφέροντα της Ευρωπαϊκής Ένωσης ή ενός ή περισσοτέρων κρατών μελών της·

γ) CONFIDENTIEL UE/EU CONFIDENTIAL: πληροφορίες και υλικό των οποίων η άνευ αδείας κοινολόγηση μπορεί να βλάψει τα ζωτικά συμφέροντα της Ευρωπαϊκής Ένωσης ή ενός ή περισσοτέρων κρατών μελών της·

δ) RESTREINT UE/EU RESTRICTED: πληροφορίες και υλικό των οποίων η άνευ αδείας κοινολόγηση μπορεί να είναι αντίθετη προς τα συμφέροντα της Ευρωπαϊκής Ένωσης ή ενός ή περισσοτέρων κρατών μελών της.

3. Οι ΔΠΕΕ φέρουν σήμανση διαβάθμισης ασφαλείας σύμφωνα με την παράγραφο 2. Μπορούν να φέρουν πρόσθετες σημάνσεις με τις οποίες ορίζεται ο τομέας δραστηριότητας με τον οποίο σχετίζονται, προσδιορίζεται ο φορέας προέλευσης, περιορίζεται η διανομή, περιορίζεται η χρήση ή δηλώνεται η δυνατότητα κοινοποίησης.

Άρθρο 3

Διαχείριση των διαβαθμίσεων

1. Οι αρμόδιες αρχές μεριμνούν για την ορθή διαβάθμιση των ΔΠΕΕ, το σαφή προσδιορισμό τους ως διαβαθμισμένων πληροφοριών, καθώς και για τη διατήρηση του επιπέδου διαβάθμισής τους μόνο για το διάστημα που είναι απαραίτητο.

2. Οι ΔΠΕΕ δεν λαμβάνουν χαμηλότερη διαβάθμιση ούτε αποχαρακτηρίζονται ούτε τροποποιείται ή αφαιρείται οποιαδήποτε από τις επισημάνσεις που αναφέρονται στο άρθρο 2 παράγραφος 3 χωρίς προηγούμενη γραπτή συγκατάθεση της πηγής προέλευσης.

3. Το Συμβούλιο εγκρίνει πολιτική ασφαλείας για τη δημιουργία ΔΠΕΕ η οποία θα περιλαμβάνει πρακτικό οδηγό των διαβαθμίσεων ασφαλείας.

Άρθρο 4

Προστασία διαβαθμισμένων πληροφοριών

1. Η προστασία των ΔΠΕΕ γίνεται σύμφωνα με την παρούσα απόφαση.

2. Ο κάτοχος κάθε ΔΠΕΕ είναι υπεύθυνος για την προστασία της σύμφωνα με την παρούσα απόφαση.

3. Όταν τα κράτη μέλη αποστέλλουν διαβαθμισμένες πληροφορίες με εθνική σήμανση διαβάθμισης ασφαλείας στις δομές ή τα δίκτυα της Ένωσης, το Συμβούλιο και η ΓΓΣ προστατεύουν τις πληροφορίες αυτές σύμφωνα με τις απαιτήσεις που ισχύουν για τις ΔΠΕΕ στο αντίστοιχο επίπεδο όπως ορίζεται στον πίνακα αντιστοιχίας των διαβαθμίσεων ασφαλείας του προσαρτήματος Β.

4. Ένα σύνολο ΔΠΕΕ μπορεί να δικαιολογεί επίπεδο προστασίας που να αντιστοιχεί σε υψηλότερη διαβάθμιση από αυτήν των επιμέρους στοιχείων του.

Άρθρο 5

Διαχείριση των κινδύνων κατά της ασφάλειας

1. Οι κίνδυνοι κατά των ΔΠΕΕ αντιμετωπίζονται στο πλαίσιο διαδικασίας. Η διαδικασία αυτή αποσκοπεί στον προσδιορισμό των γνωστών κινδύνων κατά της ασφάλειας, τον καθορισμό μέτρων ασφαλείας για τον περιορισμό των κινδύνων αυτών σε αποδεκτό επίπεδο σύμφωνα με τις βασικές αρχές και τις ελάχιστες προδιαγραφές της παρούσας απόφασης και στην εφαρμογή των εν λόγω μέτρων σύμφωνα με την έννοια της ασφάλειας εις βάθος όπως ορίζεται στο προσάρτημα Α. Η αποτελεσματικότητα των μέτρων τελεί υπό συνεχή αξιολόγηση.

2. Τα μέτρα ασφαλείας για την προστασία των ΔΠΕΕ καθ' όλη τη διάρκεια του κύκλου ζωής τους πρέπει να είναι ανάλογα ιδίως προς τη διαβάθμιση ασφαλείας τους, τη μορφή και τον όγκο των πληροφοριών ή του υλικού, την τοποθεσία και την κατασκευή των εγκαταστάσεων όπου ευρίσκονται ΔΠΕΕ και την επιτόπου εκτιμώμενη απειλή δόλιων και/ή εγκληματικών δραστηριοτήτων, συμπεριλαμβανομένης της κατασκοπείας, της δολιοφθοράς και της τρομοκρατίας.

3. Τα σχέδια έκτακτης ανάγκης λαμβάνουν υπόψη την ανάγκη προστασίας των ΔΠΕΕ σε καταστάσεις έκτακτης ανάγκης προκειμένου να εμποδίζονται η αναρμόδια πρόσβαση, η κοινολόγηση και η απώλεια ακεραιότητας ή διαθεσιμότητας.

4. Προληπτικά και επανορθωτικά μέτρα με στόχο να ελαχιστοποιούνται οι συνέπειες σοβαρών αστοχιών ή συμβάντων κατά το χειρισμό και την αποθήκευση ΔΠΕΕ πρέπει να περιλαμβάνονται στα σχέδια συνέχισης των δραστηριοτήτων.

Άρθρο 6

Εφαρμογή της παρούσας απόφασης

1. Εφόσον απαιτείται, το Συμβούλιο, κατόπιν συστάσεως της Επιτροπής Ασφαλείας, εγκρίνει πολιτικές ασφαλείας καθορίζοντας μέτρα για την εφαρμογή της παρούσας απόφασης.

2. Η Επιτροπή Ασφαλείας μπορεί να συμφωνήσει στο επίπεδό της κατευθυντήριες γραμμές ασφαλείας προκειμένου να συμπληρώσει ή να υποστηρίξει την παρούσα απόφαση και τις ενδεχόμενες πολιτικές ασφαλείας που εγκρίνει το Συμβούλιο.

Άρθρο 7

Ασφάλεια προσωπικού

1. Ως ασφάλεια προσωπικού νοείται η εφαρμογή μέτρων προκειμένου να εξασφαλίζεται ότι πρόσβαση στις ΔΠΕΕ επιτρέπεται μόνο στα πρόσωπα τα οποία έχουν:

— ανάγκη γνώσης,

— λάβει εξουσιοδότηση ασφαλείας του αντίστοιχου επιπέδου, εφόσον απαιτείται, και

— ενημερωθεί ως προς τις ευθύνες τους.

2. Οι διαδικασίες ελέγχου ασφαλείας του προσωπικού αποσκοπούν στην εξακρίβωση του κατά πόσον μπορεί να επιτραπεί σε ένα πρόσωπο, βάσει της νομιμοφροσύνης, της φερεγγυότητας και της αξιοπιστίας του, η πρόσβαση σε ΔΠΕΕ.

3. Όλα τα πρόσωπα εντός της ΓΓΣ των οποίων τα καθήκοντα καθιστούν αναγκαία την πρόσβαση σε ή τον χειρισμό ΔΠΕΕ με διαβάθμιση CONFIDENTIEL UE/EU CONFIDENTIAL ή υψηλότερη λαμβάνουν εξουσιοδότηση ασφαλείας του αντίστοιχου επιπέδου προτού τους επιτραπεί η πρόσβαση στις εν λόγω ΔΠΕΕ. Τα πρόσωπα αυτά πρέπει να έχουν λάβει άδεια από την αρμόδια για τους διορισμούς αρχή της ΓΓΣ για πρόσβαση σε ΔΠΕΕ με διαβάθμιση έως ένα συγκεκριμένο επίπεδο και έως μια συγκεκριμένη ημερομηνία.

4. Το αναφερόμενο στο άρθρο 15 παράγραφος 3 προσωπικό των κρατών μελών του οποίου τα καθήκοντα μπορεί να καθιστούν αναγκαία την πρόσβαση σε ΔΠΕΕ με διαβάθμιση CONFIDENTIEL UE/EU CONFIDENTIAL ή υψηλότερη λαμβάνει εξουσιοδότηση ασφαλείας του αντίστοιχου επιπέδου ή άλλη κατάλληλη εξουσιοδότηση βάσει των καθηκόντων του, σύμφωνα με τις εθνικές νομοθετικές και κανονιστικές διατάξεις, προτού του επιτραπεί η πρόσβαση στις εν λόγω ΔΠΕΕ.

5. Προτού τους επιτραπεί πρόσβαση σε ΔΠΕΕ και κατά τακτά χρονικά διαστήματα στη συνέχεια, όλα τα πρόσωπα ενημερώνονται και δηλώνουν ότι έχουν κατανοήσει σαφώς την ευθύνη τους να προστατεύουν τις ΔΠΕΕ σύμφωνα με την παρούσα απόφαση.

6. Οι διατάξεις εφαρμογής του παρόντος άρθρου περιέχονται στο παράρτημα I.

Άρθρο 8

Φυσική ασφάλεια

1. Φυσική ασφάλεια είναι η εφαρμογή φυσικών και τεχνικών μέτρων προστασίας προκειμένου να εμποδίζεται η αναρμόδια πρόσβαση σε ΔΠΕΕ.

2. Τα μέτρα φυσικής ασφαλείας σχεδιάζονται έτσι ώστε να μην επιτρέπεται η λαθραία ή βίαιη είσοδος αναρμοδίων, να αποτρέπονται, να παρεμποδίζονται και να ανιχνεύονται οι μη εξουσιοδοτημένες ενέργειες και να καθίσταται δυνατός ο διαχωρισμός του προσωπικού όσον αφορά την πρόσβασή του σε ΔΠΕΕ βάσει της «ανάγκης γνώσης». Τα μέτρα αυτά καθορίζονται βάσει διαδικασίας διαχείρισης κινδύνων.

3. Τα μέτρα φυσικής ασφάλειας τίθενται σε ισχύ για όλους τους χώρους, τα κτίρια, τα γραφεία, τις αίθουσες και άλλα μέρη όπου γίνεται ο χειρισμός ή η αποθήκευση ΔΠΕΕ, συμπεριλαμβανομένων των χώρων που στεγάζουν συστήματα επικοινωνίας και πληροφοριών, όπως ορίζονται στο άρθρο 10 παράγραφος 2.

4. Οι χώροι στους οποίους αποθηκεύονται ΔΠΕΕ με διαβάθμιση CONFIDENTIEL UE/EU CONFIDENTIAL ή υψηλότερη καθορίζονται ως χώροι ασφαλείας σύμφωνα με το παράρτημα II και εγκρίνονται από την αρμόδια αρχή ασφαλείας.

5. Μόνο εγκεκριμένος εξοπλισμός ή εγκεκριμένες συσκευές χρησιμοποιούνται για την προστασία ΔΠΕΕ σε επίπεδο CONFIDENTIEL UE/EU CONFIDENTIAL ή υψηλότερο.

6. Οι διατάξεις εφαρμογής του παρόντος άρθρου περιέχονται στο παράρτημα II.

Άρθρο 9

Διαχείριση διαβαθμισμένων πληροφοριών

1. Διαχείριση των διαβαθμισμένων πληροφοριών είναι η εφαρμογή διοικητικών μέτρων για τον έλεγχο των ΔΠΕΕ καθ' όλη τη διάρκεια του κύκλου ζωής τους με στόχο τη συμπλήρωση των μέτρων που προβλέπουν τα άρθρα 7, 8 και 10 και την κατ' αυτόν τον τρόπο συμβολή στην αποτροπή και ανίχνευση εσκεμμένων ή τυχαίων διαρροών ή απωλειών των εν λόγω πληροφοριών. Τα εν λόγω μέτρα αφορούν ειδικότερα τη δημιουργία, την καταχώριση, την αντιγραφή, τη μετάφραση, τον υποχαρακτηρισμό, τον αποχαρακτηρισμό, τη μεταφορά και την καταστροφή ΔΠΕΕ.

2. Οι πληροφορίες με διαβάθμιση CONFIDENTIEL UE/EU CONFIDENTIAL ή υψηλότερη καταχωρίζονται, για λόγους ασφαλείας, πριν από τη διανομή και κατά την παραλαβή. Οι αρμόδιες αρχές στη ΓΓΣ και τα κράτη μέλη καθιερώνουν γραμματειακό σύστημα προς τούτο. Πληροφορίες με διαβάθμιση TRÈS SECRET UE/EU TOP SECRET καταχωρίζονται σε ειδικές προς τούτο γραμματείες.

3. Οι υπηρεσίες και οι χώροι χειρισμού ή αποθήκευσης ΔΠΕΕ υπόκεινται σε τακτική επιθεώρηση από την αρμόδια αρχή ασφαλείας.

4. Οι ΔΠΕΕ διαβιβάζονται μεταξύ των υπηρεσιών και των εγκαταστάσεων που ευρίσκονται εκτός των περιοχών που τυγχάνουν φυσικής προστασίας ως εξής:

α) κατά κανόνα, οι ΔΠΕΕ διαβιβάζονται με ηλεκτρονικά μέσα προστατευόμενα με κρυπτογραφικά προϊόντα που έχουν εγκριθεί σύμφωνα με το άρθρο 10 παράγραφος 6,

β) όταν δεν χρησιμοποιούνται τα μέσα που αναφέρονται στο στοιχείο α), οι ΔΠΕΕ μεταφέρονται:

i) είτε με ηλεκτρονικά μέσα (π.χ. κλειδιά USB, CD, σκληρούς δίσκους) που προστατεύονται με κρυπτογραφικά προϊόντα εγκεκριμένα σύμφωνα με το άρθρο 10 παράγραφος 6, ή

ii) είτε, σε κάθε άλλη περίπτωση, όπως ορίζει η αρμόδια αρχή ασφαλείας σύμφωνα με τα σχετικά μέτρα προστασίας που ορίζονται στο παράρτημα III.

5. Οι διατάξεις εφαρμογής του παρόντος άρθρου περιέχονται στα παραρτήματα III και IV.

Άρθρο 10

Προστασία των ΔΠΕΕ που αποτελούν αντικείμενο χειρισμού σε συστήματα επικοινωνίας και πληροφοριών

1. Διασφάλιση των πληροφοριών (ΙΑ) στον τομέα των συστημάτων επικοινωνίας και πληροφοριών είναι η βεβαιότητα ότι τα συστήματα αυτά θα προστατεύουν τις πληροφορίες που χειρίζονται και θα λειτουργούν οσοδήποτε και οποτεδήποτε χρειάζεται υπό τον έλεγχο των νομίμων χρηστών. Η αποτελεσματική ΙΑ εξασφαλίζει κατάλληλα επίπεδα εμπιστευτικότητας, ακεραιότητας, μη άρνησης αναγνώρισης των πληροφοριών και γνησιότητας. Η ΙΑ βασίζεται σε διαδικασία διαχείρισης κινδύνων.

2. Ως «σύστημα επικοινωνίας και πληροφοριών» (CIS) νοείται οιοδήποτε σύστημα επιτρέπει τον χειρισμό πληροφοριών υπό ηλεκτρονική μορφή, με αυτόματα μέσα. Ένα CIS περιλαμβάνει το σύνολο των στοιχείων που απαιτούνται για τη λειτουργία του, συμπεριλαμβανομένων της υποδομής, της οργάνωσης, του προσωπικού και των πληροφοριών. Η παρούσα απόφαση εφαρμόζεται στα CIS που χειρίζονται ΔΠΕΕ.

3. Τα CIS χειρίζονται τις ΔΠΕΕ σύμφωνα με την έννοια της ΙΑ.

4. Όλα τα CIS υποβάλλονται σε διαδικασία έγκρισης της λειτουργίας. Η έγκριση λειτουργίας αποσκοπεί στη βεβαίωση ότι έχουν εφαρμοσθεί όλα τα ενδεδειγμένα μέτρα ασφαλείας και ότι έχει επιτευχθεί ικανοποιητικό επίπεδο προστασίας των ΔΠΕΕ και του CIS, σύμφωνα με την παρούσα απόφαση. Η δήλωση έγκρισης λειτουργίας καθορίζει το μέγιστο επιτρεπτό επίπεδο διαβάθμισης των πληροφοριών που μπορεί να χειρισθεί ένα CIS, καθώς και τους αντίστοιχους όρους και προϋποθέσεις.

5. Εφαρμόζονται μέτρα ασφαλείας για την προστασία CIS που χειρίζονται πληροφορίες με διαβάθμιση CONFIDENTIEL UE/EU CONFIDENTIAL και υψηλότερη από κάθε διαρροή τέτοιων πληροφοριών μέσω ακούσιων ηλεκτρομαγνητικών εκπομπών («μέτρα ασφαλείας TEMPEST»). Τα εν λόγω μέτρα ασφαλείας είναι ανάλογα με τον κίνδυνο εκμετάλλευσης και το επίπεδο διαβάθμισης των πληροφοριών.

6. Όταν η προστασία ΔΠΕΕ παρέχεται με κρυπτογραφικά προϊόντα, τα προϊόντα αυτά εγκρίνονται ως εξής:

α) η εμπιστευτικότητα των πληροφοριών με διαβάθμιση τουλάχιστον SECRET UE/UE SECRET προστατεύεται με κρυπτογραφικά προϊόντα που εγκρίνει το Συμβούλιο ως Αρχή Έγκρισης Κρυπτογραφικών Μεθόδων (CAA) κατόπιν συστάσεως της Επιτροπής Ασφαλείας,

β) η εμπιστευτικότητα των πληροφοριών με διαβάθμιση CONFIDENTIEL UE/EU CONFIDENTIAL ή RESTREINT UE/EU RESTRICTED προστατεύεται με κρυπτογραφικά προϊόντα που εγκρίνει ο γενικός γραμματέας του Συμβουλίου («γενικός γραμματέας») ως CAA, κατόπιν συστάσεως της Επιτροπής Ασφαλείας.

Παρά τα οριζόμενα στο στοιχείο β), στο πλαίσιο των εθνικών συστημάτων των κρατών μελών, η εμπιστευτικότητα των ΔΠΕΕ με διαβάθμιση CONFIDENTIEL UE/EU CONFIDENTIAL ή RESTREINT UE/EU RESTRICTED μπορεί να προστατεύεται με κρυπτογραφικά προϊόντα που εγκρίνει η CAA κράτους μέλους.

7. Κατά τη διαβίβαση ΔΠΕΕ με ηλεκτρονικά μέσα χρησιμοποιούνται εγκεκριμένα κρυπτογραφικά προϊόντα. Παρά την απαίτηση αυτή, μπορούν να χρησιμοποιούνται ειδικές διαδικασίες σε έκτακτες περιστάσεις ή ειδικές τεχνικές διαμορφώσεις όπως ορίζονται στο παράρτημα IV.

8. Οι αρμόδιες αρχές της ΓΓΣ και των κρατών μελών αντιστοίχως καθιερώνουν τις ακόλουθες λειτουργίες ΙΑ:

α) μια Αρχή ΙΑ,

β) μια Αρχή TEMPEST (TA),

γ) μια Αρχή Έγκρισης Κρυπτογραφικών Μεθόδων (CAA),

δ) μια Αρχή Διανομής Κρυπτογραφικών Μεθόδων (CDA).

9. Για κάθε σύστημα, οι αρμόδιες αρχές της ΓΓΣ και των κρατών μελών αντιστοίχως καθιερώνουν:

α) μια Αρχή Πιστοποίησης της Ασφάλειας (ΑΠΑ),

β) μια Επιχειρησιακή Αρχή ΙΑ.

10. Οι διατάξεις εφαρμογής του παρόντος άρθρου περιέχονται στο παράρτημα IV.

Άρθρο 11

Βιομηχανική ασφάλεια

1. Ως βιομηχανική ασφάλεια νοείται η εφαρμογή μέτρων διασφάλισης της προστασίας των ΔΠΕΕ από τους εργολάβους ή τους υπεργολάβους κατά τις διαπραγματεύσεις πριν από την ανάθεση της σύμβασης και καθ' όλη τη διάρκεια του κύκλου ζωής των διαβαθμισμένων συμβάσεων. Οι συμβάσεις αυτές δεν περιλαμβάνουν πρόσβαση σε πληροφορίες με διαβάθμιση TRÈS SECRET UE/EU TOP SECRET.

2. Η ΓΓΣ μπορεί να αναθέτει με σύμβαση σε βιομηχανικούς ή άλλους φορείς που έχουν την έδρα τους σε κράτος μέλος ή σε τρίτο κράτος που έχει συνάψει συμφωνία ή διοικητικό διακανονισμό σύμφωνα με το άρθρο 13 παράγραφος 2 στοιχείο α) ή β) καθήκοντα που αφορούν ή συνεπάγονται πρόσβαση σε ΔΠΕΕ ή τον χειρισμό ή την αποθήκευσή τους.

3. Κατά την ανάθεση διαβαθμισμένων συμβάσεων σε βιομηχανικούς ή άλλους φορείς, η ΓΓΣ διασφαλίζει, ως αναθέτουσα αρχή, ότι τηρούνται οι ελάχιστες προδιαγραφές βιομηχανικής ασφάλειας που καθορίζονται στην παρούσα απόφαση και αναφέρονται στη σύμβαση.

4. Η Εθνική Αρχή Ασφαλείας (ΕΑΑ), η Καθορισμένη Αρχή Ασφαλείας (ΚΑΑ) ή οποιαδήποτε άλλη αρμόδια αρχή κάθε κράτους μέλους εξασφαλίζει, στο βαθμό που επιτρέπεται δυνάμει εθνικών νομοθετικών και κανονιστικών διατάξεων, ότι οι εργολάβοι και οι υπεργολάβοι που έχουν την έδρα τους στο έδαφός τους λαμβάνουν άπαντα τα δέοντα μέτρα για την προστασία των ΔΠΕΕ κατά τις διαπραγματεύσεις πριν από την ανάθεση της σύμβασης και κατά την εκτέλεση διαβαθμισμένης σύμβασης.

5. Η ΕΑΑ, η ΚΑΑ ή οιαδήποτε άλλη αρμόδια αρχή ασφαλείας κάθε κράτους μέλους εξασφαλίζει, σύμφωνα με τις εθνικές νομοθετικές και κανονιστικές διατάξεις, ότι οι εργολάβοι ή υπεργολάβοι που έχουν την έδρα τους στο αντίστοιχο κράτος μέλος και συμμετέχουν σε διαβαθμισμένες συμβάσεις ή συμβάσεις υπεργολαβίας που απαιτούν την πρόσβαση σε πληροφορίες με διαβάθμιση CONFIDENTIEL UE/EU CONFIDENTIAL ή SECRET UE/EU SECRET μέσα στις εγκαταστάσεις τους, είτε κατά την εκτέλεση των συμβάσεων αυτών είτε κατά το προσυμβατικό στάδιο, πρέπει να διαθέτουν εξουσιοδότηση ασφαλείας φορέα (FSC) στο οικείο επίπεδο διαβάθμισης.

6. Οι υπάλληλοι του εργολάβου ή υπεργολάβου οι οποίοι, για την εκτέλεση διαβαθμισμένης σύμβασης, απαιτούν πρόσβαση σε πληροφορίες με διαβάθμιση CONFIDENTIEL UE/EU CONFIDENTIAL ή SECRET UE/EU SECRET λαμβάνουν εξουσιοδότηση ασφαλείας προσωπικού (ΕΑΠ) από την αντίστοιχη ΕΑΑ, ΚΑΑ ή άλλη αρμόδια αρχή σύμφωνα με τις εθνικές νομοθετικές και κανονιστικές διατάξεις και τις ελάχιστες προδιαγραφές που ορίζονται στο παράρτημα I.

7. Οι διατάξεις εφαρμογής του παρόντος άρθρου περιέχονται στο παράρτημα V.

Άρθρο 12

Κοινοποίηση ΔΠΕΕ

1. Το Συμβούλιο καθορίζει τους όρους υπό τους οποίους μπορεί να κοινοποιεί ΔΠΕΕ τις οποίες έχει στην κατοχή του σε άλλα θεσμικά και λοιπά όργανα ή οργανισμούς της Ένωσης. Προς το σκοπό αυτό μπορεί να προβλεφθεί κατάλληλο πλαίσιο, μεταξύ άλλων με τη σύναψη διοργανικών συμφωνιών ή άλλων σχετικών ρυθμίσεων, κατά περίπτωση.

2. Το σχετικό πλαίσιο εξασφαλίζει ότι οι ΔΠΕΕ λαμβάνουν κατάλληλη για το επίπεδο διαβάθμισής τους προστασία και σύμφωνα με βασικές αρχές και ελάχιστα πρότυπα ισοδύναμα με εκείνα που καθορίζονται στην παρούσα απόφαση.

Άρθρο 13

Ανταλλαγή διαβαθμισμένων πληροφοριών με τρίτα κράτη και διεθνείς οργανισμούς

1. Όταν το Συμβούλιο αποφασίζει ότι υπάρχει ανάγκη ανταλλαγής ΔΠΕΕ με τρίτο κράτος ή διεθνή οργανισμό, δημιουργείται το κατάλληλο πλαίσιο προς τούτο.

2. Προκειμένου να δημιουργηθεί το πλαίσιο αυτό και να ορισθούν αμοιβαίοι κανόνες για την προστασία των προς ανταλλαγή διαβαθμισμένων πληροφοριών:

α) η Ένωση συνάπτει συμφωνίες με τρίτα κράτη ή διεθνείς οργανισμούς σχετικά με διαδικασίες ασφαλείας για την ανταλλαγή και την προστασία διαβαθμισμένων πληροφοριών («συμφωνίες ασφαλείας πληροφοριών»), ή

β) ο γενικός γραμματέας μπορεί να συνάπτει διοικητικούς διακανονισμούς εξ ονόματος της ΓΓΣ σύμφωνα με την παράγραφο 17 του παραρτήματος VI εφόσον το επίπεδο διαβάθμισης των προς κοινοποίηση ΔΠΕΕ δεν είναι κατά κανόνα υψηλότερο από RESTREINT UE/EU RESTRICTED.

3. Οι συμφωνίες ασφαλείας πληροφοριών ή οι διοικητικοί διακανονισμοί που αναφέρονται στην παράγραφο 2 περιέχουν διατάξεις που εξασφαλίζουν ότι όταν τρίτα κράτη ή διεθνείς οργανισμοί λαμβάνουν ΔΠΕΕ, στις εν λόγω πληροφορίες παρέχεται η δέουσα προστασία για το επίπεδο διαβάθμισής τους και σύμφωνα με στοιχειώδεις προδιαγραφές τουλάχιστον ισοδύναμες με τις προδιαγραφές που ορίζονται στην παρούσα απόφαση.

4. Η απόφαση κοινολόγησης ΔΠΕΕ που προέρχονται από το Συμβούλιο σε τρίτο κράτος ή διεθνή οργανισμό λαμβάνεται από το Συμβούλιο κατά περίπτωση, ανάλογα με τη φύση και το περιεχόμενο των πληροφοριών, την ανάγκη γνώσης του παραλήπτη και τα σχετικά πλεονεκτήματα για την Ένωση. Εάν ο φορέας προέλευσης των διαβαθμισμένων πληροφοριών των οποίων ζητείται η κοινολόγηση δεν είναι το Συμβούλιο, τότε η ΓΓΣ ζητεί πρώτα τη γραπτή συγκατάθεση του εν λόγω φορέα. Εάν δεν μπορεί να εξακριβωθεί ο φορέας προέλευσης, τότε το Συμβούλιο αναλαμβάνει την ευθύνη αυτή.

5. Διοργανώνονται επισκέψεις αξιολόγησης για να εξακριβωθεί η αποτελεσματικότητα των μέτρων ασφαλείας που εφαρμόζονται σε τρίτο κράτος ή διεθνή οργανισμό για την προστασία των παρεχόμενων ή ανταλλασσόμενων ΔΠΕΕ.

6. Οι διατάξεις εφαρμογής του παρόντος άρθρου περιέχονται στο παράρτημα VI.

Άρθρο 14

Παραβιάσεις της ασφάλειας και διαρροή ΔΠΕΕ

1. Παραβίαση της ασφάλειας προκύπτει ως αποτέλεσμα πράξης ή παράλειψης προσώπου η οποία είναι αντίθετη προς τους κανονισμούς ασφαλείας της παρούσας οδηγίας.

2. Διαρροή ΔΠΕΕ προκύπτει όταν, εξαιτίας παραβίασης της ασφάλειας, αυτές κοινολογούνται εξ ολοκλήρου ή εν μέρει σε μη εξουσιοδοτημένα πρόσωπα.

3. Κάθε παραβίαση ή υπόνοια παραβίασης της ασφάλειας αναφέρεται αμέσως στην αρμόδια αρχή ασφαλείας.

4. Όταν είναι γνωστό ή υπάρχουν εύλογες υπόνοιες ότι επήλθε διαρροή ή απώλεια ΔΠΕΕ, η ΕΑΑ ή άλλη αρμόδια αρχή λαμβάνει όλα τα κατάλληλα μέτρα σύμφωνα με τις σχετικές νομοθετικές και κανονιστικές διατάξεις προκειμένου:

α) να ενημερωθεί ο φορέας προέλευσης,

β) να εξασφαλισθεί ότι η υπόθεση διερευνάται από προσωπικό που δεν σχετίζεται άμεσα με την παραβίαση προκειμένου να διαπιστωθούν τα πραγματικά περιστατικά,

γ) να αξιολογηθεί η τυχόν ζημία που προκλήθηκε στα συμφέροντα της Ένωσης ή των κρατών μελών,

δ) να ληφθούν τα κατάλληλα μέτρα για να αποτραπεί τυχόν επανάληψη και

ε) να ειδοποιηθούν οι αρμόδιες αρχές για τα ληφθέντα μέτρα.

5. Κάθε υπεύθυνος για παραβίαση των κανονισμών ασφαλείας της παρούσας απόφασης ενδέχεται να υποστεί πειθαρχικές κυρώσεις σύμφωνα με τους εφαρμοστέους κανόνες και κανονισμούς. Κάθε υπεύθυνος για διαρροή ή απώλεια ΔΠΕΕ υπόκειται σε πειθαρχικές κυρώσεις και/ή δικαστικές ενέργειες σύμφωνα με τους εφαρμοστέους νόμους, κανόνες και κανονισμούς.

Άρθρο 15

Ευθύνη της εκτέλεσης

1. Το Συμβούλιο λαμβάνει κάθε απαραίτητο μέτρο προκειμένου να εξασφαλίσει γενική συνοχή στην εφαρμογή της παρούσας απόφασης.

2. Ο γενικός γραμματέας λαμβάνει κάθε απαραίτητο μέτρο ώστε να εξασφαλισθεί ότι, κατά τον χειρισμό ή την αποθήκευση ΔΠΕΕ ή άλλων διαβαθμισμένων πληροφοριών, εφαρμόζεται η παρούσα απόφαση στους χώρους που χρησιμοποιεί το Συμβούλιο και εντός της ΓΓΣ, από τους υπαλλήλους και το λοιπό προσωπικό της ΓΓΣ, από το προσωπικό που έχει αποσπασθεί στη ΓΓΣ και από τους εργολήπτες της ΓΓΣ.

3. Τα κράτη μέλη λαμβάνουν κάθε κατάλληλο μέτρο, σύμφωνα με τους αντίστοιχους εθνικούς νόμους και κανονισμούς, προκειμένου να εξασφαλισθεί ότι, κατά το χειρισμό ή την αποθήκευση ΔΠΕΕ, τηρείται η παρούσα απόφαση από:

α) το προσωπικό των μόνιμων αντιπροσωπειών των κρατών μελών στην Ευρωπαϊκή Ένωση, καθώς και από τους εθνικούς αντιπροσώπους που συμμετέχουν σε συνόδους του Συμβουλίου ή συνεδριάσεις των προπαρασκευαστικών οργάνων του, ή λαμβάνουν μέρος σε άλλες δραστηριότητες του Συμβουλίου,

β) το λοιπό προσωπικό των κρατικών υπηρεσιών των κρατών μελών, συμπεριλαμβανομένου του προσωπικού που έχει αποσπασθεί σε αυτές τις κρατικές υπηρεσίες, ασχέτως του αν υπηρετούν στο έδαφος των κρατών μελών ή στο εξωτερικό,

γ) άλλα πρόσωπα στα κράτη μέλη δεόντως εξουσιοδοτημένα βάσει των καθηκόντων τους να έχουν πρόσβαση σε ΔΠΕΕ και

δ) εργολήπτες των κρατών μελών, είτε στο έδαφος των κρατών μελών είτε στο εξωτερικό.

Άρθρο 16

Η οργάνωση της ασφάλειας στο Συμβούλιο

1. Στα πλαίσια του καθήκοντός του για την εξασφάλιση γενικής συνοχής στην εφαρμογή της παρούσας απόφασης, το Συμβούλιο εγκρίνει:

α) συμφωνίες που αναφέρονται στο άρθρο 13 παράγραφος 2 στοιχείο α),

β) αποφάσεις που να επιτρέπουν ή να συγκατατίθενται στη διάθεση ΔΠΕΕ που προέρχονται από το Συμβούλιο ή βρίσκονται στην κατοχή του σε τρίτα κράτη και διεθνείς οργανισμούς σύμφωνα με την αρχή της συγκατάθεσης της πηγής προέλευσης,

γ) ετήσιο πρόγραμμα επισκέψεων αξιολόγησης που συνιστά η Επιτροπή Ασφαλείας για επισκέψεις αξιολόγησης των υπηρεσιών και των εγκαταστάσεων των κρατών μελών, καθώς και των λοιπών οργάνων, οργανισμών και μονάδων της Ένωσης που εφαρμόζουν την παρούσα απόφαση ή τις αρχές της, και επισκέψεις αξιολόγησης σε τρίτα κράτη και διεθνείς οργανισμούς προκειμένου να εξακριβωθεί η αποτελεσματικότητα των μέτρων που εφαρμόζονται για την προστασία των ΔΠΕΕ, και

δ) τις πολιτικές ασφαλείας που προβλέπονται στο άρθρο 6 παράγραφος 1.

2. Ο γενικός γραμματέας είναι η Αρχή Ασφαλείας της ΓΓΣ. Υπ' αυτή την ιδιότητα, ο γενικός γραμματέας:

α) μεριμνά για την εφαρμογή της πολιτικής ασφαλείας του Συμβουλίου και την περιοδική εξέτασή της,

β) συντονίζει με τις ΕΑΑ των κρατών μελών όλα τα θέματα ασφαλείας που αφορούν την προστασία των διαβαθμισμένων πληροφοριών σχετικά με τις δραστηριότητες του Συμβουλίου,

γ) χορηγεί στους υπαλλήλους της ΓΓΣ, στο λοιπό προσωπικό και στους αποσπασμένους εθνικούς εμπειρογνώμονες εξουσιοδότηση σύμφωνα με το άρθρο 7 παράγραφος 3 για πρόσβαση σε πληροφορίες με διαβάθμιση CONFIDENTIEL UE/EU CONFIDENTIAL ή υψηλότερη,

δ) διατάσσει, κατά περίπτωση, τη διερεύνηση οιασδήποτε πραγματικής ή εικαζόμενης διαρροής ή απώλειας διαβαθμισμένων πληροφοριών που κατέχει το Συμβούλιο ή προέρχονται από αυτό και ζητεί από τις αρμόδιες αρχές ασφαλείας να συνδράμουν στις έρευνες,

ε) αναλαμβάνει περιοδικές επιθεωρήσεις των ρυθμίσεων ασφαλείας για την προστασία των διαβαθμισμένων πληροφοριών στους χώρους της ΓΓΣ,

στ) αναλαμβάνει περιοδικές επισκέψεις για να αξιολογήσει τις ρυθμίσεις ασφαλείας για την προστασία των ΔΠΕΕ στους οργανισμούς, τις υπηρεσίες και τις μονάδες της Ένωσης που εφαρμόζουν την παρούσα απόφαση ή τις αρχές της,

ζ) αναλαμβάνει να πραγματοποιεί, από κοινού και σε συμφωνία με την ενδιαφερόμενη ΕΑΑ, περιοδικές αξιολογήσεις των ρυθμίσεων ασφαλείας για την προστασία των ΔΠΕΕ στις υπηρεσίες και τους χώρους των κρατών μελών,

η) εξασφαλίζει ότι τα μέτρα ασφαλείας συντονίζονται όπως απαιτείται με τις αρμόδιες αρχές των κρατών μελών που είναι υπεύθυνες για την προστασία των διαβαθμισμένων πληροφοριών και, ανάλογα με την περίπτωση, με τρίτα κράτη ή διεθνείς οργανισμούς, μεταξύ άλλων και για τη φύση των απειλών κατά της ασφάλειας των ΔΠΕΕ και τα μέσα προστασίας από αυτές και

θ) συνάπτει τους διοικητικούς διακανονισμούς που αναφέρονται στο άρθρο 13 παράγραφος 2 στοιχείο β).

Το Γραφείο Ασφαλείας της ΓΓΣ είναι στη διάθεση του γενικού γραμματέα για την παροχή βοήθειας σε αυτά τα καθήκοντα.

3. Για την εφαρμογή του άρθρου 15 παράγραφος 3, τα κράτη μέλη θα πρέπει:

α) να ορίσουν μια ΕΑΑ, όπως παρατίθεται στο προσάρτημα Γ, αρμόδια για τις ρυθμίσεις ασφαλείας σχετικά με την προστασία των ΔΠΕΕ, ώστε:

i) οι ΔΠΕΕ που ευρίσκονται στην κατοχή εθνικών φορέων, οργανισμών ή υπηρεσιών, δημόσιων ή ιδιωτικών, εντός της χώρας ή στο εξωτερικό, να προστατεύονται σύμφωνα με την παρούσα απόφαση,

ii) οι ρυθμίσεις ασφαλείας για την προστασία των ΔΠΕΕ να τυγχάνουν περιοδικής επιθεώρησης ή αξιολόγησης,

iii) όλα τα πρόσωπα που απασχολούνται σε κρατική υπηρεσία ή από εργολάβο και μπορούν να αποκτήσουν πρόσβαση στις πληροφορίες με διαβάθμιση τουλάχιστον CONFIDENTIEL UE/EU CONFIDENTIAL να έχουν λάβει τη δέουσα εξουσιοδότηση ασφαλείας ή άλλη κατάλληλη εξουσιοδότηση βάσει των καθηκόντων τους, σύμφωνα με τις εθνικές νομοθετικές και κανονιστικές διατάξεις,

iv) να σχεδιάζονται τα απαραίτητα προγράμματα ασφαλείας ώστε να ελαχιστοποιείται ο κίνδυνος διαρροής ή απώλειας ΔΠΕΕ,

v) τα θέματα ασφαλείας σχετικά με την προστασία των ΔΠΕΕ να συντονίζονται με άλλες αρμόδιες εθνικές αρχές, συμπεριλαμβανομένων των αναφερομένων στην παρούσα οδηγία και

vi) να δίνονται απαντήσεις στις κατάλληλες αιτήσεις ελέγχου ασφαλείας, ιδίως από τα λοιπά όργανα, τους οργανισμούς, τις μονάδες και τις επιχειρήσεις της Ένωσης που έχουν ιδρυθεί δυνάμει του τίτλου V κεφάλαιο 2 της ΣΕΕ, καθώς και από τους Ειδικούς Εντεταλμένους της ΕΕ (ΕΕΕΕ) και τις ομάδες τους που εφαρμόζουν την παρούσα απόφαση ή τις αρχές της,

β) να εξασφαλίζουν ότι οι αρμόδιες αρχές τους παρέχουν πληροφορίες και συμβουλές στις κυβερνήσεις τους και, μέσω αυτών, στο Συμβούλιο σχετικά με τη φύση των απειλών κατά της ασφάλειας των ΔΠΕΕ και τα μέσα προστασίας από αυτές.

Άρθρο 17

Επιτροπή Ασφαλείας

1. Συγκροτείται Επιτροπή Ασφαλείας. Εξετάζει και αξιολογεί κάθε θέμα ασφαλείας εντός του πεδίου εφαρμογής της παρούσας απόφασης και υποβάλλει συστάσεις στο Συμβούλιο, κατά περίπτωση.

2. Η Επιτροπή Ασφαλείας αποτελείται από αντιπροσώπους των ΕΑΑ των κρατών μελών και στις συνεδριάσεις της συμμετέχει αντιπρόσωπος της Επιτροπής και της ΕΥΕΔ. Προεδρεύεται από τον γενικό γραμματέα ή από τον ορισθέντα αντιπρόσωπό του. Συνέρχεται δε σύμφωνα με τις οδηγίες του Συμβουλίου ή κατόπιν αιτήματος του γενικού γραμματέα ή μιας ΕΑΑ.

Οι αντιπρόσωποι των λοιπών οργάνων, οργανισμών και μονάδων της Ένωσης που εφαρμόζουν την παρούσα απόφαση ή τις αρχές της μπορούν να κληθούν να συμμετάσχουν όταν συζητούνται θέματα που τους αφορούν.

3. Η Επιτροπή Ασφαλείας οργανώνει τις δραστηριότητές της κατά τρόπο ώστε να μπορεί να υποβάλλει συστάσεις για ειδικούς τομείς ασφαλείας. Καθιερώνει υποομάδα εμπειρογνωμόνων για θέματα ΙΑ και άλλες υποομάδες εμπειρογνωμόνων κατά περίπτωση. Ορίζει τα καθήκοντα αυτών των υποομάδων και οι εμπειρογνώμονες της υποβάλλουν εκθέσεις σχετικά με τις δραστηριότητές τους συμπεριλαμβανομένων, ανάλογα με την περίπτωση, τυχόν συστάσεων προς το Συμβούλιο.

Άρθρο 18

Αντικατάσταση της προηγούμενης απόφασης

1. Η παρούσα απόφαση καταργεί και αντικαθιστά την απόφαση 2011/292/ΕΕ του Συμβουλίου ([1]).

2. Όλες οι ΔΠΕΕ που διαβαθμίζονται σύμφωνα με την απόφαση 2001/264/ΕΚ του Συμβουλίου ([2]) και την απόφαση 2011/292/ΕΕ εξακολουθούν να προστατεύονται σύμφωνα με τις σχετικές διατάξεις της παρούσας απόφασης.

Άρθρο 19

Έναρξη ισχύος

Η παρούσα απόφαση αρχίζει να ισχύει από την ημέρα της δημοσίευσής της στην *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης*.

Βρυξέλλες, 23 Σεπτεμβρίου 2013.

Για το Συμβούλιο

Ο Πρόεδρος

V. JUKNA

([1]) Απόφαση 2011/292/ΕΕ του Συμβουλίου, της 31ης Μαρτίου 2011, σχετικά με τους κανονισμούς ασφαλείας για την προστασία των διαβαθμισμένων πληροφοριών της ΕΕ (ΕΕ L 141 της 27.5.2011, σ. 17).

([2]) Απόφαση 2001/264/ΕΚ του Συμβουλίου, της 19ης Μαρτίου 2001, για την έγκριση κανονισμών ασφαλείας του Συμβουλίου (ΕΕ L 101 της 11.4.2001, σ. 1).

ΠΑΡΑΡΤΗΜΑΤΑ

ΠΑΡΑΡΤΗΜΑ I

Ασφάλεια προσωπικού

ΠΑΡΑΡΤΗΜΑ II

Φυσική ασφάλεια

ΠΑΡΑΡΤΗΜΑ III

Διαχείριση διαβαθμισμένων πληροφοριών

ΠΑΡΑΡΤΗΜΑ IV

Προστασία των ΔΠΕΕ που αποτελούν αντικείμενο χειρισμού σε CIS

ΠΑΡΑΡΤΗΜΑ V

Βιομηχανική ασφάλεια

ΠΑΡΑΡΤΗΜΑ VI

Ανταλλαγή διαβαθμισμένων πληροφοριών με τρίτα κράτη και διεθνείς οργανισμούς

ΠΑΡΑΡΤΗΜΑ I

ΑΣΦΑΛΕΙΑ ΠΡΟΣΩΠΙΚΟΥ

I. ΕΙΣΑΓΩΓΗ

1. Το παρόν παράρτημα περιέχει διατάξεις για την εφαρμογή του άρθρου 7. Παραθέτει κριτήρια προκειμένου να καθοριστεί σχετικά με ένα πρόσωπο, λαμβάνοντας υπόψη τη νομιμοφροσύνη, τη φερεγγυότητα και την αξιοπιστία του, αν είναι δυνατόν να του επιτραπεί η πρόσβαση σε ΔΠΕΕ και οι διερευνητικές και διοικητικές διαδικασίες που ακολουθούνται εν προκειμένω.

II. ΧΟΡΗΓΗΣΗ ΑΔΕΙΑΣ ΠΡΟΣΒΑΣΗΣ ΣΕ ΔΠΕΕ

2. Ένα πρόσωπο λαμβάνει άδεια πρόσβασης σε διαβαθμισμένες πληροφορίες μόνον εφόσον:

α) έχει προσδιορισθεί η ανάγκη γνώσης του,

β) έχει ενημερωθεί για τους κανόνες και τις διαδικασίες ασφαλείας για την προστασία των ΔΠΕΕ και έχει αναγνωρίσει τις ευθύνες του όσον αφορά την προστασία των πληροφοριών αυτών και

γ) προκειμένου για πληροφορίες με διαβάθμιση CONFIDENTIEL UE/EU CONFIDENTIAL ή υψηλότερη:

— του έχει χορηγηθεί ΕΑΠ αντίστοιχου επιπέδου ή έχει λάβει άλλη δέουσα εξουσιοδότηση βάσει των καθηκόντων του, σύμφωνα με τις εθνικές νομοθετικές και κανονιστικές διατάξεις, ή

— στην περίπτωση των υπαλλήλων της ΓΓΣ, του λοιπού προσωπικού ή αποσπασμένων εθνικών εμπειρογνωμόνων, έχει λάβει άδεια πρόσβασης σε ΔΠΕΕ από την αρμόδια για τους διορισμούς αρχή της ΓΓΣ σύμφωνα με τις παραγράφους 16 έως 25 έως ένα συγκεκριμένο επίπεδο και έως μια συγκεκριμένη ημερομηνία.

3. Κάθε κράτος μέλος και η ΓΓΣ προσδιορίζουν τις θέσεις στο πλαίσιο της δομής τους που απαιτούν πρόσβαση σε πληροφορίες με διαβάθμιση CONFIDENTIEL UE/EU CONFIDENTIAL ή υψηλότερη και, ως εκ τούτου, απαιτούν εξουσιοδότηση ασφαλείας του αντίστοιχου επιπέδου.

III. ΑΠΑΙΤΗΣΕΙΣ ΕΛΕΓΧΟΥ ΑΣΦΑΛΕΙΑΣ ΠΡΟΣΩΠΙΚΟΥ

4. Αφού παραλάβουν δεόντως εξουσιοδοτημένη αίτηση, οι ΕΑΑ ή άλλες αρμόδιες εθνικές αρχές έχουν την ευθύνη για την εξασφάλιση της διεξαγωγής ερευνών ασφαλείας επί των υπηκόων τους οι οποίοι ζητούν πρόσβαση σε πληροφορίες με διαβάθμιση CONFIDENTIEL UE/EU CONFIDENTIAL ή υψηλότερη. Οι προδιαγραφές της έρευνας είναι σύμφωνες με τις εθνικές νομοθετικές και κανονιστικές διατάξεις σχετικά με την έκδοση ΕΑΠ ή την παροχή εγγύησης για το πρόσωπο στο οποίο θα χορηγηθεί εξουσιοδότηση πρόσβασης σε ΔΠΕΕ, κατά περίπτωση.

5. Εάν ο ενδιαφερόμενος κατοικεί στο έδαφος άλλου κράτους μέλους ή τρίτου κράτους, οι αρμόδιες εθνικές αρχές ζητούν τη συνδρομή της αρμόδιας αρχής του κράτους κατοικίας σύμφωνα με τις εθνικές νομοθετικές και κανονιστικές διατάξεις. Τα κράτη μέλη αλληλοβοηθούνται στη διεξαγωγή των ερευνών ασφαλείας σύμφωνα με τις εθνικές νομοθετικές και κανονιστικές διατάξεις.

6. Όπου επιτρέπεται βάσει των εθνικών νομοθετικών και κανονιστικών διατάξεων, οι ΕΑΑ ή άλλες αρμόδιες εθνικές αρχές μπορούν να διεξάγουν έρευνες ασφαλείας επί προσώπων που δεν είναι υπήκοοι του οικείου κράτους και που ζητούν πρόσβαση σε πληροφορίες με διαβάθμιση CONFIDENTIEL UE/EU CONFIDENTIAL ή υψηλότερη. Οι προδιαγραφές της έρευνας είναι σύμφωνες με τις εθνικές νομοθετικές και κανονιστικές διατάξεις.

Κριτήρια έρευνας ασφαλείας

7. Η νομιμοφροσύνη, η φερεγγυότητα και η αξιοπιστία ενός προσώπου για τους σκοπούς της λήψης εξουσιοδότησης ασφαλείας για την πρόσβαση σε πληροφορίες με διαβάθμιση CONFIDENTIEL UE/EU CONFIDENTIAL ή υψηλότερη ελέγχονται με έρευνα ασφαλείας. Η αρμόδια εθνική αρχή προβαίνει σε γενική αξιολόγηση βάσει των πορισμάτων της εν λόγω έρευνας ασφαλείας. Τα κυριότερα κριτήρια που χρησιμοποιούνται προς τούτο περιλαμβάνουν, στο βαθμό που είναι δυνατόν βάσει των εθνικών νομοθετικών και κανονιστικών διατάξεων, εξέταση του αν ο ενδιαφερόμενος:

α) έχει διαπράξει ή αποπειραθεί να διαπράξει, συνωμοτήσει με άλλον ή βοηθήσει και υποκινήσει άλλον να διαπράξει πράξη κατασκοπείας, τρομοκρατίας, δολιοφθοράς, προδοσίας ή στάσης,

β) είναι ή υπήρξε συνεργάτης κατασκόπων, τρομοκρατών, δολιοφθορέων, ή προσώπων για τα οποία υπάρχουν σχετικές εύλογες υπόνοιες ή συνεργάτης εκπροσώπων οργανισμών ή ξένων κρατών, συμπεριλαμβανομένων των ξένων υπηρεσιών πληροφοριών, που ενδέχεται να απειλήσουν την ασφάλεια της Ένωσης και/ή κρατών μελών, εκτός εάν οι συνεργασίες αυτές είχαν επιτραπεί στα πλαίσια επισήμων καθηκόντων,

γ) είναι ή υπήρξε μέλος οργάνωσης η οποία με βίαια, ανατρεπτικά ή άλλα παράνομα μέσα επιδιώκει μεταξύ άλλων την ανατροπή της κυβέρνησης κράτους μέλους, την αλλαγή της συνταγματικής τάξης κράτους μέλους ή τη μεταβολή της μορφής ή των πολιτικών της κυβέρνησής του,

δ) είναι ή υπήρξε υποστηρικτής οργάνωσης που περιγράφεται στο στοιχείο γ) ή συνδέεται ή συνδεόταν στενά με μέλη τέτοιων οργανώσεων,

ε) έχει εσκεμμένα αποκρύψει ή παραστήσει ψευδώς ή παραποιήσει σημαντικές πληροφορίες, ιδίως για θέματα ασφαλείας, ή έχει εσκεμμένα δηλώσει ψευδή στοιχεία κατά τη συμπλήρωση του ερωτηματολογίου ασφαλείας προσωπικού, ή κατά τη διάρκεια συνέντευξης ασφαλείας,

στ) έχει καταδικασθεί για ένα ή περισσότερα ποινικά αδικήματα,

ζ) έχει ιστορικό αλκοολισμού, χρήσης παράνομων ναρκωτικών ουσιών και/ή κατάχρησης νόμιμων ουσιών,

η) επιδεικνύει ή έχει επιδείξει διαγωγή που μπορεί να εκθέσει το άτομο αυτό σε κίνδυνο εκβιασμού ή άσκησης πιέσεων,

θ) έχει επιδείξει με έργα ή λόγια ανεντιμότητα, έλλειψη νομιμοφροσύνης, αναξιοπιστία ή αφερεγγυότητα,

ι) έχει υποπέσει σε σοβαρές ή επανειλημμένες παραβάσεις κανονισμών ασφαλείας ή έχει επιχειρήσει, ή και πραγματοποιήσει, μη εξουσιοδοτημένες ενέργειες σε σχέση με συστήματα επικοινωνίας και πληροφοριών και

ια) μπορεί να είναι εκτεθειμένος σε πιέσεις (π.χ. επειδή διαθέτει μία ή περισσότερες ιθαγένειες εκτός ΕΕ ή μέσω συγγενών ή στενών συνεργατών οι οποίοι ενδέχεται να είναι ευάλωτοι έναντι ξένων υπηρεσιών πληροφοριών, τρομοκρατικών ομάδων ή άλλων ανατρεπτικών οργανώσεων ή ατόμων οι σκοποί των οποίων μπορεί να θέσουν σε κίνδυνο τα συμφέροντα ασφαλείας της Ένωσης και/ή κρατών μελών).

8. Ανάλογα με την περίπτωση και σύμφωνα με τις εθνικές νομοθετικές και κανονιστικές διατάξεις, το οικονομικό υπόβαθρο και το ιατρικό ιστορικό ενός ατόμου μπορούν επίσης να θεωρηθούν ότι έχουν σημασία στο πλαίσιο της έρευνας ασφαλείας.

9. Ανάλογα με την περίπτωση και σύμφωνα με τις εθνικές νομοθετικές και κανονιστικές διατάξεις, η συμπεριφορά και η οικονομική κατάσταση συζύγου, συγκατοίκου ή στενού συγγενούς μπορούν επίσης να θεωρηθούν ότι έχουν σημασία στο πλαίσιο της έρευνας ασφαλείας.

Απαιτήσεις έρευνας για την πρόσβαση σε ΔΠΕΕ

Αρχική χορήγηση εξουσιοδότησης ασφαλείας

10. Η αρχική εξουσιοδότηση ασφαλείας για πρόσβαση σε πληροφορίες με διαβάθμιση CONFIDENTIEL UE/EU CONFIDENTIAL και SECRET UE/EU SECRET βασίζεται σε έρευνα ασφαλείας που καλύπτει τουλάχιστον την τελευταία πενταετία, ή το διάστημα αφότου ο ενδιαφερόμενος έκλεισε τα 18, εφόσον είναι συντομότερο, και η οποία περιλαμβάνει τα ακόλουθα:

α) τη συμπλήρωση εθνικού ερωτηματολογίου ασφαλείας προσωπικού για το επίπεδο των ΔΠΕΕ στο οποίο μπορεί να ζητεί πρόσβαση το άτομο· αφού συμπληρωθεί, το εν λόγω ερωτηματολόγιο διαβιβάζεται στην αρμόδια αρχή ασφαλείας,

β) έλεγχο ταυτότητας/ιθαγένειας/εθνικότητας —επαληθεύονται η ημερομηνία και ο τόπος γέννησης του ατόμου και εξακριβώνεται η ταυτότητά του— ελέγχεται η κατάστασή του ως προς την ιθαγένειά του και/ή την εθνικότητά του, σημερινή και παλαιότερη· αξιολογείται το ενδεχόμενο να είναι το άτομο αυτό ευάλωτο σε πιέσεις από ξένες πηγές, για παράδειγμα λόγω προηγούμενης διαμονής του ή προηγούμενων σχέσεών του, και

γ) έλεγχο εθνικών και τοπικών αρχείων — ελέγχονται τα εθνικά αρχεία ασφαλείας και τα κεντρικά ποινικά μητρώα, όταν υπάρχουν, και/ή άλλα συγκρίσιμα κρατικά ή αστυνομικά αρχεία. Ελέγχονται επίσης τα αρχεία των αρχών επιβολής του νόμου που διαθέτουν νομική δικαιοδοσία στους τόπους όπου έχει διαμείνει ή εργασθεί το πρόσωπο.

11. Η αρχική εξουσιοδότηση ασφαλείας για πρόσβαση σε πληροφορίες με διαβάθμιση TRÈS SECRET UE/EU TOP SECRET βασίζεται σε έρευνα ασφαλείας που καλύπτει τουλάχιστον την τελευταία δεκαετία, ή το διάστημα αφότου ο ενδιαφερόμενος έκλεισε τα 18, εφόσον είναι συντομότερο. Όταν διεξάγονται συνεντεύξεις κατά τα προβλεπόμενα στο στοιχείο ε), οι έρευνες οφείλουν να καλύπτουν τουλάχιστον την τελευταία επταετία ή το διάστημα αφότου ο ενδιαφερόμενος έκλεισε τα 18, εφόσον είναι συντομότερο. Πέραν των κριτηρίων της ανωτέρω παραγράφου 7, διερευνώνται και τα ακόλουθα στοιχεία προτού χορηγηθεί ΕΑΠ TRÈS SECRET UE/EU TOP SECRET· μπορούν επίσης να διερευνώνται και προτού χορηγηθεί ΕΑΠ CONFIDENTIEL UE/EU CONFIDENTIAL ή SECRET UE/EU SECRET, εφόσον το απαιτούν οι εθνικές νομοθετικές και κανονιστικές διατάξεις:

α) οικονομική κατάσταση — ζητούνται πληροφορίες σχετικά με τα οικονομικά του ατόμου, προκειμένου να εκτιμηθεί αν θα ήταν ευάλωτος σε πιέσεις από το εσωτερικό ή το εξωτερικό λόγω σοβαρών οικονομικών δυσχερειών ή να αποκαλυφθεί τυχόν ανεξήγητη ευμάρεια,

β) μόρφωση — ζητούνται πληροφορίες σχετικά με το ιστορικό της εκπαίδευσης του ατόμου σε σχολεία, πανεπιστήμια και άλλα εκπαιδευτικά ιδρύματα στα οποία φοίτησε μετά τα 18, ή επί όποιο χρονικό διάστημα κρίνει πρέπον η διερευνώσα αρχή,

γ) απασχόληση — ζητούνται πληροφορίες σχετικά με τη σημερινή και παλαιότερη απασχόληση, βάσει πηγών όπως βιβλιάρια εργασίας, εκθέσεις απόδοσης ή κρίσης και επαφών με εργοδότες και προϊσταμένους,

δ) στρατιωτική θητεία — όταν συντρέχει περίπτωση, ελέγχεται η εκπλήρωση των στρατιωτικών υποχρεώσεων του ατόμου και ο τρόπος απόλυσής του, και

ε) συνεντεύξεις —εφόσον προβλέπονται και επιτρέπονται σύμφωνα με τους εθνικούς νόμους και κανονισμούς— πραγματοποιείται μία ή περισσότερες συνεντεύξεις με τον ενδιαφερόμενο· συνεντεύξεις διενεργούνται επίσης με άλλα πρόσωπα που είναι σε θέση να εκφέρουν αμερόληπτη γνώμη για το παρελθόν, τις δραστηριότητες, τη νομιμοφροσύνη, τη φερεγγυότητα και την αξιοπιστία του ατόμου. Όταν είθισται σύμφωνα με την εθνική πρακτική να ζητείται από το υποκείμενο της έρευνας να υποδεικνύει άλλα άτομα για συστάσεις, διεξάγονται συνεντεύξεις και με αυτά, εκτός αν υπάρχουν βάσιμοι λόγοι για το αντίθετο.

12. Εφόσον είναι απαραίτητο και σύμφωνα με τις εθνικές νομοθετικές και κανονιστικές διατάξεις, μπορούν να διεξάγονται επιπλέον έρευνες ώστε να μελετηθούν όλες οι διαθέσιμες σχετικές με το άτομο πληροφορίες και να επιβεβαιωθούν ή να διαψευσθούν τα δυσμενή στοιχεία.

Ανανέωση των εξουσιοδοτήσεων ασφαλείας

13. Μετά την αρχική εξουσιοδότηση ασφαλείας και υπό τον όρο ότι το άτομο εξακολουθεί αδιαλείπτως να εργάζεται για λογαριασμό κρατικής υπηρεσίας ή στη ΓΓΣ και εξακολουθεί να έχει ανάγκη πρόσβασης σε ΔΠΕΕ, η εξουσιοδότηση ασφαλείας επανεξετάζεται με σκοπό την ανανέωση κατόπιν χρονικού διαστήματος το πολύ πενταετίας στην περίπτωση διαβάθμισης TRÈS SECRET UE/EU TOP SECRET και δεκαετίας στην περίπτωση διαβαθμίσεων SECRET UE/EU SECRET και CONFIDENTIEL UE/EU CONFIDENTIAL, με ισχύ από την ημερομηνία ανακοίνωσης του αποτελέσματος της τελευταίας έρευνας ασφαλείας στην οποία βασίστηκε. Όλες οι έρευνες ασφαλείας για την ανανέωση της εξουσιοδότησης ασφαλείας καλύπτουν το διάστημα που διέρρευσε από την προηγούμενη παρόμοια έρευνα.

14. Για την ανανέωση των εξουσιοδοτήσεων ασφαλείας, διερευνώνται τα στοιχεία που περιγράφονται στις παραγράφους 10 και 11.

15. Οι αιτήσεις ανανέωσης υποβάλλονται εγκαίρως λαμβάνοντας υπόψη το διάστημα που απαιτείται για έρευνες ασφαλείας. Ωστόσο, όταν η αρμόδια ΕΑΑ ή άλλη αρμόδια εθνική αρχή έχει λάβει τη σχετική αίτηση ανανέωσης και το αντίστοιχο ερωτηματολόγιο ασφαλείας προσωπικού πριν από τη λήξη μιας εξουσιοδότησης ασφαλείας και η απαραίτητη έρευνα ασφαλείας δεν έχει ολοκληρωθεί, η αρμόδια εθνική αρχή δύναται, εφόσον το επιτρέπουν οι εθνικές νομοθετικές και κανονιστικές διατάξεις, να παρατείνει την ισχύ της τρέχουσας εξουσιοδότησης ασφαλείας για διάστημα έως 12 μηνών. Εάν, στο τέλος αυτού του νέου δωδεκάμηνου διαστήματος, δεν έχει ακόμα ολοκληρωθεί η έρευνα ασφαλείας, ανατίθενται στο άτομο μόνο καθήκοντα που δεν απαιτούν εξουσιοδότηση ασφαλείας.

Διαδικασίες εξουσιοδοτήσεων στη ΓΓΣ

16. Όσον αφορά τους υπαλλήλους και το λοιπό προσωπικό της ΓΓΣ, η Αρχή Ασφαλείας της ΓΓΣ διαβιβάζει το συμπληρωμένο ερωτηματολόγιο ασφαλείας προσωπικού στην ΕΑΑ του κράτους μέλους του οποίου το άτομο έχει την ιθαγένεια, αιτούμενη να διεξαχθεί έρευνα ασφαλείας για το επίπεδο των ΔΠΕΕ στο οποίο το άτομο θα ζητήσει πρόσβαση.

17. Όταν πληροφορίες σημαντικές για έρευνα ασφαλείας γίνονται γνωστές στη ΓΓΣ σχετικά με πρόσωπο που έχει υποβάλει αίτηση για εξουσιοδότηση ασφαλείας για πρόσβαση σε ΔΠΕΕ, η ΓΓΣ, ενεργώντας σύμφωνα με τους οικείους κανόνες και κανονισμούς, ειδοποιεί σχετικά την αρμόδια ΕΑΑ.

18. Μετά την ολοκλήρωση της έρευνας ασφαλείας, η αρμόδια ΕΑΑ κοινοποιεί στην Αρχή Ασφαλείας της ΓΓΣ τα αποτελέσματα της εν λόγω έρευνας χρησιμοποιώντας το τυποποιημένο έντυπο αλληλογραφίας που έχει ορίσει η Επιτροπή Ασφαλείας.

α) Όταν η έρευνα ασφαλείας καταλήγει στη διαβεβαίωση ότι δεν είναι γνωστό τίποτε αρνητικό που θα έθετε υπό αμφισβήτηση τη νομιμοφροσύνη, τη φερεγγυότητα και την αξιοπιστία του προσώπου, η αρμόδια για τους διορισμούς αρχή της ΓΓΣ μπορεί να χορηγήσει στον ενδιαφερόμενο εξουσιοδότηση για πρόσβαση σε ΔΠΕΕ και να επιτρέψει την πρόσβαση σε ΔΠΕΕ έως το αντίστοιχο επίπεδο και έως συγκεκριμένη ημερομηνία.

β) Όταν η έρευνα ασφαλείας δεν καταλήγει σε αυτή τη διαβεβαίωση, η αρμόδια για τους διορισμούς αρχή της ΓΓΣ ειδοποιεί τον ενδιαφερόμενο, ο οποίος μπορεί να ζητήσει ακρόαση από την αρμόδια για τους διορισμούς αρχή. Η αρμόδια για τους διορισμούς αρχή δύναται να ζητήσει από την αρμόδια ΕΑΑ οποιεσδήποτε περαιτέρω διευκρινίσεις μπορεί να της δώσει σύμφωνα με τις εθνικές νομοθετικές και κανονιστικές διατάξεις. Εάν επιβεβαιωθεί το αποτέλεσμα, δεν χορηγείται εξουσιοδότηση για πρόσβαση σε ΔΠΕΕ.

19. Η έρευνα ασφαλείας μαζί με τα πορίσματά της υπόκειται στις νομοθετικές και κανονιστικές διατάξεις που ισχύουν εν προκειμένω στο οικείο κράτος μέλος, περιλαμβανομένων εκείνων που αφορούν την άσκηση προσφυγών. Κατά των αποφάσεων της αρμόδιας για τους διορισμούς αρχής της ΓΓΣ μπορούν να ασκηθούν προσφυγές σύμφωνα με τον κανονισμό υπηρεσιακής κατάστασης των υπαλλήλων της Ευρωπαϊκής Ένωσης και το καθεστώς που εφαρμόζεται επί του λοιπού προσωπικού της Ευρωπαϊκής Ένωσης, όπως ορίζεται στον κανονισμό (ΕΟΚ, Ευρατόμ, ΕΚΑΧ) αριθ. 259/68 του Συμβουλίου ([1]) («κανονισμός υπηρεσιακής κατάστασης των υπαλλήλων της Ευρωπαϊκής Ένωσης και καθεστώς που εφαρμόζεται επί του λοιπού προσωπικού της Ευρωπαϊκής Ένωσης»).

20. Οι εθνικοί εμπειρογνώμονες που είναι αποσπασμένοι στη ΓΓΣ σε θέση που απαιτεί πρόσβαση σε ΔΠΕΕ με διαβάθμιση CONFIDENTIEL UE/EU CONFIDENTIAL ή υψηλότερη επιδεικνύουν έγκυρο πιστοποιητικό εξουσιοδότησης ασφαλείας προσωπικού (ΠΕΑΠ) για πρόσβαση σε ΔΠΕΕ στην Αρχή Ασφαλείας της ΓΓΣ προτού αναλάβουν καθήκοντα, βάσει της οποίας η αρμόδια για τους διορισμούς αρχή χορηγεί εξουσιοδότηση πρόσβασης σε ΔΠΕΕ.

21. Η ΓΓΣ κάνει δεκτή την εξουσιοδότηση για πρόσβαση σε ΔΠΕΕ που χορηγείται από οποιοδήποτε άλλο θεσμικό ή λοιπό όργανο ή οργανισμό της Ένωσης, εφόσον διατηρεί την ισχύ της. Η εξουσιοδότηση θα καλύπτει την ανάθεση οιουδήποτε καθήκοντος στον ενδιαφερόμενο εντός της ΓΓΣ. Το θεσμικό ή λοιπό όργανο ή οργανισμός της Ένωσης στην οποία προσλαμβάνεται το πρόσωπο ενημερώνει την αρμόδια ΕΑΑ σχετικά με την αλλαγή του εργοδότη.

22. Αν η περίοδος υπηρεσίας του ατόμου δεν αρχίσει εντός 12 μηνών από την ανακοίνωση του αποτελέσματος της έρευνας ασφαλείας στην αρμόδια για τους διορισμούς αρχή της ΓΓΣ ή αν υπάρξει διακοπή 12 μηνών στην υπηρεσία του, κατά το οποίο διάστημα δεν έχει υπηρετήσει στη ΓΓΣ ή σε θέση της κρατικής διοίκησης κράτους μέλους, το αποτέλεσμα παραπέμπεται στη σχετική ΕΕΑ προκειμένου να επιβεβαιωθεί ότι εξακολουθεί να ισχύει.

([1]) Κανονισμός (ΕΟΚ, Ευρατόμ, ΕΚΑΧ) αριθ. 259/68 του Συμβουλίου, της 29ης Φεβρουαρίου 1968, περί καθορισμού του κανονισμού υπηρεσιακής καταστάσεως των υπαλλήλων και του καθεστώτος που εφαρμόζεται επί του λοιπού προσωπικού των Ευρωπαϊκών Κοινοτήτων και περί θεσπίσεως ειδικών μέτρων προσωρινώς εφαρμοστέων στους υπαλλήλους της Επιτροπής (ΕΕ L 56 της 4.3.1968, σ. 1).

23. Όταν η ΓΓΣ λάβει γνώση της ύπαρξης κινδύνου κατά της ασφάλειας εκ μέρους προσώπου που διαθέτει εξουσιοδότηση πρόσβασης σε ΔΠΕΕ, η ΓΓΣ, ενεργώντας σύμφωνα με τους οικείους κανόνες και κανονισμούς, ειδοποιεί σχετικά την αρμόδια ΕΑΑ και δύναται να ανακαλεί την πρόσβαση σε ΔΠΕΕ ή να αποσύρει την εξουσιοδότηση πρόσβασης σε ΔΠΕΕ.

24. Όταν μια ΕΑΑ κοινοποιεί στη ΓΓΣ την ανάκληση της διαβεβαίωσης που δόθηκε σύμφωνα με την παράγραφο 18 στοιχείο α) για πρόσωπο που διαθέτει εξουσιοδότηση πρόσβασης σε ΔΠΕΕ, η αρμόδια για τους διορισμούς αρχή της ΓΓΣ μπορεί να ζητήσει οποιαδήποτε διευκρίνιση μπορεί να παράσχει η ΕΑΑ σύμφωνα με τις οικείες εθνικές νομοθετικές και κανονιστικές διατάξεις. Εφόσον επιβεβαιωθούν οι δυσμενείς πληροφορίες, η εξουσιοδότηση ανακαλείται και απαγορεύεται η πρόσβαση του εν λόγω προσώπου σε ΔΠΕΕ και σε θέσεις όπου είναι δυνατή αυτή η πρόσβαση ή όπου μπορεί να θέσει σε κίνδυνο την ασφάλεια.

25. Κάθε απόφαση απόσυρσης ή ανάκλησης εξουσιοδότησης πρόσβασης σε ΔΠΕΕ από υπάλληλο ή μέλος του λοιπού προσωπικού της ΓΓΣ καθώς και, εάν είναι σκόπιμο, οι σχετικοί λόγοι κοινοποιούνται στον ενδιαφερόμενο, ο οποίος μπορεί να ζητήσει ακρόαση από την αρμόδια για τους διορισμούς αρχή. Οι πληροφορίες που παρέχει η ΕΑΑ υπόκεινται στις νομοθετικές και κανονιστικές διατάξεις που ισχύουν εν προκειμένω στο οικείο κράτος μέλος, συμπεριλαμβανομένων εκείνων που αφορούν την άσκηση προσφυγών. Κατά των αποφάσεων της αρμόδιας για τους διορισμούς αρχής της ΓΓΣ μπορούν να ασκηθούν προσφυγές σύμφωνα με τον κανονισμό υπηρεσιακής κατάστασης των υπαλλήλων των Ευρωπαϊκών Κοινοτήτων και το καθεστώς που εφαρμόζεται επί του λοιπού προσωπικού των Κοινοτήτων αυτών.

Αρχεία εξουσιοδοτήσεων ασφαλείας και πρόσβασης

26. Κάθε κράτος μέλος και η ΓΓΣ τηρούν αρχεία των ΕΑΠ και των εξουσιοδοτήσεων οι οποίες χορηγούνται για πρόσβαση σε πληροφορίες με διαβάθμιση CONFIDENTIEL UE/EU CONFIDENTIAL ή υψηλότερη. Τα αρχεία αυτά περιέχουν τουλάχιστον το επίπεδο των ΔΠΕΕ για το οποίο χορηγείται πρόσβαση στον ενδιαφερόμενο, την ημερομηνία χορήγησης της εξουσιοδότησης ασφάλειας και τη διάρκεια ισχύος της.

27. Η αρμόδια αρχή ασφαλείας μπορεί να εκδώσει ΠΕΑΠ, στο οποίο αναφέρονται το επίπεδο ΔΠΕΕ για το οποίο δικαιούται πρόσβαση το συγκεκριμένο άτομο (CONFIDENTIEL UE/EU CONFIDENTIAL ή υψηλότερη), η ημερομηνία ισχύος του σχετικού πιστοποιητικού ΕΑΠ για πρόσβαση σε ΔΠΕΕ ή εξουσιοδότηση πρόσβασης σε ΔΠΕΕ και η ημερομηνία λήξης του ίδιου του πιστοποιητικού.

Εξαιρέσεις από την απαίτηση ΕΑΠ

28. Η πρόσβαση προσώπων, δεόντως εξουσιοδοτημένων λόγω των καθηκόντων τους, σε ΔΠΕΕ στα κράτη μέλη ρυθμίζεται σύμφωνα με τις εθνικές νομοθετικές και κανονιστικές διατάξεις· τα εν λόγω άτομα ενημερώνονται σχετικά με τις υποχρεώσεις ασφαλείας που υπέχουν όσον αφορά την προστασία των ΔΠΕΕ.

IV. ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΕΥΑΙΣΘΗΤΟΠΟΙΗΣΗ ΣΕ ΘΕΜΑΤΑ ΑΣΦΑΛΕΙΑΣ

29. Όλα τα άτομα στα οποία έχει χορηγηθεί εξουσιοδότηση ασφαλείας δηλώνουν εγγράφως ότι έχουν κατανοήσει τις υποχρεώσεις τους όσον αφορά την προστασία των ΔΠΕΕ και τις συνέπειες εάν διαρρεύσουν οι ΔΠΕΕ. Τηρείται αρχείο αυτών των γραπτών δηλώσεων στο κράτος μέλος και στη ΓΓΣ, κατά περίπτωση.

30. Όλα τα πρόσωπα στα οποία επιτρέπεται να έχουν πρόσβαση σε ΔΠΕΕ ή να τις χειρίζονται πρέπει να ευαισθητοποιούνται από την αρχή, και κατά διαστήματα να ενημερώνονται σχετικά με τις απειλές για την ασφάλεια και οφείλουν να αναφέρουν αμέσως στις αρμόδιες αρχές ασφαλείας κάθε προσπάθεια προσέγγισής τους ή δραστηριότητα την οποία θεωρούν ύποπτη ή ασυνήθιστη.

31. Όλα τα πρόσωπα που παύουν να απασχολούνται σε καθήκοντα τα οποία απαιτούν πρόσβαση σε ΔΠΕΕ ευαισθητοποιούνται για τις υποχρεώσεις τους, και εφόσον απαιτείται τις αναγνωρίζουν και γραπτώς, όσον αφορά τη συνεχή προστασία των ΔΠΕΕ.

V. ΕΞΑΙΡΕΤΙΚΕΣ ΠΕΡΙΣΤΑΣΕΙΣ

32. Εφόσον επιτρέπεται σύμφωνα με τις εθνικές νομοθετικές και κανονιστικές διατάξεις, η εξουσιοδότηση ασφαλείας από αρμόδια εθνική αρχή κράτους μέλους για πρόσβαση σε εθνικές διαβαθμισμένες πληροφορίες μπορεί να επιτρέπει προσωρινά, έως ότου χορηγηθεί ΕΑΠ για πρόσβαση σε ΔΠΕΕ, την πρόσβαση εθνικών υπαλλήλων σε ΔΠΕΕ έως το αντίστοιχο επίπεδο που καθορίζεται στον πίνακα αντιστοιχίας του προσαρτήματος Β, εφόσον η προσωρινή αυτή πρόσβαση είναι αναγκαία για τα συμφέροντα της Ένωσης. Οι ΕΑΑ ενημερώνουν την Επιτροπή Ασφαλείας σε περίπτωση που οι εθνικές νομοθετικές και κανονιστικές διατάξεις δεν επιτρέπουν αυτή την προσωρινή πρόσβαση σε ΔΠΕΕ.

33. Για λόγους επείγοντος, όταν δικαιολογείται δεόντως από το συμφέρον της υπηρεσίας και εν αναμονή της ολοκλήρωσης πλήρους έρευνας ασφαλείας, η αρμόδια για τους διορισμούς αρχή της ΓΓΣ δύναται, κατόπιν συνεννόησης με την ΕΑΑ του κράτους μέλους του οποίου είναι υπήκοος το εν λόγω πρόσωπο και ανάλογα με το αποτέλεσμα των προκαταρκτικών ελέγχων σχετικά με το αν είναι γνωστή κάποια αρνητική πληροφορία, να χορηγήσει προσωρινή εξουσιοδότηση στους υπαλλήλους και το λοιπό προσωπικό της ΓΓΣ προκειμένου να έχουν πρόσβαση σε ΔΠΕΕ για συγκεκριμένο καθήκον. Αυτές οι προσωρινές εξουσιοδοτήσεις ισχύουν για διάστημα όχι ανώτερο του εξαμήνου και δεν επιτρέπουν την πρόσβαση σε πληροφορίες με διαβάθμιση TRÈS SECRET UE/EU TOP SECRET. Όλα τα άτομα στα οποία έχει χορηγηθεί προσωρινή εξουσιοδότηση δηλώνουν εγγράφως ότι έχουν κατανοήσει τις υποχρεώσεις τους όσον αφορά την προστασία των ΔΠΕΕ και τις συνέπειες σε περίπτωση διαρροής ΔΠΕΕ. Η ΓΓΣ τηρεί αρχείο των γραπτών αυτών δηλώσεων.

34. Όταν ένα άτομο πρόκειται να τοποθετηθεί σε θέση η οποία απαιτεί εξουσιοδότηση ασφαλείας επιπέδου κατά μία βαθμίδα υψηλότερου από αυτή την οποία διαθέτει, τοποθετείται προσωρινά στην εν λόγω θέση υπό τους ακόλουθους όρους:

α) η επιτακτική ανάγκη πρόσβασης σε ΔΠΕΕ ανωτέρου επιπέδου αιτιολογείται γραπτώς από τον προϊστάμενο του προσώπου,

β) η πρόσβαση περιορίζεται σε συγκεκριμένα στοιχεία των ΔΠΕΕ τα οποία απαιτούνται προς εκτέλεση του ανατεθειμένου έργου,

γ) το πρόσωπο διαθέτει έγκυρη ΕΑΠ ή εξουσιοδότηση πρόσβασης σε ΔΠΕΕ,

δ) έχουν αναληφθεί ενέργειες για τη χορήγηση εξουσιοδότησης για το επίπεδο που απαιτείται για τη συγκεκριμένη θέση,

ε) έχει ελεγχθεί ικανοποιητικά από την αρμόδια αρχή ότι το πρόσωπο δεν έχει υποπέσει σε σοβαρή ή επανειλημμένη παράβαση των κανονισμών ασφαλείας,

στ) η τοποθέτηση του προσώπου εγκρίνεται από την αρμόδια αρχή και

ζ) στην αρμόδια γραμματεία ή υπογραμματεία φυλάσσεται η έκτακτη αυτή εξουσιοδότηση, μαζί με περιγραφή των πληροφοριών για τις οποίες εγκρίθηκε η πρόσβαση.

35. Η ανωτέρω διαδικασία χρησιμοποιείται για μία και μόνη πρόσβαση σε ΔΠΕΕ επιπέδου κατά μία βαθμίδα υψηλότερου από αυτό για το οποίο το πρόσωπο έχει λάβει εξουσιοδότηση ασφαλείας. Η προσφυγή στη διαδικασία αυτή δεν πρέπει να είναι επαναλαμβανόμενη.

36. Σε πολύ εξαιρετικές περιστάσεις, όπως αποστολές σε εχθρικό περιβάλλον ή σε περιόδους αυξανόμενης διεθνούς έντασης, εφόσον αυτό απαιτείται λόγω έκτακτων μέτρων, ιδίως προκειμένου να σωθούν ζωές, τα κράτη μέλη και ο γενικός γραμματέας μπορούν να επιτρέπουν, ει δυνατόν γραπτώς, την πρόσβαση σε πληροφορίες με διαβάθμιση CONFIDENTIEL UE/EU CONFIDENTIAL ή SECRET UE/EU SECRET ατόμων που δεν διαθέτουν την απαιτούμενη εξουσιοδότηση ασφαλείας, υπό τον όρο ότι η έγκριση αυτή είναι απολύτως αναγκαία και ότι δεν υπάρχουν εύλογες αμφιβολίες ως προς τη νομιμοφροσύνη, τη φερεγγυότητα και την αξιοπιστία των συγκεκριμένων προσώπων. Η έκτακτη αυτή εξουσιοδότηση φυλάσσεται σε αρχείο, μαζί με περιγραφή των πληροφοριών για τις οποίες εγκρίθηκε πρόσβαση.

37. Στην περίπτωση πληροφοριών με διαβάθμιση TRÈS SECRET UE/EU TOP SECRET, η εν λόγω έκτακτη πρόσβαση περιορίζεται στους υπηκόους της Ένωσης στους οποίους έχει χορηγηθεί άδεια πρόσβασης είτε στο αντίστοιχο εθνικό επίπεδο του TRÈS SECRET UE/EU TOP SECRET είτε σε πληροφορίες με διαβάθμιση SECRET UE/EU SECRET.

38. Η Επιτροπή Ασφαλείας ενημερώνεται για τις περιπτώσεις στις οποίες χρησιμοποιείται η διαδικασία των παραγράφων 36 και 37.

39. Όταν οι εθνικές νομοθετικές και κανονιστικές διατάξεις κράτους μέλους προβλέπουν αυστηρότερους κανόνες για τις προσωρινές εξουσιοδοτήσεις, προσωρινές τοποθετήσεις, τη μία και μόνη πρόσβαση ή την έκτακτη πρόσβαση προσώπων σε διαβαθμισμένες πληροφορίες, οι διαδικασίες του παρόντος τμήματος εφαρμόζονται μόνο εντός των ορίων των οικείων εθνικών νομοθετικών και κανονιστικών διατάξεων.

40. Η Επιτροπή Ασφαλείας είναι αποδέκτης ετήσιας έκθεσης για τη χρησιμοποίηση των διαδικασιών που απαριθμούνται στο παρόν μέρος.

VI. ΣΥΜΜΕΤΟΧΗ ΣΕ ΣΥΝΕΔΡΙΑΣΕΙΣ ΣΤΟ ΣΥΜΒΟΥΛΙΟ

41. Υπό την επιφύλαξη της παραγράφου 28, τα πρόσωπα στα οποία έχει ανατεθεί να συμμετέχουν σε συνεδριάσεις του Συμβουλίου ή προπαρασκευαστικών οργάνων του Συμβουλίου κατά τις οποίες συζητούνται πληροφορίες με διαβάθμιση CONFIDENTIEL UE/EU CONFIDENTIAL ή υψηλότερη μπορούν να το πράξουν μόνο έπειτα από επιβεβαίωση του επιπέδου εξουσιοδότησης ασφαλείας που διαθέτουν. Προκειμένου περί αντιπροσώπων, ένα ΠΕΑΠ ή άλλο αποδεικτικό εξουσιοδότησης ασφαλείας διαβιβάζεται στο Γραφείο Ασφαλείας της ΓΓΣ από τις αρμόδιες αρχές ή, σε εξαιρετικές περιπτώσεις, παραδίδεται από τον ίδιο τον αντιπρόσωπο. Εφόσον συντρέχει περίπτωση, μπορεί να χρησιμοποιείται ενοποιημένος κατάλογος ονομάτων, όπου αναγράφεται το σχετικό αποδεικτικό εξουσιοδότησης ασφαλείας.

42. Όταν η ΕΑΠ για πρόσβαση σε ΔΠΕΕ ανακαλείται για λόγους ασφαλείας από πρόσωπο του οποίου τα καθήκοντα απαιτούν συμμετοχή σε συνεδριάσεις του Συμβουλίου ή προπαρασκευαστικών οργάνων του Συμβουλίου, η αρμόδια αρχή ενημερώνει σχετικά τη ΓΓΣ.

VII. ΔΥΝΗΤΙΚΗ ΠΡΟΣΒΑΣΗ ΣΕ ΔΠΕΕ

43. Οι ταχυμεταφορείς, οι φύλακες και οι συνοδοί λαμβάνουν εξουσιοδότηση ασφαλείας του αντίστοιχου επιπέδου ή άλλη ανάλογη έρευνα σύμφωνα με τους εθνικούς νόμους και κανονισμούς, ενημερώνονται σχετικά με τις διαδικασίες ασφαλείας για την προστασία των ΔΠΕΕ και λαμβάνουν οδηγίες για την υποχρέωσή τους να προστατεύουν τις πληροφορίες στην κατοχή τους.

ΠΑΡΑΡΤΗΜΑ II

ΦΥΣΙΚΗ ΑΣΦΑΛΕΙΑ

I. ΕΙΣΑΓΩΓΗ

1. Το παρόν παράρτημα περιέχει διατάξεις για την εφαρμογή του άρθρου 8. Ορίζει τις ελάχιστες προδιαγραφές για τη φυσική ασφάλεια των εγκαταστάσεων, των κτιρίων, των γραφείων και άλλων χώρων όπου γίνεται χειρισμός και αποθήκευση ΔΠΕΕ, συμπεριλαμβανομένων των χώρων που στεγάζουν CIS.

2. Τα μέτρα φυσικής ασφάλειας προορίζονται για να αποτρέπουν την άνευ εξουσιοδότησης πρόσβαση σε ΔΠΕΕ με τους εξής τρόπους:

α) εξασφαλίζοντας ότι οι ΔΠΕΕ διεκπεραιώνονται και αποθηκεύονται με κατάλληλο τρόπο,

β) επιτρέποντας το διαχωρισμό του προσωπικού όσον αφορά την πρόσβαση σε ΔΠΕΕ βάσει της ανάγκης γνώσης και, εφόσον απαιτείται, του ελέγχου ασφαλείας τους,

γ) αποτρέποντας, παρεμποδίζοντας και ανιχνεύοντας τις μη εξουσιοδοτημένες ενέργειες και

δ) απαγορεύοντας ή καθυστερώντας τη λαθραία ή βίαιη είσοδο αναρμοδίων.

II. ΠΡΟΔΙΑΓΡΑΦΕΣ ΚΑΙ ΜΕΤΡΑ ΦΥΣΙΚΗΣ ΑΣΦΑΛΕΙΑΣ

3. Τα μέτρα φυσικής ασφαλείας επιλέγονται βάσει αξιολόγησης κινδύνου που διενεργούν οι αρμόδιες αρχές. Τόσο η ΓΓΣ όσο και τα κράτη μέλη εφαρμόζουν διαδικασία διαχείρισης κινδύνων για την προστασία των ΔΠΕΕ στους χώρους τους προκειμένου να εξασφαλίσουν την παροχή ανάλογου επίπεδου φυσικής προστασίας κατά του εκτιμώμενου κινδύνου. Κατά τη διαδικασία διαχείρισης κινδύνων συνεκτιμώνται όλοι οι σχετικοί παράγοντες και ειδικότερα:

α) το επίπεδο διαβάθμισης των ΔΠΕΕ,

β) η μορφή και η ποσότητα των ΔΠΕΕ, λαμβάνοντας υπόψη ότι οι μεγάλες ποσότητες ή η συγκέντρωση ΔΠΕΕ ενδέχεται να απαιτούν την εφαρμογή αυστηρότερων προστατευτικών μέτρων,

γ) ο περιβάλλων χώρος και η δομή των κτιρίων ή των χώρων στέγασης των ΔΠΕΕ και

δ) η εκτιμώμενη απειλή από μυστικές υπηρεσίες στο στόχαστρο των οποίων ευρίσκονται η Ένωση ή τα κράτη μέλη και η απειλή δολιοφθοράς, τρομοκρατικών, ανατρεπτικών ή άλλων εγκληματικών δραστηριοτήτων.

4. Η αρμόδια αρχή ασφαλείας, εφαρμόζοντας την έννοια της προστασίας εις βάθος, καθορίζει το δέοντα εφαρμοστέο συνδυασμό μέτρων φυσικής ασφαλείας. Στα μέτρα αυτά περιλαμβάνονται ένα ή περισσότερα από τα ακόλουθα:

α) περιμετρικός φράκτης: φυσικό εμπόδιο που προστατεύει τα όρια ενός χώρου που χρήζει προστασίας,

β) συστήματα ανίχνευσης εισβολών (IDS): το IDS μπορεί να χρησιμοποιείται για την ενίσχυση του επιπέδου ασφαλείας ενός περιμετρικού φράκτη ή σε αίθουσες και κτίρια αντί του προσωπικού ασφαλείας ή προς επικουρία του,

γ) έλεγχος εισόδου: ο έλεγχος εισόδου μπορεί να ασκείται σε τοποθεσία, κτίριο ή κτίρια ευρισκόμενα σε μια τοποθεσία, ή σε χώρους και αίθουσες εντός ενός κτιρίου· ο έλεγχος μπορεί να διενεργείται με ηλεκτρονικά ή ηλεκτρομηχανικά μέσα, από προσωπικό ασφαλείας και/ή υπάλληλο υποδοχής και/ή άλλα φυσικά μέσα,

δ) προσωπικό ασφαλείας: εκπαιδευμένο και εποπτευόμενο προσωπικό ασφαλείας με την προσήκουσα εξουσιοδότηση ασφαλείας μπορεί να προσλαμβάνεται, μεταξύ άλλων, για την παρεμπόδιση ατόμων που σχεδιάζουν μυστική διείσδυση,

ε) κλειστό κύκλωμα τηλεόρασης (CCTV): το CCTV μπορεί να χρησιμοποιείται από το προσωπικό ασφαλείας προκειμένου να ελέγχει περιστατικά και τους συναγερμούς IDS σε μεγάλους χώρους ή σε περιμέτρους,

στ) φωτισμός ασφαλείας: ο φωτισμός ασφαλείας μπορεί να χρησιμοποιείται για την αποτροπή δυνητικών εισβολών, καθώς και για την παροχή του αναγκαίου φωτισμού για την αποτελεσματική επιτήρηση άμεσα από το προσωπικό ασφαλείας ή έμμεσα μέσω τηλεόρασης κλειστού κυκλώματος, και

ζ) κάθε άλλο κατάλληλο φυσικό μέτρο που στοχεύει στην παρεμπόδιση ή ανίχνευση της πρόσβασης μη εξουσιοδοτημένων προσώπων ή την αποτροπή απώλειας ή ζημίας των ΔΠΕΕ.

5. Η αρμόδια αρχή μπορεί να εξουσιοδοτηθεί να διενεργεί έρευνες κατά την είσοδο και έξοδο με σκοπό την αποτροπή μη εξουσιοδοτημένης εισαγωγής υλικού ή μη εξουσιοδοτημένης αφαίρεσης ΔΠΕΕ από εγκαταστάσεις ή κτίρια.

6. Όταν οι ΔΠΕΕ διατρέχουν κίνδυνο λαθροβλεψίας, έστω και τυχαίας, πρέπει να λαμβάνονται τα δέοντα μέτρα για την αποτροπή του κινδύνου.

7. Για τις νέες εγκαταστάσεις, οι προδιαγραφές φυσικής ασφαλείας και οι λειτουργικές προδιαγραφές τους καθορίζονται ως μέρος του γενικού και κατασκευαστικού σχεδιασμού των εγκαταστάσεων. Για τις ήδη υπάρχουσες εγκαταστάσεις, οι προδιαγραφές φυσικής ασφαλείας εφαρμόζονται στο μεγαλύτερο δυνατό βαθμό.

III. ΕΞΟΠΛΙΣΜΟΣ ΓΙΑ ΤΗ ΦΥΣΙΚΗ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΔΠΕΕ

8. Κατά την απόκτηση εξοπλισμού (όπως φωριαμών ασφαλείας, μηχανών καταστροφής εγγράφων, κλειδαριών θυρών, ηλεκτρονικών συστημάτων ελέγχου πρόσβασης, IDS, συστημάτων συναγερμού) για τη φυσική προστασία των ΔΠΕΕ, η αρμόδια αρχή ασφαλείας μεριμνά ώστε ο εξοπλισμός να ανταποκρίνεται στις εγκεκριμένες τεχνικές προδιαγραφές και τις ελάχιστες απαιτήσεις.

9. Οι τεχνικές προδιαγραφές του εξοπλισμού που χρησιμοποιείται για τη φυσική προστασία των ΔΠΕΕ ορίζονται σε κατευθυντήριες γραμμές ασφαλείας που εγκρίνονται από την Επιτροπή Ασφαλείας.

10. Τα συστήματα ασφαλείας επιθεωρούνται σε τακτά χρονικά διαστήματα και ο εξοπλισμός συντηρείται τακτικά. Στη συντήρηση θα πρέπει να λαμβάνεται υπόψη το αποτέλεσμα των επιθεωρήσεων ώστε να διασφαλίζεται ότι ο εξοπλισμός εξακολουθεί να λειτουργεί άριστα.

11. Η αποτελεσματικότητα κάθε μέτρου ασφαλείας και ολόκληρου του συστήματος ασφαλείας πρέπει να επαναξιολογείται σε κάθε επιθεώρηση.

IV. ΧΩΡΟΙ ΠΟΥ ΤΥΓΧΑΝΟΥΝ ΦΥΣΙΚΗΣ ΠΡΟΣΤΑΣΙΑΣ

12. Δύο τύποι χώρων που τυγχάνουν φυσικής προστασίας, ή οι εθνικοί αντίστοιχοί τους, καθορίζονται για τη φυσική προστασία των ΔΠΕΕ:

α) διοικητικοί χώροι και

β) χώροι ασφαλείας (συμπεριλαμβανομένων των χώρων τεχνικής ασφαλείας).

Στην παρούσα απόφαση, κάθε αναφορά σε διοικητικούς χώρους και χώρους ασφαλείας, συμπεριλαμβανομένων των χώρων τεχνικής ασφαλείας, νοείται ως αναφερόμενη και στο εθνικό τους αντίστοιχο.

13. Η αρμόδια αρχή ασφαλείας κρίνει αν ένας χώρος καλύπτει τις προδιαγραφές ώστε να χαρακτηρισθεί διοικητικός χώρος, χώρος ασφαλείας ή χώρος τεχνικής ασφαλείας.

14. Για τους διοικητικούς χώρους:

α) ορίζεται εμφανώς οριοθετημένη περίμετρος που επιτρέπει τον έλεγχο προσώπων και, ει δυνατόν, οχημάτων,

β) ασυνόδευτη πρόσβαση επιτρέπεται μόνο στα πρόσωπα που έχουν δέουσα εξουσιοδότηση της αρμόδιας αρχής και

γ) όλα τα άλλα πρόσωπα πρέπει να συνοδεύονται συνεχώς ή να υποβάλλονται σε ανάλογους ελέγχους.

15. Για τους χώρους ασφαλείας:

α) ορίζεται εμφανώς καθορισμένη και προστατευμένη περίμετρος στην οποία ελέγχεται κάθε είσοδος και έξοδος μέσω συστήματος ταυτοτήτων ή αναγνώρισης προσώπων,

β) ασυνόδευτη πρόσβαση επιτρέπεται μόνο στα πρόσωπα με προσήκουσα εξουσιοδότηση ασφαλείας και διαθέτουν ειδική άδεια εισόδου στο χώρο βάσει της ανάγκης γνώσης τους και

γ) όλα τα άλλα πρόσωπα πρέπει να συνοδεύονται συνεχώς ή να υποβάλλονται σε ανάλογους ελέγχους.

16. Όταν η είσοδος σε χώρο ασφαλείας συνιστά, στην πράξη, άμεση πρόσβαση στις διαβαθμισμένες πληροφορίες που φυλάσσονται στον οικείο χώρο, ισχύουν οι ακόλουθες συμπληρωματικές προϋποθέσεις:

α) αναφέρεται σαφώς το επίπεδο ανώτατης διαβάθμισης ασφαλείας των πληροφοριών που φυλάσσονται συνήθως στο χώρο,

β) όλοι οι επισκέπτες πρέπει να έχουν ειδική άδεια εισόδου στο χώρο, να συνοδεύονται συνεχώς και να έχουν λάβει την προσήκουσα εξουσιοδότηση ασφαλείας, εκτός εάν ληφθούν μέτρα τα οποία καθιστούν αδύνατη την πρόσβαση σε ΔΠΕΕ.

17. Οι χώροι ασφαλείας που προστατεύονται από τη λαθρακρόαση χαρακτηρίζονται ως χώροι τεχνικής ασφαλείας. Ισχύουν οι ακόλουθες συμπληρωματικές προϋποθέσεις:

α) οι χώροι αυτοί φέρουν εξοπλισμό IDS, κλειδώνονται όταν δεν χρησιμοποιούνται και φυλάσσονται όταν χρησιμοποιούνται· τα κλειδιά ελέγχονται σύμφωνα με το μέρος VI,

β) όλα τα πρόσωπα και το υλικό που εισέρχονται σε αυτούς τους χώρους ελέγχονται,

γ) οι χώροι αυτοί υποβάλλονται τακτικά σε φυσικούς και/ή τεχνικούς ελέγχους κατά τις απαιτήσεις της αρμόδιας αρχής ασφαλείας· οι εν λόγω έλεγχοι πραγματοποιούνται και ύστερα από κάθε μη εξουσιοδοτημένη είσοδο ή υπόνοια μη εξουσιοδοτημένης εισόδου και

δ) οι χώροι αυτοί δεν έχουν μη εξουσιοδοτημένες τηλεπικοινωνιακές γραμμές, μη εξουσιοδοτημένα τηλέφωνα ή άλλες μη εξουσιοδοτημένες τηλεπικοινωνιακές συσκευές και ηλεκτρικό ή ηλεκτρονικό εξοπλισμό.

18. Παρά τα οριζόμενα στην παράγραφο 17 στοιχείο δ), προτού χρησιμοποιηθούν σε χώρους όπου διεξάγονται συνεδριάσεις ή εργασίες που αφορούν πληροφορίες με διαβάθμιση SECRET UE/EU SECRET ή υψηλότερη και σε περιστάσεις όπου η απειλή για τις ΔΠΕΕ θεωρείται σοβαρή, οι τηλεπικοινωνιακές συσκευές και ο ηλεκτρικός ή ηλεκτρονικός εξοπλισμός παντός είδους εξετάζονται καταρχάς από την αρμόδια αρχή ασφαλείας για να εξασφαλισθεί ότι δεν είναι δυνατή η μετάδοση καταληπτών πληροφοριών μέσω του εξοπλισμού αυτού, είτε ακούσια είτε παράνομα, πέραν της περιμέτρου του χώρου ασφαλείας.

19. Οι χώροι ασφαλείας στους οποίους δεν υπάρχει προσωπικό υπηρεσίας επί 24ώρου βάσεως επιθεωρούνται, εφόσον είναι σκόπιμο, κατά τη λήξη του κανονικού ωραρίου εργασίας και σε τυχαία διαστήματα εκτός του κανονικού ωραρίου εργασίας, εκτός εάν είναι εξοπλισμένοι με IDS.

20. Χώροι ασφαλείας και χώροι τεχνικής ασφαλείας μπορούν να δημιουργούνται προσωρινά εντός διοικητικού χώρου για τη διεξαγωγή διαβαθμισμένης συνεδρίασης ή κάθε άλλο παρόμοιο σκοπό.

21. Για κάθε χώρο ασφαλείας εκπονούνται λειτουργικές διαδικασίες ασφαλείας στις οποίες αναφέρονται:

α) το επίπεδο των ΔΠΕΕ οι οποίες υποβάλλονται σε χειρισμό και αποθηκεύονται στο χώρο,

β) τα μέτρα επιτήρησης και προστασίας που πρέπει να τηρούνται,

γ) τα πρόσωπα τα οποία έχουν άδεια ασυνόδευτης πρόσβασης στο χώρο βάσει της ανάγκης γνώσης και του ελέγχου ασφαλείας τους,

δ) ενδεχομένως, οι διαδικασίες συνοδείας ή προστασίας των ΔΠΕΕ όταν επιτρέπεται σε οποιαδήποτε άλλα πρόσωπα η πρόσβαση στο χώρο, και

ε) οποιαδήποτε άλλα σχετικά μέτρα και διαδικασίες.

22. Εντός των χώρων ασφαλείας κατασκευάζονται θωρακισμένες αίθουσες. Οι τοίχοι, τα πατώματα, οι οροφές, τα παράθυρα και οι θύρες που κλειδώνουν εγκρίνονται από την αρμόδια αρχή ασφαλείας και παρέχουν προστασία ισοδύναμη με φωριαμό ασφαλείας που έχει εγκριθεί για την αποθήκευση ΔΠΕΕ του ίδιου επιπέδου διαβάθμισης.

V. ΦΥΣΙΚΑ ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ ΓΙΑ ΤΟ ΧΕΙΡΙΣΜΟ ΚΑΙ ΤΗΝ ΑΠΟΘΗΚΕΥΣΗ ΔΠΕΕ

23. Ο χειρισμός ΔΠΕΕ με διαβάθμιση RESTREINT UE/EU RESTRICTED διεξάγεται:

α) σε χώρο ασφαλείας,

β) σε διοικητικό χώρο, εφόσον οι ΔΠΕΕ προστατεύονται από την πρόσβαση μη εξουσιοδοτημένων προσώπων, ή

γ) εκτός χώρου ασφαλείας ή διοικητικού χώρου, εφόσον ο κάτοχος μεταφέρει τις ΔΠΕΕ σύμφωνα με τις παραγράφους 28 έως 41 του παραρτήματος III και έχει αναλάβει να συμμορφώνεται με τα αντισταθμιστικά μέτρα που καθορίζονται στις οδηγίες ασφαλείας που εκδίδει η αρμόδια αρχή ασφαλείας, ούτως ώστε να διασφαλίζεται ότι οι ΔΠΕΕ προστατεύονται από την πρόσβαση μη εξουσιοδοτημένων προσώπων.

24. Οι ΔΠΕΕ με διαβάθμιση RESTREINT UE/EU RESTRICTED αποθηκεύονται σε κατάλληλα έπιπλα γραφείου με κλειδαριά σε διοικητικό χώρο ή χώρο ασφαλείας. Μπορούν προσωρινά να αποθηκευθούν εκτός χώρου ασφαλείας ή διοικητικού χώρου, εφόσον ο κάτοχος έχει αναλάβει να συμμορφώνεται με τα αντισταθμιστικά μέτρα που καθορίζονται στις οδηγίες ασφαλείας που εκδίδει η αρμόδια αρχή ασφαλείας.

25. Ο χειρισμός ΔΠΕΕ με διαβάθμιση CONFIDENTIEL UE/EU CONFIDENTIAL ή SECRET UE/EU SECRET διεξάγεται:

α) σε χώρο ασφαλείας,

β) σε διοικητικό χώρο, εφόσον οι ΔΠΕΕ προστατεύονται από την πρόσβαση μη εξουσιοδοτημένων προσώπων, ή

γ) εκτός χώρου ασφαλείας ή διοικητικού χώρου, εφόσον ο κάτοχος:

i) μεταφέρει τις ΔΠΕΕ σύμφωνα με τις παραγράφους 28 έως 41 του παραρτήματος III,

ii) έχει αναλάβει να συμμορφώνεται με τα αντισταθμιστικά μέτρα που καθορίζονται στις οδηγίες ασφαλείας που εκδίδει η αρμόδια αρχή, προκειμένου να εξασφαλίζεται ότι οι ΔΠΕΕ προστατεύονται από την πρόσβαση μη εξουσιοδοτημένων προσώπων,

iii) διατηρεί ανά πάσα στιγμή τις ΔΠΕΕ υπό τον έλεγχό του και

iv) σε περίπτωση εγγράφων σε χαρτί, έχει ενημερώσει σχετικά την αρμόδια γραμματεία.

26. Οι ΔΠΕΕ με διαβάθμιση CONFIDENTIEL UE/EU CONFIDENTIAL ή SECRET UE/EU SECRET αποθηκεύονται σε χώρο ασφαλείας είτε εντός φωριαμού ασφαλείας είτε εντός θωρακισμένης αίθουσας.

27. Ο χειρισμός ΔΠΕΕ με διαβάθμιση ασφαλείας TRÈS SECRET UE/EU TOP SECRET διεξάγεται σε χώρο ασφαλείας.

28. Οι ΔΠΕΕ με διαβάθμιση TRÈS SECRET UE/EU TOP SECRET αποθηκεύονται σε χώρο ασφαλείας, στο πλαίσιο μιας εκ των κατωτέρω προϋποθέσεων:

α) εντός φωριαμού ασφαλείας, σύμφωνα με την παράγραφο 8, με τουλάχιστον έναν από τους ακόλουθους συμπληρωματικούς ελέγχους:

i) συνεχή προστασία ή επαλήθευση από προσωπικό ασφαλείας ή προσωπικό υπηρεσίας με τη δέουσα διαβάθμιση,

ii) εγκεκριμένο IDS σε συνδυασμό με προσωπικό ασφαλείας αντιμετώπισης περιστατικών,

β) εντός θωρακισμένης αίθουσας εξοπλισμένης με IDS σε συνδυασμό με προσωπικό ασφαλείας αντιμετώπισης περιστατικών.

29. Στο παράρτημα III παρατίθενται οι κανόνες που διέπουν τη μεταφορά ΔΠΕΕ εκτός των χώρων υλικής προστασίας.

VI. ΕΛΕΓΧΟΣ ΚΛΕΙΔΙΩΝ ΚΑΙ ΣΥΝΔΥΑΣΜΩΝ ΠΟΥ ΧΡΗΣΙΜΟΠΟΙΟΥΝΤΑΙ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΔΠΕΕ

30. Η αρμόδια αρχή ασφαλείας καθορίζει τις διαδικασίες για τη διαχείριση των κλειδιών και των συνδυασμών για τα γραφεία, τις αίθουσες, τις θωρακισμένες αίθουσες και τους φωριαμούς ασφαλείας. Οι διαδικασίες αυτές προστατεύουν από το ενδεχόμενο εισόδου μη εξουσιοδοτημένων ατόμων.

31. Οι συνδυασμοί απομνημονεύονται από τον μικρότερο δυνατό αριθμό ατόμων που πρέπει να τους γνωρίζουν. Οι συνδυασμοί των φωριαμών ασφαλείας στους οποίους αποθηκεύονται οι ΔΠΕΕ αλλάζουν:

α) όποτε παραλαμβάνεται νέος φωριαμός,

β) σε κάθε αλλαγή προσωπικού που γνωρίζει τον συνδυασμό,

γ) όποτε σημειώνεται διαρροή ή υπάρχουν υπόνοιες διαρροής,

δ) όποτε συντηρήθηκε ή επισκευάσθηκε κλειδαριά και

ε) ανά δωδεκάμηνο τουλάχιστον.

ΠΑΡΑΡΤΗΜΑ III

ΔΙΑΧΕΙΡΙΣΗ ΔΙΑΒΑΘΜΙΣΜΕΝΩΝ ΠΛΗΡΟΦΟΡΙΩΝ

I. ΕΙΣΑΓΩΓΗ

1. Το παρόν παράρτημα περιέχει διατάξεις για την εφαρμογή του άρθρου 9. Ορίζει τα διοικητικά μέτρα για τον έλεγχο των ΔΠΕΕ καθ' όλη τη διάρκεια του κύκλου ζωής των προκειμένου να ενισχυθούν η αποτροπή και η ανίχνευση περιπτώσεων σκόπιμης ή τυχαίας διαρροής ή απώλειας των εν λόγω πληροφοριών.

II. ΔΙΑΧΕΙΡΙΣΗ ΤΩΝ ΔΙΑΒΑΘΜΙΣΕΩΝ

Διαβαθμίσεις και σημάνσεις

2. Οι πληροφορίες λαμβάνουν διαβάθμιση όταν απαιτείται προστασία του απόρρητου χαρακτήρα τους.

3. Ο φορέας προέλευσης των ΔΠΕΕ είναι υπεύθυνος για τον ορισμό του επιπέδου διαβάθμισης ασφαλείας, σύμφωνα με τις σχετικές κατευθυντήριες γραμμές διαβάθμισης, και για την αρχική κοινοποίηση των πληροφοριών.

4. Το επίπεδο διαβάθμισης των ΔΠΕΕ ορίζεται σύμφωνα με το άρθρο 2 παράγραφος 2 και με αναφορά στην πολιτική ασφαλείας που θα εγκριθεί σύμφωνα με το άρθρο 3 παράγραφος 3.

5. Η διαβάθμιση ασφαλείας σημαίνεται με σαφή και προσήκοντα τρόπο, ανεξαρτήτως εάν οι ΔΠΕΕ είναι σε έντυπη, προφορική, ηλεκτρονική ή οποιαδήποτε άλλη μορφή.

6. Επί μέρους τμήματα δεδομένου εγγράφου (ήτοι σελίδες, παράγραφοι, τμήματα, παραρτήματα και προσαρτήματα καθώς και τυχόν συνημμένα έγγραφα) ενδέχεται να απαιτούν διαφορετικές διαβαθμίσεις και σημαίνονται αναλόγως, μεταξύ άλλων όταν αποθηκεύονται σε ηλεκτρονική μορφή.

7. Το γενικό επίπεδο διαβάθμισης ενός εγγράφου ή ενός φακέλου είναι τουλάχιστον τόσο υψηλό όσο το επίπεδο του στοιχείου του με την υψηλότερη διαβάθμιση. Όταν συγκεντρώνει πληροφορίες από διάφορες πηγές, το τελικό προϊόν επανεξετάζεται προκειμένου να καθορισθεί το γενικό του επίπεδο διαβάθμισης ασφαλείας, δεδομένου ότι μπορεί να απαιτεί υψηλότερη διαβάθμιση από τις συνιστώσες του.

8. Στο μέτρο του δυνατού, τα έγγραφα που περιέχουν μέρη με διαφορετικά επίπεδα διαβάθμισης διαρθρώνονται κατά τρόπον ώστε τα μέρη με διαφορετικό επίπεδο διαβάθμισης να προσδιορίζονται και να αποχωρίζονται εύκολα, εφόσον είναι απαραίτητο.

9. Η διαβάθμιση επιστολής ή σημειώματος που περιλαμβάνει συνημμένα έγγραφα καθορίζεται στο επίπεδο του υψηλότερα διαβαθμισμένου συνημμένου εγγράφου. Ο φορέας προέλευσης επισημαίνει σαφώς σε ποιο επίπεδο διαβαθμίζεται όταν αποχωρισθεί από τα συνημμένα έγγραφα μέσω κατάλληλη σήμανσης, π.χ.:

CONFIDENTIEL EU/EU CONFIDENTIAL

Χωρίς το (τα) συνημμένο(-α) έγγραφο(-α) RESTREINT UE/EU RESTRICTED.

Σημάνσεις

10. Εκτός των σημάνσεων διαβάθμισης ασφαλείας που προβλέπονται στο άρθρο 2 παράγραφος 2, οι διαβαθμισμένες πληροφορίες ΕΕ είναι δυνατόν να φέρουν πρόσθετες σημάνσεις, όπως:

α) αναγνωριστικό στοιχείο του φορέα προέλευσης,

β) τυχόν προειδοποιήσεις, κωδικές λέξεις ή αρκτικόλεξα που διευκρινίζουν τον τομέα δραστηριότητας που αφορά το έγγραφο, ιδιαίτερη διανομή βάσει της «ανάγκης γνώσης» ή περιορισμούς χρήσης,

γ) σημάνσεις δυνατότητας κοινοποίησης ή

δ) κατά περίπτωση, την ημερομηνία ή το συγκεκριμένο γεγονός μετά την παρέλευση των οποίων μπορούν να υποχαρακτηριστούν ή να αποχαρακτηριστούν.

Συντετμημένες σημάνσεις διαβάθμισης

11. Οι τυποποιημένες συντετμημένες σημάνσεις διαβάθμισης μπορούν να χρησιμοποιούνται ως ενδείξεις του επιπέδου διαβάθμισης των επιμέρους παραγράφων ενός κειμένου. Οι συντομογραφίες δεν αντικαθιστούν τις πλήρεις σημάνσεις διαβάθμισης.

12. Οι ακόλουθες τυποποιημένες συντομογραφίες μπορούν να χρησιμοποιούνται στα διαβαθμισμένα έγγραφα της ΕΕ ως ενδείξεις του επιπέδου διαβάθμισης τμημάτων ή ενοτήτων του κειμένου που δεν υπερβαίνουν μία σελίδα:

TRÈS SECRET UE/EU TOP SECRET	TS-UE/EU-TS
SECRET UE/EU SECRET	S-UE/EU-S
CONFIDENTIEL UE/EU CONFIDENTIAL	C-UE/EU-C
RESTREINT UE/EU RESTRICTED	R-UE/EU-R

Δημιουργία ΔΠΕΕ

13. Κατά τη σύνταξη διαβαθμισμένου εγγράφου ΕΕ:

α) το επίπεδο διαβάθμισης αναγράφεται καθαρά σε κάθε σελίδα,

β) όλες οι σελίδες αριθμούνται,

γ) το έγγραφο φέρει αριθμό αναφοράς και θέμα το οποίο δεν αποτελεί το ίδιο διαβαθμισμένη πληροφορία, εκτός αν σημειώνεται άλλως,

δ) το έγγραφο φέρει ημερομηνία και

ε) αν τα έγγραφα με διαβάθμιση SECRET UE/EU SECRET ή υψηλότερη πρόκειται να διανεμηθούν σε πολλαπλά αντίτυπα, φέρουν αριθμό αντιτύπου σε κάθε σελίδα.

14. Εάν δεν είναι δυνατή η εφαρμογή της παραγράφου 13 στις ΔΠΕΕ, λαμβάνονται άλλα κατάλληλα μέτρα σύμφωνα με τις κατευθυντήριες γραμμές ασφαλείας που καταρτίζονται σύμφωνα με το άρθρο 6 παράγραφος 2.

Υποχαρακτηρισμός και αποχαρακτηρισμός των ΔΠΕΕ

15. Κατά τη δημιουργία τους, ο φορέας προέλευσης δηλώνει, όπου είναι δυνατόν, και ιδίως για πληροφορίες χαρακτηρισμένες RESTREINT UE/EU RESTRICTED, εάν οι ΔΠΕΕ μπορούν να υποχαρακτηρισθούν ή να αποχαρακτηρισθούν σε ορισμένη ημερομηνία ή κατόπιν συγκεκριμένου γεγονότος.

16. Η ΓΓΣ επανεξετάζει τακτικά τις ΔΠΕΕ που ευρίσκονται στην κατοχή της προκειμένου να εξακριβώσει αν ισχύει ακόμα το επίπεδο διαβάθμισης. Η ΓΓΣ καθιερώνει σύστημα επανεξέτασης, τουλάχιστον ανά πενταετία, του επιπέδου διαβάθμισης των ΔΠΕΕ που έχει δημιουργήσει. Η επανεξέταση αυτή δεν είναι απαραίτητη όταν ο φορέας προέλευσης έχει δηλώσει εξαρχής ότι οι πληροφορίες υποχαρακτηρίζονται ή αποχαρακτηρίζονται αυτόματα και φέρουν ανάλογη σήμανση.

III. ΚΑΤΑΧΩΡΙΣΗ ΔΠΕΕ ΓΙΑ ΛΟΓΟΥΣ ΑΣΦΑΛΕΙΑΣ

17. Για κάθε οργανωτική μονάδα εντός της ΓΓΣ και των κρατικών υπηρεσιών των κρατών μελών στην οποία γίνεται χειρισμός των ΔΠΕΕ θα ορισθεί αρμόδια γραμματεία η οποία θα μεριμνά ώστε ο χειρισμός των ΔΠΕΕ να είναι σύμφωνος με την παρούσα απόφαση. Οι γραμματείες θα συσταθούν ως χώροι ασφαλείας όπως ορίζονται στο παράρτημα II.

18. Για τους σκοπούς της παρούσας απόφασης, ως καταχώριση για λόγους ασφαλείας («καταχώριση») νοείται η εφαρμογή διαδικασιών που επιτρέπουν την καταγραφή του κύκλου ζωής του υλικού, η οποία περιλαμβάνει τη διάδοση και την καταστροφή του.

19. Όλο το υλικό με διαβάθμιση CONFIDENTIEL UE/EU CONFIDENTIAL ή υψηλότερη καταχωρίζεται στις αρμόδιες γραμματείες κατά την άφιξη ή την αναχώρησή του από μια οργανωτική μονάδα.

20. Η Κεντρική Γραμματεία εντός της ΓΓΣ τηρεί αρχείο όλων των διαβαθμισμένων πληροφοριών που κοινοποιούνται από το Συμβούλιο και τη ΓΓΣ προς τρίτα κράτη και διεθνείς οργανισμούς, καθώς και όλων των διαβαθμισμένων πληροφοριών που λαμβάνονται από τρίτα κράτη ή διεθνείς οργανισμούς.

21. Στην περίπτωση του CIS, οι διαδικασίες καταχώρισης μπορούν να διεκπεραιώνονται με διεργασίες εντός του ίδιου του CIS.

22. Το Συμβούλιο εγκρίνει πολιτική ασφαλείας σχετικά με την καταχώριση των ΔΠΕΕ για λόγους ασφαλείας.

Γραμματείες TRÈS SECRET UE/EU TOP SECRET

23. Ορίζεται γραμματεία στα κράτη μέλη και στη ΓΓΣ η οποία θα ενεργεί ως κεντρική αρχή παραλαβής και αποστολής πληροφοριών με διαβάθμιση TRÈS SECRET UE/EU TOP SECRET. Οσάκις απαιτείται, μπορούν να ορίζονται υπογραμματείες για τον χειρισμό των πληροφοριών αυτών για λόγους καταχώρισης.

24. Οι υπογραμματείες αυτές δεν δικαιούνται να διαβιβάζουν έγγραφα με διαβάθμιση TRÈS SECRET UE/EU TOP SECRET απευθείας σε άλλες υπογραμματείες της αυτής κεντρικής γραμματείας TRÈS SECRET UE/EU TOP SECRET ή έξωθεν χωρίς τη ρητή γραπτή έγκριση της τελευταίας.

IV. ΑΝΤΙΓΡΑΦΗ ΚΑΙ ΜΕΤΑΦΡΑΣΗ ΔΙΑΒΑΘΜΙΣΜΕΝΩΝ ΕΓΓΑΦΩΝ ΤΗΣ ΕΕ

25. Τα έγγραφα με διαβάθμιση TRÈS SECRET UE/EU TOP SECRET μπορούν να αντιγραφούν ή να μεταφρασθούν μόνο με την προηγούμενη γραπτή συγκατάθεση του φορέα προέλευσης.

26. Όταν ο φορέας προέλευσης εγγράφων με διαβάθμιση SECRET UE/EU SECRET και κατωτέρω δεν έχει επιβάλει προειδοποιήσεις ως προς την αντιγραφή ή τη μετάφρασή τους, τα έγγραφα αυτά μπορούν να αντιγράφονται ή να μεταφράζονται κατόπιν εντολής του κατόχου τους.

27. Τα μέτρα ασφαλείας που εφαρμόζονται για το αρχικό έγγραφο εφαρμόζονται και στα αντίγραφα και μεταφράσεις του.

V. ΜΕΤΑΦΟΡΑ ΤΩΝ ΔΠΕΕ

28. Η μεταφορά των ΔΠΕΕ υπάγεται στα προστατευτικά μέτρα που ορίζονται στις παραγράφους 30 έως 41. Όταν οι ΔΠΕΕ διαβιβάζονται ηλεκτρονικά και παρά τα οριζόμενα στο άρθρο 9 παράγραφος 4, τα παρακάτω προστατευτικά μέτρα μπορούν να συμπληρώνονται με κατάλληλα τεχνικά αντίμετρα που ορίζονται από την αρμόδια αρχή ασφαλείας προκειμένου να ελαχιστοποιείται ο κίνδυνος απώλειας ή διαρροής.

29. Οι αρμόδιες αρχές ασφαλείας της ΓΓΣ και των κρατών μελών εκδίδουν οδηγίες όσον αφορά τη μεταφορά των ΔΠΕΕ σύμφωνα με την παρούσα απόφαση.

Εντός κτιρίου ή αυτοτελούς συνόλου κτιρίων

30. Οι ΔΠΕΕ που μεταφέρονται εντός κτιρίου ή αυτοτελούς συνόλου κτιρίων πρέπει να είναι καλυμμένες για να μην είναι δυνατή η παρατήρηση του περιεχομένου τους.

31. Εντός κτιρίου ή αυτοτελούς συνόλου κτιρίων, οι πληροφορίες με διαβάθμιση TRÈS SECRET UE/EU TOP SECRET μεταφέρονται σε σφραγισμένο φάκελο με μόνη ένδειξη το όνομα του παραλήπτη.

Εντός της Ένωσης

32. Οι ΔΠΕΕ που μεταφέρονται μεταξύ κτιρίων ή χώρων εντός της Ένωσης τοποθετούνται σε συσκευασία η οποία τις προστατεύει από άνευ αδείας κοινολόγηση.

33. Η μεταφορά πληροφοριών με διαβάθμιση CONFIDENTIEL UE/EU CONFIDENTIAL και SECRET UE/EU SECRET εντός της ΕΕ διεξάγεται ως εξής:

α) με στρατιωτικό, κρατικό ή διπλωματικό μεταφορέα, αναλόγως με την περίπτωση,

β) με ιδιόχειρη μεταφορά, εφόσον:

i) οι ΔΠΕΕ παραμένουν στην κατοχή του κομιστή, εκτός εάν φυλάσσονται σύμφωνα με τις απαιτήσεις του παραρτήματος II,

ii) οι ΔΠΕΕ δεν ανοίγονται καθ' οδόν ούτε διαβάζονται σε δημόσιους χώρους,

iii) τα άτομα ενημερώνονται ως προς τις ευθύνες τους περί ασφαλείας και

iv) κατά περίπτωση τα άτομα είναι εφοδιασμένα με πιστοποιητικό αγγελιαφόρου,

γ) με τις ταχυδρομικές υπηρεσίες ή με εμπορικές υπηρεσίες μεταφοράς, με την προϋπόθεση ότι:

i) έχουν εγκριθεί από τις σχετικές ΕΑΑ σύμφωνα με τις εθνικές διατάξεις και ρυθμίσεις και

ii) εφαρμόζουν κατάλληλα μέτρα προστασίας κατά τις ελάχιστες απαιτήσεις των κατευθυντήριων γραμμών που καταρτίζονται σύμφωνα με το άρθρο 6 παράγραφος 2.

Στην περίπτωση μεταφοράς από ένα κράτος μέλος σε άλλο, οι διατάξεις του στοιχείου γ) περιορίζονται στις πληροφορίες με διαβάθμιση έως CONFIDENTIEL UE/EU CONFIDENTIAL.

34. Οι πληροφορίες με διαβάθμιση RESTREINT UE/EU RESTRICTED δύνανται επίσης να μεταφέρονται με ταχυδρομικές υπηρεσίες ή με εμπορικές υπηρεσίες μεταφοράς. Δεν απαιτείται πιστοποιητικό αγγελιαφόρου για τη μεταφορά τέτοιων πληροφοριών.

35. Το υλικό με διαβαθμίσεις CONFIDENTIEL UE/EU CONFIDENTIAL και SECRET UE/EU SECRET (π.χ. εξοπλισμός ή μηχανήματα) που δεν μπορεί να μεταφερθεί όπως αναφέρεται στην παράγραφο 33 μεταφέρεται ως φορτίο από εμπορικές επιχειρήσεις μεταφορών σύμφωνα με το παράρτημα V.

36. Η μεταφορά πληροφοριών με διαβάθμιση TRÈS SECRET UE/EU TOP SECRET μεταξύ κτιρίων ή χώρων εντός της Ένωσης διεξάγεται με στρατιωτικό, κρατικό ή διπλωματικό μεταφορέα, αναλόγως με την περίπτωση.

Από την Ένωση προς το έδαφος τρίτου κράτους

37. Οι ΔΠΕΕ που μεταφέρονται από την Ένωση προς το έδαφος τρίτου κράτους τοποθετούνται σε συσκευασία η οποία τις προστατεύει από άνευ αδείας κοινολόγηση.

38. Η μεταφορά πληροφοριών με διαβαθμίσεις CONFIDENTIEL UE/EU CONFIDENTIAL και SECRET UE/EU SECRET από την Ένωση προς το έδαφος τρίτου κράτους διεξάγεται ως εξής:

α) με στρατιωτικό ή διπλωματικό μεταφορέα,

β) με ιδιόχειρη μεταφορά, εφόσον:

i) το δέμα φέρει επίσημη σφραγίδα, ή είναι συσκευασμένο κατά τρόπο ώστε να επισημαίνεται ότι πρόκειται για επίσημη αποστολή και δεν πρέπει να περάσει από τελωνειακό έλεγχο και έλεγχο ασφαλείας,

ii) τα πρόσωπα είναι εφοδιασμένα με πιστοποιητικό αγγελιαφόρου που προσδιορίζει το δέμα και εξουσιοδοτεί τα εν λόγω πρόσωπα να το μεταφέρουν,

iii) οι ΔΠΕΕ παραμένουν στην κατοχή του κομιστή, εκτός εάν φυλάσσονται σύμφωνα με τις απαιτήσεις του παραρτήματος II,

iv) οι ΔΠΕΕ δεν ανοίγονται καθ' οδόν ούτε διαβάζονται σε δημόσιους χώρους και

v) τα άτομα ενημερώνονται ως προς τις ευθύνες τους περί ασφαλείας.

39. Η μεταφορά πληροφοριών με διαβαθμίσεις CONFIDENTIEL UE/EU CONFIDENTIAL και SECRET UE/EU SECRET που κοινοποιούνται από την Ένωση σε τρίτο κράτος ή διεθνή οργανισμό διεξάγεται κατά τις σχετικές διατάξεις συμφωνίας για την ασφάλεια των πληροφοριών ή διοικητικής συμφωνίας σύμφωνα με το άρθρο 13 παράγραφος 2 στοιχείο α) ή β).

40. Οι πληροφορίες με διαβάθμιση RESTREINT UE/EU RESTRICTED δύνανται επίσης να μεταφέρονται με ταχυδρομικές υπηρεσίες ή με εμπορικές υπηρεσίες μεταφοράς.

41. Η μεταφορά πληροφοριών με διαβάθμιση TRÈS SECRET UE/EU TOP SECRET από την Ένωση προς το έδαφος τρίτου κράτους διεξάγεται με στρατιωτικό ή διπλωματικό μεταφορέα.

VI. ΚΑΤΑΣΤΡΟΦΗ ΔΠΕΕ

42. Τα διαβαθμισμένα έγγραφα ΕΕ που δεν χρειάζονται πλέον μπορούν να καταστρέφονται με την επιφύλαξη των οικείων κανόνων και κανονισμών περί αρχειοθέτησης.

43. Τα έγγραφα τα οποία καταχωρίζονται σύμφωνα με το άρθρο 9 παράγραφος 2 καταστρέφονται από την αρμόδια γραμματεία με εντολή του κατόχου ή αρμόδιας αρχής. Τα ημερολόγια και οι λοιπές πληροφορίες καταχώρισης ενημερώνονται αναλόγως.

44. Για τα έγγραφα με διαβαθμίσεις SECRET UE/EU SECRET ή TRÈS SECRET UE/EU TOP SECRET, η καταστροφή πραγματοποιείται παρουσία μάρτυρα ο οποίος έχει διαβάθμιση ασφαλείας τουλάχιστον έως το επίπεδο διαβάθμισης του προς καταστροφή εγγράφου.

45. Ο γραμματέας και, οσάκις απαιτείται η παρουσία του, ο μάρτυρας υπογράφουν πιστοποιητικό καταστροφής, το οποίο καταχωρίζεται στη γραμματεία. Η γραμματεία τηρεί τα πιστοποιητικά καταστροφής των εγγράφων TRÈS SECRET UE/EU TOP SECRET για δεκαετία τουλάχιστον και των εγγράφων CONFIDENTIEL UE/EU CONFIDENTIAL και SECRET UE/EU SECRET για πενταετία τουλάχιστον.

46. Τα διαβαθμισμένα έγγραφα, περιλαμβανομένων και εκείνων με διαβάθμιση RESTREINT UE/EU RESTRICTED, καταστρέφονται με μεθόδους που ανταποκρίνονται στα σχετικά ενωσιακά πρότυπα ή αντίστοιχα πρότυπα ή που έχουν εγκριθεί από κράτη μέλη σύμφωνα με εθνικές τεχνικές προδιαγραφές προκειμένου να αποφεύγεται η πλήρης ή η εν μέρει επανασύστασή τους.

47. Η καταστροφή των ηλεκτρονικών φορέων αποθήκευσης που χρησιμοποιούνται για τις ΔΠΕΕ διεξάγεται σύμφωνα με την παράγραφο 37 του παραρτήματος IV.

48. Σε κατάσταση έκτακτης ανάγκης, αν υπάρχει άμεσος κίνδυνος άνευ αδείας κοινολόγησης, οι ΔΠΕΕ καταστρέφονται από τον κάτοχο με τρόπο που να μην επιτρέπει την ανασύστασή τους πλήρως ή εν μέρει. Ο φορέας και η γραμματεία προέλευσης ενημερώνονται σχετικά με την έκτακτη καταστροφή των καταχωρισμένων ΔΠΕΕ.

VII. ΕΠΙΣΚΕΨΕΙΣ ΑΞΙΟΛΟΓΗΣΗΣ

49. Εφεξής θα χρησιμοποιείται ο όρος «επίσκεψη αξιολόγησης» προκειμένου να ορίζονται:

α) επιθεωρήσεις ή επισκέψεις αξιολόγησης σύμφωνα με το άρθρο 9 παράγραφος 3 και το άρθρο 16 παράγραφος 2 στοιχεία ε), στ) και ζ) ή

β) επισκέψεις αξιολόγησης σύμφωνα με το άρθρο 13 παράγραφος 5,

προκειμένου να αξιολογείται η αποτελεσματικότητα των μέτρων που εφαρμόζονται για την προστασία των ΔΠΕΕ.

50. Μεταξύ άλλων, επισκέψεις αξιολόγησης διεξάγονται προκειμένου:

α) να διασφαλίζεται ότι τηρούνται οι ελάχιστες απαιτούμενες προδιαγραφές για την προστασία των ΔΠΕΕ που ορίζονται από την παρούσα οδηγία,

β) να δίδεται έμφαση στη σπουδαιότητα της ασφάλειας και της αποτελεσματικής διαχείρισης των κινδύνων εντός των φορέων που επιθεωρούνται,

γ) να προτείνονται αντίμετρα για τον περιορισμό των συγκεκριμένων επιπτώσεων λόγω απώλειας εμπιστευτικότητας, ακεραιότητας ή διαθεσιμότητας των διαβαθμισμένων πληροφοριών και

δ) να ενισχύονται τα τρέχοντα προγράμματα των αρχών ασφαλείας για την εκπαίδευση και ευαισθητοποίηση στον τομέα της ασφάλειας.

51. Πριν από το τέλος κάθε ημερολογιακού έτους, το Συμβούλιο καθορίζει το πρόγραμμα επισκέψεων αξιολόγησης για το επόμενο έτος, όπως προβλέπεται από το άρθρο 16 παράγραφος 1 στοιχείο γ). Οι συγκεκριμένες ημερομηνίες κάθε επίσκεψης αξιολόγησης καθορίζονται κατόπιν συμφωνίας με το λοιπό όργανο ή οργανισμό της Ένωσης, το κράτος μέλος, το τρίτο κράτος ή τον διεθνή οργανισμό.

Διεξαγωγή επισκέψεων αξιολόγησης

52. Οι επισκέψεις αξιολόγησης διεξάγονται προκειμένου να ελεγχθούν οι σχετικοί κανόνες, κανονισμοί και διαδικασίες του φορέα όπου πραγματοποιείται η επίσκεψη και προκειμένου να εξακριβωθεί αν οι πρακτικές του φορέα είναι σύμφωνες προς τις ελάχιστες προδιαγραφές της παρούσας απόφασης και τις διατάξεις περί ανταλλαγής διαβαθμισμένων πληροφοριών με τον εν λόγω φορέα.

53. Οι επισκέψεις αξιολόγησης διενεργούνται σε δύο φάσεις. Πριν από την επίσκεψη αυτή καθεαυτή διοργανώνεται, εάν απαιτείται, προπαρασκευαστική συνάντηση με τον σχετικό φορέα. Μετά την προπαρασκευαστική αυτή συνάντηση η ομάδα αξιολόγησης καταρτίζει, κατόπιν συμφωνίας με τον ενδιαφερόμενο φορέα, λεπτομερές πρόγραμμα επίσκεψης αξιολόγησης που καλύπτει όλους τους τομείς ασφαλείας. Η ομάδα επίσκεψης αξιολόγησης πρέπει να έχει πρόσβαση σε όλους τους χώρους στους οποίους γίνεται χειρισμός ΔΠΕΕ, ειδικότερα δε στις γραμματείες και στα σημεία παρουσίας CIS.

54. Οι επισκέψεις αξιολόγησης στις εθνικές διοικήσεις των κρατών μελών, στα τρίτα κράτη και στους διεθνείς οργανισμούς διεξάγονται σε πλήρη συνεργασία με τους υπαλλήλους του φορέα, τρίτου κράτους ή διεθνούς οργανισμού όπου πραγματοποιείται η επίσκεψη.

55. Οι επισκέψεις αξιολόγησης σε λοιπά όργανα, οργανισμούς και μονάδες της Ένωσης που εφαρμόζουν την παρούσα απόφαση ή τις αρχές της διεξάγονται με τη συνδρομή εμπειρογνωμόνων της ΕΑΑ στο έδαφος της οποίας ευρίσκεται το λοιπό όργανο ή ο οργανισμός.

56. Η Επιτροπή Ασφαλείας δύναται να συμφωνεί λεπτομερείς ρυθμίσεις περί συνδρομής και συνεισφορών από εμπειρογνώμονες της ΕΑΑ για τις επισκέψεις αξιολόγησης σε λοιπά όργανα, οργανισμούς και μονάδες της Ένωσης που εφαρμόζουν την παρούσα απόφαση ή τις αρχές της, καθώς και σε τρίτα κράτη και διεθνείς οργανισμούς.

Εκθέσεις

57. Μετά το πέρας της επίσκεψης αξιολόγησης υποβάλλονται στον φορέα όπου πραγματοποιήθηκε η επίσκεψη τα κυριότερα συμπεράσματα και συστάσεις. Εν συνεχεία συντάσσεται έκθεση για την επίσκεψη αξιολόγησης. Στις περιπτώσεις στις οποίες προτείνονται διορθωτικές ενέργειες και συστάσεις, πρέπει να περιλαμβάνονται στην έκθεση επαρκώς λεπτομερή στοιχεία προς αιτιολόγηση των συμπερασμάτων. Η έκθεση διαβιβάζεται στην αρμόδια αρχή του φορέα όπου πραγματοποιήθηκε η επίσκεψη.

58. Όσον αφορά τις επισκέψεις αξιολόγησης που διενεργούνται στις κρατικές υπηρεσίες των κρατών μελών:

α) το σχέδιο έκθεσης αξιολόγησης διαβιβάζεται στην ενδιαφερόμενη ΕΑΑ για να εξακριβωθεί ότι είναι αντικειμενικά ορθό και ότι δεν περιέχει καμία πληροφορία με διαβάθμιση υψηλότερη από RESTREINT UE/EU RESTRICTED και

β) οι εκθέσεις αξιολόγησης διανέμονται στην Επιτροπή Ασφαλείας, εκτός αν η ΕΑΑ του οικείου κράτους μέλους ζητήσει να μη γίνει γενική διανομή. Η έκθεση λαμβάνει τη διαβάθμιση RESTREINT UE/EU RESTRICTED.

Συντάσσεται τακτική έκθεση υπό την ευθύνη της Αρχής ασφαλείας της ΓΓΣ (Υπηρεσίας Ασφαλείας) στην οποία επισημαίνονται τα κυριότερα ζητήματα που ανέκυψαν και τα διδάγματα που αποκομίσθηκαν από τις επισκέψεις αξιολόγησης οι οποίες διενεργήθηκαν στα κράτη μέλη εντός συγκεκριμένης περιόδου και εξετάσθηκαν από την Επιτροπή Ασφαλείας.

59. Όσον αφορά τις επισκέψεις αξιολόγησης τρίτων κρατών και διεθνών οργανισμών, η έκθεση διανέμεται στην Επιτροπή Ασφαλείας. Η έκθεση λαμβάνει τουλάχιστον διαβάθμιση RESTREINT UE/EU RESTRICTED. Τυχόν διορθωτικές ενέργειες πρέπει να επαληθεύονται αργότερα με νέα επίσκεψη και να υποβάλλεται σχετική έκθεση στην Επιτροπή Ασφαλείας.

60. Όσον αφορά τις επισκέψεις αξιολόγησης σε λοιπά όργανα, οργανισμούς και μονάδες της Ένωσης που εφαρμόζουν την παρούσα απόφαση ή τις αρχές της, οι εκθέσεις με θέμα την επίσκεψη αξιολόγησης διανέμονται στην Επιτροπή Ασφαλείας. Το σχέδιο έκθεσης με θέμα την επίσκεψη αξιολόγησης διαβιβάζεται στην ενδιαφερόμενη υπηρεσία ή οργανισμό για να εξακριβωθεί ότι είναι αντικειμενικά ορθό και δεν περιέχει καμία πληροφορία με διαβάθμιση υψηλότερη από RESTREINT UE/EU RESTRICTED. Τυχόν διορθωτικές ενέργειες επαληθεύονται αργότερα με νέα επίσκεψη και υποβάλλεται σχετική έκθεση στην Επιτροπή Ασφαλείας.

61. Η Αρχή Ασφαλείας της ΓΓΣ διεξάγει τακτικές επιθεωρήσεις οργανωτικών μονάδων της ΓΓΣ για τους σκοπούς της παραγράφου 50.

Κατάλογος ελέγχου

62. Η Αρχή Ασφαλείας της ΓΓΣ (Υπηρεσία Ασφαλείας) καταρτίζει και ενημερώνει κατάλογο ελέγχου, με τα θέματα που πρέπει να ελέγχονται κατά τη διάρκεια επίσκεψης αξιολόγησης. Ο εν λόγω κατάλογος ελέγχου διαβιβάζεται στην Επιτροπή Ασφαλείας.

63. Οι πληροφορίες για τη συμπλήρωση του καταλόγου ελέγχου λαμβάνονται κυρίως κατά τη διάρκεια της επίσκεψης από το προσωπικό διαχείρισης ασφαλείας του επιθεωρούμενου φορέα. Μόλις συμπληρωθεί με λεπτομερείς απαντήσεις, ο κατάλογος ελέγχου διαβαθμίζεται σε συμφωνία με τον επιθεωρούμενο φορέα. Δεν συνιστά μέρος της έκθεσης επιθεώρησης.

ΠΑΡΑΡΤΗΜΑ IV

ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΔΠΕΕ ΠΟΥ ΑΠΟΤΕΛΟΥΝ ΑΝΤΙΚΕΙΜΕΝΟ ΧΕΙΡΙΣΜΟΥ ΣΕ CIS

I. ΕΙΣΑΓΩΓΗ

1. Το παρόν παράρτημα περιέχει διατάξεις για την εφαρμογή του άρθρου 10.

2. Οι ακόλουθες ιδιότητες και έννοιες ΙΑ είναι ουσιαστικές για την ασφάλεια και την ορθή εφαρμογή δράσεων στο πλαίσιο συστημάτων CIS:

Γνησιότητα: η εγγύηση ότι οι πληροφορίες είναι γνήσιες και από καλόπιστες πηγές,

Διαθεσιμότητα: η ιδιότητα του συστήματος να είναι διαθέσιμο και έτοιμο προς χρήση κατόπιν αιτήματος εξουσιοδοτημένου φορέα,

Εμπιστευτικότητα: η ιδιότητα της μη κοινολόγησης πληροφοριών σε μη εξουσιοδοτημένα πρόσωπα, φορείς ή διαδικασίες,

Ακεραιότητα: η ιδιότητα της διαφύλαξης της ακρίβειας και της πληρότητας των πληροφοριών και των στοιχείων,

Μη άρνηση αναγνώρισης: η ικανότητα απόδειξης της διεξαγωγής ενέργειας ή γεγονότος, ούτως ώστε να μην είναι δυνατή η άρνηση της εν λόγω ενέργειας ή του γεγονότος.

II. ΑΡΧΕΣ ΤΗΣ ΔΙΑΣΦΑΛΙΣΗΣ ΤΩΝ ΠΛΗΡΟΦΟΡΙΩΝ

3. Οι κατωτέρω διατάξεις αποτελούν τη βάση για την ασφάλεια όλων των CIS που χειρίζονται ΔΠΕΕ. Λεπτομερείς απαιτήσεις για την εφαρμογή των διατάξεων αυτών θα καθορισθούν σε πολιτικές ασφαλείας ΙΑ και κατευθυντήριες γραμμές ασφαλείας.

Διαχείριση των κινδύνων κατά της ασφάλειας

4. Η διαχείριση κινδύνων κατά της ασφαλείας αποτελεί αναπόσπαστο μέρος του σχεδιασμού, της ανάπτυξης, της λειτουργίας και της συντήρησης των CIS. Η διαχείριση του κινδύνου (αξιολόγηση, χειρισμός, αποδοχή και κοινοποίηση) διεξάγεται ως επαναληπτική διαδικασία, από κοινού από τους εκπροσώπους των ιδιοκτητών των συστημάτων, τις αρχές των προγραμμάτων, τις επιχειρησιακές αρχές και τις αρχές έγκρισης ασφαλείας, με χρήση δοκιμασμένης, διαφανούς και πλήρως κατανοητής διαδικασίας αξιολόγησης του κινδύνου. Το πεδίο εφαρμογής των CIS και τα στοιχεία τους ορίζονται με σαφήνεια στην αρχή της διαδικασίας διαχείρισης του κινδύνου.

5. Οι αρμόδιες αρχές εξετάζουν τις εν δυνάμει απειλές που αντιμετωπίζουν τα CIS και διατηρούν ενημερωμένες και ακριβείς αξιολογήσεις κινδύνου που αντιστοιχούν στο τρέχον επιχειρησιακό περιβάλλον. Ενημερώνουν διαρκώς τις γνώσεις τους ως προς τα ζητήματα τρωτότητας και επανεξετάζουν περιοδικά την αξιολόγηση τρωτότητας προκειμένου να ανταποκρίνονται στο εξελισσόμενο περιβάλλον της τεχνολογίας των πληροφοριών (ΤΠ).

6. Ο στόχος του χειρισμού των κινδύνων κατά της ασφαλείας αποσκοπεί στην εφαρμογή δέσμης μέτρων ασφαλείας που αποτελούν μια ικανοποιητική ισορροπία μεταξύ των απαιτήσεων των χρηστών, του κόστους και του υπολειπόμενου κινδύνου κατά της ασφαλείας.

7. Οι ειδικές προδιαγραφές, η κλίμακα και ο βαθμός των λεπτομερειών που καθορίζονται από την αρμόδια ΑΠΑ για το χειρισμό CIS είναι αναλογικές προς τον αξιολογούμενο κίνδυνο, λαμβάνουν δε υπόψη όλους τους συναφείς παράγοντες και μεταξύ άλλων το επίπεδο διαβάθμισης των ΔΠΕΕ που τυγχάνουν χειρισμού σε CIS. Η έγκριση λειτουργίας περιλαμβάνει τυπική δήλωση υπολειπόμενου κινδύνου και την αποδοχή του υπολειπόμενου κινδύνου από υπεύθυνη αρχή.

Ασφάλεια καθ' όλη τη διάρκεια του κύκλου ζωής του CIS

8. Η εγγύηση της ασφαλείας αποτελεί απαίτηση σε όλη τη διάρκεια του κύκλου ζωής του CIS από το σχεδιασμό έως την απόσυρση από την υπηρεσία.

9. Ο ρόλος και η συμβολή κάθε συμμετέχοντος σε CIS φορέα ως προς την ασφάλειά του προσδιορίζεται σε κάθε φάση του κύκλου ζωής.

10. Όλα τα CIS, συμπεριλαμβανομένων των τεχνικών και μη τεχνικών μέτρων ασφαλείας, υποβάλλονται σε δοκιμές ασφαλείας κατά τη διάρκεια της διαδικασίας έγκρισης προκειμένου να εξασφαλίζεται ότι έχει επιτευχθεί το κατάλληλο επίπεδο ασφαλείας και να επαληθεύεται ότι έχουν ορθώς εφαρμοσθεί, ολοκληρωθεί και διαμορφωθεί.

11. Αξιολογήσεις ασφαλείας, επιθεωρήσεις και έλεγχοι διεξάγονται κατά τακτά διαστήματα στη διάρκεια της λειτουργίας και της συντήρησης του CIS καθώς και όταν προκύπτουν έκτακτες καταστάσεις.

12. Η τεκμηρίωση ασφαλείας ενός CIS εξελίσσεται κατά τη διάρκεια του κύκλου ζωής του ως αναπόσπαστο μέρος της διαδικασίας διαχείρισης της αλλαγής και της διαμόρφωσης.

Βέλτιστη πρακτική

13. Η ΓΓΣ και τα κράτη μέλη συνεργάζονται για την ανάπτυξη βέλτιστων πρακτικών για την προστασία των ΔΠΕΕ τις οποίες χειρίζονται τα CIS. Οι οδηγίες βέλτιστων πρακτικών περιλαμβάνουν κατάλογο τεχνικών, φυσικών, οργανωτικών και διαδικαστικών μέτρων ασφαλείας για CIS των οποίων έχει αποδειχθεί η αποτελεσματικότητα στην αντιμετώπιση δεδομένων απειλών και τρωτών σημείων.

14. Η προστασία των ΔΠΕΕ τις οποίες χειρίζονται τα CIS επωφελείται από τα διδάγματα που έχουν αποκομίσει οι αρχές που συμμετέχουν σε ΙΑ, τόσο εντός της Ένωσης όσο και εκτός αυτής.

15. Η διάδοση και επακόλουθη εφαρμογή βέλτιστων πρακτικών βοηθούν στην επίτευξη ισοδύναμου επιπέδου ασφαλείας για τα διάφορα CIS που χρησιμοποιούνται από τη ΓΓΣ και τα κράτη μέλη και τα οποία χειρίζονται ΔΠΕΕ.

Ασφάλεια εις βάθος

16. Για τον περιορισμό του κινδύνου που αντιμετωπίζουν τα CIS, εφαρμόζεται σειρά τεχνικών και μη τεχνικών μέτρων ασφαλείας, τα οποία οργανώνονται ως πολλαπλά επίπεδα άμυνας. Τα επίπεδα αυτά περιλαμβάνουν τα εξής:

α) *Αποτροπή:* μέτρα ασφαλείας που αποσκοπούν στην αποτροπή οποιουδήποτε αντίπαλου σχεδιασμού για επίθεση σε CIS,

β) *Πρόληψη:* μέτρα ασφαλείας που αποσκοπούν στην παρεμπόδιση ή στην ανάσχεση επίθεσης σε CIS,

γ) *Ανίχνευση:* μέτρα ασφαλείας που αποσκοπούν στον εντοπισμό της εμφάνισης επίθεσης σε CIS,

δ) *Ανθεκτικότητα:* μέτρα ασφαλείας που αποσκοπούν στον περιορισμό των συνεπειών της επίθεσης σε ελάχιστο σύνολο πληροφοριών ή στοιχείων CIS και στην πρόληψη περαιτέρω ζημιών και

ε) *Ανάκτηση:* μέτρα ασφαλείας που αποσκοπούν στην αποκατάσταση της ασφάλειας του CIS.

Ο βαθμός αυστηρότητας των εν λόγω μέτρων ασφαλείας καθορίζεται από την αξιολόγηση κινδύνου.

17. Η ΕΑΑ ή άλλη αρμόδια αρχή εξασφαλίζει ότι:

α) υφίστανται ικανότητες για άμυνα στον κυβερνοχώρο όσον αφορά την αντιμετώπιση απειλών που ενδέχεται να υπερβαίνουν τα όρια οργανισμών και κρατών και

β) συντονίζονται οι αντιδράσεις και ανταλλάσσονται πληροφορίες σχετικά με τις εν λόγω απειλές και συμβάντα και τον συναφή κίνδυνο (ικανότητες του υπολογιστή για ανταπόκριση σε επείγουσες καταστάσεις).

Αρχή της ελαχιστότητας και των ελάχιστων προνομίων

18. Για την αντιμετώπιση των λειτουργικών απαιτήσεων θα χρησιμοποιούνται μόνον οι βασικές λειτουργίες, συσκευές και υπηρεσίες προκειμένου να αποφεύγονται οι περιττοί κίνδυνοι.

19. Στους χρήστες CIS και στις αυτοματοποιημένες διαδικασίες θα παρέχονται μόνο οι απαραίτητες δυνατότητες πρόσβασης, προνόμια ή εξουσιοδοτήσεις για την εκτέλεση των καθηκόντων τους προκειμένου να περιορίζονται τυχόν βλάβες λόγω ατυχήματος, σφάλματος ή μη εξουσιοδοτημένης χρήσης των πόρων των CIS.

20. Οι διαδικασίες καταχώρισης που εκτελεί ένα CIS, εφόσον απαιτείται, επαληθεύονται ως μέρος της διαδικασίας έγκρισης.

Ευαισθητοποίηση ως προς τη διασφάλιση πληροφοριών

21. Η ευαισθητοποίηση ως προς τους κινδύνους και τα διαθέσιμα μέτρα ασφαλείας αποτελεί την πρώτη γραμμή άμυνας για την ασφάλεια των CIS. Ειδικότερα, το σύνολο του προσωπικού που συμμετέχει στον κύκλο ζωής του CIS, περιλαμβανομένων και των χρηστών, πρέπει να κατανοεί:

α) ότι οι διαρροές ασφαλείας μπορούν να βλάψουν σημαντικά τα CIS,

β) τις ενδεχόμενες βλάβες σε τρίτους που μπορεί να προκύψουν από τη διασυνδεσιμότητα και την αλληλεξάρτηση και

γ) την ατομική ευθύνη και την υποχρέωση λογοδοσίας τους ως προς την ασφάλεια των CIS ανάλογα με το δικό τους ρόλο στο πλαίσιο των συστημάτων και διαδικασιών.

22. Για να διασφαλισθεί ότι γίνονται αντιληπτές οι ευθύνες ως προς την ασφάλεια, η εκπαίδευση και η ευαισθητοποίηση σε θέματα ΙΑ είναι υποχρεωτική για όλα τα μέλη του προσωπικού, συμπεριλαμβανομένων των ανώτερων στελεχών και των χρηστών CIS.

Αξιολόγηση και έγκριση προϊόντων ασφαλείας ΤΠ

23. Ο απαιτούμενος βαθμός εμπιστοσύνης στα μέτρα ασφαλείας, οριζόμενος ως επίπεδο βεβαιότητας, καθορίζεται ανάλογα με την έκβαση της διαδικασίας διαχείρισης κινδύνων και σύμφωνα με τις οικείες πολιτικές και κατευθυντήριες γραμμές ασφαλείας.

24. Το επίπεδο βεβαιότητας επαληθεύεται με τη χρήση διεθνώς αναγνωρισμένων ή εθνικά εγκεκριμένων διαδικασιών και μεθόδων. Πρόκειται κυρίως για τη διενέργεια αξιολογήσεων και διεξαγωγή ελέγχων.

25. Τα κρυπτογραφικά προϊόντα προστασίας ΔΠΕΕ αξιολογούνται και εγκρίνονται από εθνική CAA κράτους μέλους.

26. Προτού προταθούν για έγκριση από το Συμβούλιο ή τον γενικό γραμματέα σύμφωνα με το άρθρο 10 παράγραφος 6, τα κρυπτογραφικά αυτά προϊόντα υφίστανται μια δεύτερη επιτυχή αξιολόγηση από εγκεκριμένη αρχή αξιολόγησης (AQUA) κράτους μέλους που δεν συμμετέχει στο σχεδιασμό ή την κατασκευή του εξοπλισμού. Ο βαθμός λεπτομέρειας που απαιτείται κατά τη δεύτερη αξιολόγηση εξαρτάται από το μελετώμενο μέγιστο επίπεδο διαβάθμισης των ΔΠΕΕ που θα προστατεύονται από τα προϊόντα αυτά. Το Συμβούλιο εγκρίνει πολιτική ασφαλείας για την αξιολόγηση και έγκριση κρυπτογραφικών προϊόντων.

27. Οσάκις δικαιολογείται για συγκεκριμένους επιχειρησιακούς λόγους, το Συμβούλιο ή ενδεχομένως ο γενικός γραμματέας μπορούν, κατόπιν συστάσεως της Επιτροπής Ασφαλείας, να αποφασίσουν ότι δεν θα εφαρμοσθούν οι προδιαγραφές των παραγράφων 25 ή 26 του παρόντος παραρτήματος και να χορηγήσουν προσωρινή έγκριση για συγκεκριμένη περίοδο, με τη διαδικασία του άρθρου 10 παράγραφος 6.

28. Το Συμβούλιο, ύστερα από σύσταση της Επιτροπής Ασφαλείας, δύναται να κάνει δεκτή τη διαδικασία αξιολόγησης, επιλογής και έγκρισης των κρυπτογραφικών προϊόντων ενός τρίτου κράτους ή διεθνούς οργανισμού και να θεωρεί συνεπώς ότι τα εν λόγω προϊόντα εγκρίνονται για την προστασία ΔΠΕΕ που κοινοποιούνται στο συγκεκριμένο τρίτο κράτος ή διεθνή οργανισμό.

29. Η AQUA πρέπει να είναι CAA ενός κράτους μέλους που έχει λάβει έγκριση βάσει κριτηρίων που έχει ορίσει το Συμβούλιο, για τη διεξαγωγή της δεύτερης αξιολόγησης των κρυπτογραφικών προϊόντων για την προστασία ΔΠΕΕ.

30. Το Συμβούλιο εγκρίνει πολιτική ασφαλείας για την αποδοχή και έγκριση μη κρυπτογραφικών προϊόντων ασφαλείας ΤΠ.

Διαβίβαση εντός χώρων ασφαλείας και διοικητικών χώρων

31. Με την επιφύλαξη των διατάξεων της παρούσας απόφασης, όταν η διαβίβαση των ΔΠΕΕ περιορίζεται εντός ασφαλών χώρων ή διοικητικών χώρων, μπορεί να χρησιμοποιείται η μη κρυπτογραφημένη διαβίβαση ή η κρυπτογράφηση σε χαμηλότερο επίπεδο βασιζόμενη στα αποτελέσματα διαδικασίας διαχείρισης του κινδύνου και με την έγκριση της ΕΠΑ.

Ασφαλής διασύνδεση CIS

32. Για τους σκοπούς της παρούσας απόφασης, ως διασύνδεση νοείται η άμεση διασύνδεση μονής ή πολλαπλής κατεύθυνσης, δύο ή περισσοτέρων συστημάτων ΤΠ για την ανταλλαγή δεδομένων και άλλων πληροφοριών (π.χ. επικοινωνία).

33. Ένα CIS πρέπει να αντιμετωπίζει οποιοδήποτε διασυνδεδεμένο σύστημα ΤΠ ως μη έμπιστο και να εφαρμόζει μέτρα προστασίας για τον έλεγχο της ανταλλαγής διαβαθμισμένων πληροφοριών.

34. Για όλες τις διασυνδέσεις CIS με άλλο σύστημα ΤΠ πρέπει να τηρούνται οι ακόλουθες βασικές απαιτήσεις:

α) οι αρμόδιες αρχές αναφέρουν και εγκρίνουν τις επαγγελματικές ή λειτουργικές απαιτήσεις για τις διασυνδέσεις αυτές,

β) η διασύνδεση υποβάλλεται σε διαδικασία διαχείρισης κινδύνου και έγκρισης και απαιτεί την έγκριση των αρμόδιων Αρχών Πιστοποίησης της Ασφάλειας (ΕΠΑ) και

γ) στην περίμετρο όλων των CIS συστήνονται υπηρεσίες περιφερειακής προστασίας (BPS).

35. Δεν επιτρέπεται διασύνδεση μεταξύ ενός CIS που έχει λάβει έγκριση με μη προστατευόμενο ή δημόσιο δίκτυο, εκτός εάν το CIS έχει εγκρίνει υπηρεσίες περιφερειακής προστασίας (BPS) που έχουν εγκατασταθεί για το σκοπό αυτό μεταξύ του CIS και του μη προστατευόμενου ή δημόσιου δικτύου. Τα μέτρα ασφαλείας για τις διασυνδέσεις αυτές επανεξετάζονται από την αρμόδια ΙΑ και εγκρίνονται από την αρμόδια ΕΠΑ.

Όταν το μη προστατευόμενο ή δημόσιο δίκτυο χρησιμοποιείται αποκλειστικά ως φορέας και τα δεδομένα έχουν κρυπτογραφηθεί από κρυπτογραφικό προϊόν που έχει λάβει έγκριση σύμφωνα με το άρθρο 10, η σύνδεση αυτή δεν θεωρείται ως διασύνδεση.

36. Η άμεση ή διαδοχική σύνδεση ενός CIS που έχει λάβει έγκριση να χειρίζεται διαβάθμιση TRÈS SECRET UE/EU TOP SECRET με μη προστατευόμενο ή δημόσιο δίκτυο απαγορεύεται.

Ηλεκτρονικοί φορείς αποθήκευσης

37. Οι ηλεκτρονικοί φορείς αποθήκευσης καταστρέφονται σύμφωνα με εγκεκριμένες από την αρμόδια αρχή ασφαλείας διαδικασίες.

38. Οι ηλεκτρονικοί φορείς αποθήκευσης επαναχρησιμοποιούνται, υποχαρακτηρίζονται ή αποχαρακτηρίζονται σύμφωνα με κατευθυντήριες γραμμές ασφαλείας που καταρτίζονται κατά το άρθρο 6 παράγραφος 2.

Καταστάσεις έκτακτης ανάγκης

39. Παρά τις διατάξεις της παρούσας απόφασης, οι κατωτέρω περιγραφόμενες ειδικές διαδικασίες μπορούν να εφαρμόζονται σε περιπτώσεις έκτακτης ανάγκης, όπως καταστάσεις επικείμενης ή πραγματικής κρίσης, σύγκρουσης ή πολέμου ή υπό εξαιρετικές επιχειρησιακές περιστάσεις.

40. Οι ΔΠΕΕ μπορούν να διαβιβάζονται με τη χρήση κρυπτογραφικών προϊόντων που έχουν λάβει έγκριση για χαμηλότερο επίπεδο διαβάθμισης ή χωρίς κρυπτογράφηση, με τη συγκατάθεση της αρμόδιας αρχής, εάν οποιαδήποτε καθυστέρηση θα ήταν ικανή να προξενήσει ζημιά σαφώς μεγαλύτερη από τη ζημιά που θα προκαλούσε η τυχόν κοινολόγηση του διαβαθμισμένου υλικού και εφόσον:

α) ο αποστολέας και ο παραλήπτης δεν διαθέτουν αντιστοίχως τους απαιτούμενους κρυπτογραφικούς χώρους ή καθόλου χώρους και

β) δεν υπάρχει άλλος τρόπος έγκαιρης μετάδοσης του διαβαθμισμένου υλικού.

41. Οι διαβαθμισμένες πληροφορίες που διαβιβάζονται υπό τις περιστάσεις που περιγράφονται στην παράγραφο 39 δεν πρέπει να φέρουν σημάνσεις ή ενδείξεις που τις διακρίνουν από μη διαβαθμισμένες πληροφορίες ή από πληροφορίες που μπορούν να προστατευθούν με τα διαθέσιμα κρυπτογραφικά προϊόντα. Οι παραλήπτες τους πρέπει να ενημερώνονται αμελλητί για το επίπεδο διαβάθμισης με άλλα μέσα.

42. Σε περίπτωση εφαρμογής της παραγράφου 39, αποστέλλεται σχετική έκθεση στην αρμόδια αρχή και στην Επιτροπή Ασφαλείας.

III. ΛΕΙΤΟΥΡΓΙΕΣ ΚΑΙ ΑΡΧΕΣ ΔΙΑΣΦΑΛΙΣΗΣ ΠΛΗΡΟΦΟΡΙΩΝ

43. Θεσπίζονται οι ακόλουθες λειτουργίες ΙΑ στα κράτη μέλη και στη ΓΓΣ. Οι λειτουργίες αυτές δεν απαιτούν τη σύσταση ενιαίων οργανωτικών μονάδων. Έχουν χωριστές εντολές. Ωστόσο, οι λειτουργίες αυτές και οι σχετικές ευθύνες μπορούν να συνδυάζονται ή να εντάσσονται στην ίδια μονάδα ή να χωρίζονται σε διαφορετικές μονάδες, υπό την προϋπόθεση ότι αποφεύγονται οι εσωτερικές συγκρούσεις συμφερόντων ή καθηκόντων.

Αρχή Διασφάλισης Πληροφοριών

44. Η ΙΑ είναι υπεύθυνη για τα εξής:

α) χάραξη πολιτικών ασφαλείας και κατευθυντήριων γραμμών ασφαλείας ΙΑ και παρακολούθηση της αποτελεσματικότητας και της συνάφειάς τους,

β) διαφύλαξη και διαχείριση τεχνικών πληροφοριών που αφορούν κρυπτογραφικά προϊόντα,

γ) διασφάλιση ότι τα μέτρα ΙΑ που επιλέγονται για την προστασία των ΔΠΕΕ τηρούν τις σχετικές πολιτικές ως προς την επιλεξιμότητα και την επιλογή τους,

δ) διασφάλιση ότι τα κρυπτογραφικά προϊόντα επιλέγονται σύμφωνα με τις πολιτικές που διέπουν την επιλεξιμότητα και την επιλογή τους,

ε) συντονισμός της εκπαίδευσης και της ευαισθητοποίησης ως προς την ΙΑ,

στ) διαβούλευση με τον πάροχο του συστήματος, τους φορείς της ασφάλειας και τους εκπροσώπους των χρηστών όσον αφορά τις πολιτικές ασφαλείας και τις κατευθυντήριες γραμμές ασφαλείας ΙΑ και

ζ) εξασφάλιση ότι υφίσταται η κατάλληλη εμπειρογνωμοσύνη στην υποομάδα εμπειρογνωμόνων της Επιτροπής Ασφαλείας για ζητήματα ΙΑ.

Αρχή TEMPEST

45. Η Αρχή TEMPEST (TA) είναι αρμόδια για την εξασφάλιση της συμμόρφωσης του CIS με τις πολιτικές και κατευθυντήριες γραμμές του TEMPEST. Εγκρίνει αντίμετρα TEMPEST για εγκαταστάσεις και προϊόντα που προορίζονται για την προστασία των ΔΠΕΕ μέχρις ορισμένου επιπέδου διαβάθμισης στο επιχειρησιακό τους περιβάλλον.

Αρχή Έγκρισης Κρυπτογραφικών Μεθόδων

46. Η Αρχή Έγκρισης Κρυπτογραφικών Μεθόδων (CAA) είναι αρμόδια να διασφαλίζει τη συμβατότητα των κρυπτογραφικών προϊόντων με την εθνική κρυπτογραφική πολιτική ή την κρυπτογραφική πολιτική του Συμβουλίου. Εγκρίνει κρυπτογραφικά προϊόντα για την προστασία ΔΠΕΕ μέχρις ορισμένου επιπέδου διαβάθμισης στο επιχειρησιακό τους περιβάλλον. Όσον αφορά τα κράτη μέλη, η CAA είναι επίσης αρμόδια για την αξιολόγηση κρυπτογραφικών μεθόδων.

Αρχή Διανομής Κρυπτογραφικών Μεθόδων

47. Η Αρχή Διανομής Κρυπτογραφικών Μεθόδων (CDA) είναι υπεύθυνη για τα εξής:

α) διαχείριση και καταμέτρηση του κρυπτογραφικού υλικού της ΕΕ,

β) εξασφάλιση της εφαρμογής των κατάλληλων διαδικασιών και της δημιουργίας διαύλων για την καταμέτρηση, τον ασφαλή χειρισμό, την αποθήκευση και τη διανομή όλου του κρυπτογραφικού υλικού της ΕΕ και

γ) διασφάλιση της μεταφοράς κρυπτογραφικού υλικού της ΕΕ από και προς άτομα ή υπηρεσίες που το χρησιμοποιούν.

Αρχή Πιστοποίησης της Ασφάλειας

48. Η ΑΠΑ κάθε συστήματος είναι επιφορτισμένη με τα εξής:

α) μέριμνα ώστε τα CIS να είναι σύμφωνα με τις οικείες πολιτικές ασφαλείας και κατευθυντήριες γραμμές ασφαλείας, με την παροχή δήλωσης έγκρισης των CIS για το χειρισμό ΔΠΕΕ μέχρις ορισμένου επιπέδου διαβάθμισης εντός του επιχειρησιακού τους περιβάλλοντος, στην οποία περιέχεται μνεία των όρων της διαπίστευσης, και των κριτηρίων βάσει των οποίων απαιτείται νέα έγκριση,

β) θέσπιση διαδικασίας πιστοποίησης ασφαλείας, σύμφωνα με τις σχετικές πολιτικές, όπου αναφέρονται με σαφήνεια οι προϋποθέσεις έγκρισης για τα CIS υπό την ευθύνη της,

γ) χάραξη στρατηγικής πιστοποίησης ασφαλείας στην οποία ορίζεται ο βαθμός λεπτομέρειας για τη διαδικασία πιστοποίησης ο οποίος είναι ανάλογος με το απαιτούμενο επίπεδο βεβαιότητας,

δ) εξέταση και έγκριση τεκμηρίωσης που αφορά την ασφάλεια, περιλαμβανομένων των δηλώσεων διαχείρισης κινδύνου και υπολειπόμενου κινδύνου, των δηλώσεων ειδικών για κάθε σύστημα απαιτήσεων ασφαλείας («SSRS»), της τεκμηρίωσης σχετικά με τον έλεγχο εφαρμογής της ασφαλείας και των λειτουργικών διαδικασιών ασφαλείας («SecOPs»), και εξασφάλιση της τήρησης των κανόνων και πολιτικών ασφαλείας του Συμβουλίου,

ε) έλεγχο της εφαρμογής των μέτρων ασφαλείας αναφορικά με τα CIS μέσω της ανάληψης ή ανάθεσης αξιολογήσεων, επιθεωρήσεων ή ελέγχων ασφαλείας,

στ) ορισμό των απαιτήσεων ασφαλείας (π.χ. επιπέδων διαβάθμισης του προσωπικού) για ευαίσθητες θέσεις αναφορικά με το CIS,

ζ) έγκριση της επιλογής των εγκεκριμένων κρυπτογραφικών προϊόντων και προϊόντων TEMPEST που χρησιμοποιούνται για την παροχή ασφαλείας σε CIS,

η) έγκριση, ή κατά περίπτωση, συμμετοχή στην κοινή έγκριση της διασύνδεσης ενός CIS με άλλα CIS, και

θ) διαβούλευση με τον πάροχο του συστήματος, τους φορείς ασφαλείας και τους εκπροσώπους των χρηστών όσον αφορά τη διαχείριση του κινδύνου ασφαλείας και ειδικότερα του υπολειπόμενου κινδύνου, καθώς και τους όρους και τις προϋποθέσεις της δήλωσης έγκρισης.

49. Η ΑΠΑ της ΓΓΣ είναι αρμόδια για την έγκριση όλων των CIS που λειτουργούν στο πλαίσιο των αρμοδιοτήτων της ΓΓΣ.

50. Οι αρμόδιες ΑΠΑ των κρατών μελών είναι αρμόδιες για την έγκριση όλων των CIS και των συνιστωσών των CIS που λειτουργούν στο πλαίσιο των αρμοδιοτήτων των κρατών μελών.

51. Το κοινό Συμβούλιο Πιστοποίησης Ασφαλείας (ΣΠΑ) είναι υπεύθυνο για την έγκριση CIS στο πλαίσιο των αρμοδιοτήτων τόσο της ΑΠΑ της ΓΓΣ όσο και των ΑΠΑ των κρατών μελών. Αποτελείται από έναν εκπρόσωπο ΑΠΑ εκάστου κράτους μέλους και στις συνεδριάσεις του συμμετέχει εκπρόσωπος ΑΠΑ της Επιτροπής. Θα καλούνται να συμμετέχουν και άλλοι φορείς που διαθέτουν κόμβους σε CIS όταν θα συζητείται το εν λόγω σύστημα.

Το ΣΠΑ προεδρεύεται από εκπρόσωπο της ΑΠΑ της ΓΓΣ. Ενεργεί με τη συναίνεση των εκπροσώπων ΑΠΑ των θεσμικών οργάνων, των κρατών μελών και άλλων φορέων που διαθέτουν κόμβους στο CIS. Το ΣΠΑ υποβάλλει περιοδικές εκθέσεις ως προς τις δραστηριότητές του στην Επιτροπή ασφαλείας και της κοινοποιεί όλες τις δηλώσεις έγκρισης λειτουργίας.

Επιχειρησιακή Αρχή Διασφάλισης Πληροφοριών

52. Η Επιχειρησιακή Αρχή ΙΑ κάθε συστήματος είναι επιφορτισμένη με τα εξής:

α) ανάπτυξη τεκμηρίωσης ως προς την ασφάλεια σύμφωνα με τις πολιτικές και τις κατευθυντήριες γραμμές ασφαλείας, ειδικότερα των SSRS, συμπεριλαμβανομένων της δήλωσης υπολειπόμενου κινδύνου, των λειτουργικών διαδικασιών ασφαλείας (SecOPs) και του κρυπτογραφικού σχεδίου στο πλαίσιο της διαδικασίας έγκρισης του CIS,

β) συμμετοχή στην επιλογή και δοκιμή των ειδικών για κάθε σύστημα τεχνικών μέτρων, συσκευών και λογισμικού ασφαλείας, επίβλεψη της εφαρμογής τους και εξασφάλιση της ασφαλούς εγκατάστασης, ρύθμισης και συντήρησής τους σύμφωνα με τις οικείες ρυθμίσεις ασφαλείας,

γ) συμμετοχή στην επιλογή μέτρων και συσκευών ασφαλείας TEMPEST εφόσον απαιτείται από τις SSRS και διασφάλιση της ασφαλούς εγκατάστασης και συντήρησής τους σε συνεργασία με την αρχή ΤΑ,

δ) παρακολούθηση της εφαρμογής των SecOps και, κατά περίπτωση, δυνατότητα μεταβίβασης αρμοδιοτήτων σχετικών με τη λειτουργική ασφάλεια στον ιδιοκτήτη του συστήματος,

ε) διαχείριση και χειρισμό κρυπτογραφικών προϊόντων, με εξασφάλιση της φύλαξης των κρυπτογραφικών και των ελεγχόμενων προϊόντων και, εφόσον απαιτείται, διασφάλιση της παραγωγής κρυπτογραφικών μεταβλητών,

στ) επανεξέταση αναλύσεων και διεξαγωγή δοκιμών στον τομέα της ασφάλειας, ιδίως για την εκπόνηση των σχετικών εκθέσεων κινδύνου, όπως απαιτεί η ΑΠΑ,

ζ) παροχή ειδικής για το CIS κατάρτισης ΙΑ και

η) εφαρμογή και λειτουργία ειδικών για το CIS μέτρων ασφαλείας.

ΠΑΡΑΡΤΗΜΑ V

ΒΙΟΜΗΧΑΝΙΚΗ ΑΣΦΑΛΕΙΑ

I. ΕΙΣΑΓΩΓΗ

1. Το παρόν παράρτημα περιέχει διατάξεις για την εφαρμογή του άρθρου 11. Ορίζει γενικές διατάξεις ασφαλείας που εφαρμόζονται στους βιομηχανικούς ή άλλους φορείς κατά τις διαπραγματεύσεις πριν από την ανάθεση σύμβασης και καθ' όλη τη διάρκεια του κύκλου ζωής των διαβαθμισμένων συμβάσεων που συνάπτει η ΓΓΣ.

2. Το Συμβούλιο εγκρίνει κατευθυντήριες γραμμές βιομηχανικής ασφαλείας στην οποία περιγράφονται ιδίως λεπτομερείς απαιτήσεις όσον αφορά τις εξουσιοδοτήσεις ασφαλείας φορέα (FSC), τα έγγραφα θεμάτων ασφαλείας (ΕΘΑ), επισκέψεις, διαβίβαση και μεταφορά των ΔΠΕΕ.

II. ΣΤΟΙΧΕΙΑ ΑΣΦΑΛΕΙΑΣ ΣΕ ΔΙΑΒΑΘΜΙΣΜΕΝΗ ΣΥΜΒΑΣΗ

Οδηγός Διαβάθμισης Ασφαλείας (ΟΔΑ)

3. Πριν από την έναρξη διαδικασίας πρόσκλησης υποβολής προσφορών ή τη σύναψη διαβαθμισμένης σύμβασης, η ΓΓΣ, ως αναθέτουσα αρχή, καθορίζει τη διαβάθμιση ασφαλείας κάθε πληροφορίας που πρέπει να παρέχεται στους υποβάλλοντες προσφορά και στους εργολάβους, καθώς και τη διαβάθμιση ασφαλείας κάθε πληροφορίας που παράγεται από τον εργολάβο. Προς τούτο, η ΓΓΣ καταρτίζει ΟΔΑ που θα χρησιμοποιείται για την εκτέλεση της σύμβασης.

4. Προκειμένου να καθορισθεί η διαβάθμιση ασφαλείας των διάφορων στοιχείων μιας διαβαθμισμένης σύμβασης, εφαρμόζονται οι ακόλουθες αρχές:

α) κατά την κατάρτιση ΟΔΑ, η ΓΓΣ λαμβάνει υπόψη κάθε σχετικό ζήτημα ασφαλείας, συμπεριλαμβανομένης της διαβάθμισης ασφαλείας των πληροφοριών που παρέχονται και που εγκρίνονται προς χρήση για τη σύμβαση από το φορέα προέλευσης των πληροφοριών,

β) η συνολική διαβάθμιση ασφαλείας της σύμβασης δεν επιτρέπεται να είναι κατώτερη από την ανώτατη διαβάθμιση οποιουδήποτε μέρους της και

γ) εφόσον απαιτείται, η ΓΓΣ συνεργάζεται με τις ΕΑΑ/ΚΑΑ των κρατών μελών ή κάθε άλλη σχετική αρμόδια αρχή ασφαλείας σε περίπτωση τυχόν μεταβολών της διαβάθμισης των πληροφοριών που παράγονται από ή παρέχονται σε εργολάβους κατά την εκτέλεση σύμβασης, και για τυχόν επακόλουθες τροποποιήσεις του ΟΔΑ.

Έγγραφο θεμάτων ασφαλείας (ΕΘΑ)

5. Οι προδιαγραφές ασφαλείας της εκάστοτε σύμβασης περιγράφονται σε έγγραφο θεμάτων ασφαλείας (ΕΘΑ). Εφόσον απαιτείται, το ΕΘΑ περιλαμβάνει τον ΟΔΑ και αποτελεί αναπόσπαστο μέρος διαβαθμισμένης σύμβασης ή υπεργολαβίας.

6. Το ΕΘΑ περιέχει τις διατάξεις που προβλέπουν ότι ο εργολάβος και/ή ο υπεργολάβος οφείλει να συμμορφώνεται προς τις ελάχιστες προδιαγραφές της παρούσας απόφασης. Η μη συμμόρφωση με τις ελάχιστες προδιαγραφές μπορεί να συνιστά επαρκή λόγο καταγγελίας της σύμβασης.

Εντολές ασφαλείας του προγράμματος/έργου (PSI)

7. Ανάλογα με το πεδίο εφαρμογής προγραμμάτων ή έργων που αφορούν την πρόσβαση σε ΔΠΕΕ ή το χειρισμό ή την αποθήκευσή τους, η αρχή ανάθεσης η οποία έχει αναλάβει τη διαχείριση του προγράμματος ή του έργου μπορεί να εκπονήσει ειδικές PSI. Οι PSI πρέπει να εγκρίνονται από τις ΕΑΑ/ΚΑΑ των κρατών μελών ή από οποιαδήποτε άλλη αρμόδια αρχή ασφαλείας που συμμετέχει στο PSI και ενδέχεται να προβλέπουν πρόσθετες απαιτήσεις ασφαλείας.

III. ΕΞΟΥΣΙΟΔΟΤΗΣΗ ΑΣΦΑΛΕΙΑΣ ΦΟΡΕΑ (FSC)

8. Η FSC χορηγείται από την ΕΑΑ/ΚΑΑ ή οποιαδήποτε άλλη αρμόδια αρχή ασφαλείας κράτους μέλους και δηλώνει, βάσει των εθνικών νομοθετικών και κανονιστικών διατάξεων, ότι ένας βιομηχανικός ή άλλος φορέας μπορεί να προστατεύει τις ΔΠΕΕ στις εγκαταστάσεις του ανάλογα με τη διαβάθμιση ασφαλείας τους (CONFIDENTIEL UE/EU CONFIDENTIAL ή SECRET UE/EU SECRET). Προσκομίζεται στη ΓΓΣ, ως αναθέτουσα αρχή, προκειμένου να παρασχεθούν ΔΠΕΕ σε εργολάβο ή υπεργολάβο ή ενδεχόμενο εργολάβο ή υπεργολάβο ή να εγκριθεί η πρόσβαση των εν λόγω προσώπων σε ΔΠΕΕ.

9. Κατά τη χορήγηση της FSC, η οικεία ΕΑΑ/ΚΑΑ προβαίνει τουλάχιστον στις εξής ενέργειες:

α) αξιολογεί την ακεραιότητα του βιομηχανικού ή άλλου φορέα,

β) αξιολογεί την κυριότητα, τον έλεγχο, ή τη δυνατότητα άσκησης αθέμιτης επιρροής που θα μπορούσε να θεωρηθεί ως κίνδυνος κατά της ασφάλειας,

γ) εξακριβώνει ότι βιομηχανικός ή άλλος φορέας έχει θεσπίσει σύστημα ασφαλείας στην εγκατάστασή του το οποίο καλύπτει όλα τα προσήκοντα μέτρα ασφαλείας τα οποία είναι αναγκαία για την προστασία πληροφοριών ή υλικού με διαβάθμιση CONFIDENTIEL UE/EU CONFIDENTIAL ή SECRET UE/EU SECRET σύμφωνα με τις απαιτήσεις της παρούσας απόφασης,

δ) εξακριβώνει ότι το καθεστώς ασφαλείας του προσωπικού —διευθυντικών στελεχών, ιδιοκτητών, εργαζομένων— που πρέπει να έχουν πρόσβαση στις πληροφορίες με διαβάθμιση CONFIDENTIEL UE/EU CONFIDENTIAL ή SECRET UE/EU SECRET έχει καθορισθεί σύμφωνα με τις απαιτήσεις της παρούσας απόφασης και

ε) εξακριβώνει ότι ο βιομηχανικός ή άλλος φορέας έχει διορίσει υπάλληλο υπεύθυνο για την ασφάλεια της εγκατάστασης ο οποίος είναι υπόλογος στη διεύθυνση για την τήρηση των υποχρεώσεων ασφαλείας εντός του φορέα.

10. Οσάκις απαιτείται, η ΓΓΣ, ως αναθέτουσα αρχή, ενημερώνει την αρμόδια ΕΑΑ/ΚΑΑ ή οποιαδήποτε άλλη αρμόδια αρχή ασφαλείας ότι απαιτείται FSC κατά το προσυμβατικό στάδιο ή για την εκτέλεση της σύμβασης. Απαιτείται FSC ή ΕΑΠ κατά το προσυμβατικό στάδιο όταν πρέπει να παρασχεθούν ΔΠΕΕ με διαβάθμιση CONFIDENTIEL UE/EU CONFIDENTIAL ή SECRET UE/EU SECRET κατά τη διάρκεια της διαδικασίας υποβολής προσφορών.

11. Η αναθέτουσα αρχή δεν αναθέτει διαβαθμισμένη σύμβαση στον προτιμώμενο υποψήφιο προτού λάβει επιβεβαίωση από την ΕΑΑ/ΚΑΑ ή οποιαδήποτε άλλη αρμόδια αρχή ασφαλείας του κράτους μέλους στο οποίο έχει την έδρα του ο εργολάβος ή υπεργολάβος ότι έχει εκδοθεί η δέουσα FSC όπου απαιτείται.

12. Η ΕΑΑ/ΚΑΑ ή κάθε άλλη αρμόδια αρχή ασφαλείας που έχει εκδώσει FSC γνωστοποιεί στη ΓΓΣ, υπό την ιδιότητά της ως αναθέτουσας αρχής, τυχόν αλλαγές που επηρεάζουν τη FSC. Σε περίπτωση υπεργολαβίας, η ΕΑΑ/ΚΑΑ ή κάθε άλλη αρμόδια αρχή ασφαλείας ενημερώνεται αναλόγως.

13. Η ανάκληση FSC από την αρμόδια ΕΑΑ/ΚΑΑ ή οποιαδήποτε άλλη αρμόδια αρχή ασφαλείας συνιστά επαρκή λόγο για τη ΓΓΣ, ως αναθέτουσα αρχή, να καταγγείλει διαβαθμισμένη σύμβαση ή να αποκλείσει συμμετέχοντα από το διαγωνισμό.

IV. ΔΙΑΒΑΘΜΙΣΜΕΝΕΣ ΣΥΜΒΑΣΕΙΣ ΕΡΓΟΛΑΒΙΑΣ ΚΑΙ ΥΠΕΡΓΟΛΑΒΙΑΣ

14. Όταν, κατά το προσυμβατικό στάδιο, παρέχονται ΔΠΕΕ σε υποψήφιο, η πρόσκληση υποβολής προσφοράς πρέπει να περιέχει διάταξη που να υποχρεώνει τον υποψήφιο ο οποίος τελικά δεν υποβάλλει προσφορά ή δεν επιλέγεται, να επιστρέψει όλα τα διαβαθμισμένα έγγραφα εντός συγκεκριμένου χρονικού διαστήματος.

15. Μόλις ανατεθεί διαβαθμισμένη σύμβαση εργολαβίας ή υπεργολαβίας, η ΓΓΣ, ως αναθέτουσα αρχή, ενημερώνει την ΕΑΑ/ΚΑΑ του εργολάβου ή του υπεργολάβου ή οποιαδήποτε άλλη αρμόδια αρχή ασφαλείας σχετικά με τις διατάξεις ασφαλείας της διαβαθμισμένης σύμβασης.

16. Σε περίπτωση καταγγελίας των συμβάσεων αυτών, η ΓΓΣ, ως αναθέτουσα αρχή, (και/ή η ΕΑΑ/ΚΑΑ ή οποιαδήποτε άλλη αρμόδια αρχή ασφαλείας, αναλόγως, σε περίπτωση υπεργολαβίας), ενημερώνει αμέσως την ΕΑΑ/ΚΑΑ ή οποιαδήποτε άλλη αρμόδια αρχή ασφαλείας του κράτους μέλους στο οποίο έχει την έδρα του ο εργολάβος ή ο υπεργολάβος.

17. Κατά κανόνα, ο εργολάβος ή υπεργολάβος οφείλει να επιστρέψει στην αναθέτουσα αρχή, άμα τη λύσει της διαβαθμισμένης σύμβασης εργολαβίας ή υπεργολαβίας, τυχόν ΔΠΕΕ που έχει στην κατοχή του.

18. Ειδικές διατάξεις για τη διάθεση των ΔΠΕΕ κατά την εκτέλεση της σύμβασης ή κατά τη λύση της ορίζονται στο ΕΘΑ.

19. Όταν ο εργολάβος ή ο υπεργολάβος έχει δικαίωμα διατήρησης των ΔΠΕΕ μετά τη λύση της σύμβασης, οι ελάχιστες προδιαγραφές που προβλέπονται στην παρούσα απόφαση συνεχίζουν να τηρούνται και το απόρρητο των ΔΠΕΕ προστατεύεται από τον εργολάβο ή τον υπεργολάβο.

20. Οι όροι υπό τους οποίους ο κύριος εργολάβος μπορεί να συνάπτει σύμβαση υπεργολαβίας καθορίζονται στην προσφορά και στη σύμβαση.

21. Ο εργολάβος λαμβάνει άδεια από τη ΓΓΣ, ως αναθέτουσα αρχή, προτού αναθέσει τμήματα διαβαθμισμένης σύμβασης σε υπεργολάβους. Δεν ανατίθεται σύμβαση υπεργολαβίας σε βιομηχανικούς ή άλλους φορείς οι οποίοι έχουν την έδρα τους σε κράτος μη μέλος της ΕΕ το οποίο δεν έχει συνάψει συμφωνία ασφάλειας πληροφοριών με την Ένωση.

22. Ο εργολάβος οφείλει να μεριμνά ώστε όλες οι υπεργολαβικές δραστηριότητες αναλαμβάνονται σύμφωνα με τις ελάχιστες προδιαγραφές της παρούσας απόφασης και δεν παρέχει ΔΠΕΕ σε υπεργολάβο χωρίς την προηγούμενη γραπτή συγκατάθεση της αναθέτουσας αρχής.

23. Όσον αφορά τις ΔΠΕΕ τις οποίες παράγει ή χειρίζεται ο εργολάβος ή ο υπεργολάβος, τα δικαιώματα του φορέα προέλευσης ασκούνται από την αναθέτουσα αρχή.

V. ΕΠΙΣΚΕΨΕΙΣ ΣΕ ΣΥΝΑΡΤΗΣΗ ΜΕ ΔΙΑΒΑΘΜΙΣΜΕΝΕΣ ΣΥΜΒΑΣΕΙΣ

24. Όταν το προσωπικό της ΓΓΣ, των εργολάβων ή υπεργολάβων χρειάζεται πρόσβαση σε πληροφορίες με τη διαβάθμιση CONFIDENTIEL UE/EU CONFIDENTIAL ή SECRET UE/EU SECRET στις αντίστοιχες εγκαταστάσεις τους για την εκτέλεση διαβαθμισμένης σύμβασης, διοργανώνονται επισκέψεις σε συνεργασία με τις ΕΑΑ/ΚΑΑ ή κάθε άλλη ενδιαφερόμενη αρχή ασφαλείας. Ωστόσο, στο πλαίσιο ειδικών σχεδίων, οι ΕΑΑ/ΚΑΑ μπορούν επίσης να συμφωνούν διαδικασία απευθείας οργάνωσης των επισκέψεων.

25. Όλοι οι επισκέπτες φέρουν τη δέουσα ΕΑΠ και έχουν ανάγκη γνώσης προκειμένου να τους επιτραπεί πρόσβαση στις διαβαθμισμένες ΔΠΕΕ που σχετίζονται με τη σύμβαση της ΓΓΣ.

26. Οι επισκέπτες δικαιούνται πρόσβαση μόνο στις ΔΠΕΕ που έχουν σχέση με το σκοπό της επίσκεψης.

VI. ΔΙΑΒΙΒΑΣΗ ΚΑΙ ΜΕΤΑΦΟΡΑ ΤΩΝ ΔΠΕΕ

27. Όσον αφορά τη διαβίβαση των ΔΠΕΕ με ηλεκτρονικά μέσα, ισχύουν οι οικείες διατάξεις του άρθρου 10 και του παραρτήματος IV.

28. Όσον αφορά τη μεταφορά των ΔΠΕΕ, ισχύουν οι οικείες διατάξεις του παραρτήματος III, σύμφωνα με τις εθνικές νομοθετικές και κανονιστικές διατάξεις.

29. Κατά τον καθορισμό των ρυθμίσεων ασφαλείας για τη μεταφορά διαβαθμισμένου υλικού ως φορτίου, εφαρμόζονται οι ακόλουθες αρχές:

α) η ασφάλεια πρέπει να είναι εγγυημένη σε όλα τα στάδια της μεταφοράς από το αρχικό σημείο προέλευσης ως τον τελικό προορισμό,

β) ο βαθμός προστασίας κάθε αποστολής στοιχείων προσδιορίζεται με βάση την ανώτατη διαβάθμιση του υλικού που περιέχεται στην αποστολή,

γ) χορηγείται FSC στο κατάλληλο επίπεδο για τις εταιρείες που πραγματοποιούν τη μεταφορά· στις περιπτώσεις αυτές, το προσωπικό που χειρίζεται την αποστολή στοιχείων λαμβάνει εξουσιοδότηση ασφαλείας σύμφωνα με το παράρτημα I,

δ) πριν από κάθε διασυνοριακή μεταφορά υλικού με διαβάθμιση CONFIDENTIEL UE/EU CONFIDENTIAL ή SECRET UE/EU SECRET, ο αποστολέας καταρτίζει σχέδιο μεταφοράς το οποίο εγκρίνεται από τις ΕΑΑ/ΚΑΑ ή οποιαδήποτε άλλη σχετική αρμόδια αρχή ασφαλείας,

ε) οι μεταφορές εκτελούνται κατά το δυνατόν από σημείο σε σημείο και ολοκληρώνονται όσο πιο γρήγορα το επιτρέπουν οι εκάστοτε συνθήκες και

στ) εφόσον είναι εφικτό, τα δρομολόγια πρέπει να διέρχονται μόνον από κράτη μέλη. δρομολόγια μέσω κρατών άλλων από τα κράτη μέλη πρέπει να πραγματοποιούνται μόνον κατόπιν εξουσιοδότησης των ΕΑΑ/ΚΑΑ ή οποιασδήποτε άλλης αρμόδιας αρχής ασφαλείας των κρατών τόσο του αποστολέα όσο και του παραλήπτη.

VII. ΜΕΤΑΦΟΡΑ ΔΠΕΕ ΣΤΟΥΣ ΕΡΓΟΛΑΒΟΥΣ ΠΟΥ ΕΥΡΙΣΚΟΝΤΑΙ ΣΕ ΤΡΙΤΑ ΚΡΑΤΗ

30. Η μεταφορά ΔΠΕΕ σε εργολάβους και υπεργολάβους που ευρίσκονται σε τρίτα κράτη διεξάγεται σύμφωνα με τα μέτρα ασφαλείας μεταξύ της ΓΓΣ, ως αναθέτουσας αρχής, και των ΕΑΑ/ΚΑΑ του ενδιαφερόμενου τρίτου κράτους όπου έχει την έδρα του ο εργολάβος.

VIII. ΠΛΗΡΟΦΟΡΙΕΣ ΜΕ ΔΙΑΒΑΘΜΙΣΗ RESTREINT UE/EU RESTRICTED

31. Σε συνεργασία με τις ΕΑΑ/ΚΑΑ των κρατών μελών κατά περίπτωση, η ΓΓΣ, ως αναθέτουσα αρχή, έχει το δικαίωμα διεξαγωγής επιθεωρήσεων στις εγκαταστάσεις των εργολάβων/υπεργολάβων βάσει συμβατικών διατάξεων προκειμένου να εξακριβώσει ότι έχουν τεθεί σε ισχύ τα οικεία μέτρα ασφαλείας για την προστασία των ΔΠΕΕ στο επίπεδο RESTREINT UE/EU RESTRICTED όπως απαιτείται στο πλαίσιο της σύμβασης.

32. Στον βαθμό που απαιτείται δυνάμει εθνικών νομοθετικών και κανονιστικών διατάξεων, η ΓΓΣ, ως αναθέτουσα αρχή, γνωστοποιεί στις ΕΑΑ/ΚΑΑ ή σε οποιαδήποτε άλλη αρμόδια αρχή ασφαλείας τις συμβάσεις ή τις συμβάσεις υπεργολαβίας που περιέχουν πληροφορίες με διαβάθμιση RESTREINT UE/EU RESTRICTED.

33. Δεν απαιτείται FSC ή ΕΑΠ για τους εργολάβους ή τους υπεργολάβους και το προσωπικό τους για τις συμβάσεις που ανατίθενται από τη ΓΓΣ και περιέχουν πληροφορίες με διαβάθμιση RESTREINT UE/EU RESTRICTED.

34. Η ΓΓΣ, ως αναθέτουσα αρχή, εξετάζει τις απαντήσεις στις προσκλήσεις υποβολής προσφορών για τις συμβάσεις που απαιτούν πρόσβαση σε πληροφορίες με διαβάθμιση RESTREINT UE/EU RESTRICTED, παρά τις οποιεσδήποτε απαιτήσεις σχετικά με FSC ή ΕΑΠ που ενδέχεται να υπάρχουν βάσει των εθνικών νομοθετικών και κανονιστικών διατάξεων.

35. Οι όροι βάσει των οποίων ο κύριος εργολάβος μπορεί να συνάπτει σύμβαση υπεργολαβίας καθορίζονται σύμφωνα με την παράγραφο 21.

36. Όταν μια σύμβαση αφορά τον χειρισμό πληροφοριών με διαβάθμιση RESTREINT UE/EU RESTRICTED σε CIS που διαχειρίζεται εργολήπτης, η ΓΓΣ ως αναθέτουσα αρχή μεριμνά ώστε η σύμβαση να καθορίζει τις απαραίτητες τεχνικές και διοικητικές προδιαγραφές όσον αφορά την έγκριση CIS σε αναλογία προς τον αξιολογούμενο κίνδυνο, λαμβάνοντας υπόψη όλους τους συναφείς παράγοντες. Το πεδίο έγκρισης του CIS συμφωνείται μεταξύ της αναθέτουσας αρχής και της οικείας ΕΑΑ/ΚΑΑ.

ΠΑΡΑΡΤΗΜΑ VI

ΑΝΤΑΛΛΑΓΗ ΔΙΑΒΑΘΜΙΣΜΕΝΩΝ ΠΛΗΡΟΦΟΡΙΩΝ ΜΕ ΤΡΙΤΑ ΚΡΑΤΗ ΚΑΙ ΔΙΕΘΝΕΙΣ ΟΡΓΑΝΙΣΜΟΥΣ

I. ΕΙΣΑΓΩΓΗ

1. Το παρόν παράρτημα περιέχει διατάξεις για την εφαρμογή του άρθρου 13.

II. ΠΛΑΙΣΙΑ ΠΟΥ ΔΙΕΠΟΥΝ ΤΗΝ ΑΝΤΑΛΛΑΓΗ ΔΙΑΒΑΘΜΙΣΜΕΝΩΝ ΠΛΗΡΟΦΟΡΙΩΝ

2. Όταν το Συμβούλιο κρίνει ότι υφίσταται μακροπρόθεσμα ανάγκη ανταλλαγής διαβαθμισμένων πληροφοριών,

— συνάπτεται συμφωνία ασφαλείας πληροφοριών, ή

— τίθεται σε εφαρμογή διοικητικός διακανονισμός,

σύμφωνα με το άρθρο 13 παράγραφος 2 και τα τμήματα III και IV και βάσει συστάσεως της Επιτροπής Ασφαλείας.

3. Όταν ΔΠΕΕ οι οποίες παράγονται για τους σκοπούς επιχείρησης ΚΠΑΑ πρόκειται να κοινοποιηθούν σε τρίτα κράτη ή διεθνείς οργανισμούς που συμμετέχουν στην επιχείρηση αυτή και εφόσον δεν υφίσταται κανένα από τα πλαίσια της παραγράφου 2, η ανταλλαγή ΔΠΕΕ με το συμβάλλον τρίτο κράτος η διεθνή οργανισμό διέπεται, σύμφωνα με το τμήμα V, από:

— συμφωνία-πλαίσιο συμμετοχής,

— ad hoc συμφωνία συμμετοχής, ή

— απουσία των ανωτέρω, από ad hoc διοικητικό διακανονισμό.

4. Ελλείψει πλαισίου προβλεπομένου στις παραγράφους 2 και 3 και όταν λαμβάνεται απόφαση κοινοποίησης ΔΠΕΕ σε τρίτο κράτος ή διεθνή οργανισμό σε κατ' εξαίρεση ad hoc βάση, σύμφωνα με το τμήμα VI, πρέπει να ζητούνται γραπτές διασφαλίσεις από το τρίτο κράτος ή το διεθνή οργανισμό για να εξασφαλίζεται ότι προστατεύουν τις ΔΠΕΕ που τους κοινοποιούνται σύμφωνα με τις βασικές αρχές και τις ελάχιστες προδιαγραφές της παρούσας απόφασης.

III. ΣΥΜΦΩΝΙΕΣ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΩΝ

5. Οι συμφωνίες για την ασφάλεια των πληροφοριών θεσπίζουν τις βασικές αρχές και τις ελάχιστες προδιαγραφές που διέπουν την ανταλλαγή διαβαθμισμένων πληροφοριών μεταξύ της Ένωσης και τρίτου κράτους ή διεθνούς οργανισμού.

6. Οι συμφωνίες για την ασφάλεια των πληροφοριών προβλέπουν τεχνικούς διακανονισμούς εφαρμογής οι οποίοι συμφωνούνται μεταξύ των αρμόδιων αρχών ασφαλείας των σχετικών οργάνων και οργανισμών της Ένωσης και της αρμόδιας αρχής ασφαλείας του εν λόγω τρίτου κράτους ή διεθνούς οργανισμού. Στους διακανονισμούς αυτούς λαμβάνεται δεόντως υπόψη το επίπεδο προστασίας που προβλέπουν οι κανονισμοί, δομές και διαδικασίες ασφαλείας που εφαρμόζονται στο εν λόγω τρίτο κράτος ή διεθνή οργανισμό. Εγκρίνονται από την Επιτροπή Ασφαλείας.

7. Ηλεκτρονική ανταλλαγή ΔΠΕΕ στο πλαίσιο συμφωνίας ασφάλειας των πληροφοριών πραγματοποιείται μόνον εφόσον προβλέπεται ρητώς στη συμφωνία ή στους αντίστοιχους τεχνικούς διακανονισμούς εφαρμογής.

8. Όταν το Συμβούλιο συνάπτει συμφωνία ασφαλείας των πληροφοριών, ορίζεται γραμματεία σε κάθε συμβαλλόμενο μέρος ως το κύριο σημείο εισόδου και εξόδου για τις ανταλλαγές διαβαθμισμένων πληροφοριών.

9. Για την αξιολόγηση της αποτελεσματικότητας των κανονισμών, δομών και διαδικασιών ασφαλείας στο οικείο τρίτο κράτος ή διεθνή οργανισμό, διεξάγονται επισκέψεις αξιολόγησης κατόπιν αμοιβαίας συμφωνίας με το συγκεκριμένο τρίτο κράτος ή διεθνή οργανισμό. Οι εν λόγω επισκέψεις αξιολόγησης διεξάγονται σύμφωνα με τις σχετικές διατάξεις του παραρτήματος III και αξιολογούν:

α) το ρυθμιστικό πλαίσιο που εφαρμόζεται για την προστασία των διαβαθμισμένων πληροφοριών,

β) τυχόν συγκεκριμένα χαρακτηριστικά της πολιτικής ασφαλείας και τον τρόπο οργάνωσης της ασφαλείας στο τρίτο κράτος ή στο διεθνή οργανισμό που ενδέχεται να έχει επιπτώσεις στο επίπεδο των προς ανταλλαγή διαβαθμισμένων πληροφοριών,

γ) τα ισχύοντα μέτρα και διαδικασίες ασφαλείας και

δ) τις διαδικασίες ελέγχου ασφαλείας για το επίπεδο των ΔΠΕΕ που θα κοινοποιηθούν.

10. Η ομάδα που διενεργεί επίσκεψη αξιολόγησης εξ ονόματος της Ένωσης αξιολογεί κατά πόσον οι κανονισμοί και οι διαδικασίες ασφαλείας στο εν λόγω τρίτο κράτος ή διεθνή οργανισμό είναι επαρκείς για την προστασία των ΔΠΕΕ στο ζητούμενο επίπεδο.

11. Τα συμπεράσματα των επισκέψεων αυτών περιέχονται σε έκθεση βάσει της οποίας η Επιτροπή Ασφαλείας καθορίζει το ανώτατο επίπεδο των προς ανταλλαγή ΔΠΕΕ σε έντυπη και, εφόσον είναι σκόπιμο, σε ηλεκτρονική μορφή με το ενδιαφερόμενο τρίτο μέρος καθώς και τους τυχόν ειδικούς όρους που διέπουν την ανταλλαγή με το εν λόγω μέρος.

12. Καταβάλλεται κάθε προσπάθεια για τη διεξαγωγή πλήρους επίσκεψης αξιολόγησης ασφαλείας στο οικείο τρίτο κράτος ή διεθνή οργανισμό πριν η Επιτροπή Ασφαλείας εγκρίνει τους διακανονισμούς εφαρμογής προκειμένου να προσδιορισθούν ο χαρακτήρας και η αποτελεσματικότητα του ισχύοντος συστήματος ασφαλείας. Ωστόσο όταν αυτό δεν είναι εφικτό, η Υπηρεσία Ασφαλείας της ΓΓΣ αποστέλλει στην Επιτροπή Ασφαλείας όσο το δυνατόν πληρέστερη έκθεση, βασιζόμενη στις πληροφορίες τις οποίες διαθέτει, προκειμένου να ενημερωθεί η Επιτροπή Ασφαλείας για τους ισχύοντες κανόνες ασφαλείας και τον τρόπο οργάνωσης της ασφάλειας στο οικείο τρίτο κράτος ή τον διεθνή οργανισμό.

13. Προτού χορηγηθούν πράγματι οι ΔΠΕΕ στο οικείο τρίτο κράτος ή διεθνή οργανισμό, η έκθεση σχετικά με την επίσκεψη αξιολόγησης ή, ελλείψει τέτοιας έκθεσης, η έκθεση που αναφέρεται στην παράγραφο 12, διαβιβάζεται στην Επιτροπή Ασφαλείας η οποία και κρίνει εάν είναι ικανοποιητική.

14. Οι αρμόδιες αρχές ασφαλείας των οργάνων και οργανισμών της Ένωσης κοινοποιούν στο τρίτο κράτος ή διεθνή οργανισμό την ημερομηνία από την οποία η Ένωση είναι σε θέση να κοινοποιήσει ΔΠΕΕ στο πλαίσιο της συμφωνίας, καθώς και το ανώτατο επίπεδο ΔΠΕΕ που μπορούν να ανταλλαχθούν σε έντυπη ή ηλεκτρονική μορφή.

15. Αν κριθεί σκόπιμο πραγματοποιούνται επακόλουθες επισκέψεις αξιολόγησης, ιδίως αν:

α) χρειάζεται να αυξηθεί το επίπεδο ΔΠΕΕ που μπορούν να κοινοποιηθούν,

β) η Ένωση έχει ενημερωθεί σχετικά με θεμελιώδεις αλλαγές στις ρυθμίσεις ασφαλείας του τρίτου κράτους ή διεθνούς οργανισμού που μπορεί να επηρεάσουν τον τρόπο με τον οποίο προστατεύει τις ΔΠΕΕ ή

γ) σημειώθηκε σοβαρό περιστατικό που αφορά την άνευ αδείας κοινολόγηση ΔΠΕΕ.

16. Όταν τεθεί σε ισχύ η συμφωνία ασφαλείας των πληροφοριών και ανταλλάσσονται οι διαβαθμισμένες πληροφορίες με το οικείο τρίτο κράτος ή τον διεθνή οργανισμό, η Επιτροπή ασφάλειας μπορεί να αποφασίσει την τροποποίηση του μέγιστου επιπέδου ΔΠΕΕ που δύνανται να ανταλλάσσονται σε έντυπη ή ηλεκτρονική μορφή, και βάσει τυχόν επισκέψεων επακόλουθης αξιολόγησης.

IV. ΔΙΟΙΚΗΤΙΚΟΙ ΔΙΑΚΑΝΟΝΙΣΜΟΙ

17. Όταν υπάρχει μακροπρόθεσμη ανάγκη ανταλλαγής πληροφοριών με διαβάθμιση κατά κανόνα όχι άνω του RESTREINT UE/EU RESTRICTED με τρίτο κράτος ή διεθνή οργανισμό, και όταν η επιτροπή ασφαλείας έχει διαπιστώσει ότι το εν λόγω μέρος δεν διαθέτει επαρκώς ανεπτυγμένο σύστημα ασφαλείας ώστε να συνάπτει συμφωνία ασφαλείας πληροφοριών, ο γενικός γραμματέας δύναται, μετά από έγκριση του Συμβουλίου, να προβεί σε διοικητικό διακανονισμό εξ ονόματος της ΓΓΣ με τις αρμόδιες αρχές του εν λόγω τρίτου κράτους ή διεθνούς οργανισμού.

18. Όταν επιβάλλεται, για επείγοντες επιχειρησιακούς λόγους, η ταχεία σύσταση πλαισίου ανταλλαγής διαβαθμισμένων πληροφοριών, το Συμβούλιο μπορεί εκτάκτως να αποφασίζει τη σύναψη διοικητικού διακανονισμού για την ανταλλαγή πληροφοριών υψηλότερου επιπέδου διαβάθμισης.

19. Οι διοικητικοί διακανονισμοί λαμβάνουν κατά κανόνα τη μορφή ανταλλαγής επιστολών.

20. Προτού χορηγηθούν πράγματι οι ΔΠΕΕ στο οικείο τρίτο κράτος ή διεθνή οργανισμό, διεξάγεται επίσκεψη αξιολόγησης όπως αναφέρεται στην παράγραφο 9 και η έκθεση ή, ελλείψει τέτοιας έκθεσης, η έκθεση που αναφέρεται στην παράγραφο 12, διαβιβάζεται στην Επιτροπή Ασφαλείας η οποία και κρίνει εάν είναι ικανοποιητική.

21. Ηλεκτρονική ανταλλαγή ΔΠΕΕ στο πλαίσιο διοικητικού διακανονισμού πραγματοποιείται μόνο εφόσον προβλέπεται ρητώς από τον διακανονισμό.

V. ΑΝΤΑΛΛΑΓΗ ΔΙΑΒΑΘΜΙΣΜΕΝΩΝ ΠΛΗΡΟΦΟΡΙΩΝ ΣΤΟ ΠΛΑΙΣΙΟ ΕΠΙΧΕΙΡΗΣΕΩΝ ΚΠΑΑ

22. Οι συμφωνίες-πλαίσια συμμετοχής διέπουν τη συμμετοχή τρίτων κρατών ή διεθνών οργανισμών στις επιχειρήσεις ΚΠΑΑ. Οι συμφωνίες αυτές περιλαμβάνουν διατάξεις για την κοινοποίηση ΔΠΕΕ που παράγονται για τους σκοπούς επιχειρήσεων ΚΠΑΑ στα συμβάλλοντα τρίτα κράτη ή διεθνείς οργανισμούς. Το ανώτατο επίπεδο διαβάθμισης των ΔΠΕΕ που μπορούν να ανταλλάσσονται είναι RESTREINT UE/EU RESTRICTED για μη στρατιωτικές επιχειρήσεις ΚΠΑΑ και CONFIDENTIEL UE/EU CONFIDENTIAL για στρατιωτικές επιχειρήσεις ΚΠΑΑ, εκτός εάν ορίζεται άλλως στην απόφαση για τη σύσταση κάθε επιχείρησης ΚΠΑΑ.

23. Οι ad hoc συμφωνίες συμμετοχής που συνάπτονται για συγκεκριμένη επιχείρηση ΚΠΑΑ περιλαμβάνουν διατάξεις για την κοινοποίηση ΔΠΕΕ που παράγονται για τους σκοπούς της εν λόγω επιχείρησης στο συμβάλλον κράτος ή διεθνή οργανισμό. Το ανώτατο επίπεδο διαβάθμισης των ΔΠΕΕ που μπορούν να ανταλλάσσονται είναι RESTREINT UE/EU RESTRICTED για μη στρατιωτικές επιχειρήσεις ΚΠΑΑ και CONFIDENTIEL UE/EU CONFIDENTIAL για στρατιωτικές επιχειρήσεις ΚΠΑΑ, εκτός εάν ορίζεται άλλως στην απόφαση για τη σύσταση κάθε επιχείρησης ΚΠΑΑ.

24. Απουσία συμφωνίας ασφάλειας των πληροφοριών και εν αναμονή της σύναψης συμφωνίας συμμετοχής, η κοινοποίηση ΔΠΕΕ που παράγονται για τους σκοπούς της επιχείρησης σε τρίτο κράτος ή διεθνή οργανισμό που συμμετέχει στην επιχείρηση διέπεται από διοικητικό διακανονισμό τον οποίο συνάπτει ο Ύπατος Εκπρόσωπος ή υπόκειται σε απόφαση σχετικά με ad hoc κοινοποίηση σύμφωνα με το μέρος VI. ΔΠΕΕ ανταλλάσσονται στο πλαίσιο τέτοιας συμφωνίας υπό τον όρο ότι εξακολουθεί να προβλέπεται η συμμετοχή του τρίτου κράτους ή διεθνούς οργανισμού. Το ανώτατο επίπεδο διαβάθμισης των ΔΠΕΕ που μπορούν να ανταλλάσσονται είναι RESTREINT UE/EU RESTRICTED για μη στρατιωτικές επιχειρήσεις ΚΠΑΑ και CONFIDENTIEL UE/EU CONFIDENTIAL για στρατιωτικές επιχειρήσεις ΚΠΑΑ, εκτός εάν ορίζεται άλλως στην απόφαση για τη σύσταση κάθε επιχείρησης ΚΠΑΑ.

25. Στις διατάξεις περί διαβαθμισμένων πληροφοριών που περιλαμβάνονται σε συμφωνίες πλαίσια συμμετοχής, ad hoc συμφωνίες συμμετοχής και ad hoc διακανονισμούς συμμετοχής που αναφέρονται στις παραγράφους 22 έως 24 προβλέπεται ότι το οικείο τρίτο κράτος ή διεθνής οργανισμός διασφαλίζει ότι το αποσπώμενο στις επιχειρήσεις προσωπικό του θα προστατεύει τις ΔΠΕΕ σύμφωνα με τους κανόνες ασφαλείας του Συμβουλίου και με περαιτέρω οδηγίες των αρμοδίων αρχών, περιλαμβανομένης και της ιεραρχίας της επιχείρησης.

26. Εάν συναφθεί εν συνεχεία συμφωνία ασφαλείας των πληροφοριών μεταξύ της Ένωσης και συμβάλλοντος τρίτου κράτους ή διεθνούς οργανισμού, η συμφωνία ασφαλείας των πληροφοριών υπερισχύει των διατάξεων σχετικά με την ανταλλαγή διαβαθμισμένων πληροφοριών που προβλέπονται σε τυχόν συμφωνίες-πλαίσια συμμετοχής, ad hoc συμφωνίες συμμετοχής ή ad hoc διοικητικούς διακανονισμούς, όσον αφορά την ανταλλαγή και το χειρισμό των ΔΠΕΕ.

27. Εάν δεν προβλέπεται ρητώς από την εν λόγω συμφωνία ή τον διακανονισμό, δεν επιτρέπεται η ηλεκτρονική ανταλλαγή ΔΠΕΕ στο πλαίσιο συμφωνίας-πλαισίου συμμετοχής, ad hoc συμφωνίας συμμετοχής ή ad hoc διοικητικού διακανονισμού με τρίτο κράτος ή διεθνή οργανισμό.

28. Οι ΔΠΕΕ που παράγονται για τους σκοπούς επιχείρησης ΚΠΑΑ μπορούν να κοινολογούνται στο προσωπικό που έχει αποσπασθεί στην εν λόγω επιχείρηση από τρίτα κράτη ή διεθνείς οργανισμούς σύμφωνα με τις παραγράφους 22 έως 27. Όταν εγκρίνεται η πρόσβαση του προσωπικού αυτού σε ΔΠΕΕ σε χώρους ή σε CIS επιχείρησης ΚΠΑΑ, εφαρμόζονται μέτρα (όπως καταγραφή των κοινολογούμενων ΔΠΕΕ) για τον περιορισμό του κινδύνου απώλειας ή διαρροής. Τα μέτρα αυτά περιγράφονται στα οικεία έγγραφα σχεδιασμού ή αποστολής.

29. Απουσία συμφωνίας ασφάλειας των πληροφοριών, η κοινοποίηση ΔΠΕΕ, σε περίπτωση συγκεκριμένης και άμεσης επιχειρησιακής ανάγκης, στο κράτος υποδοχής στο έδαφος του οποίου διεξάγεται επιχείρηση ΚΠΑΑ μπορεί να διέπεται από διοικητικό διακανονισμό τον οποίο συνάπτει ο Ύπατος Εκπρόσωπος. Η δυνατότητα αυτή προβλέπεται στην απόφαση για τη σύσταση της επιχείρησης ΚΠΑΑ. Οι ΔΠΕΕ που ανταλλάσσονται υπό τις συνθήκες αυτές περιορίζονται στις πληροφορίες που παράγονται για τους σκοπούς της επιχείρησης ΚΠΑΑ και η διαβάθμισή τους δεν υπερβαίνει τη RESTREINT UE/EU RESTRICTED, εκτός αν προβλέπεται υψηλότερο επίπεδο διαβάθμισης στην απόφαση που θεσπίζει την επιχείρηση ΚΠΑΑ. Βάσει του εν λόγω διοικητικού διακανονισμού, ζητείται από το κράτος υποδοχής να αναλάβει την προστασία των ΔΠΕΕ σύμφωνα με ελάχιστες προδιαγραφές τουλάχιστον ισοδύναμες με τις οριζόμενες στην παρούσα απόφαση.

30. Απουσία συμφωνίας ασφάλειας των πληροφοριών, η κοινοποίηση ΔΠΕΕ σε σχετικά τρίτα κράτη και διεθνείς οργανισμούς, εκτός από όσους συμμετέχουν σε επιχείρηση ΚΠΑΑ, μπορεί να διέπεται από διοικητικό διακανονισμό τον οποίο συνάπτει ο Ύπατος Εκπρόσωπος. Όπου κρίνεται σκόπιμο, η δυνατότητα αυτή καθώς και τυχόν σχετικές προϋποθέσεις προβλέπονται στην απόφαση με την οποία θεσπίζεται η επιχείρηση ΚΠΑΑ. Οι ΔΠΕΕ που ανταλλάσσονται υπό τις συνθήκες αυτές περιορίζονται στις πληροφορίες που παράγονται για τους σκοπούς της επιχείρησης ΚΠΑΑ και η διαβάθμισή τους δεν υπερβαίνει τη RESTREINT UE/EU RESTRICTED, εκτός αν προβλέπεται υψηλότερο επίπεδο διαβάθμισης στην απόφαση που θεσπίζει την επιχείρηση ΚΠΑΑ. Βάσει του εν λόγω διοικητικού διακανονισμού, ζητείται από το κράτος υποδοχής να αναλάβει την προστασία των ΔΠΕΕ σύμφωνα με ελάχιστες προδιαγραφές τουλάχιστον ισοδύναμες με τις οριζόμενες στην παρούσα απόφαση.

31. Δεν απαιτούνται διακανονισμοί εφαρμογής ή επισκέψεις αξιολόγησης προ της εφαρμογής των διατάξεων περί κοινοποίησης ΔΠΕΕ στο πλαίσιο των παραγράφων 22, 23 και 24.

VI. ΕΚΤΑΚΤΗ AD HOC ΚΟΙΝΟΠΟΙΗΣΗ ΔΠΕΕ

32. Όταν δεν υφίσταται πλαίσιο σύμφωνα με τα τμήματα III έως V, και το Συμβούλιο ή κάποιο από τα προπαρασκευαστικά του όργανα κρίνει ότι υπάρχει έκτακτη ανάγκη κοινοποίησης ΔΠΕΕ σε τρίτο κράτος ή διεθνή οργανισμό, η ΓΓΣ:

α) στο μέτρο του δυνατού, ελέγχει με τις αρχές ασφαλείας του οικείου τρίτου κράτους ή διεθνούς οργανισμού ότι οι κανονισμοί, δομές και διαδικασίες ασφαλείας του διασφαλίζουν ότι οι κοινοποιούμενες σε αυτό ΔΠΕΕ θα προστατεύονται βάσει κριτηρίων εξίσου αυστηρών με τα οριζόμενα στην παρούσα απόφαση, και

β) καλεί την Επιτροπή Ασφαλείας, βάσει των διαθέσιμων πληροφοριών, να εκδώσει σύσταση όσον αφορά την κατάλληλη εμπιστοσύνη προς τους κανόνες, τις δομές και τις διαδικασίες ασφαλείας του τρίτου κράτους ή διεθνούς οργανισμού αποδέκτη των ΔΠΕΕ.

33. Εάν η Επιτροπή Ασφαλείας εκδώσει ευνοϊκή σύσταση όσον αφορά την κοινοποίηση των ΔΠΕΕ, το ζήτημα παραπέμπεται στην Επιτροπή των Μονίμων Αντιπροσώπων (ΕΜΑ) η οποία λαμβάνει τη σχετική απόφαση.

34. Εάν η Επιτροπή Ασφαλείας δεν εκδώσει ευνοϊκή σύσταση για την κοινοποίηση των ΔΠΕΕ:

α) για θέματα που αφορούν την ΚΕΠΠΑ/ΚΠΑΑ, η Επιτροπή Πολιτικής και Ασφάλειας εξετάζει το ζήτημα και διατυπώνει σύσταση για λήψη απόφασης από την ΕΜΑ,

β) για τα υπόλοιπα θέματα, η ΕΜΑ εξετάζει το ζήτημα και λαμβάνει σχετική απόφαση.

35. Εφόσον κρίνεται σκόπιμο, και με την επιφύλαξη της προηγούμενης γραπτής συγκατάθεσης του φορέα προέλευσης, η ΕΜΑ δύναται να αποφασίσει ότι οι διαβαθμισμένες πληροφορίες μπορούν να κοινοποιηθούν μόνο εν μέρει ή μόνο εφόσον υποχαρακτηρισθούν ή αποχαρακτηρισθούν προηγουμένως, ή ότι οι προς παροχή πληροφορίες πρέπει να ετοιμασθούν χωρίς αναφορά στην πηγή ή το αρχικό επίπεδο διαβάθμισης της ΕΕ.

36. Μετά την απόφαση κοινοποίησης των ΔΠΕΕ, η ΓΓΣ προωθεί το εν λόγω έγγραφο το οποίο φέρει σήμανση κοινοποιησιμότητας στην οποία αναφέρεται το τρίτο κράτος ή ο διεθνής οργανισμός στον οποίο κοινοποιήθηκε. Πριν από ή κατά την κοινοποίηση, το εν λόγω τρίτο μέρος δεσμεύεται γραπτώς να προστατεύσει τις ΔΠΕΕ που λαμβάνει σύμφωνα με τις βασικές αρχές και τις ελάχιστες προδιαγραφές που περιγράφονται στην παρούσα απόφαση.

VII. ΑΡΜΟΔΙΟΤΗΤΑ ΚΟΙΝΟΠΟΙΗΣΗΣ ΔΠΕΕ ΣΕ ΤΡΙΤΑ ΚΡΑΤΗ Ή ΔΙΕΘΝΕΙΣ ΟΡΓΑΝΙΣΜΟΥΣ

37. Όταν υφίσταται πλαίσιο σύμφωνα με την παράγραφο 2 για την ανταλλαγή διαβαθμισμένων πληροφοριών με τρίτο κράτος ή διεθνή οργανισμό, το Συμβούλιο λαμβάνει απόφαση με την οποία εξουσιοδοτεί τον γενικό γραμματέα να κοινοποιήσει τις ΔΠΕΕ, σύμφωνα με την αρχή της συγκατάθεσης του φορέα προέλευσης των πληροφοριών, στο οικείο τρίτο κράτος ή διεθνή οργανισμό. Ο γενικός γραμματέας δύναται να μεταβιβάζει την αρμοδιότητα αυτή σε ανώτατα στελέχη της ΓΓΣ.

38. Όταν υφίσταται συμφωνία ασφάλειας των πληροφοριών σύμφωνα με την παράγραφο 2 πρώτη περίπτωση, το Συμβούλιο μπορεί να λάβει την απόφαση να εξουσιοδοτήσει τον Ύπατο Εκπρόσωπο να κοινοποιήσει ΔΠΕΕ που παράγονται στο Συμβούλιο στον τομέα της κοινής εξωτερικής πολιτικής και της πολιτικής ασφάλειας, αφού εξασφαλίσει τη συγκατάθεση του φορέα προέλευσης του πρωτογενούς υλικού που ενδεχομένως περιέχουν, στο οικείο τρίτο κράτος ή διεθνή οργανισμό. Ο Ύπατος Εκπρόσωπος δύναται να μεταβιβάζει την αρμοδιότητα αυτή σε ανώτατα στελέχη της ΕΥΕΔ ή σε ΕΕΕΕ.

39. Όταν υφίσταται πλαίσιο σύμφωνα με την παράγραφο 2 ή την παράγραφο 3 για την ανταλλαγή διαβαθμισμένων πληροφοριών με τρίτο κράτος ή διεθνή οργανισμό, ο Ύπατος Εκπρόσωπος εξουσιοδοτείται να κοινοποιήσει ΔΠΕΕ, σύμφωνα με την απόφαση για τη σύσταση της επιχείρησης ΚΠΑΑ και με την αρχή της συγκατάθεσης του φορέα προέλευσης των πληροφοριών. Ο Ύπατος Εκπρόσωπος δύναται να μεταβιβάζει την αρμοδιότητα αυτή σε ανώτατα στελέχη της ΕΥΕΔ, στους διοικητές επιχείρησης, αποστολής ή δύναμης της ΕΕ ή στους επικεφαλής αποστολής της ΕΕ.

Προσαρτήματα

Προσάρτημα Α

Ορισμοί

Προσάρτημα Β

Αντιστοιχία των διαβαθμίσεων ασφαλείας

Προσάρτημα Γ

Κατάλογος των εθνικών αρχών ασφαλείας (ΕΑΑ)

Προσάρτημα Δ

Κατάλογος συντμήσεων

Προσάρτημα Α

ΟΡΙΣΜΟΙ

Για τους σκοπούς της παρούσας απόφασης, ισχύουν οι ακόλουθοι ορισμοί:

«Πιστοποίηση» είναι η διαδικασία που καταλήγει σε τυπική δήλωση της Αρχής Πιστοποίησης της Ασφάλειας (ΕΠΑ) ότι το δεδομένο σύστημα έχει λάβει έγκριση να λειτουργεί με καθορισμένο βαθμό ασφαλείας, με συγκεκριμένο τρόπο ασφαλείας στο επιχειρησιακό του περιβάλλον και με αποδεκτό βαθμό κινδύνου, βασιζόμενο στην παραδοχή ότι εφαρμόζεται εγκεκριμένο σύνολο τεχνικών, φυσικών, οργανωτικών και διαδικαστικών μέτρων ασφαλείας.

«Στοιχείο» είναι οτιδήποτε έχει αξία για τον οργανισμό, τις επιχειρήσεις και τη συνέχιση των δραστηριοτήτων, περιλαμβανομένων των πηγών πληροφοριών που υποστηρίζουν την αποστολή του οργανισμού.

«Εξουσιοδότηση για πρόσβαση σε ΔΠΕΕ» είναι η απόφαση που λαμβάνει η αρμόδια για τους διορισμούς αρχή της ΓΓΣ βάσει διαβεβαίωσης που δίνει η αρμόδια αρχή κράτους μέλους ότι υπάλληλος, μέλος του λοιπού προσωπικού της ΓΓΣ ή αποσπασμένος εθνικός εμπειρογνώμων μπορεί, υπό τον όρο ότι έχει προσδιοριστεί η ανάγκη γνώσης του και ότι έχει ενημερωθεί καταλλήλως σχετικά με τις ευθύνες του, να έχει πρόσβαση σε ΔΠΕΕ μέχρις ενός συγκεκριμένου επιπέδου (CONFIDENTIEL UE/EU CONFIDENTIAL ή υψηλότερου) έως προκαθορισμένη ημερομηνία.

«Κύκλος ζωής CIS» είναι η συνολική διάρκεια ύπαρξης ενός CIS, που περιλαμβάνει την έναρξη της διαδικασίας, την αρχική σύλληψη, τον προγραμματισμό, την ανάλυση απαιτήσεων, τον σχεδιασμό, την ανάπτυξη, τη δοκιμή, την εφαρμογή, τη λειτουργία, τη συντήρηση και τον παροπλισμό.

«Διαβαθμισμένη σύμβαση» είναι η σύμβαση που συνάπτεται μεταξύ της ΓΓΣ και ενός εργολάβου για την προμήθεια υλικού, την εκτέλεση έργου ή την παροχή υπηρεσιών, της οποίας η υλοποίηση απαιτεί ή περιλαμβάνει την πρόσβαση σε ΔΠΕΕ ή τη δημιουργία τους.

«Διαβαθμισμένη σύμβαση υπεργολαβίας» είναι η σύμβαση που συνάπτεται μεταξύ ενός εργολάβου της ΓΓΣ και ενός άλλου εργολάβου (ήτοι του υπεργολάβου) για την προμήθεια υλικού, την εκτέλεση έργου ή την παροχή υπηρεσιών, της οποίας η υλοποίηση απαιτεί ή περιλαμβάνει την πρόσβαση σε ΔΠΕΕ ή τη δημιουργία τους.

«Σύστημα επικοινωνίας και πληροφοριών» (CIS) — βλέπε άρθρο 10 παράγραφος 2.

«Εργολάβος» είναι το φυσικό ή νομικό πρόσωπο που έχει τη νομική ικανότητα ανάληψης συμβάσεων.

«Κρυπτογραφικό υλικό» είναι οι κρυπτογραφικοί αλγόριθμοι, το κρυπτογραφικό υλικό και οι ενότητες λογισμικού, καθώς και τα προϊόντα που περιέχουν λεπτομέρειες εφαρμογής και τη συναφή τεκμηρίωση και το υλικό πληκτρολόγησης.

«Κρυπτογραφικό προϊόν» είναι το προϊόν του οποίου η πρωταρχική και κύρια λειτουργία είναι η παροχή υπηρεσιών ασφαλείας (εμπιστευτικότητα, ακεραιότητα, γνησιότητα, μη άρνηση αναγνώρισης των πληροφοριών) μέσω ενός ή περισσότερων κρυπτογραφικών μηχανισμών.

«Επιχείρηση ΚΠΑΑ» είναι η επιχείρηση διαχείρισης στρατιωτικών και μη στρατιωτικών κρίσεων σύμφωνα με τον τίτλο V κεφάλαιο 2 της Συνθήκης ΕΕ.

«Αποχαρακτηρισμός» είναι η κατάργηση οποιασδήποτε διαβάθμισης ασφαλείας.

«Ασφάλεια εις βάθος» είναι η εφαρμογή μιας σειράς μέτρων ασφαλείας, τα οποία οργανώνονται ως πολλαπλά επίπεδα άμυνας.

«Καθορισμένη αρχή ασφαλείας» (ΚΑΑ) είναι η αρχή η οποία είναι υπόλογη στην Εθνική Αρχή Ασφαλείας (ΕΑΑ) κράτους μέλους και έχει καθήκον, αφενός, να ενημερώνει τους βιομηχανικούς και άλλους φορείς σχετικά με την εθνική πολιτική στα θέματα βιομηχανικής ασφαλείας και, αφετέρου, να τους καθοδηγεί και να τους παρέχει συνδρομή κατά την εφαρμογή αυτής της εθνικής πολιτικής. Τα καθήκοντα της ΚΑΑ μπορούν να εκτελούνται από την ΕΑΑ ή από οποιαδήποτε άλλη αρμόδια αρχή.

«Έγγραφο» είναι κάθε καταγεγραμμένη πληροφορία ανεξαρτήτως φυσικής μορφής ή χαρακτηριστικών.

«Υποχαρακτηρισμός» είναι η μείωση του επιπέδου της διαβάθμισης ασφαλείας.

«Διαβαθμισμένες πληροφορίες ΕΕ» (ΔΠΕΕ) — βλέπε άρθρο 2 παράγραφος 1.

«Εξουσιοδότηση ασφαλείας φορέα» (FSC) είναι η διοικητική απόφαση της ΕΑΑ/ΚΑΑ η οποία βεβαιώνει ότι, από πλευράς ασφαλείας, ο φορέας μπορεί να εξασφαλίσει επαρκές επίπεδο προστασίας ΔΠΕΕ ορισμένης διαβάθμισης ασφαλείας.

«Χειρισμός» ΔΠΕΕ είναι όλες οι δυνατές ενέργειες στις οποίες είναι δυνατόν να υποβληθούν οι ΔΠΕΕ καθ' όλη τη διάρκεια του κύκλου ζωής τους. Περιλαμβάνει τη δημιουργία, την επεξεργασία, τη μεταφορά, τον υποχαρακτηρισμό, τον αποχαρακτηρισμό και την καταστροφή τους. Σε σχέση με το CIS περιλαμβάνει επίσης τη συλλογή, την επίδειξη, τη διαβίβαση και την αποθήκευσή τους.

«Κάτοχος» είναι το δεόντως εξουσιοδοτημένο πρόσωπο με προσδιορισμένη ανάγκη γνώσης που κατέχει ένα στοιχείο ΔΠΕΕ και είναι αντιστοίχως υπεύθυνο για την προστασία του.

«Βιομηχανικός ή άλλος φορέας» είναι ο φορέας που ασχολείται με την προμήθεια φυσικών αγαθών, την εκτέλεση έργων ή την παροχή υπηρεσιών· ο ορισμός αυτός αφορά βιομηχανικούς, εμπορικούς, επιστημονικούς, ερευνητικούς, εκπαιδευτικούς ή αναπτυξιακούς φορείς, φορείς παροχής υπηρεσιών ή αυτοαπασχολούμενους.

«Βιομηχανική ασφάλεια» — βλέπε άρθρο 11 παράγραφος 1.

«Διασφάλιση των πληροφοριών» — βλέπε άρθρο 10 παράγραφος 1.

«Διασύνδεση» — βλέπε παράρτημα IV παράγραφος 32.

«Διαχείριση διαβαθμισμένων πληροφοριών» — βλέπε άρθρο 9 παράγραφος 1.

«Υλικό» είναι κάθε έγγραφο, φορέας δεδομένων ή στοιχείο μηχανημάτων ή εξοπλισμού που έχει ήδη κατασκευασθεί ή ευρίσκεται υπό κατασκευή.

«Φορέας προέλευσης» είναι το όργανο, οργανισμός ή υπηρεσία της ΕΕ, κράτος μέλος, τρίτο κράτος ή διεθνής οργανισμός υπό την εξουσία του οποίου διαβαθμισμένες πληροφορίες έχουν δημιουργηθεί και/ή εισαχθεί στις δομές της ΕΕ.

«Ασφάλεια προσωπικού» — βλέπε άρθρο 7 παράγραφος 1.

«Εξουσιοδότηση ασφαλείας προσωπικού» (ΕΑΠ) είναι η δήλωση αρμόδιας αρχής κράτους μέλους στην οποία προβαίνει μετά την ολοκλήρωση έρευνας ασφαλείας από τις αρμόδιες αρχές του εν λόγω κράτους μέλους και πιστοποιεί ότι ένα άτομο μπορεί να έχει πρόσβαση σε διαβαθμισμένες πληροφορίες μέχρις ενός συγκεκριμένου επιπέδου (ισοδύναμου με CONFIDENTIEL UE/EU CONFIDENTIAL ή ανώτερου) έως προκαθορισμένη ημερομηνία.

«Πιστοποιητικό ελέγχου ασφαλείας προσωπικού» (ΠΕΑΠ) είναι το πιστοποιητικό που εκδίδει αρμόδια αρχή με το οποίο πιστοποιείται ότι συγκεκριμένο άτομο έχει υποστεί έλεγχο ασφαλείας και διαθέτει έγκυρο πιστοποιητικό διαβάθμισης ασφαλείας από την αρμόδια για τους διορισμούς αρχή για πρόσβαση σε ΔΠΕΕ και στο οποίο αναφέρονται το επίπεδο των ΔΠΕΕ στις οποίες μπορεί να έχει πρόσβαση (CONFIDENTIEL UE/EU CONFIDENTIAL ή υψηλότερο), η ημερομηνία ισχύος της σχετικής ΕΑΠ και η ημερομηνία λήξης του πιστοποιητικού.

«Φυσική ασφάλεια» — βλέπε άρθρο 8 παράγραφος 1.

«Πρόγραμμα/Σχέδιο εντολών ασφαλείας» (PSI) είναι ο κατάλογος των διαδικασιών ασφαλείας που εφαρμόζονται σε συγκεκριμένο πρόγραμμα/σχέδιο για την τυποποίησή τους. Μπορεί να αναθεωρείται μέσω του προγράμματος/σχεδίου.

«Καταχώριση» — βλέπε παράρτημα III παράγραφος 18.

«Υπολειπόμενος κίνδυνος» είναι ο κίνδυνος που εξακολουθεί να υφίσταται και μετά την εφαρμογή των μέτρων ασφαλείας, δεδομένου ότι δεν είναι δυνατόν να αντιμετωπισθούν όλες οι απειλές και να εξαλειφθούν όλες οι τρωτότητες.

«Κίνδυνος» είναι η πιθανότητα μια δεδομένη απειλή να εκμεταλλευθεί τα εσωτερικά και εξωτερικά τρωτά σημεία ενός οργανισμού ή των συστημάτων που χρησιμοποιεί και να προκαλέσει βλάβη στον οργανισμό και στα υλικά ή άυλα στοιχεία του. Μετράται ως ο συνδυασμός της ενδεχόμενης υλοποίησης των απειλών και των συνεπειών τους.

— «Αποδοχή του κινδύνου» είναι η απόφαση με την οποία συμφωνείται ότι υφίσταται υπολειπόμενος κίνδυνος μετά τον χειρισμό του.

— Η «αξιολόγηση κινδύνου» συνίσταται στον εντοπισμό των απειλών και των τρωτών σημείων και στη διεξαγωγή σχετικής ανάλυσης του κινδύνου, ήτοι ανάλυση της ενδεχόμενης υλοποίησης και των συνεπειών της.

— Η «κοινοποίηση του κινδύνου» συνίσταται στην ευαισθητοποίηση ως προς τους κινδύνους μεταξύ των κοινοτήτων των χρηστών CIS, στην ενημέρωση των αρχών έγκρισης ως προς τους κινδύνους αυτούς και στην υποβολή σχετικών εκθέσεων στις επιχειρησιακές αρχές.

— Ο «χειρισμός του κινδύνου» συνίσταται στην άμβλυνση, αναίρεση ή μείωση του κινδύνου (μέσω κατάλληλου συνδυασμού τεχνικών, φυσικών, οργανωτικών ή διαδικαστικών μέτρων), μεταφορά ή παρακολούθηση του κινδύνου.

«Έγγραφο θεμάτων ασφαλείας» (ΕΘΑ) είναι το σύνολο ειδικών συμβατικών όρων, που εκδίδει η αναθέτουσα αρχή, το οποίο αποτελεί αναπόσπαστο μέρος διαβαθμισμένης σύμβασης που συνεπάγεται πρόσβαση σε ΔΠΕΕ ή δημιουργία τέτοιων πληροφοριών και καθορίζει τις απαιτήσεις ασφαλείας ή τα στοιχεία της σύμβασης που χρειάζονται προστασία.

«Οδηγός διαβαθμίσεων ασφαλείας» («ΟΔΑ») είναι το έγγραφο στο οποίο περιγράφονται τα στοιχεία προγράμματος ή σύμβασης που είναι διαβαθμισμένα και καθορίζεται η εφαρμοστέα διαβάθμιση ασφαλείας. Ο ΟΔΑ μπορεί να επεκτείνεται καθ' όλη τη διάρκεια του προγράμματος ή της σύμβασης και ενδέχεται να γίνεται εκ νέου διαβάθμιση των στοιχείων, ακόμα και σε κατώτερη βαθμίδα· όταν υπάρχει ΟΔΑ, πρέπει να αποτελεί τμήμα του ΕΘΑ.

«Έρευνα ασφαλείας» είναι οι διαδικασίες έρευνας που διενεργούνται από την αρμόδια εθνική αρχή κράτους μέλους σύμφωνα με τους σχετικούς νόμους και κανονισμούς που ισχύουν στο εν λόγω κράτος μέλος για την εξασφάλιση διαβεβαίωσης ότι δεν είναι γνωστό τίποτε αρνητικό που να εμποδίζει τη χορήγηση στο εν λόγω πρόσωπο ΕΑΠ ή εξουσιοδότησης για πρόσβαση σε ΔΠΕΕ μέχρις ενός συγκεκριμένου επιπέδου (CONFIDENTIEL UE/EU CONFIDENTIAL ή υψηλότερου).

«Επίπεδο ασφαλείας λειτουργίας» είναι ο ορισμός των προϋποθέσεων υπό τις οποίες λειτουργεί το CIS βάσει της ταξινόμησης των πληροφοριών τις οποίες χειρίζεται και των επιπέδων διαβάθμισης, των τυπικών εγκρίσεων πρόσβασης και της «ανάγκης γνώσης» των χρηστών του. Για το χειρισμό ή τη διαβίβαση διαβαθμισμένων πληροφοριών υφίστανται τέσσερις τρόποι λειτουργίας: απόλυτο επίπεδο, υψηλό επίπεδο, τμηματικό επίπεδο και πολλαπλό επίπεδο:

— «Απόλυτο επίπεδο ασφαλείας» είναι το επίπεδο λειτουργίας στο οποίο όλα τα πρόσωπα που έχουν πρόσβαση στο CIS ελέγχονται σύμφωνα με τον ανώτατο βαθμό διαβάθμισης των πληροφοριών που χειρίζεται το CIS και έχουν την ίδια ανάγκη γνώσης όλων των πληροφοριών που χειρίζεται το CIS,

— «Υψηλό επίπεδο ασφαλείας» είναι το επίπεδο λειτουργίας στο οποίο όλα τα πρόσωπα που έχουν πρόσβαση στο CIS ελέγχονται σύμφωνα με τον ανώτατο βαθμό διαβάθμισης των πληροφοριών που χειρίζεται το CIS, αλλά δεν έχουν όλα την ίδια ανάγκη γνώσης των πληροφοριών που χειρίζεται το CIS· έγκριση πρόσβασης στις πληροφορίες μπορεί να δοθεί από πρόσωπο,

— «Τμηματικό επίπεδο ασφαλείας» είναι το επίπεδο λειτουργίας στο οποίο όλα τα πρόσωπα που έχουν πρόσβαση στο CIS ελέγχονται σύμφωνα με τον ανώτατο βαθμό διαβάθμισης των πληροφοριών που χειρίζεται το CIS, αλλά δεν διαθέτουν όλα τα πρόσωπα που έχουν πρόσβαση στο CIS τυπική έγκριση πρόσβασης σε όλες τις πληροφορίες που χειρίζεται το CIS· για την τυπική έγκριση απαιτείται τυπικός έλεγχος από την κεντρική αρχή διαχείρισης της πρόσβασης ο οποίος διαφέρει από τη διακριτική ευχέρεια προσώπου να εγκρίνει την πρόσβαση,

— «Πολλαπλό επίπεδο ασφαλείας» είναι το επίπεδο λειτουργίας στο οποίο δεν ελέγχονται όλα τα πρόσωπα που έχουν πρόσβαση στο CIS σύμφωνα με τον ανώτατο βαθμό διαβάθμισης των πληροφοριών που χειρίζεται το σύστημα ούτε έχουν την ίδια ανάγκη γνώσης των πληροφοριών που χειρίζεται το CIS.

«Διαδικασία διαχείρισης κινδύνων ασφαλείας» είναι το σύνολο της διαδικασίας εντοπισμού, ελέγχου και ελαχιστοποίησης αβέβαιων γεγονότων που μπορούν να θίξουν την ασφάλεια οργανισμού ή οποιουδήποτε από τα συστήματα που χρησιμοποιεί. Καλύπτει το σύνολο των δραστηριοτήτων σχετικά με τους κινδύνους, περιλαμβανομένων της αξιολόγησης, της επεξεργασίας, της αποδοχής και της κοινοποίησης.

«TEMPEST» είναι η έρευνα, η μελέτη και ο έλεγχος του κινδύνου διαρροής μέσω ηλεκτρομαγνητικών εκπομπών και τα μέτρα εξάλειψης των εκπομπών αυτών.

«Απειλή» είναι η πιθανή αιτία ανεπιθύμητου συμβάντος που μπορεί να θίξει ένα οργανισμό ή οποιοδήποτε από τα συστήματα που χρησιμοποιεί· οι απειλές μπορεί να είναι τυχαίες ή εσκεμμένες (δόλιες) και χαρακτηρίζονται από απειλητικά στοιχεία, πιθανούς στόχους και μεθόδους επίθεσης.

«Τρωτότητα» είναι η οποιαδήποτε αδυναμία που μπορούν να εκμεταλλευθούν μία ή περισσότερες απειλές. Η τρωτότητα μπορεί να οφείλεται σε κάποια παράλειψη ή να απορρέει από κάποια αδυναμία των ελέγχων όσον αφορά την αυστηρότητα, την πληρότητα ή τη σταθερότητά τους, μπορεί δε να είναι τεχνικής, διαδικαστικής, φυσικής, οργανωτικής ή επιχειρησιακής φύσεως.

Προσάρτημα Β

ΑΝΤΙΣΤΟΙΧΙΑ ΤΩΝ ΔΙΑΒΑΘΜΙΣΕΩΝ ΑΣΦΑΛΕΙΑΣ

ΕΕ	TRÈS SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
Βέλγιο	Très Secret (Loi 11.12.1998) Zeer Geheim (Wet 11.12.1998)	Secret (Loi 11.12.1998) Geheim (Wet 11.12.1998)	Confidentiel (Loi 11.12.1998) Vertrouwelijk (Wet 11.12.1998)	Βλέπε ([1]) κατωτέρω
Βουλγαρία	Строго секретно	Секретно	Поверително	За служебно ползване
Τσεχική Δημοκρατία	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Δανία	YDERST HEMMELIGT	HEMMELIGT	FORTROLIGT	TIL TJENESTEBRUG
Γερμανία	STRENG GEHEIM	GEHEIM	VS ([2])— VERTRAULICH	VS — NUR FÜR DEN DIENSTGEBRAUCH
Εσθονία	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Ιρλανδία	Top Secret	Secret	Confidential	Restricted
Ελλάδα	Άκρως Απόρρητο Συντμ: ΑΑΠ	Απόρρητο Συντμ: (ΑΠ)	Εμπιστευτικό Συντμ: (ΕΜ)	Περιορισμένης Χρήσης Συντμ: (ΠΧ)
Ισπανία	SECRETO	RESERVADO	CONFIDENCIAL	DIFUSIÓN LIMITADA
Γαλλία	Très Secret Défense	Secret Défense	Confidentiel Défense	Βλέπε ([3]) παρακάτω
Κροατία	VRLO TAJNO	TAJNO	POVJERLJIVO	OGRANIČENO
Ιταλία	Segretissimo	Segreto	Riservatissimo	Riservato
Κύπρος	Άκρως Απόρρητο Συντμ: (ΑΑΠ)	Απόρρητο Συντμ: (ΑΠ)	Εμπιστευτικό Συντμ: (ΕΜ)	Περιορισμένης Χρήσης Συντμ: (ΠΧ)
Λετονία	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Λιθουανία	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
Λουξεμβούργο	Très Secret Lux	Secret Lux	Confidentiel Lux	Restreint Lux
Ουγγαρία	Szigorúan titkos!	Titkos!	Bizalmas!	Korlátozott terjesztésű!
Μάλτα	L-Ogħla Segretezza Top Secret	Sigriet Secret	Kunfidenzjali Confidential	Ristrett Restricted ([4])
Κάτω Χώρες	Stg. ZEER GEHEIM	Stg. GEHEIM	Stg. CONFIDENTIEEL	Dep. VERTROUWELIJK
Αυστρία	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Πολωνία	Ściśle Tajne	Tajne	Poufne	Zastrzeżone
Πορτογαλία	Muito Secreto	Secreto	Confidencial	Reservado

ΕΕ	TRÈS SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
Ρουμανία	Strict secret de importanță deosebită	Strict secret	Secret	Secret de serviciu
Σλοβενία	STROGO TAJNO	TAJNO	ZAUPNO	INTERNO
Σλοβακία	Prísne tajné	Tajné	Dôverné	Vyhradené
Φινλανδία	ERITTÄIN SALAINEN YTTERST HEMLIG	SALAINEN HEMLIG	LUOTTAMUKSELLINEN KONFIDENTIELL	KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG
Σουηδία (5)	HEMLIG/TOP SECRET HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET	HEMLIG/SECRET HEMLIG	HEMLIG/CONFIDEN-TIAL HEMLIG	HEMLIG/RESTRICTED HEMLIG
Ηνωμένο Βασίλειο	UK TOP SECRET	UK SECRET	UK CONFIDENTIAL	UK RESTRICTED

(1) Η «Diffusion Restreinte/Beperkte Verspreiding» δεν αποτελεί διαβάθμιση ασφαλείας στο Βέλγιο. Το Βέλγιο χειρίζεται και προστατεύει τις πληροφορίες «RESTREINT UE/EU RESTRICTED» κατά τρόπο εξίσου αυστηρό με τα πρότυπα και τις διαδικασίες που περιγράφονται στους κανόνες ασφαλείας του Συμβουλίου της Ευρωπαϊκής Ένωσης.

(2) Γερμανία: VS = Verschlusssache.

(3) Η Γαλλία δεν χρησιμοποιεί την κατηγορία διαβάθμισης «RESTREINT» στο εθνικό της σύστημα. Η Γαλλία χειρίζεται και προστατεύει τις πληροφορίες «RESTREINT UE/EU RESTRICTED» κατά τρόπο εξίσου αυστηρό με τα πρότυπα και τις διαδικασίες που περιγράφονται στους κανόνες ασφαλείας του Συμβουλίου της Ευρωπαϊκής Ένωσης.

(4) Για τη Μάλτα, οι ενδείξεις στα μαλτέζικα και στα αγγλικά μπορούν να χρησιμοποιούνται εναλλακτικά.

(5) Σουηδία: οι σημάνσεις διαβάθμισης ασφαλείας στην άνω σειρά χρησιμοποιούνται από τις αρχές άμυνας και οι ενδείξεις στην κάτω σειρά από άλλες αρχές.

Προσάρτημα Γ

ΚΑΤΑΛΟΓΟΣ ΕΘΝΙΚΩΝ ΑΡΧΩΝ ΑΣΦΑΛΕΙΑΣ (ΕΑΑ)

ΒΕΛΓΙΟ
Autorité nationale de Sécurité
SPF Affaires étrangères, Commerce extérieur et Coopération au Développement
15, rue des Petits Carmes
1000 Bruxelles

Τηλ. Γραμματείας: +32 25014542
Φαξ +32 25014596
E-mail: nvo-ans@diplobel.fed.be

ΒΟΥΛΓΑΡΙΑ
State Commission on Information Security
90 Cherkovna Str.
1505 Sofia

Τηλ. +359 29333600
Φαξ +359 29873750
E-mail: dksi@government.bg
Ιστοσελίδα: www.dksi.bg

ΤΣΕΧΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Národní bezpečnostní úřad
(National Security Authority)
Na Popelce 2/16
150 06 Praha 56

Τηλ. +420 257283335
Φαξ +420 257283110
E-mail: czech.nsa@nbu.cz
Ιστοσελίδα: www.nbu.cz

ΔΑΝΙΑ
Politiets Efterretningstjeneste
(Danish Security Intelligence Service)
Klausdalsbrovej 1
2860 Søborg

Τηλ. +45 33148888
Φαξ +45 33430190

Forsvarets Efterretningstjeneste
(Δανέζικη Υπηρεσία Πληροφοριών Άμυνας)
Kastellet 30
2100 Copenhagen Ø

Τηλ. +45 33325566
Φαξ +45 33931320

ΓΕΡΜΑΝΙΑ
Bundesministerium des Innern
Referat ÖS III 3
Alt-Moabit 101 D
D-11014 Berlin

Τηλ. +49 30186810
Φαξ +49 30186811441
E-mail: oesIII3@bmi.bund.de

ΕΣΘΟΝΙΑ
National Security Authority Department
Estonian Ministry of Defence
Sakala 1
15094 Tallinn

Τηλ. +372 717 0019, +372 7170117
Φαξ +372 7170213
E-mail: nsa@mod.gov.ee

ΙΡΛΑΝΔΙΑ
National Security Authority
Department of Foreign Affairs
76 - 78 Harcourt Street
Dublin 2

Τηλ. +353 14780822
Φαξ +353 14082959

ΕΛΛΑΔΑ
Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ)
Διεύθυνση Ασφαλείας και Αντιπληροφοριών
ΣΤΓ 1020 -Χολαργός (Αθήνα)
Ελλάδα

Τηλ. +30 2106572045 (ώρες γραφείου)
+30 2106572009 (ώρες γραφείου)
Φαξ +30 2106536279
+30 2106577612

Hellenic National Defence General Staff (HNDGS)
Counter Intelligence and Security Directorate (NSA)
227-231 HOLARGOS
STG 1020 ATHENS

Τηλ. +30 2106572045
+30 2106572009
Φαξ +30 2106536279
+30 2106577612

ΙΣΠΑΝΙΑ
Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Avenida Padre Huidobro s/n
28023 Madrid

Τηλ. +34 913725000
Φαξ +34 913725808
E-mail: nsa-sp@areatec.com

ΓΑΛΛΙΑ
Secrétariat général de la défense et de la sécurité nationale
Sous-direction Protection du secret (SGDSN/PSD)
51 Boulevard de la Tour-Maubourg
75700 Paris 07 SP

Τηλ. +33 171758177
Φαξ +33 171758200

ΚΡΟΑΤΙΑ
Office of the National Security Council
Croatian NSA
Jurjevska 34
10000 Zagreb
Croatia

Τηλ. +385 14681222
Φαξ +385 14686049
www.uvns.hr

ΛΟΥΞΕΜΒΟΥΡΓΟ
Autorité nationale de Sécurité
Boîte postale 2379
1023 Luxembourg

Τηλ. +352 24782210 central
+352 24782253 direct
Φαξ +352 24782243

ΙΤΑΛΙΑ
Presidenza del Consiglio dei Ministri
D.I.S. - U.C.Se.
Via di Santa Susanna, 15
00187 Roma

Τηλ. +39 0661174266
Φαξ +39 064885273

ΟΥΓΓΑΡΙΑ
Nemzeti Biztonsági Felügyelet
(National Security Authority of Hungary)
H-1024 Budapest, Szilágyi Erzsébet fasor 11/B

Τηλ. +36 (1) 7952303
Φαξ +36 (1) 7950344
Ταχυδρομική διεύθυνση:
H-1357 Budapest, PO Box 2
E-mail: nbf@nbf.hu
Ιστοσελίδα: www.nbf.hu

ΚΥΠΡΟΣ
ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ
ΣΤΡΑΤΙΩΤΙΚΟ ΕΠΙΤΕΛΕΙΟ ΤΟΥ ΥΠΟΥΡΓΟΥ
Εθνική Αρχή Ασφάλειας (ΕΑΑ)
Υπουργείο Άμυνας
Λεωφόρος Εμμανουήλ Ροΐδη 4
1432 Λευκωσία, Κύπρος

Τηλέφωνα: +357 22807569, +357 22807643,
+357 22807764
Τηλεομοιότυπο: +357 22302351

Ministry of Defence
Minister's Military Staff
National Security Authority (NSA)
4 Emanuel Roidi street
1432 Nicosia

Τηλ. +357 22807569, +357 22807643, +357 22807764
Φαξ +357 22302351
E-mail: cynsa@mod.gov.cy

ΜΑΛΤΑ
Ministry for Home Affairs and National Security
P.O. Box 146
MT-Valletta

Τηλ. +356 21249844
Φαξ +356 25695321

ΛΕΤΟΝΙΑ
National Security Authority
Constitution Protection Bureau of the Republic of Latvia
P.O.Box 286
LV-1001 Riga

Τηλ. +371 67025418
Φαξ +371 67025454
E-mail: ndi@sab.gov.lv

ΚΑΤΩ ΧΩΡΕΣ
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Postbus 20010
2500 EA Den Haag

Τηλ. +31 703204400
Φαξ +31 703200733

Ministerie van Defensie
Beveiligingsautoriteit
Postbus 20701
2500 ES Den Haag

Τηλ. +31 703187060
Φαξ +31 703187522

ΛΙΘΟΥΑΝΙΑ
Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija
(The Commission for Secrets Protection Coordination of the Republic of Lithuania
National Security Authority)
Gedimino 40/1
LT-01110 Vilnius

Τηλ. +370 706 66701, +370 706 66702
Φαξ +370 706 66700
E-mail: nsa@vsd.lt

ΑΥΣΤΡΙΑ
Informationssicherheitskommission
Bundeskanzleramt
Ballhausplatz 2
1014 Wien

Τηλ. +43 1531152594
Φαξ +43 1531152615
E-mail: ISK@bka.gv.at

ΠΟΛΩΝΙΑ Agencja Bezpieczeństwa Wewnętrznego – ABW (Internal Security Agency) 2A Rakowiecka St. 00-993 Warszawa Τηλ. +48 225857360 Φαξ +48 225858509 E-mail: nsa@abw.gov.pl Ιστοσελίδα: www.abw.gov.pl	**ΣΛΟΒΑΚΙΑ** Národný bezpečnostný úrad (National Security Authority) Budatínska 30 P.O. Box 16 850 07 Bratislava Τηλ. +421 268692314 Φαξ +421 263824005 Ιστοσελίδα: www.nbusr.sk
ΠΟΡΤΟΓΑΛΙΑ Presidência do Conselho de Ministros Autoridade Nacional de Segurança Rua da Junqueira, 69 1300-342 Lisboa Τηλ. +351 213031710 Φαξ +351 213031711	**ΦΙΝΛΑΝΔΙΑ** National Security Authority Ministry for Foreign Affairs P.O. Box 453 FI-00023 Government Τηλ. +358 16055890 Φαξ +358 916055140 E-mail: NSA@formin.fi
ΡΟΥΜΑΝΙΑ Oficiul Registrului Național al Informațiilor Secrete de Stat (Romanian NSA – ORNISS National Registry Office for Classified Information) Str. Mureș nr. 4, sector 1 012275 București Τηλ. +40 212245830 Φαξ +40 212240714 E-mail: nsa.romania@nsa.ro Ιστοσελίδα: www.orniss.ro	**ΣΟΥΗΔΙΑ** Utrikesdepartementet (Ministry for Foreign Affairs) UD-RS S 10339 Stockholm Τηλ. +46 84051000 Φαξ +46 87231176 E-mail: ud-nsa@foreign.ministry.se
ΣΛΟΒΕΝΙΑ Urad Vlade RS za varovanje tajnih podatkov Gregorčičeva 27 1000 Ljubljana Τηλ. +386 14781390 Φαξ +386 14781399 E-mail: gp.uvtp@gov.si	**ΗΝΩΜΕΝΟ ΒΑΣΙΛΕΙΟ** UK National Security Authority Room 335, 3rd Floor 70 Whitehall London SW1A 2AS Τηλ. 1: +44 2072765645 Τηλ. 2: +44 2072765497 Φαξ +44 2072765651 E-mail: UK-NSA@cabinet-office.x.gsi.gov.uk

Προσάρτημα Δ

ΛΙΣΤΑ ΣΥΝΤΜΗΣΕΩΝ

Ακρώνυμο	Σημασία
ΑΑΑΕ (TA)	Αρχή Αντιμετώπισης Ανεπιθύμητων Εκπομπών (TEMPEST Authority)
ΑΔΑ (IAA)	Αρχή Διαπίστευσης Ασφαλείας (Information Assurance Authority)
ΑΔΚ (CDA)	Αρχή Διανομής Κρυπτοϋλικών (Crypto Distribution Authority)
ΑΕΚ (CAA)	Αρχή Έγκρισης Κρυπτογράφησης (Crypto Approval Authority)
ΑΕΠΑ (SAA)	Αρχή Έκδοσης Πιστοποιητικού Ασφαλείας (Security Accreditation Authority)
ΓΤΣ (GSC)	Γενική Γραμματεία του Συμβουλίου (General Secretariat of the Council)
ΔΑΑ (DSA)	Διορισμένη Αρχή Ασφαλείας (Designated Security Authority)
ΔΑΕΕ (ECSD)	Διεύθυνση Ασφάλειας της Ευρωπαϊκής Επιτροπής (European Commission Security Directorate)
ΔΑΛ (SecOPs)	Διαδικασίες Ασφαλούς Λειτουργίας (Security Operating Procedures)
ΔΠ (IA)	Διασφάλιση Πληροφοριών (Information Assurance)
ΔΠΕΕ (EUCI)	Διαβαθμισμένες Πληροφορίες της Ευρωπαϊκής Ένωσης (EU Classified Information)
ΕΑΠ (PSC)	Εξουσιοδότηση Ασφάλειας Προσωπικού (Personnel Security Clearance)
ΕΑΑ (NSA)	Εθνική Αρχή Ασφαλείας (National Security Authority)
ΕΑΕ (FSC)	Εξουσιοδότηση Ασφάλειας Εγκαταστάσεων (Facility Security Clearance)
ΕΑΕΕ (EUSR)	Ειδικός Αντιπρόσωπος της Ευρωπαϊκής Ένωσης (EU Special Representative)
ΕΔΑΑ (SSRS)	Επακριβής Δήλωση Απαιτήσεων Ασφάλειας (System-Specific Security Requirement Statement)
ΕΜΑ (COREPER)	Επιτροπή Μονίμων Αντιπροσώπων (Committee of Permanent Representatives)
ΕΠΑ (SAL)	Επιστολή Πτυχών Ασφαλείας (Security Aspects Letter)
ΙΤ	Πληροφορική (Information Technology)
ΚΕΠΠΑ (CFSP)	Κοινή Εξωτερική Πολιτική και Πολιτική Ασφάλειας (Common Foreign and Security Policy)
ΚΚΤ (CCTV)	Κλειστό Κύκλωμα Τηλεόρασης (Closed Circuit Television)
ΚΠΑ (AQUA)	Κατάλληλα Πιστοποιημένη Αρχή (Appropriately Qualified Authority)
ΚΠΑΑ (CSDP)	Κοινή Πολιτική Ασφαλείας και Άμυνας (Common Security and Defence Policy)
ΟΑΠΕ (PSI)	Οδηγίες Ασφαλείας Προγράμματος/Έργου (Programme/Project Security Instructions)
ΟΔΑ (SCG)	Οδηγίες Διαβάθμισης Ασφαλείας (Security Classification Guide)
ΠΕΑΠ (PSCC)	Πιστοποιητικό Εξουσιοδότησης Ασφάλειας Προσωπικού (Personnel Security Clearance Certificate)
ΣΑΕ (IDS)	Σύστημα Ανίχνευσης Εισβολών (Intrusion Detection System)
ΣΔΑ (SAB)	Συμβούλιο Διαπίστευσης Ασφαλείας (Security Accreditation Board)
ΣΕΠ (CIS)	Συστήματα Επικοινωνιών Πληροφορικής (Communication and Information Systems handling EUCI)
ΥΠΠ (BPS)	Υπηρεσίες Περιμετρικής Προστασίας (Boundary Protection Services)