Το έγγραφο αυτό συνιστά βοήθημα τεκμηρίωσης και δεν δεσμεύει τα κοινοτικά όργανα

►**B**

ΑΠΟΦΑΣΗ ΤΗΣ ΕΠΙΤΡΟΠΗΣ

της 29ης Νοεμβρίου 2001

για την τροποποίηση του εσωτερικού κανονισμού της

[κοινοποιηθείσα υπό τον αριθμό Ε(2001) 3031]

(2001/844/ΕΚ, ΕΚΑΧ, Ευρατόμ)

(ΕΕ L 317 της 3.12.2001, σ. 1)

Τροποποιείται από:

		Επίσημη Εφημερίδα		
		αριθ.	σελίδα	ημερομηνία
►**M1**	Απόφαση της Επιτροπής 2005/94/ΕΚ, Ευρατόμ, της 3ης Φεβρουαρίου 2005	L 31	66	4.2.2005
►**M2**	Απόφαση της Επιτροπής 2006/70/ΕΚ, Ευρατόμ, της 31ης Ιανουαρίου 2006	L 34	32	7.2.2006
►**M3**	Απόφαση της Επιτροπής 2006/548/ΕΚ, Ευρατόμ, της 2ας Αυγούστου 2006	L 215	38	5.8.2006

▼B

ΑΠΟΦΑΣΗ ΤΗΣ ΕΠΙΤΡΟΠΗΣ

της 29ης Νοεμβρίου 2001

για την τροποποίηση του εσωτερικού κανονισμού της

[κοινοποιηθείσα υπό τον αριθμό Ε(2001) 3031]

(2001/844/ΕΚ, ΕΚΑΧ, Ευρατόμ)

Η ΕΠΙΤΡΟΠΗ ΤΩΝ ΕΥΡΩΠΑΪΚΩΝ ΚΟΙΝΟΤΗΤΩΝ,

Έχοντας υπόψη:

τη συνθήκη για την ίδρυση της Ευρωπαϊκής Κοινότητας, και ιδίως το άρθρο 218 παράγραφος 2,

τη συνθήκη για την ίδρυση της Ευρωπαϊκής Κοινότητας Άνθρακα και Χάλυβα, και ιδίως το άρθρο 16,

τη συνθήκη για την ίδρυση της Ευρωπαϊκής Κοινότητας Ατομικής Ενέργειας, και ιδίως το άρθρο 131,

τη συνθήκη για την Ευρωπαϊκή Ένωση, και ιδίως το άρθρο 28 παράγραφος 1 και το άρθρο 41 παράγραφος 1,

ΑΠΟΦΑΣΙΖΕΙ:

Άρθρο 1

Οι διατάξεις της Επιτροπής σχετικά με την ασφάλεια, το κείμενο των οποίων προσαρτάται στην παρούσα απόφαση, προστίθενται ως παράρτημα στον εσωτερικό κανονισμό της Επιτροπής.

Άρθρο 2

Η παρούσα απόφαση αρχίζει να ισχύει την ημέρα της δημοσίευσής της στην *Επίσημη Εφημερίδα των Ευρωπαϊκών Κοινοτήτων*.

Εφαρμόζεται από την 1η Δεκεμβρίου 2001.

▼B

ΠΑΡΑΡΤΗΜΑ

ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΕΠΙΤΡΟΠΗΣ ΣΧΕΤΙΚΑ ΜΕ ΤΗΝ ΑΣΦΑΛΕΙΑ

Εκτιμώντας τα εξής:

(1) Για την ανάπτυξη των δραστηριοτήτων της Επιτροπής σε τομείς που απαιτούν κάποιο βαθμό εμπιστευτικότητας, είναι σκόπιμο να καθιερωθεί ένα πλήρες σύστημα ασφάλειας που θα καλύπτει την Επιτροπή, τα λοιπά θεσμικά όργανα, τους φορείς, τις υπηρεσίες και τους οργανισμούς που έχουν συσταθεί από ή με βάση τη συνθήκη ΕΚ ή τη συνθήκη για την Ευρωπαϊκή Ένωση, τα κράτη μέλη, καθώς και οποιουσδήποτε άλλους αποδέκτες διαβαθμισμένων πληροφοριών της ΕΕ, που καλούνται στο εξής «διαβαθμισμένες πληροφορίες ΕΕ».

(2) Για την προστασία της αποτελεσματικότητας του συστήματος ασφαλείας που θεσπίζεται με τις παρούσες διατάξεις, η Επιτροπή θα διαθέτει διαβαθμισμένες πληροφορίες ΕΕ μόνο στους εξωτερικούς φορείς που παρέχουν εγγυήσεις ότι έχουν λάβει όλα τα απαραίτητα μέτρα για την τήρηση κανόνων αυστηρά ισοδύναμων με εκείνους των παρουσών διατάξεων.

(3) Οι παρούσες διατάξεις εκδίδονται με την επιφύλαξη του κανονισμού αριθ. 3 της 31ης Ιουλίου 1958, περί εφαρμογής του άρθρου 24 της συνθήκης γιατην ίδρυση της Ευρωπαϊκής Κοινότητας Ατομικής Ενέργειας ([1]), του κανονισμού (ΕΟΚ) αριθ. 1588/90 του Συμβουλίου, της 11ης Ιουνίου 1990, σχετικά με τη διαβίβαση στη Στατιστική Υπηρεσία των Ευρωπαϊκών Κοινοτήτων πληροφοριών που καλύπτονται από το στατιστικό απόρρητο ([2]) και με την επιφύλαξη της απόφασης C(95) 1510 τελικό της Επιτροπής, της 23ης Νοεμβρίου 1995, για την προστασία των συστημάτων πληροφορικής.

(4) Η Επιτροπή δημιουργεί ένα σύστημα ασφαλείας με βάση τις αρχές που θεσπίζονται στην απόφαση 2001/264/ΕΚ του Συμβουλίου, της 19ης Μαρτίου 2001, για την έγκριση των κανονισμών ασφαλείας του Συμβουλίου ([3]), με σκοπό τη διασφάλιση της ομαλής λειτουργίας της διαδικασίας λήψης αποφάσεων της Ένωσης.

(5) Η Επιτροπή υπογραμμίζει τη σημασία της συμμετοχής των άλλων θεσμικών οργάνων, όπου ενδείκνυται, στην εφαρμογή των κανόνων και προδιαγραφών εμπιστευτικότητας των αναγκαίων για την προστασία των συμφερόντων της Ένωσης και των κρατών μελών της.

(6) Η Επιτροπή αναγνωρίζει την ανάγκη να δημιουργήσει τη δική της έννοια της ασφάλειας, λαμβάνοντας υπόψη όλα τα στοιχεία σχετικά με την ασφάλεια, καθώς και τον ειδικό χαρακτήρα της Επιτροπής ως θεσμικού οργάνου.

(7) Οι παρούσες διατάξεις εκδίδονται με την επιφύλαξη του άρθρου 255 της συνθήκης και του κανονισμού (ΕΚ) αριθ. 1049/2001 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 30ής Μαΐου 2001, για την πρόσβαση του κοινού στα έγγραφα του Ευρωπαϊκού Κοινοβουλίου, του Συμβουλίου και της Επιτροπής ([4]).

▼M2

(8) Οι παρούσες διατάξεις ισχύουν με την επιφύλαξη του άρθρου 286 της συνθήκης και του κανονισμού (ΕΚ) αριθ. 45/2001 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 18ης Δεκεμβρίου 2000, σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα όργανα και τους οργανισμούς της Κοινότητας και σχετικά με την ελεύθερη κυκλοφορία των δεδομένων αυτών.

▼B

Άρθρο 1

Οι διατάξεις της Επιτροπής σχετικά με την ασφάλεια εμφαίνονται στο παράρτημα.

Άρθρο 2

1. Το αρμόδιο για θέματα ασφαλείας Μέλος της Επιτροπής λαμβάνει τα ενδεδειγμένα μέτρα για να διασφαλίσει ότι, κατά τον χειρισμό διαβαθμισμένων πληροφοριών ΕΕ, τηρούνται στο πλαίσιο της Επιτροπής οι διατάξεις που αναφέρονται στο άρθρο 1 από μονίμους υπαλλήλους και το λοιπό προσωπικό της Επιτροπής, από το αποσπασμένο προσωπικό στην Επιτροπή, καθώς και σε όλους τους τόπους εργασίας της Επιτροπής, συμπεριλαμβανομένων των Αντιπροσωπειών και των Γραφείων στην Ένωση, καθώς και των Αντιπροσωπειών σε τρίτες χώρες και από εξωτερικούς συμβασιούχους της Επιτροπής.

([1]) ΕΕ αριθ. 17 της 6.10.1958, σ. 406/58.
([2]) ΕΕ L 151 της 15.6.1990, σ. 1.
([3]) ΕΕ L 101 της 11.4.2001, σ. 1.
([4]) ΕΕ L 145 της 31.5.2001, σ. 43.

▼**M3**

Όταν μια σύμβαση ή μια συμφωνία επιχορήγησης μεταξύ της Κοινότητας και ενός εξωτερικού εργολάβου ή δικαιούχου συνεπάγεται την επεξεργασία διαβαθμισμένων πληροφοριών ΕΕ στις εγκαταστάσεις του εργολάβου ή του δικαιούχου, τα ενδεδειγμένα μέτρα που λαμβάνονται από τον εν λόγω εξωτερικό εργολάβο ή δικαιούχο για να διασφαλιστεί ότι τηρούνται οι κανόνες που αναφέρονται στο άρθρο 1, κατά τον χειρισμό διαβαθμισμένων πληροφοριών ΕΕ, αποτελούν αναπόσπαστο τμήμα της σύμβασης ή της συμφωνίας επιχορήγησης.

▼**B**

2. Επιτρέπεται στα κράτη μέλη, στα λοιπά θεσμικά όργανα, τους φορείς, τις υπηρεσίες και τους οργανισμούς που έχουν συσταθεί από ή με βάση τις συνθήκες, να λαμβάνουν διαβαθμισμένες πληροφορίες ΕΕ, υπό τον όρο ότι θα διασφαλίζουν ότι, όταν χειρίζονται διαβαθμισμένες πληροφορίες ΕΕ, θα εφαρμόζονται στις υπηρεσίες και τις εγκαταστάσεις τους, διατάξεις αυστηρά ισοδύναμες με εκείνες που αναφέρονται στο άρθρο 1, ιδίως από:

α) τα μέλη των μόνιμων αντιπροσωπειών των κρατών μελών στην Ευρωπαϊκή Ένωση καθώς και τα μέλη των εθνικών αντιπροσωπειών που συμμετέχουν σε συνεδριάσεις της Επιτροπής ή συνεδριάσεις των επιτροπών και ομάδων της ή λαμβάνουν μέρος σε άλλες δραστηριότητες της Επιτροπής,

β) άλλα μέλη των εθνικών διοικήσεων των κρατών μελών τα οποία χειρίζονται διαβαθμισμένες πληροφορίες ΕΕ, ασχέτως του αν υπηρετούν στο έδαφος των κρατών μελών ή στο εξωτερικό,

γ) εξωτερικούς συμβασιούχους και αποσπασμένο προσωπικό που χειρίζονται διαβαθμισμένες πληροφορίες ΕΕ.

Άρθρο 3

Επιτρέπεται σε τρίτες χώρες, διεθνείς οργανισμούς και άλλους φορείς να λαμβάνουν διαβαθμισμένες πληροφορίες ΕΕ (ΔΠΕΕ) υπό τον όρο ότι θα διασφαλίζουν ότι, όταν χειρίζονται ΔΠΕΕ, θα τηρούνται διατάξεις αυστηρά ισοδύναμες με εκείνες που αναφέρονται στο άρθρο 1.

Άρθρο 4

Βάσει των θεμελιωδών αρχών και των στοιχειωδών προδιαγραφών ασφαλείας που περιέχονται στο μέρος I του παραρτήματος, ο αρμόδιος για θέματα ασφάλειας Επίτροπος δύναται να λαμβάνει μέτρα σύμφωνα με το μέρος II του παραρτήματος.

Άρθρο 5

Η παρούσα απόφαση αντικαθιστά από την ημερομηνία έναρξη της εφαρμογής της:

α) την απόφαση C (94) 3282 της Επιτροπής, της 30ής Νοεμβρίου 1994, σχετικά με τα μέτρα ασφαλείας που εφαρμόζονται για διαβαθμισμένες πληροφορίες που παράγονται ή διαβιβάζονται στο πλαίσιο των δραστηριοτήτων της Ευρωπαϊκής Ένωσης·

β) την απόφαση C (1999) 423 της Επιτροπής, της 25ης Φεβρουαρίου 1999, σχετικά με τις διαδικασίες με τις οποίες μπορεί να παρασχεθεί πρόσβαση στους μονίμους υπαλλήλους και το λοιπό προσωπικό της Ευρωπαϊκής Επιτροπής σε διαβαθμισμένες πληροφορίες που διαθέτει η Επιτροπή.

Άρθρο 6

Από την έναρξη της ισχύος των παρουσών διατάξεων, όλες οι διαβαθμισμένες πληροφορίες που διαθέτει η Επιτροπή μέχρι την εν λόγω ημερομηνία, με εξαίρεση τις διαβαθμισμένες πληροφορίες Euratom, πρέπει:

α) εφόσον έχουν δημιουργηθεί από την Επιτροπή, να θεωρούνται ότι έχουν διαβαθμιστεί εκ νέου, ελλείψει βαθμού ασφαλείας, ως «►**M1** RESTREINT UE ◄», εκτός και αν ο συντάκτης τους αποφασίσει να δώσει άλλον χαρακτηρισμό μέχρι την 31η Ιανουαρίου 2002. Στην περίπτωση αυτή, ο συντάκτης πρέπει να ενημερώσει όλους τους παραλήπτες του συγκεκριμένου εγγράφου·

β) εφόσον δημιουργήθηκαν από συντάκτες εκτός της Επιτροπής, διατηρούν την αρχική διαβάθμισή τους και επομένως αντιμετωπίζονται ως διαβαθμισμένες πληροφορίες ΕΕ ισοδύναμου επιπέδου, εκτός εάν ο συντάκτης αποφασίσει τον αποχαρακτηρισμό ή τον υποχαρακτηρισμό των πληροφοριών.

▼B

ΠΑΡΑΡΤΗΜΑ

ΔΙΑΤΑΞΕΙΣ ΑΣΦΑΛΕΙΑΣ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΠΙΤΡΟΠΗΣ

Πίνακας περιεχομένων

ΜΕΡΟΣ Ι: ΒΑΣΙΚΕΣ ΑΡΧΕΣ ΚΑΙ ΕΛΑΧΙΣΤΑ ΠΡΟΤΥΠΑ ΑΣΦΑΛΕΙΑΣ

1. ΕΙΣΑΓΩΓΗ

2. ΓΕΝΙΚΕΣ ΑΡΧΕΣ

3. ΤΑ ΒΑΣΙΚΑ ΣΤΟΙΧΕΙΑ ΤΗΣ ΑΣΦΑΛΕΙΑΣ

4. ΑΡΧΕΣ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΤΩΝ ΠΛΗΡΟΦΟΡΙΩΝ

4.1. **Στόχοι**

4.2. **Ορισμοί**

4.3. **Διαβάθμιση**

4.4. **Στόχοι των μέτρων ασφαλείας**

5. ΟΡΓΑΝΩΣΗ ΤΗΣ ΑΣΦΑΛΕΙΑΣ

5.1. **Κοινές στοιχειώδεις προδιαγραφές**

5.2. **Οργάνωση**

6. ΑΞΙΟΠΙΣΤΙΑ ΤΟΥ ΠΡΟΣΩΠΙΚΟΥ

6.1. **Έλεγχος ασφαλείας (διαβάθμιση) του προσωπικού**

6.2. **Αρχεία ελέγχων ασφαλείας του προσωπικού**

6.3. **Εκπαίδευση του προσωπικού σε θέματα ασφαλείας**

6.4. **Ευθύνες της διεύθυνσης**

6.5. **Καθεστώς ασφαλείας που εφαρμόζεται στο προσωπικό**

7. ΥΛΙΚΗ ΑΣΦΑΛΕΙΑ

7.1. **Ανάγκη προστασίας**

7.2. **Έλεγχος**

7.3. **Ασφάλεια των κτιρίων**

7.4. **Σχέδια έκτακτης ανάγκης**

8. ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΩΝ

9. ΠΡΟΛΗΨΗ ΤΩΝ ΔΟΛΙΟΦΘΟΡΩΝ ΚΑΙ ΑΛΛΩΝ ΜΟΡΦΩΝ ΚΑΚΟΒΟΥΛΗΣ ΦΘΟΡΑΣ ΕΚ ΠΡΟΘΕΣΕΩΣ

10. ΚΟΙΝΟΠΟΙΗΣΗ ΔΙΑΒΑΘΜΙΣΜΕΝΩΝ ΠΛΗΡΟΦΟΡΙΩΝ ΣΕ ΤΡΙΤΑ ΚΡΑΤΗ Ή ΔΙΕΘΝΕΙΣ ΟΡΓΑΝΙΣΜΟΥΣ

ΜΕΡΟΣ ΙΙ: Η ΟΡΓΑΝΩΣΗ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΣΤΗΝ ΕΠΙΤΡΟΠΗ

11. ΤΟ ΑΡΜΟΔΙΟ ΓΙΑ ΘΕΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΜΕΛΟΣ ΤΗΣ ΕΠΙΤΡΟΠΗΣ

12. Η ΣΥΜΒΟΥΛΕΥΤΙΚΗ ΟΜΑΔΑ ΤΗΣ ΕΠΙΤΡΟΠΗΣ ΓΙΑ ΤΗΝ ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ

13. ΤΟ ΣΥΜΒΟΥΛΙΟ ΑΣΦΑΛΕΙΑΣ ΤΗΣ ΕΠΙΤΡΟΠΗΣ

14. Η ►M2 ΔΙΕΥΘΥΝΣΗ ΑΣΦΑΛΕΙΑΣ ΤΗΣ ΕΠΙΤΡΟΠΗΣ ◄

15. ΕΠΙΘΕΩΡΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ

16. ΔΙΑΒΑΘΜΙΣΕΙΣ, ΕΝΔΕΙΞΕΙΣ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΣΗΜΑΝΣΕΙΣ

▼**B**

16.1. **Επίπεδα διαβάθμισης**

16.2. **Ενδείξεις ασφαλείας**

16.3. **Σημάνσεις**

16.4. **Επίθεση της διαβάθμισης**

16.5. **Επίθεση ενδείξεων ασφαλείας**

17. ΔΙΑΧΕΙΡΙΣΗ ΤΩΝ ΔΙΑΒΑΘΜΙΣΕΩΝ

17.1. **Γενικά**

17.2. **Εφαρμογή των διαβαθμίσεων**

17.3. **Υποχαρακτηρισμός και αποχαρακτηρισμός**

18. ΥΛΙΚΗ ΑΣΦΑΛΕΙΑ

18.1. **Γενικά**

18.2. **Απαιτήσεις ασφάλειας**

18.3. **Μέτρα υλικής ασφάλειας**

18.3.1. *Περιοχές ασφαλείας*

18.3.2. *Διοικητικός χώρος*

18.3.3. *Έλεγχοι εισόδου και εξόδου*

18.3.4. *Περιπολίες των φυλάκων*

18.3.5. *Φωριαμοί ασφαλείας και θωρακισμένες αίθουσες*

18.3.6. *Κλειδαριές*

18.3.7. *Έλεγχος των κλειδιών και των συνδυασμών*

18.3.8. *Συσκευές ανίχνευσης εισόδου αναρμοδίων*

18.3.9. *Εγκεκριμένος εξοπλισμός*

18.3.10. *Υλική προστασία των φωτοαντιγραφικών συσκευών και συσκευών τηλεομοιοτυπίας (φαξ)*

18.4. **Προστασία κατά της λαθροβλεψίας και της λαθρακρόασης**

18.4.1. *Λαθροβλεψία*

18.4.2. *Λαθρακρόαση*

18.4.3. *Εισαγωγή ηλεκτρονικού εξοπλισμού και καταγραφικών συσκευών*

18.5. **Τεχνικώς ασφαλείς χώροι**

19. ΓΕΝΙΚΟΙ ΚΑΝΟΝΕΣ ΣΧΕΤΙΚΑ ΜΕ ΤΗΝ ΑΡΧΗ ΤΗΣ ΑΝΑΓΚΗΣ ΝΑ ΓΝΩΡΙΖΕΙ ΚΑΙ ΤΟΥΣ ΕΛΕΓΧΟΥΣ ΑΣΦΑΛΕΙΑΣ ΤΟΥ ΠΡΟΣΩΠΙΚΟΥ

19.1. **Γενικά**

19.2. **Ειδικοί κανόνες σχετικά με την πρόσβαση σε πληροφορίες με διαβίβαση TRES SECRET UE/EU TOP SECRET**

19.3. **Ειδικοί κανόνες σχετικά με την πρόσβαση σε πληροφορίες με διαβίβαση SECRET UE ή CONFIDENTIEL UE**

19.4. **Ειδικοί κανόνες σχετικά με την πρόσβαση σε πληροφορίες με διαβίβαση RESTREINT UE**

19.5. **Μεταθέσεις**

19.6. **Ειδικές εντολές**

▼B

20. ΔΙΑΔΙΚΑΣΙΑ ΕΛΕΓΧΟΥ ΑΣΦΑΛΕΙΑΣ ΓΙΑ ΤΟΥΣ ΥΠΑΛΛΗΛΟΥΣ ΚΑΙ ΤΟ ΛΟΙΠΟ ΠΡΟΣΩΠΙΚΟ ΤΗΣ ΕΠΙΤΡΟΠΗΣ

21. ΠΡΟΕΤΟΙΜΑΣΙΑ, ΔΙΑΝΟΜΗ, ΔΙΑΒΙΒΑΣΗ, ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ ΣΧΕΤΙΚΑ ΜΕ ΤΟ ΠΡΟΣΩΠΙΚΟ ΤΩΝ ΜΕΤΑΦΟΡΕΩΝ ΚΑΙ ΣΥΜΠΛΗΡΩΜΑΤΙΚΑ ΑΝΤΙΤΥΠΑ Ή ΜΕΤΑΦΡΑΣΕΙΣ ΚΑΙ ΑΠΟΣΠΑΣΜΑΤΑ ΔΙΑΒΑΘΜΙΣΜΕΝΩΝ ΕΓΓΡΑΦΩΝ ΕΕ

21.1. **Προετοιμασία**

21.2. **Διανομή**

21.3. **Διαβίβαση διαβαθμισμένων εγγράφων ΕΕ**

21.3.1. *Συσκευασία και αποδείξεις παραλαβής*

21.3.2. *Διαβίβαση στο εσωτερικό ενός κτιρίου ή μιας ομάδας κτιρίων*

21.3.3. *Διαβίβαση στο εσωτερικό μιας χώρας*

21.3.4. *Διαβίβαση από ένα κράτος σε άλλο*

21.3.5. *Διαβίβαση διαβαθμισμένων εγγράφων ΕΕ*

21.4. **Μέτρα ασφαλείας σχετικά με το προσωπικό των μεταφορέων**

21.5. **Ηλεκτρονικά και άλλα μέσα τεχνικής διαβίβασης**

21.6. **Συμπληρωματικά αντίγραφα, μεταφράσεις και αποσπάσματα διαβαθμισμένων εγγράφων ΕΕ**

22. ΓΡΑΜΜΑΤΕΙΕΣ ΔΠΕΕ, ΑΠΟΓΡΑΦΕΣ, ΑΡΧΕΙΟΘΕΤΗΣΗ ΚΑΙ ΚΑΤΑΣΤΡΟΦΗ ΔΠΕΕ

22.1. **Τοπικές γραμματείες ΔΠΕΕ**

22.2. **Γραμματεία TRES SECRET UE/EU TOP SECRET**

22.2.1. *Γενικά*

22.2.2. *Γενική γραμματεία TRES SECRET UE/EU TOP SECRET*

22.2.3. *Υπογραμματεία TRES SECRET UE/EU TOP SECRET*

22.3. **Απογραφές και έλεγχοι διαβαθμισμένων εγγράφων ΕΕ**

22.4. **Αρχειοθέτηση διαβαθμισμένων πληροφοριών ΕΕ**

22.5. **Καταστροφή διαβαθμισμένων εγγράφων ΕΕ**

22.6. **Καταστροφή σε καταστάσεις ανάγκης**

23. ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ ΓΙΑ ΕΙΔΙΚΕΣ ΣΥΝΕΔΡΙΑΣΕΙΣ ΠΡΑΓΜΑΤΟΠΟΙΟΥΜΕΝΕΣ ΕΚΤΟΣ ΤΩΝ ΓΡΑΦΕΙΩΝ ΤΗΣ ΕΠΙΤΡΟΠΗΣ, ΣΤΙΣ ΟΠΟΙΕΣ ΕΜΠΛΕΚΟΝΤΑΙ ΔΙΑΒΑΘΜΙΣΜΕΝΕΣ ΠΛΗΡΟΦΟΡΙΕΣ ΕΕ

23.1. **Γενικά**

23.2. **Αρμοδιότητες**

23.2.1. ► **M2** *Διεύθυνση Ασφαλείας της Επιτροπής* ◄

23.2.2. *Υπεύθυνος ασφαλείας της συνεδρίασης (ΥΑΣ)*

23.3 **Μέτρα ασφαλείας**

23.3.1. *Περιοχές ασφαλείας*

23.3.2. *Άδειες εισόδου*

23.3.3. *Έλεγχος φωτογραφικού και ακουστικού εξοπλισμού*

23.3.4. *Έλεγχος χαρτοφυλάκων, φορητών υπολογιστών και δεμάτων*

23.3.5. *Τεχνική ασφάλεια*

▼B

23.3.6. *Έγγραφα των αντιπροσωπειών*

23.3.7. *Ασφαλής φύλαξη των εγγράφων*

23.3.8. *Επιθεώρηση γραφείων*

23.3.9. *Διάθεση διαβαθμισμένων απορριμμάτων ΕΕ*

24. ΠΑΡΑΒΙΑΣΕΙΣ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΔΙΑΡΡΟΗ ΔΙΑΒΑΘΜΙΣΜΕΝΩΝ ΠΛΗΡΟΦΟΡΙΩΝ ΕΕ

24.1. **Ορισμοί**

24.2. **Αναφορά παραβιάσεων της ασφάλειας**

24.3. **Δικαστικές ενέργειες**

25. ΠΡΟΣΤΑΣΙΑ ΔΙΑΒΑΘΜΙΣΜΕΝΩΝ ΠΛΗΡΟΦΟΡΙΩΝ ΕΕ ΔΙΑΚΙΝΟΥΜΕΝΩΝ ΣΕ ΣΥΣΤΗΜΑΤΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ

25.1. **Εισαγωγή**

25.1.1. *Γενικά*

25.1.2. *Απειλές κατά των συστημάτων και τρωτά σημεία τους*

25.1.3. *Κύριος σκοπός των μέτρων ασφαλείας*

25.1.4. *Δήλωση απαιτήσεων ασφαλείας ανταποκρινόμενων στο ιδιαίτερο σύστημα (SSRS)*

25.1.5. *Επίπεδα ασφάλειας της λειτουργίας*

25.2. **Ορισμοί**

25.3. **Αρμοδιότητες ασφαλείας**

25.3.1. *Γενικά*

25.3.2. *Αρχή διαπίστευσης της ασφάλειας (ΑΔΑ)*

25.3.3. *Αρχή INFOSEC (ΙΑ)*

25.3.4. *Ιδιοκτήτης τεχνικών συστημάτων (TSO)*

25.3.5. *Ιδιοκτήτης πληροφοριών (ΙΠ)*

25.3.6. *Χρήστες*

25.3.7. *Κατάρτιση INFOSEC*

25.4. **Μη τεχνικά μέτρα ασφάλειας**

25.4.1. *Ασφάλεια προσωπικού*

25.4.2. *Υλική ασφάλεια*

25.4.3. *Έλεγχος της πρόσβασης σε ένα σύστημα*

25.5. **Τεχνικά μέτρα ασφάλειας**

25.5.1. *Ασφάλεια πληροφοριών*

25.5.2. *Έλεγχος και λογοδότηση πληροφοριών*

25.5.3. *Χειρισμός και έλεγχος αφαιρετών πληροφορικών μέσων αποθήκευσης*

25.5.4. *Αποχαρακτηρισμός και καταστροφή πληροφορικών μέσων αποθήκευσης*

25.5.5. *Ασφάλεια επικοινωνιών*

25.5.6. *Εγκατάσταση και ασφάλεια ακτινοβολίας*

25.6. **Ασφάλεια κατά το χειρισμό**

▼B

25.6.1. *Λειτουργικές διαδικασίες ασφαλείας (SecOPs)*

25.6.2. *Διαχείριση της προστασίας/διάταξη λογισμικού*

25.6.3. *Έλεγχος παρουσίας δόλιου λογισμικού/ιών υπολογιστών*

25.6.4. *Συντήρηση*

25.7. **Προμήθειες**

25.7.1. *Γενικά*

25.7.2. *Διαπίστευση*

25.7.3. *Αξιολόγηση και πιστοποίηση*

25.7.4. *Στερεότυπος έλεγχος των χαρακτηριστικών ασφαλείας για συνεχιζόμενη διαπίστευση*

25.8. **Προσωρινή ή περιστασιακή χρήση**

25.8.1. *Ασφάλεια μικροϋπολογιστών/προσωπικών υπολογιστών*

25.8.2. *Χρήση ιδιωτικού εξοπλισμού πληροφορικής για επίσημη εργασία στους κόλπους της Επιτροπής*

25.8.3. *Χρήση εξοπλισμού πληροφορικής που ανήκει σε εργολάβους ή παρέχεται από εθνικές αρχές, για επίσημη εργασία στους κόλπους της Επιτροπής*

26. ΚΟΙΝΟΠΟΙΗΣΗ ΔΙΑΒΑΘΜΙΣΜΕΝΩΝ ΠΛΗΡΟΦΟΡΙΩΝ ΕΕ ΣΕ ΤΡΙΤΑ ΚΡΑΤΗ Ή ΔΙΕΘΝΕΙΣ ΟΡΓΑΝΙΣΜΟΥΣ

26.1.1. *Αρχές που διέπουν την κοινοποίηση διαβαθμισμένων πληροφοριών ΕΕ*

26.1.2. *Επίπεδα*

26.1.3. *Συμφωνίες για ασφάλεια*

ΠΡΟΣΑΡΤΗΜΑ 1: ΠΙΝΑΚΑΣ ΤΩΝ ΕΘΝΙΚΩΝ ΔΙΑΒΑΘΜΙΣΕΩΝ ΑΣΦΑΛΕΙΑΣ

ΠΡΟΣΑΡΤΗΜΑ 2: ΠΡΑΚΤΙΚΟΣ ΟΔΗΓΟΣ ΔΙΑΒΑΘΜΙΣΗΣ

ΠΡΟΣΑΡΤΗΜΑ 3: ΚΑΤΕΥΘΥΝΤΗΡΙΕΣ ΓΡΑΜΜΕΣ ΓΙΑ ΤΗΝ ΚΟΙΝΟΠΟΙΗΣΗ ΔΙΑΒΑΘΜΙΣΜΕΝΩΝ ΠΛΗΡΟΦΟΡΙΩΝ ΕΕ ΣΕ ΤΡΙΤΑ ΚΡΑΤΗ Ή ΔΙΕΘΝΕΙΣ ΟΡΓΑΝΙΣΜΟΥΣ: ΣΥΝΕΡΓΑΣΙΑ ΕΠΙΠΕΔΟΥ 1

ΠΡΟΣΑΡΤΗΜΑ 4: ΚΑΤΕΥΘΥΝΤΗΡΙΕΣ ΓΡΑΜΜΕΣ ΓΙΑ ΤΗΝ ΔΙΑΒΙΒΑΣΗ ΔΙΑΒΑΘΜΙΣΜΕΝΩΝ ΠΛΗΡΟΦΟΡΙΩΝ ΕΕ ΣΕ ΤΡΙΤΑ ΚΡΑΤΗ Ή ΔΙΕΘΝΕΙΣ ΟΡΓΑΝΙΣΜΟΥΣ: ΣΥΝΕΡΓΑΣΙΑ ΕΠΙΠΕΔΟΥ 2

ΠΡΟΣΑΡΤΗΜΑ 5: ΚΑΤΕΥΘΥΝΤΗΡΙΕΣ ΓΡΑΜΜΕΣ ΓΙΑ ΤΗΝ ΔΙΑΒΙΒΑΣΗ ΔΙΑΒΑΘΜΙΣΜΕΝΩΝ ΠΛΗΡΟΦΟΡΙΩΝ ΕΕ ΣΕ ΤΡΙΤΑ ΚΡΑΤΗ Ή ΔΙΕΘΝΕΙΣ ΟΡΓΑΝΙΣΜΟΥΣ: ΣΥΝΕΡΓΑΣΙΑ ΕΠΙΠΕΔΟΥ 3

ΠΡΟΣΑΡΤΗΜΑ 6: ΚΑΤΑΛΟΓΟΣ ΣΥΝΤΟΜΟΓΡΑΦΙΩΝ

▼B

ΜΕΡΟΣ Ι: ΒΑΣΙΚΕΣ ΑΡΧΕΣ ΚΑΙ ΕΛΑΧΙΣΤΑ ΠΡΟΤΥΠΑ ΑΣΦΑΛΕΙΑΣ

1. ΕΙΣΑΓΩΓΗ

Οι παρούσες διατάξεις θεσπίζουν τις βασικές αρχές και τα ελάχιστα πρότυπα ασφάλειας που θα πρέπει να τηρούνται κατά τον ενδεδειγμένο τρόπο από την Επιτροπή, σε όλους τους τόπους δραστηριοτήτων της, καθώς και από όλους τους αποδέκτες διαβαθμισμένων πληροφοριών ΕΕ (ΔΠΕΕ), έτσι ώστε να περιφρουρείται η ασφάλεια και να διασφαλίζεται η θέσπιση κοινών προτύπων προστασίας.

2. ΓΕΝΙΚΕΣ ΑΡΧΕΣ

Η πολιτική της Επιτροπής για την ασφάλεια αποτελεί αναπόσπαστο τμήμα της γενικής πολιτικής της για την εσωτερική διαχείριση και, κατά συνέπεια, βασίζεται στις αρχές που διέπουν τη γενική πολιτική της.

Οι εν λόγω αρχές περιλαμβάνουν τη νομιμότητα, τη διαφάνεια, τη λογοδοσία και την επικουρικότητα (αναλογικότητα).

Η νομιμότητα καταδεικνύει την ανάγκη να ακολουθείται αυστηρά το νομικό πλαίσιο κατά την άσκηση των λειτουργιών ασφαλείας, καθώς και την ανάγκη τήρησης των νομικών απαιτήσεων. Σημαίνει επίσης ότι οι αρμοδιότητες στον τομέα της ασφάλειας πρέπει να βασίζονται στις κατάλληλες νομικές διατάξεις. Οι διατάξεις του κανονισμού υπηρεσιακής κατάστασης εφαρμόζονται πλήρως, ιδίως το άρθρο 17, σχετικά με την υποχρέωση του προσωπικού να αντιμετωπίζει με διακριτικότητα τις πληροφορίες της Επιτροπής, καθώς και ο τίτλος VI σχετικά με τα πειθαρχικά μέτρα. Τέλος, σημαίνει ότι οι παραβάσεις στον τομέα της ασφάλειας, στο πλαίσιο της υπευθυνότητας της Επιτροπής, θα πρέπει να αντιμετωπίζονται κατά τρόπο που συνάδει με την πολιτική της Επιτροπής σχετικά με τα πειθαρχικά μέτρα, καθώς και με την πολιτική της σχετικά με τη συνεργασία με τα κράτη μέλη στον τομέα της ποινικής δικαιοσύνης.

Η διαφάνεια καταδεικνύει την ανάγκη για σαφήνεια όσον αφορά όλους τους κανόνες και τις διατάξεις της ασφάλειας, για εξισορρόπηση μεταξύ των διαφόρων υπηρεσιών και των διαφόρων τομέων (φυσική ασφάλεια σε αντίθεση με την προστασία των πληροφοριών, κ.λπ.) και την ανάγκη για μια συνεκτική και διαρθρωμένη πολιτική ευαισθητοποίησης σχετικά με την ασφάλεια. Καθορίζει επίσης την ανάγκη για σαφείς γραπτές γενικές κατευθύνσεις με σκοπό την εφαρμογή μέτρων ασφαλείας.

Η λογοδοσία σημαίνει ότι θα πρέπει να καθορίζονται σαφώς οι αρμοδιότητες στον τομέα της ασφάλειας. Επιπλέον, καταδεικνύει την ανάγκη να δοκιμάζεται τακτικά η ορθή εκτέλεση των εν λόγω αρμοδιοτήτων.

Η επικουρικότητα ή αναλογικότητα σημαίνει ότι η ασφάλεια πρέπει να οργανώνεται στο χαμηλότερο δυνατό επίπεδο και όσο το δυνατόν στενότερα σε συνεργασία με τις Γενικές Διευθύνσεις και τις υπηρεσίες της Επιτροπής. Καταδεικνύει επίσης το γεγονός ότι οι δραστηριότητες ασφάλειας πρέπει να περιορίζονται στα στοιχεία εκείνα που πράγματι απαιτούνται. Τέλος, σημαίνει ότι τα μέτρα ασφάλειας πρέπει να είναι ανάλογα των συμφερόντων που πρέπει να προστατευθούν και της πραγματικής ή δυνητικής απειλής για τα εν λόγω συμφέροντα, προβλέποντας μια άμυνα που προκαλεί τις λιγότερες δυνατές διαταραχές.

3. ΤΑ ΒΑΣΙΚΑ ΣΤΟΙΧΕΙΑ ΤΗΣ ΑΣΦΑΛΕΙΑΣ

Η ορθή διαχείριση της ασφαλείας στηρίζεται στα εξής στοιχεία:

α) εντός κάθε κράτους μέλους, ένα εθνικό οργανισμό ασφαλείας υπεύθυνο για:

   1. τη συγκέντρωση και καταγραφή στοιχείων για περιπτώσεις κατασκοπείας, δολιοφθορών, τρομοκρατίας και άλλες ανατρεπτικές δραστηριότητες, και

   2. την παροχή πληροφοριών και συμβουλών στην κυβέρνηση της χώρας του και, μέσω αυτής, στην Επιτροπή, σχετικά με τη φύση των απειλών κατά της ασφαλείας και τα μέσα για την προστασία από αυτές·

β) εντός κάθε κράτους μέλους, και εντός της Επιτροπής, μια τεχνικής φύσεως αρχή ασφάλειας πληροφοριών (INFOSEC) υπεύθυνη για τη συνεργασία με την οικεία αρχή ασφαλείας προκειμένου να παρέχουν πληροφορίες και συμβουλές σχετικά με τις τεχνικής φύσεως απειλές κατά της ασφαλείας και τα μέσα για την προστασία από αυτές·

γ) ύπαρξη τακτικής συνεργασίας μεταξύ των κυβερνητικών υπηρεσιών και των ανάλογων υπηρεσιών των ευρωπαϊκών θεσμικών οργάνων, προκειμένου να εντοπίζονται και να προτείνονται ενδεχομένως:

   1. τα πρόσωπα, οι πληροφορίες και οι πόροι που χρήζουν προστασίας, και

   2. τα κοινά πρότυπα προστασίας·

▼B

δ) στενή συνεργασία μεταξύ της ►M2 Διεύθυνσης Ασφαλείας της Επιτροπής ◄ και των υπηρεσιών ασφάλειας των λοιπών ευρωπαϊκών θεσμικών οργάνων, καθώς και με την υπηρεσία ασφάλειας του NATO (NOS).

4. ΑΡΧΕΣ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΤΩΝ ΠΛΗΡΟΦΟΡΙΩΝ

4.1. **Στόχοι**

Η ασφάλεια πληροφοριών εξυπηρετεί τους παρακάτω κύριους στόχους:

α) την προστασία των διαβαθμισμένων πληροφοριών ΕΕ (ΔΠΕΕ) από την κατασκοπεία, διαρροή ή κοινολόγηση άνευ αδείας·

β) την προστασία των πληροφοριών ΕΕ που διακινούνται στα συστήματα και στα δίκτυα επικοινωνιών και πληροφορικής από κάθε κίνδυνο για την εμπιστευτικότητα, την αξιοπιστία και τη διαθεσιμότητά τους·

γ) την προστασία των εγκαταστάσεων της Επιτροπής στις οποίες αποθηκεύονται πληροφορίες ΕΕ από το ενδεχόμενο δολιοφθοράς και κακόβουλης εκ προθέσεως φθοράς·

δ) σε περίπτωση αστοχίας, την εκτίμηση της ζημίας, τον περιορισμό των συνεπειών της και τη λήψη των αναγκαίων επανορθωτικών μέτρων.

4.2. **Ορισμοί**

Στους εν λόγω κανόνες:

α) με τον όρο «διαβαθμισμένες πληροφορίες ΕΕ» (ΔΠΕΕ) νοείται κάθε πληροφορία και υλικό, των οποίων η άνευ αδείας κοινολόγηση μπορεί να βλάψει σε ποικίλο βαθμό τα συμφέροντα της ΕΕ ή ενός ή περισσοτέρων κρατών μελών της, ασχέτως του εάν η πληροφορία αυτή προέρχεται από την ΕΕ ή έχει ληφθεί από κράτος μέλος, τρίτο κράτος ή διεθνή οργανισμό·

β) ως «έγγραφο» νοείται κάθε επιστολή, σημείωμα, κείμενο πρακτικών, έκθεση, υπόμνημα, σήμα/μήνυμα, σκαρίφημα, φωτογραφία, διαφάνεια, φιλμ, χάρτης, διάγραμμα, σχέδιο, σημειωματάριο, μεμβράνη πολυγράφου, καρμπόν, μελανοταινία γραφομηχανής ή εκτυπωτή, μαγνητοταινία, κασέτα, δισκέτα υπολογιστή, CD-ROM ή οποιοδήποτε άλλο υλικό μέσο στο οποίο καταγράφονται πληροφορίες·

γ) ως «υλικό» νοείται κάθε «έγγραφο» όπως ορίζεται στο στοιχείο β) καθώς και κάθε στοιχείο εξοπλισμού που έχει ήδη κατασκευασθεί ή βρίσκεται υπό κατασκευή·

δ) ο όρος «ανάγκη να γνωρίζει» σημαίνει την ανάγκη ενός υπαλλήλου να έχει πρόσβαση σε διαβαθμισμένες πληροφορίες ΕΕ (ΔΠΕΕ), έτσι ώστε να είναι σε θέση να εκτελέσει τα καθήκοντά του·

ε) ως «εξουσιοδότηση» νοείται η απόφαση του ►M2 διευθυντή της Διεύθυνσης Ασφαλείας της Επιτροπής ◄ να εγκρίνει μια συγκεκριμένη πρόσβαση σε διαβαθμισμένες πληροφορίες ΕΕ (ΔΠΕΕ) έως ενός συγκεκριμένου επιπέδου, βάσει θετικού πορίσματος του ελέγχου ασφάλειας (εξέτασης), που πραγματοποιείται από μια εθνική αρχή ασφαλείας δυνάμει της εθνικής νομοθεσίας·

στ) ως «διαβάθμιση» νοείται ο καθορισμός ενός ενδεδειγμένου επιπέδου ασφαλείας για πληροφορίες των οποίων η μη εξουσιοδοτημένη αποκάλυψη θα μπορούσε να προκαλέσει σε κάποιο βαθμό ζημία στα συμφέροντα της Επιτροπής ή των κρατών μελών·

ζ) ως «υποχαρακτηρισμός» (diclassement) νοείται η μείωση του βαθμού ασφαλείας·

η) ως «αποχαρακτηρισμός» (diclassification) νοείται η άρση οποιασδήποτε διαβάθμισης·

θ) ως «αρχικός συντάκτης» νοείται ο δεόντως εξουσιοδοτημένος συντάκτης ενός διαβαθμισμένου εγγράφου. Στην Επιτροπή, οι προϊστάμενοι υπηρεσιών δύνανται να εξουσιοδοτούν το προσωπικό τους να παράγει διαβαθμισμένες πληροφορίες ΕΕ·

ι) με τον όρο «υπηρεσίες της Επιτροπής» νοούνται οι υπηρεσίες της Επιτροπής, συμπεριλαμβανομένων των ιδιαίτερων γραφείων, σε όλους τους τόπους δραστηριότητας της Επιτροπής, συμπεριλαμβανομένου του κοινού κέντρου ερευνών, των αντιπροσωπειών και τωνγΓραφείων της ένωσης και των αντιπροσωπειών σε τρίτες χώρες.

4.3. **Διαβάθμιση**

α) Όσον αφορά την εμπιστευτικότητα, απαιτείται μέριμνα και πείρα κατά την επιλογή των πληροφοριών και του υλικού που πρέπει να προστατεύεται και κατά την εκτίμηση του αναγκαίου βαθμού προστασίας. Είναι βασικό ο βαθμός προστασίας να ανταποκρίνεται στην κρισιμότητα των συγκεκριμένων προστατευτέων πληροφοριών και υλικών. Για να διασφαλιστεί η ομαλή ροή των πληροφοριών, λαμβάνονται μέτρα για την αποφυγή τόσο της υπερβολικής όσο και της ανεπαρκούς διαβάθμισης.

▼B

β) Το σύστημα διαβάθμισης αποτελεί το μέσο με το οποίο υλοποιούνται οι αρχές αυτές· παρόμοιο σύστημα διαβάθμισης πρέπει να εφαρμόζεται και κατά τον προγραμματισμό και τη διοργάνωση τρόπων αντιμετώπισης της κατασκοπείας, των δολιοφθορών, της τρομοκρατίας και των άλλων απειλών, ούτως ώστε να εξασφαλίζεται ο μέγιστος βαθμός ασφαλείας στους κυριότερους χώρους εντός των οποίων αποθηκεύονται διαβαθμισμένες πληροφορίες καθώς και στα πλέον ευαίσθητα σημεία των χώρων αυτών.

γ) Την ευθύνη για τη διαβάθμιση των πληροφοριών έχει αποκλειστικά ο αρχικός συντάκτης των εν λόγω πληροφοριών.

δ) Το επίπεδο διαβάθμισης δύναται να βασίζεται αποκλειστικά στο περιεχόμενο των εν λόγω πληροφοριών.

ε) Σε περίπτωση που ένας αριθμός πληροφοριακών στοιχείων αποτελεί μια ενότητα, το επίπεδο διαβάθμισης που θα πρέπει να εφαρμόζεται για το σύνολο, θα είναι τουλάχιστον του ιδίου επιπέδου με εκείνο της υψηλότερης διαβάθμισης. Μια συλλογή πληροφοριών δύναται ωστόσο να έχει υψηλότερη διαβάθμιση σε σχέση με τα επιμέρους στοιχεία της.

στ) Οι διαβαθμίσεις καθορίζονται μόνον εφόσον είναι απαραίτητο και για τον απαιτούμενο χρόνο.

4.4. **Στόχοι των μέτρων ασφαλείας**

Τα μέτρα ασφαλείας:

α) καλύπτουν όλα τα πρόσωπα που έχουν πρόσβαση σε διαβαθμισμένες πληροφορίες, τα μέσα επεξεργασίας διαβαθμισμένων πληροφοριών, όλους τους χώρους όπου υπάρχουν τέτοιες πληροφορίες, και τις σημαντικές εγκαταστάσεις,

β) σχεδιάζονται κατά τρόπο που να επισημαίνονται τα πρόσωπα των οποίων η θέση ενδέχεται να δημιουργεί κινδύνους στην ασφάλεια των διαβαθμισμένων πληροφοριών και των σημαντικών εγκαταστάσεων στις οποίες αποθηκεύονται αυτές και να προβλέπεται ο αποκλεισμός τους ή η απομάκρυνσή τους,

γ) εμποδίζουν κάθε μη εξουσιοδοτημένο πρόσωπο να έχει πρόσβαση σε διαβαθμισμένες πληροφορίες ή στις εγκαταστάσεις όπου αποθηκεύονται αυτές,

δ) εξασφαλίζουν ότι οι διαβαθμισμένες πληροφορίες διανέμονται μόνο με βάση την αρχή «ανάγκη γνώσης», αρχή θεμελιώδους σημασίας για όλες τις πτυχές της ασφαλείας,

ε) εξασφαλίζουν την αξιοπιστία (δηλαδή εμποδίζουν την αλλοίωση ή την άνευ αδείας τροποποίηση ή διαγραφή στοιχείων) και τη διαθεσιμότητα (δηλαδή δεν αρνούνται την πρόσβαση στα πρόσωπα που απαιτείται να έχουν γνώση αυτών και διαθέτουν σχετική εξουσιοδότηση) όλων των πληροφοριών, διαβαθμισμένων ή μη, και ιδίως των πληροφοριών που αποτελούν αντικείμενο αποθήκευσης, επεξεργασίας ή διαβίβασης με ηλεκτρομαγνητικά μέσα.

5. ΟΡΓΑΝΩΣΗ ΤΗΣ ΑΣΦΑΛΕΙΑΣ

5.1. **Κοινές στοιχειώδεις προδιαγραφές**

Η Επιτροπή διασφαλίζει την τήρηση των κοινών ελάχιστων προτύπων ασφαλείας από όλους τους αποδέκτες των διαβαθμισμένων πληροφοριών ΕΕ, τόσο μέσα στο θεσμικό όργανο όσο και στο πλαίσιο της ευθύνης του, π.χ. από όλες τις υπηρεσίες και τους συμβασιούχους, έτσι ώστε οι διαβαθμισμένες πληροφορίες ΕΕ να δύνανται να διαβιβάζονται με τη βεβαιότητα ότι θα αντιμετωπιστούν με τη δέουσα προσοχή. Στις εν λόγω στοιχειώδεις προδιαγραφές περιλαμβάνονται κριτήρια για τον έλεγχο ασφαλείας του προσωπικού και ρυθμίσεις για την προστασία των διαβαθμισμένων πληροφοριών ΕΕ.

Η Επιτροπή επιτρέπει την πρόσβαση εξωτερικών φορέων σε ΔΠΕΕ μόνο υπό τον όρο ότι διασφαλίζουν ότι τηρούνται, κατά τον χειρισμό των ΔΠΕΕ, διατάξεις τουλάχιστον εξίσου ισοδύναμες με τις παρούσες στοιχειώδεις προδιαγραφές.

▼M3

Οι στοιχειώδεις αυτές προδιαγραφές ισχύουν επίσης όταν η Επιτροπή αναθέτει με σύμβαση ή συμφωνία επιχορήγησης, καθήκοντα που αφορούν, συνεπάγονται ή/και περιλαμβάνουν διαβαθμισμένες πληροφορίες ΕΕ σε βιομηχανικούς ή άλλους φορείς: οι εν λόγω κοινές στοιχειώδεις προδιαγραφές περιλαμβάνονται στο σημείο 27 του μέρους ΙΙ.

▼B

5.2. **Οργάνωση**

Στην Επιτροπή η ασφάλεια οργανώνεται σε δύο επίπεδα:

α) στο επίπεδο της Επιτροπής στο σύνολό της υπάρχει η►M2 Διεύθυνση Ασφαλείας της Επιτροπής ◄ με μια αρχή διαπίστευσης ασφάλειας (ΑΔΑ), η οποία επίσης λειτουργεί και ως κρυπτογραφική υπηρεσία (ΚΡΥ) και ως αρχή

▼B

TEMPEST, καθώς και με μια αρχή INFOSEC και μία ή περισσότερες κεντρικές γραμματείες ΔΠΕΕ, καθεμία με ένα ή περισσότερους ελεγκτικούς υπαλλήλους γραμματείας (ΕΥΓ)·

β) στο επίπεδο των υπηρεσιών της Επιτροπής, η ασφάλεια είναι αρμοδιότητα ενός ή περισσότερων τοπικών υπευθύνων ασφαλείας (ΤΥΑ), ενός ή περισσότερων υπευθύνων ασφάλειας κεντρικών συστημάτων πληροφορικής (ΥΑΚΠ), υπευθύνων ασφάλειας τοπικών συστημάτων πληροφορικής (ΤΥΑΠ) και τοπικών γραμματειών διαβαθμισμένων πληροφοριών ΕΕ με ένα ή περισσότερους ελεγκτικούς υπαλλήλους γραμματείας·

γ) οι κεντρικοί φορείς ασφάλειας θα παρέχουν επιχειρησιακές κατευθύνσεις στους τοπικούς φορείς ασφάλειας.

6. ΑΞΙΟΠΙΣΤΙΑ ΤΟΥ ΠΡΟΣΩΠΙΚΟΥ

6.1. **Έλεγχος ασφαλείας (διαβάθμιση) του προσωπικού**

Όλα τα πρόσωπα που απαιτείται να έχουν πρόσβαση σε πληροφορίες με διαβάθμιση ►**M1** CONFIDENTIEL UE ◄ ή ανώτερη πρέπει να ελέγχονται καταλλήλως προτού τους επιτραπεί η πρόσβαση. Ανάλογος έλεγχος ασφαλείας απαιτείται και στην περίπτωση προσώπων των οποίων τα καθήκοντα περιλαμβάνουν τον τεχνικό χειρισμό ή τη συντήρηση των συστημάτων επικοινωνιών και επεξεργασίας πληροφοριών που περιέχουν διαβαθμισμένες πληροφορίες. Ο έλεγχος αυτός εξακριβώνει κατά πόσον τα πρόσωπα αυτά:

α) είναι αναμφιβόλως έμπιστα,

β) διαθέτουν χαρακτήρα και διακριτικότητα που να μη δημιουργούν ερωτηματικά για την αξιοπιστία τους όσον αφορά τον χειρισμό διαβαθμισμένων πληροφοριών, ή

γ) ενδέχεται να είναι ευάλωτα σε πιέσεις από ξένους παράγοντες ή άλλες πηγές.

Ιδιαίτερα προσεκτικός έλεγχος γίνεται επί προσώπων τα οποία:

δ) πρόκειται να έχουν πρόσβαση σε πληροφορίες ►**M1** TRES SECRET UE/EU TOP SECRET ◄,

ε) καταλαμβάνουν θέσεις που συνεπάγονται τακτική πρόσβαση σε σημαντικό όγκο πληροφοριών ►**M1** SECRET UE ◄,

στ) έχουν καθήκοντα τέτοια που τους παρέχουν ειδική πρόσβαση σε ασφαλή συστήματα επικοινωνιών και επεξεργασίας πληροφοριών και, ως εκ τούτου, έχουν τη δυνατότητα να προσπελάσουν χωρίς εξουσιοδότηση μεγάλο όγκο διαβαθμισμένων πληροφοριών ΕΕ ή να επιφέρουν σοβαρό πλήγμα στην αποστολή με πράξεις δολιοφθοράς τεχνικής φύσεως.

Στις περιπτώσεις που περιγράφονται στα στοιχεία δ), ε) και στ), γίνεται όσο το δυνατόν μεγαλύτερη χρήση της τεχνικής της διερεύνησης του παρελθόντος και του περιβάλλοντος των προσώπων.

Όταν πρόσωπα τα οποία δεν υπάρχει αποδεδειγμένη «ανάγκη να γνωρίζουν» χρησιμοποιούνται σε περιστάσεις οι οποίες ενδέχεται να τους παρέχουν πρόσβαση σε διαβαθμισμένες πληροφορίες ΕΕ (π.χ. κλητήρες, προσωπικό ασφαλείας, συντήρησης μηχανημάτων, καθαριότητας κ.λπ.), πρέπει προηγουμένως να υφίστανται τον δέοντα έλεγχο ασφαλείας.

6.2. **Αρχεία ελέγχων ασφαλείας του προσωπικού**

Κάθε υπηρεσία της Επιτροπής που χειρίζεται διαβαθμισμένες πληροφορίες ΕΕ ή στεγάζει ασφαλή συστήματα επικοινωνιών ή επεξεργασίας πληροφοριών, τηρεί αρχεία των ελέγχων ασφαλείας που έχουν πραγματοποιηθεί για το προσωπικό της. Η διαβάθμιση που έχει λάβει ένας υπάλληλος επαληθεύεται σε κάθε νέα περίσταση ώστε να εξασφαλίζεται ότι είναι η πρέπουσα και για τα νέα καθήκοντά του, επανεξετάζεται δε κατά προτεραιότητα όταν υπάρχουν ενδείξεις ότι η συνέχιση της εργασίας του υπαλλήλου αυτού σε περιβάλλον διαβαθμισμένων πληροφοριών είναι ασυμβίβαστη πλέον με την προστασία της ασφαλείας. Ο τοπικός υπάλληλος ασφαλείας της υπηρεσίας της Επιτροπής τηρεί αρχεία των ελέγχων ασφαλείας στον τομέα του.

6.3. **Εκπαίδευση του προσωπικού σε θέματα ασφαλείας**

Όλοι οι εργαζόμενοι σε θέσεις από όπου μπορούν να έχουν πρόσβαση σε διαβαθμισμένες πληροφορίες υπόκεινται σε συστηματική αρχική εκπαίδευση, καθώς και σε τακτά διαστήματα στη συνέχεια, για την ανάγκη ασφαλείας και τις ρυθμίσεις για την επίτευξή της. Οι εν λόγω εργαζόμενοι υποχρεούνται να πιστοποιούν εγγράφως ότι έχουν αναγνώσει και κατανοούν πλήρως τις παρούσες διατάξεις ασφαλείας.

▼B

6.4. **Ευθύνες της διεύθυνσης**

Τα διευθυντικά στελέχη πρέπει να γνωρίζουν ποιοι από το προσωπικό τους εργάζονται σε περιβάλλον διαβαθμισμένων πληροφοριών ή έχουν πρόσβαση σε ασφαλή συστήματα επικοινωνιών ή επεξεργασίας πληροφοριών, καθώς και να καταγράφουν και να αναφέρουν όλα τα περιστατικά ή τα εμφανή τρωτά σημεία που ενδέχεται να έχουν επιπτώσεις στην ασφάλεια.

6.5. **Καθεστώς ασφαλείας που εφαρμόζεται στο προσωπικό**

Θεσμοθετούνται διαδικασίες που εξασφαλίζουν ότι, όταν υπάρχουν αρνητικές πληροφορίες για κάποιο πρόσωπο, εξετάζεται κατά πόσο το πρόσωπο αυτό εργάζεται σε περιβάλλον διαβαθμισμένων πληροφοριών ή έχει πρόσβαση σε ασφαλή συστήματα επικοινωνιών ή επεξεργασίας πληροφοριών και ενημερώνεται η►**M2** Διεύθυνση Ασφαλείας της Επιτροπής ◄. Εάν διαπιστωθεί ότι το πρόσωπο αυτό αποτελεί κίνδυνο για την ασφάλεια, τότε του απαγορεύεται η πρόσβαση ή απομακρύνεται από θέσεις στις οποίες θα μπορούσε να δημιουργήσει κίνδυνο για την ασφάλεια.

7. ΥΛΙΚΗ ΑΣΦΑΛΕΙΑ

7.1. **Ανάγκη προστασίας**

Η αυστηρότητα των μέτρων υλικής ασφαλείας που εφαρμόζονται για την προστασία των διαβαθμισμένων πληροφοριών ΕΕ είναι ανάλογη με τη διαβάθμιση, τον όγκο των πληροφοριών και του υλικού και την υφισταμένη απειλή. Όλοι οι κάτοχοι διαβαθμισμένων πληροφοριών ΕΕ ακολουθούν ομοιόμορφες διαδικασίες όσον αφορά τη διαβάθμιση των πληροφοριών αυτών και εφαρμόζουν κοινές προδιαγραφές ασφαλείας σχετικά με τη φύλαξη, τη διαβίβαση και τη διάθεση πληροφοριών και υλικού που απαιτούν προστασία.

7.2. **Έλεγχος**

Προτού εγκαταλείψουν αφύλακτους τους χώρους όπου αποθηκεύονται διαβαθμισμένες πληροφορίες ΕΕ, τα πρόσωπα που είναι επιφορτισμένα με τη φύλαξή τους βεβαιώνονται ότι αυτές είναι καλώς προστατευμένες και ότι έχουν ενεργοποιηθεί όλοι οι μηχανισμοί ασφαλείας (κλειδαριές, συναγερμοί κ.λπ.). Διεξάγονται και περαιτέρω έλεγχοι μετά το πέρας των κανονικών ωρών εργασίας.

7.3. **Ασφάλεια των κτιρίων**

Τα κτίρια όπου στεγάζονται διαβαθμισμένες πληροφορίες ΕΕ ή ασφαλή συστήματα επικοινωνιών και επεξεργασίας πληροφοριών προστατεύονται από το ενδεχόμενο εισόδου μη εξουσιοδοτημένων ατόμων. Η φύση της προστασίας των διαβαθμισμένων πληροφοριών ΕΕ, π.χ. κάγκελα στα παράθυρα, κλειδαριές στις πόρτες, φύλακες στις εισόδους, αυτόματα συστήματα ελέγχου των εισερχομένων, έλεγχοι ασφαλείας και περίπολοι, συστήματα συναγερμού, συστήματα ανίχνευσης κινήσεων και σκύλοι-φύλακες, εξαρτάται από:

α) τη διαβάθμιση, τον όγκο και τη θέση εντός του κτιρίου των προστατευόμενων πληροφοριών και υλικού,

β) την ποιότητα των φωριαμών ασφαλείας όπου φυλάσσονται αυτές οι πληροφορίες και το υλικό, και

γ) τη φύση της κατασκευής και τη θέση του κτιρίου.

Η φύση της προστασίας των συστημάτων επικοινωνιών και επεξεργασίας πληροφοριών εξαρτάται και αυτή από την εκτίμηση της αξίας των συγκεκριμένων περιουσιακών στοιχείων, από το μέγεθος της ενδεχόμενης ζημίας σε περίπτωση παραβίασης της ασφαλείας, από τη φύση της κατασκευής και τη θέση του κτιρίου στο οποίο στεγάζεται το σύστημα και από τη θέση του συστήματος εντός του κτιρίου.

7.4. **Σχέδια έκτακτης ανάγκης**

Εκπονούνται εκ των προτέρων αναλυτικά σχέδια προστασίας των διαβαθμισμένων πληροφοριών για τις περιπτώσεις έκτακτης ανάγκης σε τοπικό ή εθνικό επίπεδο.

8. ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΩΝ

Η ασφάλεια των πληροφοριών (INFOSEC) αναφέρεται στον προσδιορισμό και στην εφαρμογή μέτρων ασφαλείας για την προστασία των διαβαθμισμένων πληροφοριών ΕΕ που αποτελούν αντικείμενο επεξεργασίας, αποθήκευσης ή διαβίβασης σε συστήματα επικοινωνιών, επεξεργασίας πληροφοριών ή άλλα ηλεκτρονικά συστήματα από το ενδεχόμενο να θιγεί, τυχαία ή εσκεμμένα, η εμπιστευτικότητα, η ακεραιότητα ή η διαθεσιμότητά τους. Λαμβάνονται επαρκή μέτρα κατά της πρόσβασης μη εξουσιοδοτημένων χρηστών σε διαβαθμισμένες πληροφορίες ΕΕ, κατά της άρνησης πρόσβασης εξουσιοδοτημένων χρηστών σε διαβαθμισμένες πληροφορίες ΕΕ, και κατά της αλλοίωσης ή της άνευ αδείας τροποποίησης ή εξάλειψης διαβαθμισμένων πληροφοριών ΕΕ.

▼B

9. ΠΡΟΛΗΨΗ ΤΩΝ ΔΟΛΙΟΦΘΟΡΩΝ ΚΑΙ ΑΛΛΩΝ ΜΟΡΦΩΝ ΚΑΚΟΒΟΥΛΗΣ ΦΘΟΡΑΣ ΕΚ ΠΡΟΘΕΣΕΩΣ

Η λήψη προληπτικών μέτρων για την υλική προστασία σημαντικών εγκαταστάσεων που στεγάζουν διαβαθμισμένες πληροφορίες αποτελεί την καλύτερη διασφάλιση έναντι δολιοφθοράς και κακόβουλης εκ προθέσεως φθοράς, ο δε έλεγχος ασφαλείας του προσωπικού δεν συνιστά επαρκές και αποτελεσματικό υποκατάστατο. Η αρμόδια εθνική αρχή πρέπει να παρέχει στοιχεία για το ενδεχόμενο πράξεων κατασκοπείας, δολιοφθοράς, τρομοκρατίας και άλλων ανατρεπτικών δραστηριοτήτων.

10. ΚΟΙΝΟΠΟΙΗΣΗ ΔΙΑΒΑΘΜΙΣΜΕΝΩΝ ΠΛΗΡΟΦΟΡΙΩΝ ΣΕ ΤΡΙΤΑ ΚΡΑΤΗ Ή ΔΙΕΘΝΕΙΣ ΟΡΓΑΝΙΣΜΟΥΣ

Η απόφαση για την κοινοποίηση διαβαθμισμένων πληροφοριών ΕΕ προελεύσεως Επιτροπής σε τρίτο κράτος ή σε διεθνή οργανισμό λαμβάνεται από την Επιτροπή εν σώματι. Εάν πηγή των πληροφοριών των οποίων ζητείται η κοινοποίηση δεν είναι τη Επιτροπή, τότε η Επιτροπή ζητεί πρώτα τη συγκατάθεση της εν λόγω πηγής. Εάν δεν είναι δυνατόν να καθοριστεί συγκεκριμένη πηγή, τότε η Επιτροπή αναλαμβάνει αυτή την ευθύνη κοινοποίησης.

Στην περίπτωση που η Επιτροπή δέχεται διαβαθμισμένες πληροφορίες από τρίτα κράτη, διεθνείς οργανισμούς ή άλλα τρίτα μέρη, οι πληροφορίες αυτές τυγχάνουν προστασίας ανάλογης προς τη διαβάθμισή τους και ισοδύναμης προς τις προδιαγραφές ασφαλείας που καθορίζονται στις προκείμενες διατάξεις για τις διαβαθμισμένες πληροφορίες ΕΕ, ή αποτελούν αντικείμενο του υψηλότερου βαθμού προστασίας τον οποίο απαιτεί το τρίτο μέρος που παρέχει τις πληροφορίες. Μπορεί να συμφωνείται και η διεξαγωγή αμοιβαίων ελέγχων.

Οι ανωτέρω αρχές εφαρμόζονται σύμφωνα με τις λεπτομερείς ρυθμίσεις που προβλέπονται στο μέρος II τμήμα 26 και στα προσαρτήματα 3, 4 και 5.

ΜΕΡΟΣ II: Η ΟΡΓΑΝΩΣΗ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΣΤΗΝ ΕΠΙΤΡΟΠΗ

11. ΤΟ ΑΡΜΟΔΙΟ ΓΙΑ ΘΕΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΜΕΛΟΣ ΤΗΣ ΕΠΙΤΡΟΠΗΣ

Το αρμόδιο για θέματα ασφάλειας μέλος της Επιτροπής:

α) μεριμνά για την εφαρμογή της πολιτικής ασφαλείας της Επιτροπής·

β) εξετάζει τα προβλήματα ασφαλείας που του αναφέρονται από την Επιτροπή ή τα αρμόδια κλιμάκιά της·

γ) μελετά τα θέματα που συνεπάγονται μεταβολές στην πολιτική ασφαλείας της Επιτροπής, σε στενή συνεργασία με τις εθνικές αρχές ασφαλείας («ΕΑΑ») ή άλλες αρμόδιες αρχές των κρατών μελών.

Ειδικότερα, το αρμόδιο για θέματα ασφάλειας μέλος της Επιτροπής είναι υπεύθυνο για:

α) να συντονίζει όλα τα θέματα ασφαλείας που αφορούν δραστηριότητες της Επιτροπής·

β) να απευθύνει στις καθορισμένες για τον σκοπό αυτό αρχές των κρατών μελών αιτήματα παροχής εκ μέρους των ΕΑΑ εγκρίσεων ελέγχου ασφαλείας για το προσωπικό που εργάζεται στην Επιτροπή σύμφωνα με το τμήμα 20·

γ) να διερευνά ή να διατάσσει τη διερεύνηση κάθε διαρροής διαβαθμισμένων πληροφοριών ΕΕ η οποία, κατά τα φαινόμενα, έχει προέλθει από την Επιτροπή·

δ) να ζητεί από τις αρμόδιες αρχές ασφαλείας να διερευνούν τις διαρροές διαβαθμισμένων πληροφοριών ΕΕ που φαίνεται να έχουν προέλθει εκτός της Επιτροπής και να συντονίζει τις έρευνες στην περίπτωση που συμμετέχουν σε αυτές περισσότερες της μίας αρχές ασφαλείας·

ε) να ελέγχει κατά διαστήματα τις ρυθμίσεις ασφαλείας για την προστασία των διαβαθμισμένων πληροφοριών ΕΕ·

στ) να διατηρεί στενό σύνδεσμο με όλες τις εμπλεκόμενες αρχές ασφαλείας για γενικότερο συντονισμό της ασφαλείας·

ζ) να επανεξετάζει τακτικά την πολιτική ασφαλείας της Επιτροπής και τις σχετικές ρυθμίσεις και, εφόσον απαιτείται, να προβαίνει στις κατάλληλες συστάσεις. Σχετικά, το αρμόδιο για θέματα ασφάλειας μέλος της Επιτροπής υποβάλλει στην Επιτροπή το ετήσιο σχέδιο επιθεώρησης που έχει καταρτιστεί από την ►M2 Διεύθυνση Ασφαλείας της Επιτροπής ◄.

▼B

12. Η ΣΥΜΒΟΥΛΕΥΤΙΚΗ ΟΜΑΔΑ ΤΗΣ ΕΠΙΤΡΟΠΗΣ ΓΙΑ ΤΗΝ ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ

Ιδρύεται μια συμβουλευτική ομάδα για την πολιτική ασφάλειας. Απαρτίζεται από το αρμόδιο για θέματα ασφάλειας μέλος της Επιτροπής ή τον αναπληρωτή του, ο οποίος προεδρεύει, και από εκπροσώπους των ΕΑΑ κάθε κράτους μέλους. Μπορούν επίσης να προσκαλούνται εκπρόσωποι και άλλων Ευρωπαϊκών θεσμικών οργάνων. Εκπρόσωποι των αποκεντρωμένων οργανισμών της ΕΚ και της ΕΕ επίσης μπορούν να καλούνται να συμμετάσχουν στις εργασίες όταν συζητούνται θέματα που τους αφορούν.

Η συμβουλευτική ομάδα της Επιτροπής για την πολιτική ασφάλειας συνέρχεται κατόπιν αιτήσεως του προέδρου της ή οποιουδήποτε από τα μέλη της. Έργο της ομάδας είναι να εξετάζει και να αξιολογεί όλα τα σημαντικά θέματα ασφαλείας και να υποβάλλει τις κατάλληλες συστάσεις στην Επιτροπή.

▼M2

13. ΤΟ ΣΥΜΒΟΥΛΙΟ ΑΣΦΑΛΕΙΑΣ ΤΗΣ ΕΠΙΤΡΟΠΗΣ

Ιδρύεται Συμβούλιο Ασφαλείας της Επιτροπής. Απαρτίζεται από τον γενικό διευθυντή Διοίκησης και Προσωπικού, ο οποίος προεδρεύει, ένα μέλος του γραφείου του αρμόδιου για θέματα ασφαλείας επιτρόπου, ένα μέλος του Γραφείου του Προέδρου, τον αναπληρωτή γενικό γραμματέα ο οποίος προεδρεύει της ομάδας διαχείρισης κρίσεων της Επιτροπής, τους γενικούς διευθυντές της Νομικής Υπηρεσίας, Εξωτερικών Σχέσεων, Δικαιοσύνης, Ελευθερίας και Ασφαλείας, του Κοινού Κέντρου Ερευνών, Πληροφορικής και της Υπηρεσίας Εσωτερικού Ελέγχου, καθώς και από τον διευθυντή της Διεύθυνσης Ασφαλείας της Επιτροπής, ή τους εκπροσώπους τους. Μπορούν να προσκαλούνται και άλλοι υπάλληλοι της Επιτροπής. Αρμοδιότητά του είναι η αξιολόγηση των μέτρων ασφαλείας στην Επιτροπή και η υποβολή συστάσεων στον τομέα αυτό προς το αρμόδιο για θέματα ασφαλείας μέλος της Επιτροπής.

▼B

14. Η ►M2 ΔΙΕΥΘΥΝΣΗ ΑΣΦΑΛΕΙΑΣ ΤΗΣ ΕΠΙΤΡΟΠΗΣ ◄

Για την εκπλήρωση των αρμοδιοτήτων που αναφέρονται στο τμήμα 11 το αρμόδιο για θέματα ασφαλείας μέλος της Επιτροπής έχει στη διάθεσή του την►M2 Διεύθυνση Ασφαλείας της Επιτροπής ◄ με σκοπό τον συντονισμό, την εποπτεία και την εφαρμογή των μέτρων ασφαλείας.

Ο ►M2 δευθυντής της Διεύθυνσης Ασφαλείας της Επιτροπής ◄ είναι ο κύριος σύμβουλος του αρμοδίου για θέματα ασφαλείας μέλους της Επιτροπής σε θέματα ασφαλείας και ενεργεί ως γραμματέας της συμβουλευτικής ομάδας για την πολιτική ασφαλείας. Υπό την ιδιότητα αυτή, διευθύνει την αναπροσαρμογή των κανονισμών ασφαλείας και συντονίζει τα μέτρα ασφαλείας με τις αρμόδιες αρχές των κρατών μελών και, ενδεχομένως, με τους διεθνείς οργανισμούς που συνδέονται με την Επιτροπή με συμφωνίες σε θέματα ασφαλείας. Για τον σκοπό αυτό, ενεργεί ως αξιωματικός-σύνδεσμος.

Ο ►M2 δευθυντής της Διεύθυνσης Ασφαλείας της Επιτροπής ◄ είναι υπεύθυνος για τη διαπίστευση των συστημάτων και δικτύων πληροφορικής στην Επιτροπή. Ο ►M2 δευθυντής της Διεύθυνσης Ασφαλείας της Επιτροπής ◄ αποφασίζει, σε συμφωνία με την αρμόδια ΕΑΑ, για τη διαπίστευση των συστημάτων και δικτύων πληροφορικής στα οποία συμμετέχουν η Επιτροπή αφενός, και αφετέρου κάθε άλλος αποδέκτης διαβαθμισμένων πληροφοριών ΕΕ.

15. ΕΠΙΘΕΩΡΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ

Η►M2 Διεύθυνση Ασφαλείας της Επιτροπής ◄διενεργεί περιοδικές επιθεωρήσεις των ρυθμίσεων ασφαλείας για την προστασία των διαβαθμισμένων πληροφοριών ΕΕ.

Η►M2 Διεύθυνση Ασφαλείας της Επιτροπής ◄ μπορεί να επικουρείται στο έργο αυτό από τις υπηρεσίες ασφαλείας άλλων θεσμικών οργάνων της ΕΕ που κατέχουν ΔΠΕΕ ή από τις εθνικές υπηρεσίες ασφαλείας των κρατών μελών ([1]).

Κατόπιν αιτήσεως κράτους μέλους, η ΕΑΑ του μπορεί να διεξαγάγει επιθεώρηση των ΔΠΕΕ στην Επιτροπή, από κοινού με την ►M2 Διεύθυνση Ασφαλείας της Επιτροπής ◄ και με αμοιβαία συμφωνία.

([1]) Με την επιφύλαξη της Σύμβασης της Βιέννης του 1961 για τις διπλωματικές σχέσεις και του πρωτοκόλλου περί προνομίων και ασυλιών των Ευρωπαϊκών Κοινοτήτων της 8ης Απριλίου 1965.

▼B

16. ΔΙΑΒΑΘΜΙΣΕΙΣ, ΕΝΔΕΙΞΕΙΣ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΣΗΜΑΝΣΕΙΣ

16.1. **Επίπεδα διαβάθμισης** ([1])

Οι πληροφορίες διαβαθμίζονται σύμφωνα με τα παρακάτω επίπεδα (βλέπε επίσης προσάρτημα 2):

►**M1** TRES SECRET UE/EU TOP SECRET ◄: Η διαβάθμιση αυτή εφαρμόζεται μόνο στις πληροφορίες και το υλικό των οποίων η άνευ αδείας κοινολόγηση μπορεί να βλάψει σοβαρότατα τα ζωτικά συμφέροντα της Ευρωπαϊκής Ένωσης ή ενός ή περισσοτέρων κρατών μελών της.

►**M1** SECRET UE ◄: Η διαβάθμιση αυτή εφαρμόζεται μόνο στις πληροφορίες και το υλικό των οποίων η άνευ αδείας κοινολόγηση μπορεί να βλάψει σοβαρά τα ζωτικά συμφέροντα της Ευρωπαϊκής Ένωσης ή ενός ή περισσοτέρων κρατών μελών της.

►**M1** CONFIDENTIEL UE ◄: Η διαβάθμιση αυτή εφαρμόζεται στις πληροφορίες και το υλικό των οποίων η άνευ αδείας κοινολόγηση μπορεί να βλάψει τα ζωτικά συμφέροντα της Ευρωπαϊκής Ένωσης ή ενός ή περισσοτέρων κρατών μελών της.

►**M1** RESTREINT UE ◄: Η διαβάθμιση αυτή εφαρμόζεται στις πληροφορίες και το υλικό των οποίων η άνευ αδείας κοινολόγηση είναι αντίθετη προς τα συμφέροντα της Ευρωπαϊκής Ένωσης ή ενός ή περισσοτέρων κρατών μελών της.

Δεν επιτρέπεται καμία άλλη διαβάθμιση.

16.2. **Ενδείξεις ασφαλείας**

Για τον περιορισμό της ισχύος της διαβάθμισης (που σημαίνει για τις διαβαθμισμένες πληροφορίες αυτόματο υποχαρακτηρισμό ή αποχαρακτηρισμό) μπορεί να χρησιμοποιείται μια συμφωνημένη ένδειξη ασφαλείας. Η ένδειξη αυτή είναι είτε «ΕΩΣ … (ώρα/ημερομηνία)» είτε «ΕΩΣ … (γεγονός)».

Στις περιπτώσεις που υπάρχει ανάγκη περιορισμένης διανομής και ειδικού χειρισμού, πέραν των όσων απαιτούνται βάσει της διαβάθμισης ασφαλείας, τίθενται πρόσθετες ενδείξεις ασφαλείας, όπως ΚΡΥΠΤΟ ή άλλες αναγνωρισμένες από την ΕΕ ενδείξεις ασφαλείας.

Οι σημάνσεις ασφαλείας χρησιμοποιούνται μόνο σε συνδυασμό με μια διαβάθμιση.

16.3. **Σημάνσεις**

Μπορεί να χρησιμοποιείται μια σήμανση με την οποία υποδηλώνεται ο τομέας που καλύπτεται από το συγκεκριμένο έγγραφο ή η περιορισμένη διανομή του με βάση την «ανάγκη γνώσης» ή (για τις μη διαβαθμισμένες πληροφορίες) δηλώνεται η λήξη της απαγόρευσης κυκλοφορίας.

Μια σήμανση δεν αποτελεί διαβάθμιση και δεν πρέπει να χρησιμοποιείται στη θέση αυτής.

Η σήμανση ΕΠΑΑ τίθεται σε όλα τα έγγραφα και στα αντίγραφά τους που αφορούν την ασφάλεια και την άμυνα της Ένωσης ή ενός ή περισσοτέρων κρατών μελών της, ή που αφορούν τη στρατιωτική ή μη στρατιωτική διαχείριση μιας κρίσεως.

16.4. **Επίθεση της διαβάθμισης**

Η διαβάθμιση τίθεται ως εξής:

α) σε έγγραφα ►**M1** RESTREINT UE ◄, με μηχανικά ή ηλεκτρονικά μέσα·

β) σε έγγραφα ►**M1** CONFIDENTIEL UE ◄, με μηχανικά μέσα ή ιδιοχείρως ή με εκτύπωση σε προσφραγισμένο ταξινομημένο χαρτί·

γ) σε έγγραφα ►**M1** SECRET UE ◄ και ►**M1** TRES SECRET UE/EU TOP SECRET ◄, με μηχανικά μέσα ή ιδιοχείρως.

16.5. **Επίθεση ενδείξεων ασφαλείας**

Οι ενδείξεις ασφαλείας τίθενται αμέσως κάτω από τη διαβάθμιση, με τα ίδια μέσα που τίθενται και οι διαβαθμίσεις.

17. ΔΙΑΧΕΙΡΙΣΗ ΤΩΝ ΔΙΑΒΑΘΜΙΣΕΩΝ

17.1. **Γενικά**

Οι πληροφορίες διαβαθμίζονται μόνον όταν απαιτείται. Η διαβάθμιση επισημαίνεται σαφώς και καταλλήλως και διατηρείται μόνον εφόσον οι συγκεκριμένες πληροφορίες απαιτείται να προστατευθούν.

([1]) Στο προσάρτημα 1 περιλαμβάνεται συγκριτικός πίνακας των διαβαθμίσεων ασφαλείας της ΕΕ, του ΝΑΤΟ, της ΔΕΕ και των κρατών μελών.

▼B

Αποκλειστικός υπεύθυνος για τη διαβάθμιση των πληροφοριών και για τον τυχόν μεταγενέστερο υποχαρακτηρισμό ή αποχαρακτηρισμό τους είναι ο αρχικός συντάκτης του εγγράφου.

Οι υπάλληλοι και το λοιπό προσωπικό της Επιτροπής διαβαθμίζουν, υποχαρακτηρίζουν ή αποχαρακτηρίζουν πληροφορίες κατόπιν εντολής του προϊσταμένου της υπηρεσίας τους ή σε συμφωνία μαζί του.

Οι αναλυτικές ρυθμίσεις για τον χειρισμό των διαβαθμισμένων εγγράφων έχουν εκπονηθεί κατά τρόπο που να εξασφαλίζεται ότι προστατεύονται αναλόγως των πληροφοριών που περιέχουν.

Ο αριθμός των προσώπων που επιτρέπεται να συντάσσουν έγγραφα ►**M1** TRES SECRET UE/EU TOP SECRET ◄ περιορίζεται στο απολύτως αναγκαίο, τα δε ονόματά τους συμπεριλαμβάνονται σε κατάλογο που καταρτίζεται από την►**M2** Διεύθυνση Ασφαλείας της Επιτροπής ◄.

17.2. **Εφαρμογή των διαβαθμίσεων**

Η διαβάθμιση ενός εγγράφου καθορίζεται από το επίπεδο ευαισθησίας του περιεχομένου του κατά τα οριζόμενα στο τμήμα16. Είναι σημαντικό η διαβάθμιση να χρησιμοποιείται σωστά και με φειδώ. Αυτό ισχύει ιδίως για τη διαβάθμιση ►**M1** TRES SECRET UE/EU TOP SECRET ◄.

Ο συντάκτης ενός εγγράφου το οποίο πρόκειται να λάβει διαβάθμιση οφείλει να έχει πάντοτε κατά νου τους προαναφερόμενους κανόνες και να αποφεύγει την τάση προς υπερβολικά υψηλή ή χαμηλή διαβάθμιση.

Ένας πρακτικός οδηγός για τις διαβαθμίσεις περιλαμβάνεται στο προσάρτημα 2.

Επί μέρους σελίδες, παράγραφοι, τμήματα, παραρτήματα και προσαρτήματα ενός εγγράφου καθώς και τα επισυναπτόμενα σε αυτό έγγραφα ενδέχεται να απαιτούν διαφορετικές διαβαθμίσεις και πρέπει να διαβαθμίζονται αναλόγως. Η διαβάθμιση του όλου εγγράφου αντιστοιχεί σε εκείνη του τμήματός του με την υψηλότερη διαβάθμιση.

Η διαβάθμιση μιας επιστολής ή ενός σημειώματος που περιλαμβάνει επισυναπτόμενα έγγραφα καθορίζεται στο επίπεδο του υψηλότερα διαβαθμισμένου εγγράφου. Ο συντάκτης επισημαίνει σαφώς σε ποιο επίπεδο πρέπει να διαβαθμιστεί η εν λόγω επιστολή ή το εν λόγω σημείωμα όταν αποχωριστεί από τα επισυναπτόμενα έγγραφα.

Η πρόσβαση του κοινού εξακολουθεί να διέπεται από τον κανονισμό (ΕΚ) αριθ. 1049/2001.

17.3. **Υποχαρακτηρισμός και αποχαρακτηρισμός**

Τα διαβαθμισμένα έγγραφα ΕΕ μπορούν να υποχαρακτηρίζονται ή να αποχαρακτηρίζονται μόνο κατόπιν αδείας του συντάκτη, και, εφόσον απαιτείται, αφού ζητηθεί η γνώμη των λοιπών ενδιαφερομένων. Ο υποχαρακτηρισμός ή αποχαρακτηρισμός επιβεβαιώνεται γραπτώς. Ο συντάκτης ενημερώνει τους παραλήπτες του εγγράφου για τη μεταβολή της διαβάθμισης, οι δε παραλήπτες ενημερώνουν σχετικά τους διαδοχικούς παραλήπτες στους οποίους έχουν διαβιβάσει το πρωτότυπο ή αντίγραφο του εγγράφου.

Ει δυνατόν, οι συντάκτες αναγράφουν επί των διαβαθμισμένων εγγράφων την ημερομηνία, την προθεσμία ή το γεγονός μετά τα οποία μπορούν να υποχαρακτηρίζονται ή αποχαρακτηρίζονται. Σε αντίθετη περίπτωση, επανεξετάζουν τα έγγραφα το αργότερο ανά πενταετία, ώστε να επιβεβαιώνεται ότι η αρχική διαβάθμιση εξακολουθεί να είναι αναγκαία.

18. ΥΛΙΚΗ ΑΣΦΑΛΕΙΑ

18.1. **Γενικά**

Οι κύριοι στόχοι των μέτρων υλικής ασφάλειας είναι η απαγόρευση της πρόσβασης μη εξουσιοδοτημένων προσώπων σε διαβαθμισμένες πληροφορίες ΕΕ ή/και υλικό, η αποφυγή της κλοπής και της φθοράς εξοπλισμού και άλλων περιουσιακών στοιχείων και η πρόληψη της παρενόχλησης ή τυχόν άλλης μορφής επίθεσης κατά του προσωπικού, άλλων υπαλλήλων και επισκεπτών.

18.2. **Απαιτήσεις ασφάλειας**

Όλοι οι χώροι, τα κτίρια, οι αίθουσες, τα συστήματα επικοινωνίας και πληροφοριών, κ.λπ. όπου γίνεται αποθήκευση ή/και χειρισμός διαβαθμισμένων πληροφοριών και υλικού ΕΕ προστατεύονται με τα ενδεδειγμένα μέτρα υλικής ασφάλειας.

Για τη λήψη απόφασης σχετικά με τον απαιτούμενο βαθμό προστασίας όσον αφορά την υλική ασφάλεια, λαμβάνονται υπόψη όλοι οι σχετικοί παράγοντες, όπως:

α) η διαβάθμιση των πληροφοριών ή/και του υλικού·

▼**B**

β) ο όγκος και η μορφή (π.χ. αποθήκευση σε έντυπη ή ηλεκτρονική μορφή) των σχετικών πληροφοριών·

γ) η σε τοπικό επίπεδο αξιολογούμενη από υπηρεσίες πληροφοριών, απειλή δολιοφθοράς, τρομοκρατικών ενεργειών και άλλων ανατρεπτικών ή/και ή εγκληματικών δραστηριοτήτων, που έχουν ως στόχο την ΕΕ, τα κράτη μέλη ή/και άλλα θεσμικά όργανα ή τρίτους που κατέχουν διαβαθμισμένες πληροφορίες της ΕΕ.

Τα εφαρμοζόμενα μέτρα υλικής ασφάλειας αποσκοπούν:

α) στην εμπόδιση της λαθραίας ή βιαίας εισόδου αναρμοδίων·

β) στην αποτροπή, παρεμπόδιση και ανίχνευση ενεργειών τυχόν αναξιόπιστου προσωπικού·

γ) στην παρεμπόδιση της πρόσβασης σε διαβαθμισμένες πληροφορίες ΕΕ, σε πρόσωπα που δεν απαιτείται να γνωρίζουν.

18.3. **Μέτρα υλικής ασφάλειας**

18.3.1. *Περιοχές ασφαλείας*

Οι χώροι στους οποίους γίνεται χειρισμός και αποθήκευση πληροφοριών με βαθμό διαβάθμισης ►**M1** CONFIDENTIEL UE ◄ ή υψηλότερο, οργανώνονται και διαμορφώνονται ως εξής:

α) Χώρος Ασφαλείας Κατηγορίας Ι: χώρος στον οποίο γίνεται χειρισμός και η αποθήκευση πληροφοριών με διαβάθμιση ►**M1** CONFIDENTIEL UE ◄ ή υψηλότερη, κατά τρόπον ώστε η είσοδος στο συγκεκριμένο χώρο να αποτελεί, ουσιαστικά, πρόσβαση σε διαβαθμισμένες πληροφορίες. Για έναν τέτοιο χώρο απαιτούνται:

   i) μια σαφώς καθορισμένη και προστατευόμενη περίμετρος στην οποία ελέγχεται κάθε είσοδος και έξοδος·

   ii) ένα σύστημα ελέγχου της εισόδου, το οποίο επιτρέπει την είσοδο μόνο στα πρόσωπα που έχουν υποστεί τον δέοντα έλεγχο ασφαλείας και έχουν ειδική άδεια εισόδου στον εν λόγω χώρο,

   iii) προσδιορισμός της διαβάθμισης των πληροφοριών που φυλάσσονται συνήθως στο χώρο αυτό, δηλαδή των πληροφοριών στις οποίες δίνει πρόσβαση η είσοδος στον εν λόγω χώρο.

β) Χώρος Ασφαλείας Κατηγορίας ΙΙ: χώρος στον οποίο γίνεται χειρισμός και η αποθήκευση πληροφοριών με διαβάθμιση ►**M1** CONFIDENTIEL UE ◄ ή υψηλότερη, κατά τέτοιον τρόπο ώστε να μπορούν να προστατεύονται με εσωτερικούς ελέγχους, προκειμένου να μη μπορούν να έχουν πρόσβαση σ' αυτές μη εξουσιοδοτημένα πρόσωπα, π.χ. κτίρια όπου στεγάζονται υπηρεσίες, στα οποία γίνεται τακτικά χειρισμός και αποθήκευση πληροφοριών με διαβάθμιση ►**M1** CONFIDENTIEL UE ◄ ή υψηλότερη. Για έναν τέτοιο χώρο απαιτούνται:

   i) μια σαφώς καθορισμένη και προστατευόμενη περίμετρος στην οποία ελέγχεται κάθε είσοδος και έξοδος·

   ii) ένα σύστημα ελέγχου της εισόδου, το οποίο επιτρέπει την χωρίς συνοδεία είσοδο μόνο στα πρόσωπα που έχουν υποστεί τον δέοντα έλεγχο ασφαλείας και έχουν ειδική άδεια εισόδου στον εν λόγω χώρο. Για όλα τα άλλα πρόσωπα, θα προβλέπεται η ύπαρξη συνοδών ή ισοδύναμων ελέγχων, προκειμένου να προλαμβάνεται η πρόσβαση μη εξουσιοδοτημένων προσώπων σε διαβαθμισμένες πληροφορίες ΕΕ και η ανεξέλεγκτη είσοδος σε χώρους που υπόκεινται σε τεχνικές επιθεωρήσεις ασφαλείας.

   Οι χώροι στους οποίους δεν υπάρχει προσωπικό υπηρεσίας σε 24ωρη βάση επιθεωρούνται αμέσως μετά τις κανονικές ώρες εργασίας για να διασφαλίζεται ότι οι διαβαθμισμένες πληροφορίες ΕΕ έχουν ασφαλισθεί καταλλήλως.

18.3.2. *Διοικητικός χώρος*

Γύρω από τους χώρους ασφαλείας κατηγορίας Ι ή κατηγορίας ΙΙ καθώς και στις προσβάσεις τους, ενδέχεται να προβλεφθεί ένας διοικητικός χώρος μικρότερου βαθμού ασφαλείας. Ο χώρος αυτός απαιτεί μια εμφανώς οριοθετημένη περίμετρο που να επιτρέπει τον έλεγχο του προσωπικού και των οχημάτων. Στους εν λόγω διοικητικούς χώρους γίνεται χειρισμός και αποθήκευση μόνο πληροφοριών ►**M1** RESTREINT UE ◄ ή μη διαβαθμισμένων πληροφοριών.

18.3.3. *Έλεγχοι εισόδου και εξόδου*

Η είσοδος και η έξοδος στους ή από τους χώρους ασφαλείας κατηγορίας Ι και κατηγορίας ΙΙ, ελέγχονται με σύστημα ειδικής ταυτότητας ή προσωπικής αναγνώρισης που ισχύει για όλο το προσωπικό που εργάζεται συνήθως στους συγκεκριμένους χώρους. Θα καθιερωθεί επίσης ένα σύστημα ελέγχων των επισκεπτών προκειμένου να απαγορεύεται η πρόσβαση μη εξουσιοδοτημένων προσώπων σε διαβαθμισμένες πληροφορίες ΕΕ. Τα συστήματα ειδικής ταυτότητας μπορούν να υποστηρίζονται από αυτοματοποιημένη αναγνώριση της ταυτότητας, ως συμπλήρωμα αλλά όχι ως πλήρες υποκατάστατο των φυλάκων. Τυχόν μεταβολή της

▼**B**

αξιολόγησης κινδύνου μπορεί να συνεπάγεται την ενίσχυση των μέτρων ελέγχου εισόδου και εξόδου, για παράδειγμα κατά τη διάρκεια της επίσκεψης σημαντικών προσωπικοτήτων.

18.3.4. *Περιπολίες των φυλάκων*

Στους χώρους ασφαλείας κατηγορίας Ι και κατηγορίας ΙΙ πραγματοποιούνται περιπολίες εκτός των κανονικών ωρών εργασίας, με σκοπό την προστασία των περιουσιακών στοιχείων της ΕΕ από διαρροή, ζημία ή απώλεια. Η συχνότητα των περιπολιών εξαρτάται από τις τοπικές συνθήκες, αλλά κατά κανόνα πρέπει να πραγματοποιούνται περιπολίες κάθε 2 ώρες.

18.3.5. *Φωριαμοί ασφαλείας και θωρακισμένες αίθουσες*

Για την αποθήκευση διαβαθμισμένων πληροφοριών ΕΕ χρησιμοποιούνται φωριαμοί τριών κατηγοριών:

— κατηγορία Α: φωριαμοί που έχουν εγκριθεί σε εθνικό επίπεδο για την αποθήκευση πληροφοριών με διαβάθμιση ►**M1** TRES SECRET UE/EU TOP SECRET ◄, σε χώρους ασφαλείας κατηγορίας Ι ή κατηγορίας ΙΙ·

— κατηγορία Β: φωριαμοί που έχουν εγκριθεί σε εθνικό επίπεδο για την αποθήκευση πληροφοριών με διαβάθμιση ►**M1** SECRET UE ◄ ή ►**M1** CONFIDENTIEL UE ◄, σε χώρους ασφαλείας κατηγορίας Ι ή κατηγορίας ΙΙ·

— κατηγορία Γ: έπιπλα γραφείου κατάλληλα μόνο για την αποθήκευση πληροφοριών ►**M1** RESTREINT UE ◄.

Για τις θωρακισμένες αίθουσες που κατασκευάζονται εντός χώρου ασφαλείας κατηγορίας Ι ή κατηγορίας ΙΙ, και για όλους τους χώρους ασφαλείας κατηγορίας Ι, όπου διαβαθμισμένες πληροφορίες με χαρακτηρισμό ►**M1** CONFIDENTIEL UE ◄ αποθηκεύονται σε ανοικτά ράφια ή εμφαίνονται σε σχεδιαγράμματα, χάρτες κ.λπ., οι τοίχοι, τα πατώματα και οι οροφές, καθώς και οι θύρες που κλειδώνουν, απαιτείται να πιστοποιούνται από την αρχή πιστοποίησης ασφαλείας (ΑΠΑ) ότι προσφέρουν ισοδύναμη προστασία με την κατηγορία του φωριαμού ασφαλείας που έχει εγκριθεί για την αποθήκευση πληροφοριών της ίδιας διαβάθμισης.

18.3.6. *Κλειδαριές*

Οι κλειδαριές στους φωριαμούς ασφαλείας και τις θωρακισμένες αίθουσες όπου αποθηκεύονται διαβαθμισμένες πληροφορίες ΕΕ, πληρούν τις ακόλουθες προδιαγραφές:

— ομάδα Α: εγκεκριμένες σε εθνικό επίπεδο για φωριαμούς κατηγορίας Α·

— ομάδα Β: εγκεκριμένες σε εθνικό επίπεδο για φωριαμούς κατηγορίας Β·

— ομάδα Γ: κατάλληλες μόνο για έπιπλα γραφείου κατηγορίας Γ.

18.3.7. *Έλεγχος των κλειδιών και των συνδυασμών*

Τα κλειδιά των φωριαμών ασφαλείας δεν πρέπει να βγαίνουν από τα κτίρια της Επιτροπής. Οι συνδυασμοί των φωριαμών ασφαλείας απομνημονεύονται από τα πρόσωπα που πρέπει να τους γνωρίζουν. Για χρήση ανάγκης, ο τοπικός υπεύθυνος ασφαλείας της οικείας υπηρεσίας της Επιτροπής, είναι υπεύθυνος να κατέχει αντικλείδια καθώς και να διατηρεί γραπτά στοιχεία για κάθε συνδυασμό. Οι συνδυασμοί φυλάσσονται σε χωριστούς σφραγισμένους αδιαφανείς φακέλους. Τα κλειδιά καθημερινής χρήσης, τα αντικλείδια ασφαλείας και οι συνδυασμοί φυλάσσονται σε χωριστούς φωριαμούς ασφαλείας. Για τα εν λόγω κλειδιά και συνδυασμούς παρέχεται προστασία ασφαλείας τουλάχιστον ισοδύναμη προς το υλικό στο οποίο παρέχουν πρόσβαση.

Η γνώση των συνδυασμών των φωριαμών ασφαλείας περιορίζεται σε όσο το δυνατόν λιγότερα πρόσωπα. Οι συνδυασμοί πρέπει να αλλάζουν:

α) όποτε παραλαμβάνεται νέος φωριαμός,

β) όποτε αλλάζει το οικείο προσωπικό,

γ) όποτε σημειώνεται διαρροή ή υπάρχουν υπόνοιες διαρροής,

δ) κατά προτίμηση ανά εξάμηνο και τουλάχιστον κάθε δώδεκα μήνες.

18.3.8. *Συσκευές ανίχνευσης εισόδου αναρμοδίων*

Όταν χρησιμοποιούνται για την προστασία των διαβαθμισμένων πληροφοριών ΕΕ συστήματα συναγερμού, κλειστά κυκλώματα τηλεόρασης και άλλες ηλεκτρικές συσκευές, πρέπει να προβλέπεται εφεδρική παροχή ηλεκτρικού ρεύματος για περιπτώσεις επείγουσας ανάγκης, για να διασφαλίζεται η συνεχής λειτουργία του συστήματος σε περίπτωση διακοπής της κύριας παροχής ενέργειας. Μια άλλη βασική απαίτηση είναι να σημαίνει συναγερμός ή να ειδοποιείται με άλλον αξιόπιστο τρόπο το προσωπικό επιτήρησης όποτε σημειώνεται βλάβη των εν λόγω συστημάτων ή επιχειρείται παρέμβαση σ' αυτά.

▼B

18.3.9. *Εγκεκριμένος εξοπλισμός*

Η ►M2 Διεύθυνση Ασφαλείας της Επιτροπής ◄ διατηρεί ενημερωμένους καταλόγους, ανά τύπο και μοντέλο του εξοπλισμού ασφαλείας που έχει εγκρίνει για την προστασία των διαβαθμισμένων πληροφοριών, υπό διάφορες συγκεκριμένες περιστάσεις και συνθήκες. Για την κατάρτιση των καταλόγων αυτών, η ►M2 Διεύθυνση Ασφαλείας της Επιτροπής ◄ βασίζεται, μεταξύ άλλων, σε πληροφορίες που παρέχονται από τις εθνικές αρχές ασφαλείας (ΕΑΑ).

18.3.10. *Υλική προστασία των φωτοαντιγραφικών συσκευών και συσκευών τηλεομοιοτυπίας (φαξ)*

Οι φωτοαντιγραφικές συσκευές και οι συσκευές τηλεομοιοτυπίας (φαξ) προστατεύονται υλικώς στο βαθμό που απαιτείται έτσι ώστε να διασφαλίζεται ότι μόνο εξουσιοδοτημένα πρόσωπα μπορούν να τις χρησιμοποιούν για την επεξεργασία διαβαθμισμένων πληροφοριών και ότι όλο το διαβαθμισμένο υλικό ελέγχεται δεόντως.

18.4. **Προστασία κατά της λαθροβλεψίας και της λαθρακρόασης**

18.4.1. *Λαθροβλεψία*

Λαμβάνονται όλα τα ενδεδειγμένα μέτρα, μέρα και νύχτα, προκειμένου να διασφαλίζεται ότι τα μη εξουσιοδοτημένα πρόσωπα δεν θα μπορούν να δουν, έστω και συμπτωματικώς, διαβαθμισμένες πληροφορίες ΕΕ.

18.4.2. *Λαθρακρόαση*

Οι υπηρεσίες ή οι χώροι όπου συζητούνται τακτικά πληροφορίες με διαβάθμιση ►M1 SECRET UE ◄ ή υψηλότερη, προστατεύονται από κρούσματα παθητικής ή ενεργητικής λαθρακρόασης εφόσον υφίσταται σχετικός κίνδυνος. Υπεύθυνη για την αξιολόγηση του κινδύνου αυτού είναι η ►M2 Διεύθυνση Ασφαλείας της Επιτροπής ◄, έπειτα από διαβούλευση, εφόσον χρειάζεται, με τις ΕΑΑ.

18.4.3. *Εισαγωγή ηλεκτρονικού εξοπλισμού και καταγραφικών συσκευών*

Δεν επιτρέπεται η εισαγωγή κινητών τηλεφώνων, προσωπικών υπολογιστών, ηχογραφικών συσκευών, φωτογραφικών μηχανών και άλλων ηλεκτρονικών ή καταγραφικών συσκευών σε χώρους ασφαλείας, χωρίς προηγούμενη έγκριση του προϊσταμένου της ►M2 Διεύθυνσης Ασφαλείας της Επιτροπής ◄.

Για την καθορισμό των προς λήψη προστατευτικών μέτρων σε χώρους ευαίσθητους όσον αφορά την παθητική λαθρακρόαση (π.χ. μόνωση τοίχων, θυρών, πατωμάτων και οροφών, μέτρηση αποκαλυπτικών εκπομπών) και την ενεργητική λαθρακρόαση (π.χ. αναζήτηση μικροφώνων), η ►M2 Διεύθυνση Ασφαλείας της Επιτροπής ◄ μπορεί να ζητά τη συνδρομή εμπειρογνωμόνων των ΕΑΑ.

Ομοίως, όταν το απαιτούν οι περιστάσεις, ο κάθε είδους τηλεπικοινωνιακός εξοπλισμός και ο κάθε είδους ηλεκτρικός ή ηλεκτρονικός εξοπλισμός γραφείου που χρησιμοποιείται κατά τις συνεδριάσεις σε επίπεδο ►M1 SECRET UE ◄ ή υψηλότερο, μπορεί να ελέγχεται από ειδικούς τεχνικούς ασφαλείας των ΕΑΑ, έπειτα από αίτηση του προϊσταμένου της ►M2 Διεύθυνσης Ασφαλείας της Επιτροπής ◄.

18.5. **Τεχνικώς ασφαλείς χώροι**

Ορισμένοι χώροι μπορούν να χαρακτηρισθούν ως τεχνικώς ασφαλείς. Στους χώρους αυτούς διενεργείται ειδικός έλεγχος εισόδου. Όταν δεν χρησιμοποιούνται, οι χώροι αυτοί διατηρούνται κλειδωμένοι με εγκεκριμένη μέθοδο και όλα τα σχετικά κλειδιά θεωρούνται ως κλειδιά ασφαλείας. Στους χώρους αυτούς διενεργούνται τακτικά υλικές επιθεωρήσεις, οι οποίες διενεργούνται επίσης έπειτα από τυχόν μη εγκεκριμένη είσοδο στους χώρους αυτούς ή εφόσον υπάρχουν υπόνοιες τέτοιας εισόδου.

Τηρείται λεπτομερής κατάσταση του εξοπλισμού και της επίπλωσης προκειμένου να παρακολουθούνται οι μετακινήσεις τους. Κανένα στοιχείο επίπλωσης ή εξοπλισμού δεν εισάγεται σε τέτοιο χώρο χωρίς προσεκτική επιθεώρηση από ειδικά εκπαιδευμένο προσωπικό ασφαλείας, προκειμένου να ανιχνευθούν τυχόν συσκευές υποκλοπής. Κατά κανόνα, η εγκατάσταση γραμμών επικοινωνίας σε τεχνικώς ασφαλείς χώρους, δεν επιτρέπεται χωρίς προηγούμενη έγκριση από την αρμόδια αρχή.

19. ΓΕΝΙΚΟΙ ΚΑΝΟΝΕΣ ΣΧΕΤΙΚΑ ΜΕ ΤΗΝ ΑΡΧΗ ΤΗΣ ΑΝΑΓΚΗΣ ΝΑ ΓΝΩΡΙΖΕΙ ΚΑΙ ΤΟΥΣ ΕΛΕΓΧΟΥΣ ΑΣΦΑΛΕΙΑΣ ΤΟΥ ΠΡΟΣΩΠΙΚΟΥ

19.1. **Γενικά**

Η πρόσβαση σε διαβαθμισμένες πληροφορίες ΕΕ επιτρέπεται μόνο στα πρόσωπα που όντως έχουν «ανάγκη γνώσης», για την εκτέλεση των καθηκόντων ή των αποστολών τους. Η πρόσβαση σε πληροφορίες ►M1 TRES SECRET UE/EU

▼B

TOP SECRET ◄, ►M1 SECRET UE ◄ και ►M1 CONFIDENTIEL UE ◄ θα επιτρέπεται μόνο στα πρόσωπα που έχουν υποστεί με επιτυχία τον ενδεδειγμένο έλεγχο ασφαλείας.

Για τον καθορισμό της «ανάγκης γνώσης» αρμόδια είναι η υπηρεσία στην οποία πρόκειται να απασχοληθεί το συγκεκριμένο πρόσωπο.

Κάθε υπηρεσία είναι αρμόδια για τις αιτήσεις σχετικά με τον έλεγχο ασφαλείας του προσωπικού της.

Κατόπιν του ελέγχου ασφαλείας εκδίδεται «προσωπικό πιστοποιητικό ασφαλείας ΕΕ», όπου αναγράφονται το επίπεδο των διαβαθμισμένων πληροφοριών στις οποίες μπορεί να έχει πρόσβαση το ελεγχθέν πρόσωπο καθώς και η ημερομηνία λήξης της ισχύος του.

Το προσωπικό πιστοποιητικό ασφαλείας ΕΕ για συγκεκριμένη διαβάθμιση, μπορεί να παρέχει στον κάτοχό του πρόσβαση σε πληροφορίες χαμηλότερης διαβάθμισης.

Πρόσωπα άλλα πλην των μονίμων υπαλλήλων ή του λοιπού προσωπικού, όπως είναι οι συμβασιούχοι, οι εμπειρογνώμονες ή σύμβουλοι, με τα οποία χρειάζεται ενδεχομένως να συζητηθούν ή στα οποία χρειάζεται ενδεχομένως να επιδειχθούν διαβαθμισμένες πληροφορίες ΕΕ, πρέπει να έχουν υποστεί επιτυχώς προσωπικό έλεγχο ασφαλείας ΕΕ, όσον αφορά τις διαβαθμισμένες πληροφορίες ΕΕ και να ενημερώνονται για την ευθύνη τους σχετικά με την ασφάλεια.

Την πρόσβαση του κοινού θα εξακολουθήσει να διέπει ο κανονισμός (ΕΚ) αριθ. 1049/2001.

19.2. **Ειδικοί κανόνες σχετικά με την πρόσβαση σε πληροφορίες με διαβάθμιση ►M1 TRES SECRET UE/EU TOP SECRET ◄**

Όλα τα πρόσωπα που πρόκειται να έχουν πρόσβαση σε πληροφορίες με διαβάθμιση ►M1 TRES SECRET UE/EU TOP SECRET ◄, υποβάλλονται προηγουμένως σε έλεγχο ασφαλείας, προκειμένου να επιτραπεί η πρόσβαση στις εν λόγω πληροφορίες.

Όλα τα πρόσωπα που πρέπει να έχουν πρόσβαση σε πληροφορίες με διαβάθμιση ►M1 TRES SECRET UE/EU TOP SECRET ◄, ορίζονται από το μέλος της Επιτροπής που είναι αρμόδιο για θέματα ασφαλείας και τα ονόματά τους καταχωρούνται στην οικεία γραμματεία ►M1 TRES SECRET UE/EU TOP SECRET ◄. Για τη σύσταση και τη διατήρηση της εν λόγω γραμματείας αρμόδια είναι η ►M2 Διεύθυνση Ασφαλείας της Επιτροπής ◄.

Προτού αποκτήσουν πρόσβαση σε πληροφορίες ►M1 TRES SECRET UE/EU TOP SECRET ◄, όλα τα πρόσωπα υπογράφουν βεβαίωση ότι έχουν ενημερωθεί για τις διαδικασίες ασφαλείας της Επιτροπής και ότι κατανοούν πλήρως την ειδική τους ευθύνη για τη διασφάλιση των πληροφοριών ►M1 TRES SECRET UE/EU TOP SECRET ◄ και τις συνέπειες που προβλέπονται από τους κανόνες της ΕΕ και το εθνικό δίκαιο ή τους εθνικούς διοικητικούς κανόνες, σε περίπτωση που διαβαθμισμένες πληροφορίες περιέρχονται σε μη εξουσιοδοτημένα πρόσωπα, είτε εκ προθέσεως είτε εξ αμελείας.

Στην περίπτωση προσώπων τα οποία έχουν πρόσβαση σε πληροφορίες ►M1 TRES SECRET UE/EU TOP SECRET ◄, σε συνεδριάσεις κ.λπ., ο αρμόδιος υπάλληλος ελέγχου της υπηρεσίας ή του οργανισμού στον οποίο απασχολείται το εν λόγω πρόσωπο, γνωστοποιεί στον οργανισμό που διοργανώνει τη συνεδρίαση ότι τα συγκεκριμένα πρόσωπα διαθέτουν τη σχετική άδεια.

Τα ονόματα όλων των προσώπων τα οποία παύουν να απασχολούνται σε καθήκοντα που απαιτούν πρόσβαση σε πληροφορίες ►M1 TRES SECRET UE/EU TOP SECRET ◄, διαγράφονται από τον κατάλογο ►M1 TRES SECRET UE/EU TOP SECRET ◄. Επίσης, εφιστάται και πάλι η προσοχή όλων αυτών των προσώπων στην ειδική ευθύνη τους για τη διασφάλιση πληροφοριών με διαβάθμιση ►M1 TRES SECRET UE/EU TOP SECRET ◄. Τα πρόσωπα αυτά υπογράφουν επίσης δήλωση ότι δεν θα χρησιμοποιήσουν ούτε θα διαβιβάσουν σε άλλους πληροφορίες με διαβάθμιση ►M1 TRES SECRET UE/EU TOP SECRET ◄, τις οποίες κατέχουν.

19.3. **Ειδικοί κανόνες σχετικά με την πρόσβαση σε πληροφορίες με διαβάθμιση ►M1 SECRET UE ◄ ή ►M1 CONFIDENTIEL UE ◄**

Όλα τα πρόσωπα που πρόκειται να έχουν πρόσβαση σε πληροφορίες ►M1 SECRET UE ◄ και ►M1 CONFIDENTIEL UE ◄, υφίστανται προηγουμένως έλεγχο ασφαλείας του ενδεδειγμένου βαθμού.

Όλα τα πρόσωπα που πρόκειται να έχουν πρόσβαση σε πληροφορίες ►M1 SECRET UE ◄ και ►M1 CONFIDENTIEL UE ◄, ενημερώνονται σχετικά με τις κατάλληλες διατάξεις ασφαλείας, καθώς και για τις συνέπειες τυχόν αμέλειας.

▼B

Στην περίπτωση προσώπων που έχουν πρόσβαση σε πληροφορίες ►M1 SECRET UE ◄ και ►M1 CONFIDENTIEL UE ◄, κατά τη διάρκεια συνεδριάσεων κ.λπ., ο υπεύθυνος ασφαλείας του οργανισμού όπου εργάζεται το εν λόγω πρόσωπο, κοινοποιεί στον οργανισμό που διοργανώνει τη συνεδρίαση, ότι τα συγκεκριμένα πρόσωπα διαθέτουν τη σχετική άδεια.

19.4. **Ειδικοί κανόνες σχετικά με την πρόσβαση σε πληροφορίες με διαβάθμιση ►M1 RESTREINT UE ◄**

Οι έχοντες πρόσβαση σε πληροφορίες ►M1 RESTREINT UE ◄ ενημερώνονται για τους προκείμενους κανόνες ασφαλείας καθώς και για τις συνέπειες τυχόν αμέλειας.

19.5. **Μεταθέσεις**

Όταν ένα μέλος του προσωπικού μετατίθεται από μια θέση η οποία ενέχει το χειρισμό διαβαθμισμένου υλικού ΕΕ, η Γραμματεία επιβλέπει την κατάλληλη παράδοση του υλικού αυτού από τον απερχόμενο στο νέο υπάλληλο.

Όταν ένα μέλος του προσωπικού μετατίθεται σε άλλη θέση που προϋποθέτει το χειρισμό διαβαθμισμένου υλικού ΕΕ, ο τοπικός υπεύθυνος ασφαλείας του παρέχει τη σχετική ενημέρωση.

19.6. **Ειδικές εντολές**

Τα πρόσωπα τα οποία απαιτείται να χειρίζονται διαβαθμισμένες πληροφορίες ΕΕ θα πρέπει, για πρώτη φορά κατά την ανάληψη των καθηκόντων τους και στη συνέχεια περιοδικά, να ενημερώνονται για:

α) τους κινδύνους που ενέχουν για την ασφάλεια οι ακριτομυθίες·

β) τις προφυλάξεις που πρέπει να παίρνουν στις σχέσεις τους με τον τύπο και με εκπροσώπους ομάδων με ειδικά συμφέροντα·

γ) την απειλή που συνιστούν οι δραστηριότητες υπηρεσιών πληροφοριών οι οποίες έχουν ως στόχο την ΕΕ και τα κράτη μέλη, σε ό,τι αφορά τις διαβαθμισμένες πληροφορίες και δραστηριότητες ΕΕ,

δ) την υποχρέωση να αναφέρουν αμέσως στις ενδεδειγμένες αρχές ασφαλείας κάθε τυχόν προσέγγιση ή ελιγμό που προκαλεί υπόνοιες κατασκοπευτικής δραστηριότητας ή τυχόν ασυνήθεις περιστάσεις που αφορούν την ασφάλεια.

Όλα τα πρόσωπα που έχουν κανονικά συχνές επαφές με αντιπροσώπους χωρών των οποίων οι υπηρεσίες πληροφοριών έχουν ως στόχο την ΕΕ και τα κράτη μέλη σε ό,τι αφορά διαβαθμισμένες πληροφορίες και δραστηριότητες ΕΕ, ενημερώνονται για τις τεχνικές που είναι γνωστό ότι χρησιμοποιούνται από τις διάφορες υπηρεσίες πληροφοριών.

Δεν υπάρχουν διατάξεις ασφαλείας της Επιτροπής σχετικά με τα ιδιωτικά ταξίδια, ασχέτως προορισμού, του προσωπικού που έχει άδεια πρόσβασης σε διαβαθμισμένες πληροφορίες ΕΕ. Ωστόσο, η ►M2 Διεύθυνση Ασφαλείας της Επιτροπής ◄ γνωστοποιεί στους υπαλλήλους και το λοιπό προσωπικό που υπάγονται στην αρμοδιότητά της, τους ταξιδιωτικούς κανονισμούς οι οποίοι ενδέχεται να ισχύουν γι' αυτούς.

20. ΔΙΑΔΙΚΑΣΙΑ ΕΛΕΓΧΟΥ ΑΣΦΑΛΕΙΑΣ ΓΙΑ ΤΟΥΣ ΥΠΑΛΛΗΛΟΥΣ ΚΑΙ ΤΟ ΛΟΙΠΟ ΠΡΟΣΩΠΙΚΟ ΤΗΣ ΕΠΙΤΡΟΠΗΣ

α) Μόνο οι υπάλληλοι και το λοιπό προσωπικό της Επιτροπής, ή πρόσωπα τα οποία εργάζονται στα πλαίσια των δραστηριοτήτων της Επιτροπής και τα οποία, λόγω των καθηκόντων τους και για τις ανάγκες της υπηρεσίας, απαιτείται να λάβουν γνώση ή να κάνουν χρήση διαβαθμισμένων πληροφοριών που έχει στην κατοχή της Επιτροπή, έχουν πρόσβαση στις πληροφορίες αυτές.

β) Για να έχουν πρόσβαση σε πληροφορίες με τη διαβάθμιση ►M1 TRES SECRET UE/EU TOP SECRET ◄, ►M1 SECRET UE ◄ και ►M1 CONFIDENTIEL UE ◄, τα πρόσωπα που μνημονεύονται στην παράγραφο α) ανωτέρω, πρέπει να έχουν λάβει σχετική άδεια, σύμφωνα με τη διαδικασία των παραγράφων γ) και δ) του παρόντος τμήματος.

γ) Η άδεια χορηγείται μόνο στα πρόσωπα τα οποία έχουν υποστεί έλεγχο ασφαλείας από τις αρμόδιες εθνικές αρχές των κρατών μελών (ΕΑΑ), σύμφωνα με τη διαδικασία των παραγράφων θ) έως ιδ).

δ) Ο προϊστάμενος της ►M2 Διεύθυνσης Ασφαλείας της Επιτροπής ◄ είναι αρμόδιος για τη χορήγηση των αδειών που αναφέρονται στις παραγράφους α), β) και γ).

ε) Χορηγεί την άδεια αφού λάβει τη γνώμη των αρμόδιων εθνικών αρχών των κρατών μελών, βάσει του ελέγχου ασφαλείας που διενεργείται σύμφωνα με τις παραγράφους θ) έως ιδ).

▼B

στ) Η ►M2 Διεύθυνση Ασφαλείας της Επιτροπής ◄ διατηρεί ενημερωμένο κατάλογο όλων των ευαίσθητων θέσεων, που προβλέπονται από τις σχετικές υπηρεσίες της Επιτροπής, καθώς και όλων των προσώπων στα οποία έχει χορηγηθεί (προσωρινή) άδεια.

ζ) Η άδεια, η οποία έχει πενταετή ισχύ, δεν μπορεί να υπερβεί τη διάρκεια των καθηκόντων βάσει των οποίων χορηγείται. Μπορεί να ανανεωθεί σύμφωνα με τη διαδικασία της παραγράφου ε).

η) Η άδεια ανακαλείται από τον προϊστάμενο της ►M2 Διεύθυνσης Ασφαλείας της Επιτροπής ◄ εφόσον κρίνει ότι υπάρχουν βάσιμοι λόγοι ανάκλησης της αδείας. Κάθε απόφαση ανάκλησης αδείας πρέπει να κοινοποιείται στον ενδιαφερόμενο, ο οποίος μπορεί να ζητήσει ακρόαση από την ►M2 Διεύθυνση Ασφαλείας της Επιτροπής ◄, καθώς και στην αρμόδια εθνική αρχή.

θ) Ο έλεγχος ασφαλείας διενεργείται με τη συνδρομή του ενδιαφερομένου προσώπου και με αίτηση του προϊσταμένου της ►M2 Διεύθυνσης Ασφαλείας της Επιτροπής ◄. Η αρμόδια για τον έλεγχο εθνική αρχή είναι η αρχή του κράτους μέλους του οποίου είναι υπήκοος το πρόσωπο το οποίο αφορά η άδεια. Εφόσον το συγκεκριμένο πρόσωπο δεν είναι υπήκοος ενός κράτους μέλους της ΕΕ, ο προϊστάμενος της ►M2 Διεύθυνσης Ασφαλείας της Επιτροπής ◄ θα ζητήσει να διεξαχθεί έλεγχος ασφαλείας από το κράτος μέλος του τόπου κατοικίας του εν λόγω προσώπου ή του τόπου συνήθους διαμονής του.

ι) Στο πλαίσιο της διαδικασίας ελέγχου, μπορεί να ζητηθεί από τον ενδιαφερόμενο να συμπληρώσει έντυπο με προσωπικές πληροφορίες.

ια) Ο προϊστάμενος της ►M2 Διεύθυνσης Ασφαλείας της Επιτροπής ◄ προσδιορίζει στην αίτησή του το είδος και το επίπεδο των διαβαθμισμένων πληροφοριών που πρόκειται να τεθούν στη διάθεση του ενδιαφερομένου, ώστε οι αρμόδιες εθνικές αρχές να μπορέσουν να διενεργήσουν τη διαδικασία ελέγχου και να δώσουν τη γνώμη τους ως προς το επίπεδο της άδειας που θα ήταν σκόπιμο να χορηγηθεί στο εν λόγω πρόσωπο.

ιβ) Το σύνολο της διαδικασίας ελέγχου ασφαλείας μαζί με τα πορίσματά της υπόκεινται στους κανόνες και τις ρυθμίσεις που ισχύουν εν προκειμένω στο οικείο κράτος μέλος, περιλαμβανομένων των κανόνων και ρυθμίσεων που αφορούν τις ενστάσεις και προσφυγές.

ιγ) Όταν οι αρμόδιες εθνικές αρχές του κράτους μέλους δίνουν θετική γνώμη, ο προϊστάμενος της ►M2 Διεύθυνσης Ασφαλείας της Επιτροπής ◄ μπορεί να χορηγεί την άδεια στο ενδιαφερόμενο πρόσωπο.

ιδ) Η αρνητική γνώμη των αρμόδιων εθνικών αρχών γνωστοποιείται στον ενδιαφερόμενο, ο οποίος μπορεί να ζητήσει ακρόαση από τον προϊστάμενο της ►M2 Διεύθυνσης Ασφαλείας της Επιτροπής ◄. Εφόσον το κρίνει αναγκαίο, ο προϊστάμενος της ►M2 Διεύθυνσης Ασφαλείας της Επιτροπής ◄ μπορεί να ζητήσει από τις αρμόδιες εθνικές αρχές οιαδήποτε περαιτέρω διευκρίνιση μπορούν να παράσχουν. Εάν επιβεβαιωθεί η αρνητική γνώμη, η άδεια δεν χορηγείται.

ιε) Όλα τα πρόσωπα στα οποία χορηγείται άδεια κατά την έννοια των παραγράφων δ) και ε), λαμβάνουν, κατά τη στιγμή χορήγησης της άδειας και στη συνέχεια σε τακτικά διαστήματα, τις τυχόν αναγκαίες οδηγίες σχετικά με την προστασία διαβαθμισμένων πληροφοριών και με τα μέσα για τη διασφάλιση της προστασίας αυτής. Τα πρόσωπα αυτά υπογράφουν δήλωση με την οποία βεβαιώνουν ότι έλαβαν τις οδηγίες και αναλαμβάνουν να τις τηρούν.

ιστ) Ο προϊστάμενος της ►M2 Διεύθυνσης Ασφαλείας της Επιτροπής ◄ λαμβάνει τα τυχόν αναγκαία μέτρα για την εφαρμογή του παρόντος τμήματος, ιδίως όσον αφορά τους κανόνες που διέπουν την πρόσβαση στον κατάλογο των δεόντως εξουσιοδοτημένων προσώπων.

ιζ) Κατ' εξαίρεση, εφόσον απαιτείται από την υπηρεσία, ο προϊστάμενος της ►M2 Διεύθυνσης Ασφαλείας της Επιτροπής ◄ μπορεί, αφού ενημερώσει τις αρμόδιες εθνικές αρχές και εφόσον δεν υπάρξει αντίδραση εκ μέρους των εντός ενός μηνός, να χορηγεί προσωρινή άδεια μέγιστης διάρκειας έξι μηνών, εν αναμονή του αποτελέσματος του ελέγχου που μνημονεύεται στην παράγραφο θ).

ιη) Οι ούτως χορηγούμενες προσωρινές και υπό αίρεση άδειες δεν παρέχουν πρόσβαση σε πληροφορίες με διαβάθμιση ►M1 TRES SECRET UE/EU TOP SECRET ◄. Η πρόσβαση στις πληροφορίες αυτές περιορίζεται στους υπαλλήλους που έχουν όντως υποστεί έλεγχο επιτυχώς, σύμφωνα με την παράγραφο θ). Εν αναμονή του πορίσματος του ελέγχου, οι υπάλληλοι για τους οποίους έχει ζητηθεί πρόσβαση σε πληροφορίες του επιπέδου διαβάθμισης ►M1 TRES SECRET UE/EU TOP SECRET ◄ μπορούν να λαμβάνουν προσωρινή και υπό αίρεση άδεια πρόσβασης σε πληροφορίες που έχουν βαθμό ασφαλείας έως και ►M1 SECRET UE ◄.

▼B

21. ΠΡΟΕΤΟΙΜΑΣΙΑ, ΔΙΑΝΟΜΗ, ΔΙΑΒΙΒΑΣΗ, ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ ΣΧΕΤΙΚΑ ΜΕ ΤΟ ΠΡΟΣΩΠΙΚΟ ΤΩΝ ΜΕΤΑΦΟΡΕΩΝ ΚΑΙ ΣΥΜΠΛΗΡΩΜΑΤΙΚΑ ΑΝΤΙΤΥΠΑ Ή ΜΕΤΑΦΡΑΣΕΙΣ ΚΑΙ ΑΠΟΣΠΑΣΜΑΤΑ ΔΙΑΒΑΘΜΙΣΜΕΝΩΝ ΕΓΓΡΑΦΩΝ ΕΕ

21.1. **Προετοιμασία**

1. Η διαβαθμίσεις ΕΕ εφαρμόζονται όπως ορίζεται στο τμήμα 16 και για τη διαβάθμιση ►**M1** CONFIDENTIEL UE ◄ ή υψηλότερη, εμφαίνονται στο κέντρο του άνω και του κάτω μέρους κάθε σελίδας, ενώ κάθε σελίδα πρέπει να αριθμείται. Κάθε διαβαθμισμένο έγγραφο ΕΕ φέρει αριθμό αναφοράς και ημερομηνία. Στα έγγραφα με διαβάθμιση ►**M1** TRES SECRET UE/EU TOP SECRET ◄ ή ►**M1** SECRET UE ◄, ο εν λόγω αριθμός αναφοράς εμφαίνεται σε κάθε σελίδα. Εάν τα έγγραφα πρόκειται να διανεμηθούν σε πολλαπλά αντίτυπα, στην πρώτη σελίδα κάθε αντιτύπου αναγράφεται ο αριθμός αντιτύπου και ο συνολικός αριθμός σελίδων. Στην πρώτη σελίδα των εγγράφων που είναι διαβαθμισμένα τουλάχιστον ως ►**M1** CONFIDENTIEL UE ◄, πρέπει να αναφέρονται όλα τα παραρτήματα και τα συνημμένα έγγραφα.

2. Τα έγγραφα που διαβαθμίζονται τουλάχιστον ως ►**M1** CONFIDENTIEL UE ◄ πρέπει να δακτυλογραφούνται, να μεταφράζονται, να αποθηκεύονται, να φωτοαντιγράφονται, να αναπαράγονται μαγνητικά ή να αντιγράφονται σε μικροφίλμ, μόνον από άτομα διαβαθμισμένα για πρόσβαση σε πληροφορίες ΕΕ, διαβαθμισμένες τουλάχιστον μέχρι τον κατάλληλο βαθμό ασφαλείας του συγκεκριμένου εγγράφου.

3. Οι διατάξεις που διέπουν την αναπαραγωγή διαβαθμισμένων εγγράφων μέσω υπολογιστή καθορίζονται στο τμήμα 25.

21.2. **Διανομή**

1. Οι διαβαθμισμένες πληροφορίες ΕΕ διανέμονται μόνον σε άτομα που πρέπει να τις γνωρίζουν και έχουν την κατάλληλη διαβάθμιση ασφαλείας. Η αρχική διανομή καθορίζεται από τον αρχικό συντάκτη.

2. Τα έγγραφα με διαβάθμιση ►**M1** TRES SECRET UE/EU TOP SECRET ◄ κυκλοφορούν μέσω των γραμματειών ►**M1** TRES SECRET UE/EU TOP SECRET ◄ (βλέπε τμήμα 22.2). Όσον αφορά τα μηνύματα ►**M1** TRES SECRET UE/EU TOP SECRET ◄, η αρμόδια γραμματεία μπορεί να επιτρέπει στον προϊστάμενο του κέντρου επικοινωνιών να παράγει τον αριθμό αντιγράφων που ορίζεται στον κατάλογο παραληπτών.

3. Τα έγγραφα με διαβάθμιση έως ►**M1** SECRET UE ◄, επιτρέπεται να αναδιανέμονται από τον αρχικό παραλήπτη σε άλλους παραλήπτες ανάλογα με την ανάγκη να λάβουν γνώση. Ωστόσο, οι συντάκτριες αρχές αναφέρουν σαφώς τις τυχόν υποχρεώσεις γνωστοποίησης που επιθυμούν να επιβάλλουν. Όταν επιβάλλονται οι εν λόγω υποχρεώσεις γνωστοποίησης, οι παραλήπτες αναδιανέμουν τα έγγραφα μόνον με την άδεια των συντακτριών αρχών.

4. Κάθε έγγραφο με διαβάθμιση ►**M1** CONFIDENTIEL UE ◄ ή υψηλότερη, καταγράφεται, κατά την είσοδό του ή την έξοδό του από μια ΓΔ ή υπηρεσία, από την οικεία Γραμματεία ΔΠΕΕ της υπηρεσίας. Τα στοιχεία που καταγράφονται (αριθμός αναφοράς, ημερομηνία και, κατά περίπτωση, αριθμός αντιτύπου) πρέπει να επαρκούν για την αναγνώριση των εγγράφων και να καταχωρούνται σε μητρώο ή σε ειδικό και προστατευμένο ηλεκτρονικό μέσο (βλέπε τμήμα 22.1).

21.3. **Διαβίβαση διαβαθμισμένων εγγράφων ΕΕ**

21.3.1. *Συσκευασία και αποδείξεις παραλαβής*

1. Τα έγγραφα με διαβάθμιση τουλάχιστον ►**M1** CONFIDENTIEL UE ◄ διαβιβάζονται εντός ανθεκτικών και αδιαφανών διπλών φακέλων. Στον εσωτερικό φάκελο αναγράφεται η ενδεδειγμένη διαβάθμιση ασφαλείας ΕΕ καθώς και, εφόσον είναι δυνατόν, η πλήρης υπηρεσιακή ιδιότητα και διεύθυνση του αποδέκτη.

2. Μόνον ένας ελεγκτικός υπάλληλος γραμματείας (βλέπε τμήμα 22.1) ή ο αναπληρωτής του επιτρέπεται να ανοίγουν τον εσωτερικό φάκελο και να χορηγούν απόδειξη παραλαβής των εγγράφων που περιέχει, εκτός εάν ο φάκελος απευθύνεται σε συγκεκριμένο παραλήπτη. Στην περίπτωση αυτήν, η αρμόδια γραμματεία (βλέπε τμήμα 22.1) πρωτοκολλά την άφιξη του φακέλου, μόνον δε ο παραλήπτης επιτρέπεται να ανοίγει τον εσωτερικό φάκελο και να χορηγεί απόδειξη παραλαβής για τα έγγραφα που περιέχει.

3. Ο εσωτερικός φάκελος πρέπει να περιέχει έντυπο απόδειξης. Η απόδειξη, η οποία δεν είναι διαβαθμισμένη, πρέπει να αναγράφει τον αριθμό αναφοράς, την ημερομηνία και τον αριθμό αντιτύπου του εγγράφου αλλά ποτέ το θέμα του.

4. Ο εσωτερικός φάκελος τίθεται εντός του εξωτερικού φακέλου, ο οποίος φέρει αριθμό δέματος για να είναι δυνατόν να χορηγείται απόδειξη παραλαβής. Ο βαθμός ασφαλείας δεν αναγράφεται ποτέ στον εξωτερικό φάκελο.

▼B

5. Για τα έγγραφα με διαβάθμιση τουλάχιστον ►M1 CONFIDENTIEL UE ◄, οι μεταφορείς και οι αγγελιαφόροι λαμβάνουν αποδείξεις με τον αριθμό δέματος.

21.3.2. *Διαβίβαση στο εσωτερικό ενός κτιρίου ή μιας ομάδας κτιρίων*

Εντός ενός συγκεκριμένου κτιρίου ή ομάδας κτιρίων, τα διαβαθμισμένα έγγραφα επιτρέπεται να μεταφέρονται εντός σφραγισμένου φακέλου που φέρει μόνον το όνομα του παραλήπτη, υπό την προϋπόθεση ότι μεταφέρονται από άτομα διαβαθμισμένα για τον αντίστοιχο βαθμό ασφαλείας των εγγράφων.

21.3.3. *Διαβίβαση στο εσωτερικό μιας χώρας*

1. Εντός μιας χώρας, τα έγγραφα με διαβάθμιση ►M1 TRES SECRET UE/EU TOP SECRET ◄ πρέπει να αποστέλλονται μόνο μέσω επίσημης υπηρεσίας αγγελιοφόρων ή μέσω ατόμων τα οποία έχουν εξουσιοδοτημένη πρόσβαση σε πληροφορίες ►M1 TRES SECRET UE/EU TOP SECRET ◄.

2. Όταν χρησιμοποιείται υπηρεσία αγγελιοφόρων για τη διαβίβαση ενός εγγράφου ►M1 TRES SECRET UE/EU TOP SECRET ◄, εκτός των ορίων ενός κτιρίου ή συγκροτήματος κτιρίων, πρέπει να τηρούνται οι διατάξεις του παρόντος κεφαλαίου περί συσκευασίας και απόδειξης παραλαβής. Οι υπηρεσίες παράδοσης πρέπει να διαθέτουν το κατάλληλο προσωπικό ώστε να εξασφαλίζεται ότι τα δέματα που περιέχουν έγγραφα ►M1 TRES SECRET UE/EU TOP SECRET ◄, να παραμένουν συνεχώς υπό την άμεση εποπτεία αρμόδιου υπαλλήλου.

3. Κατ' εξαίρεση, επιτρέπεται να μεταφέρουν έγγραφα ►M1 TRES SECRET UE/EU TOP SECRET ◄ εκτός των ορίων ενός κτιρίου ή ομάδας κτιρίων, άλλοι υπάλληλοι πλην των αγγελιοφόρων, προκειμένου να τα χρησιμοποιούν επιτόπου σε συνεδριάσεις και συζητήσεις, εφόσον:

   α) ο κομιστής έχει εξουσιοδοτημένη πρόσβαση στα εν λόγω έγγραφα ►M1 TRES SECRET UE/EU TOP SECRET ◄·

   β) ο τρόπος μεταφοράς πληροί τους εθνικούς κανόνες που διέπουν τη διαβίβαση εγγράφων με διαβάθμιση ►M1 TRES SECRET UE/EU TOP SECRET ◄·

   γ) ο υπάλληλος δεν εγκαταλείπει ποτέ αφύλακτα τα έγγραφα ►M1 TRES SECRET UE/EU TOP SECRET ◄·

   δ) λαμβάνονται μέτρα ώστε να τηρείται κατάλογος των μεταφερόμενων εγγράφων και να πρωτοκολλείται στη Γραμματεία ►M1 TRES SECRET UE/EU TOP SECRET ◄ που κατέχει τα έγγραφα, και να αντιπαραβάλλεται προς την καταγραφή αυτήν κατά την επιστροφή τους.

4. Εντός μιας συγκεκριμένης χώρας, τα έγγραφα ►M1 SECRET UE ◄ και ►M1 CONFIDENTIEL UE ◄ επιτρέπεται να αποστέλλονται είτε με το ταχυδρομείο, εφόσον η διαβίβαση αυτή επιτρέπεται δυνάμει εθνικών κανονισμών και συμφωνεί με τις διατάξεις τους, είτε από υπηρεσία αγγελιοφόρων ή από πρόσωπα που έχουν εξουσιοδοτημένη πρόσβαση σε διαβαθμισμένες πληροφορίες ΕΕ.

5. Με βάση τους κανόνες αυτούς, η ►M2 Διεύθυνση Ασφαλείας της Επιτροπής ◄ θα προβεί στη σύνταξη οδηγιών σχετικά με την προσωπική μεταφορά διαβαθμισμένων εγγράφων ΕΕ. Ο κομιστής υποχρεούται να διαβάζει και να υπογράφει τις οδηγίες αυτές. Ειδικότερα, οι οδηγίες πρέπει να καθιστούν σαφές ότι τα έγγραφα ουδέποτε:

   α) εγκαταλείπονται από τον κομιστή, εκτός εάν φυλάσσονται ασφαλώς σύμφωνα με τις διατάξεις του τμήματος 18·

   β) εγκαταλείπονται αφύλακτα σε συγκοινωνιακά μέσα ή ιδιωτικά οχήματα, ή σε δημόσιους χώρους όπως εστιατόρια ή ξενοδοχεία. Τα έγγραφα απαγορεύεται να αποθηκεύονται σε χρηματοκιβώτια ξενοδοχείων ή να εγκαταλείπονται αφύλακτα σε δωμάτια ξενοδοχείων·

   γ) διαβάζονται σε δημόσιους χώρους, όπως αεροσκάφη ή τρένα.

21.3.4. *Διαβίβαση από ένα κράτος σε άλλο*

1. Το υλικό που έχει διαβάθμιση τουλάχιστον ►M1 CONFIDENTIEL UE ◄ πρέπει να μεταφέρεται μέσω υπηρεσιών διπλωματικών ΕΕ ή στρατιωτικών μεταφορών.

2. Ωστόσο, είναι δυνατόν να επιτρέπεται η αυτοπρόσωπη μεταφορά υλικού διαβαθμισμένου ως ►M1 SECRET UE ◄ ή ►M1 CONFIDENTIEL UE ◄, εάν οι συνθήκες μεταφοράς εξασφαλίζουν ότι δεν είναι δυνατόν να περιπέσουν στα χέρια μη εξουσιοδοτημένου ατόμου.

3. Το αρμόδιο για θέματα ασφαλείας μέλος της Επιτροπής δύναται να επιτρέπει την αυτοπρόσωπη μεταφορά όταν δεν υπάρχουν διπλωματικοί ή στρατιωτικοί μεταφορείς ή όταν η χρήση των μεταφορέων αυτών θα οδηγούσε σε καθυστέρηση που θα έβλαπτε τις δραστηριότητες της ΕΕ και ο παραλήπτης χρειάζεται επειγόντως το συγκεκριμένο υλικό. Η ►M2 Διεύθυνση Ασφαλείας της Επιτροπής ◄ θα εκπονήσει οδηγίες για την αυτοπρόσωπη μεταφορά,

▼B

διεθνώς, υλικού διαβαθμισμένου μέχρι και ►M1 SECRET UE ◄, από άλλα πρόσωπα πλην των διπλωματικών και στρατιωτικών μεταφορέων. Βάσει των οδηγιών αυτών πρέπει να απαιτείται:

α) ο κομιστής να έχει την κατάλληλη διαβάθμιση ασφαλείας·

β) να καταγράφονται, στην κατάλληλη υπηρεσία ή γραμματεία, όλα τα υλικά που μεταφέρονται κατ' αυτόν τον τρόπο·

γ) να φέρουν τα δέματα ή οι σάκοι που περιέχουν υλικό ΕΕ, επίσημη σφραγίδα που να εμποδίζει ή να αποτρέπει τον έλεγχο από τελωνεία, καθώς και ετικέτες με αναγνωριστικά στοιχεία και οδηγίες προς τον ανευρίσκοντα·

δ) να φέρει ο κομιστής πιστοποιητικό αγγελιαφόρου ή/και εντολή αποστολής, αναγνωρισμένη από όλα τα κράτη μέλη της ΕΕ, που να τον εξουσιοδοτεί να μεταφέρει το συγκεκριμένο δέμα·

ε) κατά τη χερσαία μεταφορά, να μην πραγματοποιείται διέλευση από κράτος που δεν είναι μέλος της ΕΕ ή από τα σύνορά του, εκτός εάν το κράτος αποστολής έχει λάβει ειδικές εγγυήσεις από το εν λόγω κράτος·

στ) οι ταξιδιωτικές ρυθμίσεις του κομιστή όσον αφορά τους προορισμούς, τα ακολουθούμενα δρομολόγια και τα χρησιμοποιούμενα μεταφορικά μέσα, να συμφωνούν με τους κανόνες της ΕΕ ή — εάν οι σχετικοί εθνικοί κανονισμοί είναι αυστηρότεροι — να συμφωνούν με τους εν λόγω κανονισμούς·

ζ) να παραμείνει διαρκώς το υλικό στην κατοχή του κομιστή, εκτός εάν φυλάσσεται σύμφωνα με τις διατάξεις περί ασφαλούς φύλαξης του τμήματος 18·

η) να μην εγκαταλείπεται το υλικό αφύλακτο σε δημόσια ή ιδιωτικά οχήματα ή σε δημόσιους χώρους όπως εστιατόρια ή ξενοδοχεία· Το υλικό δεν πρέπει να τίθεται σε χρηματοκιβώτια ξενοδοχείων ούτε να εγκαταλείπεται αφύλακτο σε δωμάτια ξενοδοχείων·

θ) αν το μεταφερόμενο υλικό περιέχει έγγραφα, να μην διαβάζονται τα έγγραφα αυτά σε δημόσιους χώρους (π.χ. αεροσκάφη, τρένα κ.λπ.).

4. Το άτομο στο οποίο ανατίθεται η μεταφορά διαβαθμισμένου υλικού πρέπει να διαβάζει και να υπογράφει τις οδηγίες ασφαλείας οι οποίες περιέχουν, τουλάχιστον, τις προαναφερόμενες οδηγίες και τις ακολουθητέες διαδικασίες σε περίπτωση έκτακτης ανάγκης ή όταν τελωνειακοί υπάλληλοι ή υπάλληλοι ασφαλείας αερολιμένων ζητούν να εξετάσουν το δέμα που περιέχει το διαβαθμισμένο υλικό.

21.3.5. *Διαβίβαση διαβαθμισμένων «εγγράφων ΕΕ»*

Για τη μεταφορά εγγράφων ►M1 RESTREINT UE ◄ δεν προβλέπονται ειδικές διατάξεις, πλην του ότι οι συνθήκες μεταφοράς πρέπει να εξασφαλίζουν ότι τα έγγραφα να είναι αδύνατον να πέσουν στα χέρια μη εξουσιοδοτημένων ατόμων.

21.4. **Μέτρα ασφαλείας σχετικά με το προσωπικό των μεταφορέων**

Όλοι οι μεταφορείς και αγγελιοφόροι που απασχολούνται με τη μεταφορά εγγράφων με διαβάθμιση ►M1 SECRET UE ◄ και ►M1 CONFIDENTIEL UE ◄, πρέπει να διαθέτουν την κατάλληλη διαβάθμιση ασφαλείας.

21.5. **Ηλεκτρονικά και άλλα μέσα τεχνικής διαβίβασης**

1. Τα μέτρα ασφαλείας για τις επικοινωνίες, αποσκοπούν στην εξασφάλιση της ασφαλούς διαβίβασης διαβαθμισμένων πληροφοριών ΕΕ. Οι λεπτομερείς κανόνες για την διαβίβαση των εν λόγω διαβαθμισμένων πληροφοριών ΕΕ εμφαίνονται στο τμήμα 25.

2. Μόνον δεόντως διαπιστευμένα κέντρα επικοινωνιών και δίκτυα ή/και τερματικά και συστήματα, επιτρέπεται να διαβιβάζουν πληροφορίες με διαβάθμιση ►M1 CONFIDENTIEL UE ◄ και ►M1 SECRET UE ◄.

21.6. **Συμπληρωματικά αντίγραφα, μεταφράσεις και αποσπάσματα διαβαθμισμένων εγγράφων ΕΕ**

1. Μόνον ο αρχικός συντάκτης μπορεί να επιτρέπει την αντιγραφή ή τη μετάφραση εγγράφων με διαβάθμιση ►M1 TRES SECRET UE/EU TOP SECRET ◄.

2. Εάν άτομα χωρίς διαβάθμιση ►M1 TRES SECRET UE/EU TOP SECRET ◄ χρειάζονται πληροφορίες οι οποίες, μολονότι περιέχονται σε έγγραφο ►M1 TRES SECRET UE/EU TOP SECRET ◄, δεν έχουν την διαβάθμιση αυτή, είναι δυνατόν να επιτραπεί στον προϊστάμενο της Γραμματείας ►M1 TRES SECRET UE/EU TOP SECRET ◄ (βλέπε τμήμα 22.2), να παράγει τον απαιτούμενο αριθμό αποσπασμάτων από το έγγραφο αυτό. Ταυτόχρονα, ο προϊστάμενος αυτός λαμβάνει τα απαιτούμενα μέτρα για να εξασφαλίσει ότι στα αποσπάσματα αυτά αποδίδεται η κατάλληλη διαβάθμιση ασφαλείας.

▼B

3. Τα έγγραφα με διαβάθμιση έως ►M1 SECRET UE ◄, επιτρέπεται να αναπαράγονται και να μεταφράζονται από τον παραλήπτη, στο πλαίσιο των εθνικών κανονισμών ασφαλείας και υπό τον όρο ότι τηρείται αυστηρά η αρχή «ανάγκη γνώσης». Τα μέτρα ασφαλείας που εφαρμόζονται για το αρχικό έγγραφο εφαρμόζονται και στα αντίγραφα ή/και μεταφράσεις του.

22. ΓΡΑΜΜΑΤΕΙΕΣ ΔΠΕΕ, ΑΠΟΓΡΑΦΕΣ, ΑΡΧΕΙΟΘΕΤΗΣΗ ΚΑΙ ΚΑΤΑΣΤΡΟΦΗ ΔΠΕΕ

22.1. **Τοπικές γραμματείες ΔΠΕΕ**

1. Σε κάθε υπηρεσία εντός της Επιτροπής, ανάλογα με τις ανάγκες, μία ή περισσότερες τοπικές γραμματείες ΔΠΕΕ θα είναι αρμόδιες για την καταγραφή, την αναπαραγωγή, την αποστολή, την αρχειοθέτηση και την καταστροφή εγγράφων με διαβάθμιση ►M1 SECRET UE ◄ και ►M1 CONFIDENTIEL UE ◄.
2. Εφόσον μια υπηρεσία δεν διαθέτει τοπική γραμματεία ΔΠΕΕ, θα ενεργεί ως γραμματεία ΔΠΕΕ, η τοπική γραμματεία ΔΠΕΕ της Γενικής Γραμματείας.
3. Οι τοπικές γραμματείες ΔΠΕΕ υπάγονται στον προϊστάμενο της υπηρεσίας από τον οποίο λαμβάνουν εντολές. Ο προϊστάμενος των εν λόγω γραμματειών είναι ο ελεγκτικός υπάλληλος γραμματείας (ΕΥΓ).
4. Υπόκεινται στον έλεγχο του τοπικού υπευθύνου ασφαλείας, όσον αφορά την εφαρμογή των διατάξεων για το χειρισμό εγγράφων ΔΠΕΕ και την τήρηση των σχετικών μέτρων ασφαλείας.
5. Οι υπάλληλοι που είναι τοποθετημένοι στις τοπικές γραμματείες ΔΠΕΕ έχουν εξουσιοδοτημένη πρόσβαση σε ΔΠΕΕ σύμφωνα με το τμήμα 20.
6. Υπό την εποπτεία των προϊσταμένων των σχετικών υπηρεσιών, οι τοπικές γραμματείες ΔΠΕΕ:
   α) διαχειρίζονται τις εργασίες καταχώρησης, αναπαραγωγής, μετάφρασης, διαβίβασης, αποστολής και καταστροφής των πληροφοριών αυτών·
   β) ενημερώνουν τα μητρώα για τις διαβαθμισμένες πληροφορίες·
   γ) ερωτούν περιοδικώς τους συντάκτες των πληροφοριών σχετικά με την ανάγκη διατήρησης του χαρακτηρισμού των πληροφοριών.
7. Η τοπική γραμματεία ΔΠΕΕ τηρεί μητρώο των ακόλουθων στοιχείων:
   α) ημερομηνία παραγωγής των διαβαθμισμένων πληροφοριών·
   β) βαθμός ασφαλείας·
   γ) ημερομηνία λήξης του χαρακτηρισμού·
   δ) ονοματεπώνυμο και υπηρεσία του συντάκτη·
   ε) αποδέκτης ή αποδέκτες, με αύξοντα αριθμό·
   στ) το θέμα·
   ζ) αριθμός·
   η) αριθμός των αντιτύπων που έχουν διανεμηθεί·
   θ) απογραφή των διαβαθμισμένων πληροφοριών που υποβάλλονται στην υπηρεσία·
   ι) μητρώο αποχαρακτηρισμού και υποχαρακτηρισμού διαβαθμισμένων πληροφοριών.
8. Οι γενικοί κανόνες που προβλέπονται στο τμήμα 21 ισχύουν για την τοπική γραμματεία ΔΠΕΕ της Επιτροπής, εκτός εάν τροποποιούνται από τους ειδικούς κανόνες του παρόντος τμήματος.

22.2. **Γραμματεία ►M1 TRES SECRET UE/EU TOP SECRET ◄**

22.2.1. *Γενικά*

1. Μια κεντρική γραμματεία ►M1 TRES SECRET UE/EU TOP SECRET ◄ διασφαλίζει την καταγραφή, τη διεκπεραίωση και τη διανομή των εγγράφων ►M1 TRES SECRET UE/EU TOP SECRET ◄ σύμφωνα με τις διατάξεις περί ασφαλείας. Ο προϊστάμενος της γραμματείας ►M1 TRES SECRET UE/EU TOP SECRET ◄ είναι ο ελεγκτικός υπάλληλος γραμματείας ►M1 TRES SECRET UE/EU TOP SECRET ◄.
2. Η κεντρική γραμματεία ►M1 TRES SECRET UE/EU TOP SECRET ◄ λειτουργεί ως η κύρια αρχή παραλαβής και αποστολής στην Επιτροπή, με άλλα θεσμικά όργανα της ΕΕ, διεθνείς οργανισμούς και τρίτα κράτη με τα οποία η Επιτροπή έχει συμφωνίες επί διαδικασιών ασφαλείας για την ανταλλαγή διαβαθμισμένων πληροφοριών.
3. Εφόσον απαιτείται, συγκροτούνται υπογραμματείες αρμόδιες για την εσωτερική διαχείριση των εγγράφων ►M1 TRES SECRET UE/EU TOP SECRET ◄· οι υπογραμματείες τηρούν ενημερωμένα αρχεία της κυκλοφορίας κάθε εγγράφου για το οποίο είναι υπεύθυνες.

▼B

4. Οι υπογραμματείες ►M1 TRES SECRET UE/EU TOP SECRET ◄ συγκροτούνται όπως προβλέπεται στο τμήμα 22.2.3 για την κάλυψη μακροπρόθεσμων αναγκών και εξαρτώνται από κεντρική γραμματεία ►M1 TRES SECRET UE/EU TOP SECRET ◄. Εάν χρειάζεται μόνον προσωρινή και περιστασιακή πρόσβαση σε έγγραφα ►M1 TRES SECRET UE/EU TOP SECRET ◄, τα έγγραφα αυτά επιτρέπεται να κυκλοφορούν χωρίς να συγκροτείται υπογραμματεία ►M1 TRES SECRET UE/EU TOP SECRET ◄, υπό την προϋπόθεση ότι θεσπίζονται κανόνες για να εξασφαλίζεται ότι τα έγγραφα αυτά παραμένουν υπό τον έλεγχο της ενδεδειγμένης γραμματείας ►M1 TRES SECRET UE/EU TOP SECRET ◄ και ότι τηρούνται όλα τα μέτρα υλικής ασφάλειας και ασφάλειας προσωπικού.

5. Οι υπογραμματείες δεν διαβιβάζουν έγγραφα ►M1 TRES SECRET UE/EU TOP SECRET ◄ απευθείας σε άλλες υπογραμματείες της ίδιας κεντρικής γραμματείας ►M1 TRES SECRET UE/EU TOP SECRET ◄ χωρίς τη ρητή της άδεια.

6. Όλες οι ανταλλαγές εγγράφων ►M1 TRES SECRET UE/EU TOP SECRET ◄ μεταξύ υπογραμματειών που δεν υπάγονται στην ίδια κεντρική γραμματεία πρέπει να δρομολογούνται μέσω των κεντρικών γραμματειών ►M1 TRES SECRET UE/EU TOP SECRET ◄.

22.2.2. *Κεντρική γραμματεία* ►M1 *TRES SECRET UE/EU TOP SECRET* ◄

Ως ο ελεγκτικός υπάλληλος, ο προϊστάμενος της κεντρικής γραμματείας ►M1 TRES SECRET UE/EU TOP SECRET ◄ είναι αρμόδιος για:

α) τη διαβίβαση εγγράφων ►M1 TRES SECRET UE/EU TOP SECRET ◄ σύμφωνα με τις διατάξεις που ορίζονται στο τμήμα 21.3·

β) την τήρηση καταλόγου όλων των εξαρτώμενων από αυτόν υπογραμματειών ►M1 TRES SECRET UE/EU TOP SECRET ◄ καθώς και των ονομάτων και των υπογραφών των διορισμένων ελεγκτικών υπαλλήλων και των εξουσιοδοτημένων αναπληρωτών τους·

γ) τη διατήρηση των αποδείξεων από τα μητρώα για όλα τα έγγραφα ►M1 TRES SECRET UE/EU TOP SECRET ◄ που διανέμει η κεντρική γραμματεία·

δ) τη διατήρηση αρχείου των διατηρούμενων και διανεμόμενων εγγράφων ►M1 TRES SECRET UE/EU TOP SECRET ◄·

ε) την τήρηση ενημερωμένου καταλόγου όλων των κεντρικών γραμματειών ►M1 TRES SECRET UE/EU TOP SECRET ◄ με τις οποίες αλληλογραφεί συνήθως, καθώς και των ονομάτων και των υπογραφών των διορισμένων ελεγκτικών υπαλλήλων τους και των εξουσιοδοτημένων αναπληρωτών τους·

στ) την υλική διαφύλαξη όλων των εγγράφων ►M1 TRES SECRET UE/EU TOP SECRET ◄ που έχει στην κατοχή της η γραμματεία σύμφωνα με τους κανονισμούς του τμήματος 18.

22.2.3. *Υπογραμματεία* ►M1 *TRES SECRET UE/EU TOP SECRET* ◄

Ως ο ελεγκτικός υπάλληλος, ο προϊστάμενος μιας υπογραμματείας ►M1 TRES SECRET UE/EU TOP SECRET ◄ είναι αρμόδιος για:

α) τη διαβίβαση εγγράφων ►M1 TRES SECRET UE/EU TOP SECRET ◄ σύμφωνα με τις διατάξεις του τμήματος 21.3·

β) την τήρηση ενημερωμένου καταλόγου όλων των ατόμων που είναι εξουσιοδοτημένα να έχουν πρόσβαση σε πληροφορίες ►M1 TRES SECRET UE/EU TOP SECRET ◄ υπό τον έλεγχό του·

γ) τη διανομή εγγράφων ►M1 TRES SECRET UE/EU TOP SECRET ◄ σύμφωνα με τις οδηγίες του συντάκτη ή βάσει της αρχής «ανάγκη γνώσης», αφού ελέγξει πρώτα ότι ο παραλήπτης διαθέτει την απαιτούμενη διαβάθμιση ασφαλείας·

δ) την τήρηση ενημερωμένου αρχείου όλων των εγγράφων ►M1 TRES SECRET UE/EU TOP SECRET ◄ τα οποία διατηρούνται ή διανέμονται υπό τον έλεγχό του ή τα οποία έχουν διαβιβαστεί σε άλλες γραμματείες ►M1 TRES SECRET UE/EU TOP SECRET ◄, και τη διατήρηση όλων των σχετικών αποδείξεων·

ε) την τήρηση ενημερωμένου καταλόγου των γραμματειών ►M1 TRES SECRET UE/EU TOP SECRET ◄ με τις οποίες του επιτρέπεται να ανταλλάσσει έγγραφα ►M1 TRES SECRET UE/EU TOP SECRET ◄, καθώς και των ονομάτων και των υπογραφών των ελεγκτικών υπαλλήλων τους και των εξουσιοδοτημένων αναπληρωτών τους·

στ) την υλική διαφύλαξη όλων των εγγράφων ►M1 TRES SECRET UE/EU TOP SECRET ◄ που έχει στην κατοχή της η υπογραμματεία σύμφωνα με τους κανονισμούς του τμήματος 18.

▼B

22.3. **Απογραφές και έλεγχοι διαβαθμισμένων εγγράφων ΕΕ**

1. Ανά έκαστο έτος, κάθε γραμματεία ►M1 TRES SECRET UE/EU TOP SECRET ◄ που αναφέρεται στο παρόν τμήμα διεξάγει αναλυτική απογραφή των εγγράφων ►M1 TRES SECRET UE/EU TOP SECRET ◄. Ένα έγγραφο θεωρείται εντάξει εάν η γραμματεία έχει όντως στην κατοχή της το έγγραφο, ή διαθέτει απόδειξη παραλαβής από τη γραμματεία ►M1 TRES SECRET UE/EU TOP SECRET ◄ στην οποία έχει μεταφερθεί το έγγραφο, πρωτόκολλο καταστροφής του εγγράφου ή εντολή υποχαρακτηρισμού ή αποχαρακτηρισμού του εγγράφου. Οι γραμματείες διαβιβάζουν τα αποτελέσματα των ετήσιων απογραφών στο αρμόδιο επί θεμάτων ασφαλείας μέλος της Επιτροπής, πριν από την 1η Απριλίου κάθε έτους.

2. Οι υπογραμματείες ►M1 TRES SECRET UE/EU TOP SECRET ◄ διαβιβάζουν τα αποτελέσματα της ετήσιας απογραφής τους στην κεντρική γραμματεία στην οποία λογοδοτούν, σε ημερομηνία την οποία ορίζει η τελευταία.

3. Τα έγγραφα με διαβάθμιση ΕΕ κατώτερη του ►M1 TRES SECRET UE/EU TOP SECRET ◄ υποβάλλονται σε εσωτερικό έλεγχο σύμφωνα με τις οδηγίες του αρμόδιου επί θεμάτων ασφαλείας μέλους της Επιτροπής.

4. Οι εργασίες αυτές επιτρέπουν να λαμβάνεται η γνώμη των κατόχων όσον αφορά:

   α) τη δυνατότητα υποχαρακτηρισμού ή αποχαρακτηρισμού ορισμένων εγγράφων·

   β) τα προς καταστροφή έγγραφα.

22.4. **Αρχειοθέτηση διαβαθμισμένων πληροφοριών ΕΕ**

1. Οι ΔΠΕΕ αποθηκεύονται υπό προϋποθέσεις ανταποκρινόμενες σε όλες τις απαριθμούμενες στο τμήμα 18 σχετικές απαιτήσεις.

2. Προκειμένου να ελαχιστοποιούνται τα προβλήματα αποθήκευσης, επιτρέπεται στους ελεγκτικούς υπαλλήλους όλων των γραμματειών να αναπαράγουν σε μικροφίλμ ή να αποθηκεύουν κατ' άλλο τρόπο σε μαγνητικό ή οπτικό υπόθεμα προς αρχειοθέτηση έγγραφα με διαβάθμιση ►M1 TRES SECRET UE/EU TOP SECRET ◄, ►M1 SECRET UE ◄ και ►M1 CONFIDENTIEL UE ◄, εφόσον:

   α) οι εργασίες παραγωγής μικροφίλμ ή αποθήκευσης εκτελούνται από προσωπικό με ισχύουσα διαβάθμιση για τον αντίστοιχο ενδεδειγμένο βαθμό ασφαλείας·

   β) το υπόθεμα μικροφίλμ/αποθήκευσης προστατεύεται εξίσου ασφαλώς όπως και τα πρωτότυπα έγγραφα·

   γ) η παραγωγή μικροφίλμ/αποθήκευση των εγγράφων ►M1 TRES SECRET UE/EU TOP SECRET ◄ γνωστοποιείται στο συντάκτη·

   δ) οι ρόλοι φωτογραφικής ταινίας ή οι άλλοι τύποι υποθέματος περιέχουν μόνον έγγραφα με την ίδια διαβάθμιση ►M1 TRES SECRET UE/EU TOP SECRET ◄, ►M1 SECRET UE ◄ ή ►M1 CONFIDENTIEL UE ◄·

   ε) η αναπαραγωγή σε μικροφίλμ/αποθήκευση ενός εγγράφου ►M1 TRES SECRET UE/EU TOP SECRET ◄ ή ►M1 SECRET UE ◄ αναφέρεται σαφώς στο μητρώο που χρησιμοποιείται για την ετήσια απογραφή·

   στ) τα πρωτότυπα έγγραφα, από τα οποία παρήχθησαν μικροφίλμ ή τα οποία αποθηκεύθηκαν κατ' άλλον τρόπο, καταστρέφονται σύμφωνα με τους κανόνες που παρατίθενται στο τμήμα 22.5.

3. Οι κανόνες αυτοί εφαρμόζονται και σε κάθε άλλη επιτρεπόμενη μορφή αποθήκευσης, όπως ηλεκτρομαγνητικά υποθέματα και δίσκοι οπτικής ανάγνωσης.

22.5. **Καταστροφή διαβαθμισμένων εγγράφων ΕΕ**

1. Για να αποφεύγεται η περιττή συσσώρευση διαβαθμισμένων εγγράφων ΕΕ, όσα έγγραφα είναι πεπαλαιωμένα και, κατά τη γνώμη του προϊσταμένου της υπηρεσίας στην κατοχή της οποίας ευρίσκονται, πλεονάζουν, καταστρέφονται το συντομότερο δυνατό ως εξής:

   α) τα έγγραφα ►M1 TRES SECRET UE/EU TOP SECRET ◄ καταστρέφονται μόνον από την αρμόδια για τη διαβάθμιση αυτή κεντρική γραμματεία. Κάθε καταστρεφόμενο έγγραφο πρέπει να καταγράφεται σε πρωτόκολλο καταστροφής, το οποίο υπογράφεται από τον ελεγκτικό υπάλληλο ►M1 TRES SECRET UE/EU TOP SECRET ◄ και από τον υπάλληλο ο οποίος παρίσταται κατά την καταστροφή και ο οποίος πρέπει να έχει διαβάθμιση ►M1 TRES SECRET UE/EU TOP SECRET ◄. Σχετική σημείωση καταχωρείται στο βιβλίο ημερολογίου·

   β) η γραμματεία διατηρεί τα πρωτόκολλα καταστροφής, μαζί με τα φύλλα διανομής, επί δέκα έτη. Αντίγραφά τους αποστέλλονται στο συντάκτη ή στην αρμόδια κεντρική γραμματεία μόνον όταν ζητούνται ρητώς·

▼B

γ) τα έγγραφα ►M1 TRES SECRET UE/EU TOP SECRET ◄, καθώς και η πάσης φύσεως διαβαθμισμένη φύρα που προκύπτει από τη σύνταξη εγγράφων ►M1 TRES SECRET UE/EU TOP SECRET ◄, όπως κακέκτυπα αντίγραφα, σχέδια εγγράφων, δακτυλογραφημένα σημειώματα και δισκέτες Η/Υ, καταστρέφονται υπό την επίβλεψη ελεγκτικού υπαλλήλου γραμματείας ►M1 TRES SECRET UE/EU TOP SECRET ◄, με καύση, πολτοποίηση, θρυμματισμό με ψαλίδισμα ή καθ' οιονδήποτε άλλο τρόπο που τα μετατρέπει σε μη αναγνωρίσιμη και μη ανασυστάσιμη μορφή.

2. Τα έγγραφα ►M1 SECRET UE ◄ καταστρέφονται από την αρμόδια για τη διαβάθμιση αυτή γραμματεία, υπό την επίβλεψη ατόμου με ανάλογη διαβάθμιση ασφαλείας, με μια από τις μεθόδους που αναφέρονται στην παράγραφο 1 στοιχείο γ). Τα καταστρεφόμενα έγγραφα ►M1 SECRET UE ◄ καταγράφονται σε υπογραφόμενο πρωτόκολλο καταστροφής το οποίο διατηρείται από τη γραμματεία, μαζί με τα έντυπα διανομής, επί τρία τουλάχιστον έτη.

3. Τα έγγραφα ►M1 CONFIDENTIEL UE ◄ καταστρέφονται από την αρμόδια για τη διαβάθμιση αυτή γραμματεία, υπό την επίβλεψη ατόμου με ανάλογη διαβάθμιση ασφαλείας, με μια από τις μεθόδους που αναφέρονται στην παράγραφο 1 στοιχείο γ). Η καταστροφή τους καταγράφεται σύμφωνα με τις οδηγίες του αρμόδιου επί θεμάτων ασφαλείας μέλους της Επιτροπής.

4. Τα έγγραφα ►M1 RESTREINT UE ◄ καταστρέφονται από την αρμόδια για τη διαβάθμιση αυτή γραμματεία ή από το χρήστη, σύμφωνα με τις οδηγίες του αρμόδιου επί θεμάτων ασφαλείας μέλους της Επιτροπής.

22.6. **Καταστροφή σε καταστάσεις ανάγκης**

1. Οι υπηρεσίες της Επιτροπής καταρτίζουν σχέδια, βάσει των τοπικών συνθηκών, για τη διασφάλιση του διαβαθμισμένου υλικού ΕΕ σε περίπτωση κρίσης, τα οποία περιλαμβάνουν, εφόσον απαιτείται, σχέδια καταστροφής και εκκένωσης σε κατάσταση ανάγκης. Η Επιτροπή εκδίδει τις οδηγίες που κρίνονται αναγκαίες ώστε να μην περιπέσουν διαβαθμισμένες πληροφορίες ΕΕ εις χείρας μη εξουσιοδοτημένων ατόμων.

2. Οι ρυθμίσεις για τη διασφάλιση ή/και καταστροφή του υλικού ►M1 SECRET UE ◄ και ►M1 CONFIDENTIEL UE ◄ σε περίπτωση κρίσης δεν πρέπει ποτέ να επηρεάζουν αρνητικά τη διασφάλιση ή την καταστροφή υλικού ►M1 TRES SECRET UE/EU TOP SECRET ◄, συμπεριλαμβανομένου του κρυπτογραφικού εξοπλισμού, η μεταχείριση του οποίου έχει προτεραιότητα έναντι κάθε άλλης εργασίας.

3. Τα προς λήψη μέτρα για τη διασφάλιση και την καταστροφή του κρυπτογραφικού εξοπλισμού σε κατάσταση ανάγκης καλύπτονται από ειδικές οδηγίες.

4. Οι οδηγίες χρειάζεται να είναι επί τόπου διαθέσιμες εντός σφραγισμένου φακέλου. Πρέπει να υπάρχουν διαθέσιμα μέσα/εργαλεία για την καταστροφή.

23. ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ ΓΙΑ ΕΙΔΙΚΕΣ ΣΥΝΕΔΡΙΑΣΕΙΣ ΠΡΑΓΜΑΤΟΠΟΙΟΥΜΕΝΕΣ ΕΚΤΟΣ ΤΩΝ ΓΡΑΦΕΙΩΝ ΤΗΣ ΕΠΙΤΡΟΠΗΣ, ΣΤΙΣ ΟΠΟΙΕΣ ΕΜΠΛΕΚΟΝΤΑΙ ΔΙΑΒΑΘΜΙΣΜΕΝΕΣ ΠΛΗΡΟΦΟΡΙΕΣ ΕΕ

23.1. **Γενικά**

Όταν πραγματοποιούνται συνεδριάσεις της Επιτροπής ή άλλες σημαντικές συνεδριάσεις εκτός των γραφείων της Επιτροπής και εφόσον δικαιολογείται από ιδιαίτερες απαιτήσεις ασφαλείας λόγω της ιδιαίτερης ευαισθησίας των προς συζήτηση θεμάτων ή πληροφοριών, λαμβάνονται τα κατωτέρω περιγραφόμενα μέτρα ασφαλείας. Τα μέτρα αυτά αφορούν μόνον την προστασία των διαβαθμισμένων πληροφοριών ΕΕ· ενδέχεται να απαιτείται προγραμματισμός και άλλων μέτρων ασφαλείας.

23.2. **Αρμοδιότητες**

23.2.1. ►M2 *Διεύθυνση Ασφαλείας της Επιτροπής* ◄

Η►M2 Διεύθυνση Ασφαλείας της Επιτροπής ◄ συνεργάζεται με τις αρμόδιες αρχές του κράτους μέλους όπου πραγματοποιείται μια συνεδρίαση (κράτος μέλος υποδοχής) ώστε να κατοχυρώνεται η ασφάλεια των συνεδριάσεων της Επιτροπής ή άλλων σημαντικών συνεδριάσεων, και για την ασφάλεια των μελών και του προσωπικού της αντιπροσωπείας. Όσον αφορά την προστασία της ασφάλειας, το γραφείο ασφαλείας εξασφαλίζει συγκεκριμένα ότι:

α) καταρτίζονται σχέδια για την αντιμετώπιση απειλών κατά της ασφάλειας και σχετικών με την ασφάλεια επεισοδίων, όπου τα σχετικά μέτρα καλύπτουν ιδίως την ασφαλή φύλαξη των διαβαθμισμένων εγγράφων ΕΕ στα γραφεία·

β) λαμβάνονται μέτρα για να παρέχεται πρόσβαση στο σύστημα επικοινωνιών της Επιτροπής για την παραλαβή και τη διαβίβαση διαβαθμισμένων μηνυμάτων ΕΕ. Θα ζητείται από το κράτος μέλος υποδοχής να παρέχει πρόσβαση σε ασφαλή τηλεφωνικά συστήματα.

▼B

Η►M2 Διεύθυνση Ασφαλείας της Επιτροπής ◄ λειτουργεί ως σύμβουλος ασφαλείας κατά την προετοιμασία της συνεδρίασης· θα πρέπει να εκπροσωπείται εκεί για να υποβοηθεί και συμβουλεύει τον υπεύθυνο ασφαλείας της συνεδρίασης (ΥΑΣ) και τις αντιπροσωπείες εφόσον απαιτείται.

Κάθε αντιπροσωπεία που συμμετέχει σε συνεδρίαση θα κληθεί να ορίσει έναν υπεύθυνο ασφαλείας, ο οποίος θα είναι αρμόδιος για την αντιμετώπιση θεμάτων ασφαλείας εντός της αντιπροσωπείας του και θα αποτελεί τον σύνδεσμο με τον υπεύθυνο ασφαλείας της συνεδρίασης, καθώς και με τον εκπρόσωπο της►M2 Διεύθυνσης Ασφαλείας της Επιτροπής ◄, όπως απαιτείται.

23.2.2. *Υπεύθυνος ασφαλείας της συνεδρίασης (ΥΑΣ)*

Ορίζεται υπεύθυνος ασφαλείας της συνεδρίασης, αρμόδιος για τη γενική προετοιμασία και τον έλεγχο των γενικών εσωτερικών μέτρων ασφαλείας και για το συντονισμό με τις υπόλοιπες οικείες υπηρεσίες ασφαλείας. Τα μέτρα που λαμβάνει ο ΥΑΣ αφορούν κατά κανόνα:

α) προστατευτικά μέτρα στον τόπο της συνεδρίασης, ώστε να διασφαλίζεται ότι η συνεδρίαση διεξάγεται χωρίς επεισόδια ικανά να απειλήσουν την ασφάλεια τυχόν διαβαθμισμένων πληροφοριών ΕΕ που πιθανώς να χρησιμοποιηθούν κατά τη συνεδρίαση αυτή·

β) τον έλεγχο του προσωπικού που επιτρέπεται να έχει πρόσβαση στο χώρο της συνεδρίασης, στους χώρους των αντιπροσωπειών και στις αίθουσες συνεδριάσεων, και τον έλεγχο του τυχόν εξοπλισμού·

γ) μόνιμο συντονισμό με τις αρμόδιες αρχές του κράτους μέλους υποδοχής και με την►M2 Διεύθυνση Ασφαλείας της Επιτροπής ◄·

δ) την προσθήκη οδηγιών ασφαλείας στο φάκελο της συνεδρίασης, λαμβάνοντας δεόντως υπόψη τις απαιτήσεις που προβλέπονται από τους παρόντες κανόνες ασφαλείας και κάθε άλλης οδηγίας που κρίνεται αναγκαία.

23.3. **Μέτρα ασφαλείας**

23.3.1. *Περιοχές ασφαλείας*

Δημιουργούνται οι ακόλουθοι χώροι ασφαλείας:

α) ένας χώρος ασφαλείας κατηγορίας ΙΙ, αποτελούμενος από μια αίθουσα σύνταξης, τα γραφεία της Επιτροπής και μηχανήματα αναπαραγωγής εγγράφων, καθώς και τα γραφεία των αντιπροσωπειών εφόσον είναι σκόπιμο·

β) ένας χώρος ασφαλείας κατηγορίας Ι, αποτελούμενος από την αίθουσα συνεδριάσεων και τους θαλάμους των διερμηνέων και των μηχανικών ήχου·

γ) διοικητικοί χώροι, αποτελούμενοι από την αίθουσα τύπου και τα μέρη του τόπου της συνεδρίασης τα οποία χρησιμοποιούνται για διοικητικές εργασίες, εστίαση και κατάλυμα, και το χώρο που γειτνιάζει άμεσα με το Κέντρο Τύπου και τον τόπο της συνεδρίασης.

23.3.2. *Άδειες εισόδου*

Ο ΥΑΣ εκδίδει τις κατάλληλες ειδικές ταυτότητες που ζητούν οι αντιπροσωπείες, ανάλογα με τις ανάγκες τους. Εφόσον απαιτείται, είναι δυνατόν να γίνεται διάκριση όσον αφορά την πρόσβαση στους διάφορους χώρους ασφαλείας.

Οι οδηγίες ασφαλείας της συνεδρίασης θα πρέπει να απαιτούν από όλους τους ενδιαφερομένους να φέρουν πάντοτε και εμφανώς την ειδική τους ταυτότητα εντός του χώρου της συνεδρίασης, ώστε να μπορούν να ελέγχονται από το προσωπικό ασφαλείας.

Εκτός από τους εφοδιασμένους με την ειδική ταυτότητα συμμετέχοντες, στο χώρο της συνεδρίασης επιτρέπεται η είσοδος σε όσο γίνεται λιγότερα άτομα. Ο ΥΑΣ επιτρέπει στις εθνικές αντιπροσωπείες να δέχονται επισκέπτες κατά τη διάρκεια της συνεδρίασης μόνο εφόσον το ζητήσουν. Στους επισκέπτες θα πρέπει να χορηγείται ειδική ταυτότητα επισκέπτη. Προς τούτο, συμπληρώνεται ειδικό έντυπο με το ονοματεπώνυμο του επισκέπτη και το ονοματεπώνυμο του ατόμου που επισκέπτεται. Οι επισκέπτες πρέπει να συνοδεύονται πάντα από φύλακα ή από το άτομο που επισκέπτονται. Το έντυπο άδειας εισόδου επισκέπτη φέρεται από το άτομο που συνοδεύει τον επισκέπτη, το οποίο και το επιστρέφει, μαζί με την ειδική ταυτότητα επισκέπτη, στο προσωπικό ασφαλείας κατά την αποχώρηση του επισκέπτη από το χώρο της συνεδρίασης.

23.3.3. *Έλεγχος φωτογραφικού και ακουστικού εξοπλισμού*

Στο χώρο ασφαλείας κατηγορίας Ι απαγορεύεται να εισέρχονται μηχανές λήψης εικόνων ή ηχογράφησης, πλην του εξοπλισμού των φωτογράφων και των μηχανικών ήχου που είναι δεόντως εξουσιοδοτημένοι από τον ΥΑΣ.

23.3.4. *Έλεγχος χαρτοφυλάκων, φορητών υπολογιστών και δεμάτων*

Οι κάτοχοι άδειας εισόδου στους οποίους επιτρέπεται η πρόσβαση σε χώρο ασφαλείας μπορούν κανονικά να φέρουν μαζί τους χαρτοφύλακες και φορητούς υπολογιστές (με δική τους πηγή ηλεκτρισμού) χωρίς έλεγχο. Όσον αφορά τα

▼B

δέματα για τις αντιπροσωπείες, οι αντιπροσωπείες επιτρέπεται να τα παραλαμβάνουν αφού είτε επιθεωρηθούν από τον υπάλληλο ασφαλείας της αντιπροσωπείας, είτε εξεταστούν με ειδικό μηχάνημα, είτε ανοιχθούν προς επιθεώρηση από το προσωπικό ασφαλείας. Εάν ο ΥΑΣ το κρίνει αναγκαίο, είναι δυνατόν να λαμβάνονται αυστηρότερα μέτρα για την επιθεώρηση των χαρτοφυλάκων και των δεμάτων.

23.3.5. *Τεχνική ασφάλεια*

Η αίθουσα συνεδριάσεων μπορεί να καθίσταται τεχνικώς ασφαλής από ομάδα τεχνικής ασφάλειας, η οποία μπορεί να διενεργεί και ηλεκτρονική επιτήρηση κατά τη συνεδρίαση.

23.3.6. *Έγγραφα των αντιπροσωπειών*

Οι αντιπροσωπείες είναι υπεύθυνες για τη μεταφορά διαβαθμισμένων εγγράφων ΕΕ από και προς τις συνεδριάσεις. Οι αντιπροσωπείες είναι επίσης υπεύθυνες για τον έλεγχο και την ασφάλεια των ανωτέρω εγγράφων κατά τη χρήση τους στους διατεθέντες σε αυτές χώρους. Είναι δυνατόν να ζητείται η βοήθεια του κράτους μέλους υποδοχής για τη μεταφορά διαβαθμισμένων εγγράφων από και προς το χώρο της συνεδρίασης.

23.3.7. *Ασφαλής φύλαξη των εγγράφων*

Εάν η Επιτροπή ή οι αντιπροσωπείες δεν μπορούν να αποθηκεύσουν τα διαβαθμισμένα έγγραφά τους σύμφωνα με τα εγκεκριμένα πρότυπα, μπορούν να παραδώσουν τα έγγραφα αυτά, κλεισμένα μέσα σε σφραγισμένους φακέλους, στον υπεύθυνο ασφαλείας της συνεδρίασης, έναντι αποδείξεως, ώστε ο υπάλληλος αυτός να μπορεί να τα αποθηκεύει σύμφωνα με τα εγκεκριμένα πρότυπα.

23.3.8. *Επιθεώρηση γραφείων*

Ο υπεύθυνος ασφαλείας της συνεδρίασης φροντίζει για την επιθεώρηση των γραφείων της Επιτροπής και των αντιπροσωπειών στο τέλος κάθε ημέρας εργασίας ώστε να βεβαιώνεται ότι όλα τα διαβαθμισμένα έγγραφα ΕΕ διατηρούνται σε ασφαλή χώρο. Σε αντίθετη περίπτωση, λαμβάνει τα ενδεδειγμένα μέτρα.

23.3.9. *Διάθεση διαβαθμισμένων απορριμμάτων ΕΕ*

Όλα τα απορρίμματα αντιμετωπίζονται ως διαβαθμισμένο υλικό ΕΕ, οι δε κάλαθοι ή σάκοι αχρήστων θα πρέπει να παραδίδονται στην Επιτροπή και στις αντιπροσωπείες προς διάθεση. Πριν εγκαταλείψουν τους διατεθέντες χώρους, η Επιτροπή και οι αντιπροσωπείες παραδίδουν τα απορρίμματά τους στον υπεύθυνο ασφαλείας της συνεδρίασης, ο οποίος φροντίζει για την καταστροφή τους κατά τα κεκανονισμένα.

Μετά το πέρας της συνεδρίασης, όλα τα έγγραφα που ευρίσκονται στην κατοχή της Επιτροπής ή των αντιπροσωπειών, αλλά δεν χρειάζονται πλέον, πρέπει να αντιμετωπίζονται ως απορρίμματα. Πριν αρθούν τα μέτρα ασφαλείας που εφαρμόζονται κατά τη συνεδρίαση, πρέπει να ερευνώνται διεξοδικά οι χώροι της Επιτροπής και των αντιπροσωπειών. Τα έγγραφα για τα οποία έχει χορηγηθεί υπογεγραμμένη απόδειξη πρέπει, στο μέτρο του εφικτού, να καταστρέφονται σύμφωνα με το τμήμα 22.5.

24. ΠΑΡΑΒΙΑΣΕΙΣ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΔΙΑΡΡΟΗ ΔΙΑΒΑΘΜΙΣΜΕΝΩΝ ΠΛΗΡΟΦΟΡΙΩΝ ΕΕ

24.1. **Ορισμοί**

Παραβίαση της ασφάλειας συμβαίνει ως αποτέλεσμα μιας πράξης ή μιας παράλειψης αντίθετης προς διάταξη περί ασφαλείας της Επιτροπής, με την οποία τίθενται σε κίνδυνο ή διαρρέουν διαβαθμισμένες πληροφορίες ΕΕ.

Διαρροή διαβαθμισμένων πληροφοριών ΕΕ συμβαίνει όταν οι πληροφορίες αυτές έχουν καταλήξει εξ ολοκλήρου ή εν μέρει εις χείρας μη εξουσιοδοτημένων προσώπων, δηλαδή προσώπων που είτε δεν διαθέτουν την κατάλληλη διαβάθμιση ασφαλείας είτε δεν έχουν την απαραίτητη «ανάγκη γνώσης», ή όταν θεωρείται πιθανό να έχει συμβεί κάτι τέτοιο.

Οι διαβαθμισμένες πληροφορίες ΕΕ μπορούν να διαρρεύσουν ως αποτέλεσμα απροσεξίας, αμέλειας ή ακριτομυθίας καθώς και ως συνέπεια των δραστηριοτήτων υπηρεσιών που έχουν ως στόχο την ΕΕ ή τα κράτη μέλη της, όσον αφορά τις διαβαθμισμένες πληροφορίες και δραστηριότητες ΕΕ, ή ανατρεπτικών οργανώσεων.

24.2. **Αναφορά παραβιάσεων της ασφάλειας**

Όλα τα πρόσωπα τα οποία απαιτείται να χειρίζονται διαβαθμισμένες πληροφορίες ΕΕ πρέπει να έχουν ενημερωθεί διεξοδικά για τις ευθύνες τους επί του θέματος αυτού. Οφείλουν να αναφέρουν πάραυτα οποιαδήποτε παραβίαση της ασφάλειας υποπέσει στην αντίληψή τους.

▼B

Όταν ένας τοπικός υπεύθυνος ασφαλείας ή υπεύθυνος ασφαλείας της συνεδρίασης ανακαλύπτει ή πληροφορείται παραβίαση της ασφάλειας σχετικά με διαβαθμισμένες πληροφορίες ΕΕ ή απώλεια ή εξαφάνιση διαβαθμισμένου υλικού ΕΕ, λαμβάνει εγκαίρως μέτρα προκειμένου να:

α) διασφαλίζει τα αποδεικτικά στοιχεία·

β) βεβαιώνει τα πραγματικά περιστατικά·

γ) εκτιμά και να ελαχιστοποιεί την προξενηθείσα ζημία·

δ) προλαμβάνει την επανάληψη·

ε) ειδοποιεί τις ενδεδειγμένες αρχές για τις συνέπειες της παραβίασης της ασφάλειας.

Στο πλαίσιο αυτό, παρέχονται τα ακόλουθα στοιχεία:

i) μια περιγραφή των συγκεκριμένων πληροφοριών, καθώς και η διαβάθμισή τους, ο αριθμός του εγγράφου ή αντιγράφου, η ημερομηνία, ο συντάκτης τους, το θέμα τους και το πεδίο εφαρμογής τους,

ii) μια συνοπτική περιγραφή των περιστάσεων παραβίασης της ασφάλειας, καθώς και η ημερομηνία και το διάστημα κατά το οποίο οι πληροφορίες ήταν εκτεθειμένες σε κίνδυνο διαρροής·

iii) μια δήλωση για το κατά πόσον έχει ενημερωθεί ο συντάκτης τους.

Αποτελεί καθήκον κάθε αρχής ασφαλείας, μόλις ειδοποιηθεί για μια τέτοια παραβίαση της ασφάλειας, να αναφέρει το γεγονός πάραυτα στην►**M2** Διεύθυνση Ασφαλείας της Επιτροπής ◄.

Οι περιπτώσεις που αφορούν πληροφορίες ►**M1** RESTREINT UE ◄ αναφέρονται μόνο όταν παρουσιάζουν ασυνήθιστα χαρακτηριστικά.

Το αρμόδιο επί θεμάτων ασφαλείας μέλος της Επιτροπής, μόλις πληροφορηθεί μια παραβίαση της ασφάλειας:

α) ενημερώνει την αρχή από όπου προήλθαν οι υπόψη διαβαθμισμένες πληροφορίες·

β) δίνει εντολή στις αρμόδιες αρχές ασφαλείας να διεξαγάγουν έρευνες·

γ) συντονίζει τις έρευνες όταν υπεισέρχονται πλείονες αρχές ασφαλείας·

δ) φροντίζει να του υποβληθεί έκθεση για τις περιστάσεις της παραβίασης, την ημερομηνία ή την περίοδο κατά την οποία ενδεχομένως συνέβη και αποκαλύφθηκε, με λεπτομερή περιγραφή του περιεχομένου και της διαβάθμισης του εμπλεκόμενου υλικού. Στην έκθεση αναφέρονται επίσης η ζημία την οποία υπέστησαν τα συμφέροντα της ΕΕ ή ενός ή περισσοτέρων κρατών μελών της και οι ενέργειες που έγιναν για την αποτροπή επανάληψης του συμβάντος.

Η αρχή που ανακάλυψε την παραβίαση ενημερώνει τους αποδέκτες των πληροφοριών και δίνει τις κατάλληλες οδηγίες.

24.3. **Δικαστικές ενέργειες**

Κάθε μεμονωμένο άτομο υπεύθυνο για τη διαρροή διαβαθμισμένων πληροφοριών ΕΕ υπόκειται σε πειθαρχική δίωξη σύμφωνα με τους οικείους κανόνες και κανονισμούς, ειδικότερα τον τίτλο VI του κανονισμού υπηρεσιακής κατάστασης. Η δίωξη αναλαμβάνεται με την επιφύλαξη τυχόν περαιτέρω δικαστικών ενεργειών.

Στις περιπτώσεις που ενδείκνυται, με βάση την αναφερόμενη στο τμήμα 24.2 έκθεση, το αρμόδιο επί θεμάτων ασφαλείας μέλος της Επιτροπής λαμβάνει όλα τα αναγκαία μέτρα ώστε να επιτρέψει στις αρμόδιες εθνικές αρχές να κινήσουν διαδικασίες ποινικής δίωξης.

25. ΠΡΟΣΤΑΣΙΑ ΔΙΑΒΑΘΜΙΣΜΕΝΩΝ ΠΛΗΡΟΦΟΡΙΩΝ ΕΕ ΔΙΑΚΙΝΟΥΜΕΝΩΝ ΣΕ ΣΥΣΤΗΜΑΤΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ

25.1. **Εισαγωγή**

25.1.1. *Γενικά*

Η ασκούμενη πολιτική και οι απαιτήσεις ασφαλείας ισχύουν για όλα τα συστήματα και δίκτυα επικοινωνιών και πληροφορικής (εφεξής αποκαλούμενα «συστήματα») στα οποία διακινούνται πληροφορίες με διαβάθμιση ►**M1** CONFIDENTIEL UE ◄ ή υψηλότερη. Ισχύουν συμπληρωματικώς προς την απόφαση C(95) 1510 τελικό της Επιτροπής της 23ης Νοεμβρίου 1995 για την προστασία των συστημάτων πληροφορικής.

Τα συστήματα στα οποία διακινούνται πληροφορίες ►**M1** RESTREINT UE ◄ επίσης απαιτείται να καλύπτονται από μέτρα ασφαλείας ώστε να προστατεύεται ο εμπιστευτικός χαρακτήρας των πληροφοριών αυτών. Όλα τα συστήματα πρέπει να καλύπτονται από μέτρα ασφαλείας ώστε να προστατεύονται η ακεραιότητα και η διαθεσιμότητα αυτών των συστημάτων και των πληροφοριών τις οποίες περιέχουν.

▼**B**

Η ασκούμενη από την Επιτροπή πολιτική ασφαλείας στην πληροφορική συνίσταται στα εξής:

— αποτελεί αναπόσπαστο μέρος της ασφάλειας γενικότερα, συμπληρώνει δε όλα τα στοιχεία της ασφάλειας πληροφοριών, ασφάλειας προσώπων και υλικής ασφάλειας·

— προβλέπει κατανομή ευθυνών μεταξύ των ιδιοκτητών τεχνικών συστημάτων, των ιδιοκτητών ΔΠΕΕ οι οποίες είναι αποθηκευμένες ή διακινούνται σε τεχνικά συστήματα, των ειδημόνων επί θεμάτων ασφαλείας και των χρηστών συστημάτων πληροφορικής·

— δίνει περιγραφή των αρχών που διαπνέουν την ασφάλεια και των απαιτήσεων εκάστου συστήματος πληροφορικής·

— προβλέπει την έγκριση των ανωτέρων αρχών και απαιτήσεων, από οριζόμενη αρχή·

— συνεκτιμά τις ειδικές απειλές και τα τρωτά σημεία στο χώρο της πληροφορικής.

25.1.2. *Απειλές κατά των συστημάτων και τρωτά σημεία τους*

Ως απειλή ορίζεται η λανθάνουσα ευκαιρία τυχαίας ή εσκεμμένης διακινδύνευσης της ασφάλειας. Στην περίπτωση των συστημάτων, η εν λόγω διακινδύνευση συνεπάγεται απώλεια μίας ή περισσότερων από τις ιδιότητες της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας. Ως τρωτό σημείο ορίζεται μια αδυναμία ή έλλειψη ελέγχων που διευκολύνει ή καθιστά δυνατή την ενεργοποίηση μιας απειλής εις βάρος συγκεκριμένου περιουσιακού στοιχείου ή στόχου.

Οι διαβαθμισμένες ή αδιαβάθμιστες πληροφορίες ΕΕ που διακινούνται στα συστήματα υπό συμπυκνωμένη μορφή με σκοπό την ταχεία ανάκτηση, κοινοποίηση και χρήση είναι εκτεθειμένες σε πολλές απειλές. Στις απειλές αυτές περιλαμβάνεται η πρόσβαση μη εξουσιοδοτημένων χρηστών στις πληροφορίες ή, αντιστρόφως, η άρνηση πρόσβασης στους εξουσιοδοτημένους χρήστες. Υπάρχουν επίσης οι κίνδυνοι κοινολόγησης άνευ αδείας, αλλοίωσης, τροποποίησης ή διαγραφής των πληροφοριών. Επί πλέον, τα χρησιμοποιούμενα πολύπλοκα και ενίοτε εύθραυστα μηχανήματα είναι δαπανηρά και συχνά δύσκολο να επιδιορθωθούν ή να αντικατασταθούν ταχέως.

25.1.3. *Κύριος σκοπός των μέτρων ασφαλείας*

Ο κύριος σκοπός των μέτρων ασφαλείας που αναφέρονται στο παρόν τμήμα συνίσταται στην παροχή προστασίας από το ενδεχόμενο άνευ αδείας κοινολόγησης διαβαθμισμένων πληροφοριών ΕΕ (απώλεια εμπιστευτικού χαρακτήρα) καθώς και απώλειας της ακεραιότητας και της διαθεσιμότητας των πληροφοριών. Για την επίτευξη επαρκούς προστασίας της ασφάλειας συστήματος που διακινεί διαβαθμισμένες πληροφορίες ΕΕ, από την►**M2** Διεύθυνση Ασφαλείας της Επιτροπής ◄ καθορίζονται τα κατάλληλα πρότυπα συμβατικής ασφάλειας καθώς και ενδεδειγμένες ειδικές διαδικασίες και τεχνικές ασφαλείας σχεδιασμένες ειδικώς για κάθε σύστημα.

25.1.4. *Δήλωση απαιτήσεων ασφαλείας ανταποκρινόμενων στο ιδιαίτερο σύστημα (SSRS)*

Για όλα τα συστήματα που διακινούν πληροφορίες με διαβάθμιση ►**M1** CONFIDENTIEL UE ◄ ή υψηλότερη απαιτείται να εκδίδεται δήλωση απαιτήσεων ασφαλείας ανταποκρινόμενων στο ιδιαίτερο σύστημα (SSRS) από τον ιδιοκτήτη τεχνικών συστημάτων (TSO, βλέπε τμήμα 25.3.4) και τον ιδιοκτήτη πληροφοριών (βλέπε τμήμα 25.3.5), σε συνεργασία με εισηγήσεις και βοήθεια, όπως απαιτείται, από το προσωπικό του σχεδίου καιτην►**M2** Διεύθυνση Ασφαλείας της Επιτροπής ◄ (ως αρχής INFOSEC -IA, βλέπε τμήμα 25.3.3), η οποία έχει λάβει την έγκριση της αρχής διαπίστευσης της ασφάλειας (ΑΔΑ, βλέπε τμήμα 25.3.2).

Απαιτείται μια SSRS και στις περιπτώσεις όπου η διαθεσιμότητα και ακεραιότητα των πληροφοριών με διαβάθμιση ►**M1** RESTREINT UE ◄ ή χωρίς διαβάθμιση κρίνεται καίριας σημασίας από την αρχή διαπίστευσης της ασφάλειας (ΑΔΑ).

Η SSRS διατυπώνεται το συντομότερο μετά την έναρξη σύλληψης ενός σχεδίου και αναπτύσσεται και ενισχύεται ανάλογα με την εξέλιξή του, εκπληρώνοντας διαφορετικούς ρόλους κατά τα διάφορα στάδια του κύκλου ζωής του σχεδίου και του συστήματος.

25.1.5. *Επίπεδα ασφάλειας της λειτουργίας*

Όλα τα συστήματα στα οποία διακινούνται πληροφορίες με διαβάθμιση ►**M1** CONFIDENTIEL UE ◄ ή υψηλότερη πρέπει να έχουν διαπιστευθεί για να λειτουργούν σε ένα ή, όταν αυτό δικαιολογείται από τις απαιτήσεις λειτουργίας σε διαφορετικά χρονικά διαστήματα, σε περισσότερα από ένα, από τα ακόλουθα επίπεδα ασφαλείας, ή τα εθνικά τους ισοδύναμα:

α) απόλυτο

β) υψηλό και

▼B

γ) πολλαπλό.

25.2. **Ορισμοί**

Ως «διαπίστευση» νοείται η άδεια και η έγκριση που χορηγείται σε ένα σύστημα να επεξεργάζεται διαβαθμισμένες πληροφορίες ΕΕ στο λειτουργικό του περιβάλλον.

Σημείωση:

Η διαπίστευση αυτή πρέπει να διενεργείται αφού πρώτα εφαρμοστούν όλες οι ενδεδειγμένες διαδικασίες ασφαλείας και έχει επιτευχθεί ικανοποιητικό επίπεδο προστασίας των πόρων του συστήματος. Η διαπίστευση θα πρέπει κανονικά να διενεργείται βάσει της SSRS στην οποία περιλαμβάνονται και τα εξής:

α) δήλωση για το στόχο της διαπίστευσης του συστήματος· συγκεκριμένα, ποιο(-α) επίπεδο(-α) διαβάθμισης πληροφοριών πρόκειται να εφαρμοστεί(-ούν) σε αυτό και ποιο(-α) είναι το (τα) προτεινόμενο(-α) επίπεδο(-α) ασφάλειας της λειτουργίας του συστήματος ή του δικτύου·

β) εκπόνηση μιας έκθεσης διαχείρισης κινδύνου, στην οποία καθορίζονται οι απειλές και τα τρωτά σημεία καθώς και τα μέτρα για την αντιμετώπισή τους·

γ) οι λειτουργικές διαδικασίες ασφάλειας στις οποίες περιλαμβάνονται μια αναλυτική περιγραφή των προτεινόμενων λειτουργιών (π.χ. τρόποι λειτουργίας, υπηρεσίες προς παροχή) και μια περιγραφή των χαρακτηριστικών ασφαλείας του συστήματος βάσει των οποίων παρέχεται η διαπίστευση·

δ) το σχέδιο εφαρμογής και συντήρησης των χαρακτηριστικών ασφαλείας·

ε) το σχέδιο για την αρχική και τις επακόλουθες δοκιμές της ασφάλειας του συστήματος ή του δικτύου, την αξιολόγησή της και την πιστοποίησή της και

στ) την πιστοποίηση, όπου απαιτείται, από κοινού με άλλα στοιχεία της διαπίστευσης.

Ως «κεντρικός υπεύθυνος ασφαλείας πληροφοριών» (CISO) νοείται ο υπάλληλος μιας κεντρικής υπηρεσίας πληροφορικής που συντονίζει και επιβλέπει μέτρα ασφαλείας για συγκεντρωτικώς οργανωμένα συστήματα.

Ως «πιστοποίηση» νοείται η έκδοση επίσημης δήλωσης, βασισμένης σε ανεξάρτητη εξέταση της διεξαγωγής και των αποτελεσμάτων μιας αξιολόγησης, για τον βαθμό στον οποίο ένα σύστημα πληροί τις απαιτήσεις ασφαλείας ή ένα προϊόν ασφάλειας των υπολογιστών τις προκαθορισμένες προδιαγραφές ασφαλείας.

Ως «ασφάλεια επικοινωνιών» (COMSEC) νοείται η εφαρμογή μέτρων ασφάλειας στις τηλεπικοινωνίες ώστε να εμποδιστεί η πρόσβαση μη εξουσιοδοτημένων προσώπων σε σημαντικές πληροφορίες οι οποίες ενδέχεται να προκύψουν από την κατοχή και μελέτη τέτοιων τηλεπικοινωνιών, ή προκειμένου να διασφαλισθεί η γνησιότητα των τηλεπικοινωνιών αυτών.

Σημείωση:

Στα μέτρα αυτά περιλαμβάνονται μέτρα για την ασφάλεια της κρυπτογράφησης, των διαβιβάσεων και των εκπομπών· επίσης, περιλαμβάνονται μέτρα για την ασφάλεια των διαδικασιών, του υλικού, του προσωπικού, των εγγράφων και των υπολογιστών.

Ως «ασφάλεια υπολογιστών» (COMPUSEC) νοείται η εφαρμογή μέτρων προστασίας των χαρακτηριστικών ασφαλείας του υλικού, του υλικολογισμικού και του λογισμικού σε σύστημα υπολογιστών ώστε να υπάρχει προστασία έναντι, ή πρόληψη, κοινολόγησης άνευ αδείας, αλλοίωσης, τροποποίησης/διαγραφής πληροφοριών ή άρνησης εξυπηρέτησης.

Ως «προϊόν ασφάλειας υπολογιστών» νοείται ένα γενικό στοιχείο ασφάλειας των υπολογιστών, που προορίζεται να ενσωματώνεται σε σύστημα πληροφορικής για την ενίσχυση ή την εξασφάλιση της εμπιστευτικότητας, της ακεραιότητας ή της διαθεσιμότητας των διακινούμενων πληροφοριών.

Ως «απόλυτο επίπεδο ασφάλειας της λειτουργίας» νοείται το επίπεδο λειτουργίας στο οποίο ΟΛΑ τα μεμονωμένα άτομα που έχουν πρόσβαση στο σύστημα ελέγχονται σύμφωνα με τον υψηλότερο βαθμό διαβάθμισης των πληροφοριών που διακινούνται στο σύστημα, ενώ παράλληλα έχουν και τον ίδιο βαθμό ανάγκης να γνωρίζουν ΟΛΕΣ τις πληροφορίες που διακινούνται στο σύστημα.

Σημειώσεις:

(1) Ο «ίδιος βαθμός ανάγκης να γνωρίζουν» σημαίνει ότι δεν είναι υποχρεωτικό τα χαρακτηριστικά ασφαλείας των υπολογιστών να παρέχουν τη δυνατότητα διαχωρισμού των πληροφοριών εντός του συστήματος.

(2) Τα υπόλοιπα χαρακτηριστικά ασφαλείας (π.χ. όσον αφορά την υλική ασφάλεια, το προσωπικό και τις διαδικασίες) ανταποκρίνονται στις απαιτήσεις της υψηλότερης διαβάθμισης και όλων των κατηγοριών πληροφοριών που διακινούνται στο σύστημα.

▼B

Ως «αξιολόγηση» νοείται η λεπτομερής τεχνική εξέταση, από ενδεδειγμένη αρχή, των πτυχών ασφαλείας ενός συστήματος ή ενός προϊόντος κρυπτογράφησης ή ασφάλειας των υπολογιστών.

Σημειώσεις:

(1) Με την αξιολόγηση διερευνάται η ύπαρξη της απαιτούμενης λειτουργικότητας ασφάλειας και η απουσία επικίνδυνων παρενεργειών από τη λειτουργικότητα αυτή, και εκτιμάται το απρόσβλητο αυτής της λειτουργικότητας.

(2) Με την αξιολόγηση καθορίζεται ο βαθμός στον οποίο ικανοποιούνται οι απαιτήσεις ασφαλείας ενός συστήματος, ή οι ισχυρισμοί περί ασφαλείας ενός προϊόντος ασφάλειας των υπολογιστών, και προσδιορίζεται το επίπεδο βεβαιότητας του συστήματος ή της κρυπτογράφησης ή ο βαθμός εμπιστοσύνης στη λειτουργία του προϊόντος ασφάλειας των υπολογιστών.

Ως «ιδιοκτήτης πληροφοριών» (ΙΠ) νοείται η αρχή (προϊστάμενος τμήματος) που έχει την ευθύνη της δημιουργίας, επεξεργασίας και χρήσης πληροφοριών, συμπεριλαμβανομένης της απόφασης σε ποίο να επιτρέπεται η πρόσβαση στις εν λόγω πληροφορίες.

Ως «ασφάλεια πληροφοριών» (INFOSEC) νοείται η εφαρμογή μέτρων ασφαλείας για την προστασία των πληροφοριών που αποτελούν αντικείμενο επεξεργασίας, αποθήκευσης ή διαβίβασης σε συστήματα επικοινωνιών, πληροφορικής ή άλλα ηλεκτρονικά συστήματα από το ενδεχόμενο να θιγεί, τυχαία ή εσκεμμένα, η εμπιστευτικότητα, η ακεραιότητα ή η διαθεσιμότητά τους, καθώς και για την πρόληψη της απώλειας της ακεραιότητας και της διαθεσιμότητας των ίδιων των συστημάτων.

Στα «μέτρα INFOSEC» περιλαμβάνονται μέτρα για την ασφάλεια των υπολογιστών, των διαβιβάσεων, των εκπομπών και της κρυπτογράφησης, καθώς και η ανίχνευση, η τεκμηρίωση και η αντιμετώπιση απειλών εναντίον των πληροφοριών και των συστημάτων.

Ως «χώρος πληροφορικής» νοείται ο χώρος που περιλαμβάνει ένα ή περισσότερους υπολογιστές, τα επί τόπου περιφερειακά και τις μονάδες αποθήκευσής τους, τις μονάδες ελέγχου και το ειδικό για το σκοπό αυτό δίκτυο και εξοπλισμό επικοινωνιών.

Σημείωση:

Δεν συμπεριλαμβάνεται ο τυχόν ξεχωριστός χώρος στον οποίο ευρίσκονται εγκατεστημένα τα απομακρυσμένα περιφερειακά ή τερματικά/σταθμοί εργασίας, ακόμα κι αν οι συσκευές αυτές είναι συνδεδεμένες με μηχανήματα του χώρου πληροφορικής.

Ως «δίκτυο πληροφορικής» νοείται η γεωγραφικά κατανεμημένη οργάνωση συστημάτων πληροφορικής διασυνδεδεμένων με στόχο την ανταλλαγή δεδομένων, στα οποία συμπεριλαμβάνονται τα συστατικά στοιχεία των διασυνδεδεμένων συστημάτων πληροφορικής και η διεπαφή τους με τα σχετικά δεδομένα ή δίκτυα επικοινωνιών.

Σημειώσεις:

(1) Ένα δίκτυο πληροφορικής μπορεί να χρησιμοποιεί τις υπηρεσίες ενός ή περισσοτέρων δικτύων επικοινωνιών διασυνδεδεμένων για την ανταλλαγή δεδομένων· διάφορα δίκτυα πληροφορικής μπορούν να χρησιμοποιούν τις υπηρεσίες ενός κοινού δικτύου επικοινωνιών.

(2) Ένα δίκτυο πληροφορικής καλείται «τοπικό» εάν συνδέει διάφορους υπολογιστές στον ίδιο τόπο.

Ως «χαρακτηριστικά ασφαλείας δικτύου πληροφορικής» νοούνται τα χαρακτηριστικά ασφαλείας των επί μέρους συστημάτων πληροφορικής που συναποτελούν το δίκτυο, καθώς και τα πρόσθετα συστατικά στοιχεία και χαρακτηριστικά που σχετίζονται με το ίδιο το δίκτυο (π.χ. δικτυακές επικοινωνίες, μηχανισμοί και διαδικασίες σήμανσης της ασφάλειας, έλεγχοι πρόσβασης, προγράμματα και αυτόματες καταγραφές ενεργειών) τα οποία απαιτούνται για την παροχή αποδεκτού επιπέδου προστασίας των διαβαθμισμένων πληροφοριών.

Ως «σύστημα πληροφορικής» νοείται συγκρότημα μηχανημάτων, μεθόδων και διαδικασιών, και ενδεχομένως προσωπικού, οργανωμένο κατά τρόπο που να επιτελεί λειτουργίες επεξεργασίας πληροφοριών.

Σημειώσεις:

(1) Αυτό θεωρείται ότι σημαίνει συγκρότημα μονάδων διατεταγμένο για το χειρισμό πληροφοριών εντός του συστήματος,

(2) Τα συστήματα αυτά ενδέχεται να εξυπηρετούν σκοπούς άντλησης στοιχείων, διοίκησης, ελέγχου, επικοινωνιών, επιστημονικών ή διοικητικών εφαρμογών καθώς και επεξεργασίας κειμένου,

▼B

(3) Τα όρια ενός συστήματος καθορίζονται σε γενικές γραμμές ως τα στοιχεία που ευρίσκονται υπό τον έλεγχο ενός μοναδικού ιδιοκτήτη τεχνικών συστημάτων (TSO),

(4) Ένα σύστημα πληροφορικής μπορεί να περιλαμβάνει υποσυστήματα, ορισμένα από τα οποία είναι και τα ίδια συστήματα πληροφορικής.

Τα «γνωρίσματα ασφαλείας συστήματος πληροφορικής» περιλαμβάνουν όλες τις λειτουργίες, τα χαρακτηριστικά και τα γνωρίσματα του υλικού/υλικολογισμικού/λογισμικού· τις διαδικασίες λειτουργίας, τις διαδικασίες λογοδοσίας, τους ελέγχους πρόσβασης, το χώρο πληροφορικής, το χώρο απομακρυσμένων τερματικών/σταθμών εργασίας καθώς και τους διαχειριστικούς περιορισμούς, την υλική δομή και τις συσκευές, το προσωπικό και τους ελέγχους των επικοινωνιών που απαιτούνται για την εξασφάλιση αποδεκτού επιπέδου προστασίας των διαβαθμισμένων πληροφοριών που διακινούνται σε ένα σύστημα πληροφορικής.

Ως «τοπικός υπεύθυνος ασφαλείας πληροφορικής» (LISO) νοείται ο υπάλληλος της Επιτροπής που είναι αρμόδιος για να συντονίζει και επιβλέπει μέτρα ασφαλείας εντός του πεδίου ευθύνης του.

Ως «πολλαπλό επίπεδο ασφάλειας της λειτουργίας» νοείται το επίπεδο λειτουργίας στο οποίο ΟΡΙΣΜΕΝΑ ΜΟΝΟ από τα μεμονωμένα άτομα που έχουν πρόσβαση στο σύστημα έχουν λάβει διαβάθμιση ασφαλείας του υψηλότερου βαθμού για τις πληροφορίες που διακινούνται στο σύστημα, και παράλληλα ΟΡΙΣΜΕΝΑ ΜΟΝΟ από τα μεμονωμένα άτομα που έχουν πρόσβαση στο σύστημα έχουν τον ίδιο βαθμό ανάγκης να γνωρίζουν τις πληροφορίες που διακινούνται εντός του συστήματος.

Σημειώσεις:

(1) Αυτός ο τρόπος λειτουργίας επιτρέπει, τη στιγμή αυτή, το χειρισμό πληροφοριών διαφορετικής διαβάθμισης και διαφόρων κατηγοριών, και

(2) Το γεγονός ότι δεν έχουν όλα τα μεμονωμένα άτομα λάβει διαβάθμιση ασφαλείας του υψηλότερου βαθμού, σε συνδυασμό με την έλλειψη του ίδιου βαθμού ανάγκης να γνωρίζουν, σημαίνει ότι τα γνωρίσματα ασφαλείας των υπολογιστών πρέπει οπωσδήποτε να παρέχουν τη δυνατότητα επιλεκτικής πρόσβασης και διαχωρισμού των πληροφοριών που περιέχονται στο σύστημα.

Ως «χώρος απομακρυσμένων τερματικών/σταθμών εργασίας» νοείται χώρος ο οποίος περιλαμβάνει ορισμένο εξοπλισμό υπολογιστών, τα επί τόπου περιφερειακά ή τερματικά/σταθμούς εργασίας και τυχόν συνδεδεμένα με αυτά μηχανήματα επικοινωνιών, χωριστά από το χώρο πληροφορικής.

Ως «λειτουργικές διαδικασίες ασφαλείας» νοούνται οι διαδικασίες τις οποίες δημιουργεί ο ιδιοκτήτης τεχνικών συστημάτων, όπου καθορίζονται οι αρχές που πρέπει να θεσπίζονται για θέματα ασφαλείας, οι ακολουθητέες διαδικασίες λειτουργίας και οι ευθύνες του προσωπικού.

Ως «υψηλό επίπεδο ασφάλειας της λειτουργίας» νοείται το επίπεδο λειτουργίας στο οποίο ΟΛΑ τα μεμονωμένα άτομα που έχουν πρόσβαση στο σύστημα έχουν λάβει διαβάθμιση ασφαλείας του υψηλότερου βαθμού για τις πληροφορίες που διακινούνται στο σύστημα, αλλά ΟΡΙΣΜΕΝΑ ΜΟΝΟ από τα μεμονωμένα άτομα που έχουν πρόσβαση στο σύστημα έχουν τον ίδιο βαθμό ανάγκης να γνωρίζουν τις πληροφορίες που διακινούνται εντός του συστήματος.

Σημειώσεις:

(1) Η έλλειψη «ίδιου βαθμού ανάγκης να γνωρίζουν» σημαίνει ότι τα γνωρίσματα ασφαλείας των υπολογιστών πρέπει οπωσδήποτε να παρέχουν τη δυνατότητα επιλεκτικής πρόσβασης και διαχωρισμού των πληροφοριών που περιέχονται στο σύστημα.

(2) Τα υπόλοιπα χαρακτηριστικά ασφαλείας (π.χ. όσον αφορά την υλική ασφάλεια, το προσωπικό και τις διαδικασίες) ανταποκρίνονται στις απαιτήσεις της υψηλότερης διαβάθμισης και όλων των κατηγοριών πληροφοριών που διακινούνται στο σύστημα.

(3) Όλες οι πληροφορίες που διακινούνται ή καθίστανται διαθέσιμες σε ένα σύστημα σύμφωνα με αυτό το επίπεδο λειτουργίας προστατεύονται, όπως και τα στοιχεία που προκύπτουν από αυτές, ως δυνητικά εμπίπτουσες στην κατηγορία πληροφοριών και στο υψηλότερο επίπεδο διαβάθμισης που χρησιμοποιούνται έως ότου ληφθεί άλλη απόφαση, εκτός εάν υπάρχει ικανοποιητικός βαθμός εμπιστοσύνης στις όποιες λειτουργικότητες σήμανσης υπάρχουν.

Η «δήλωση απαιτήσεων ασφαλείας ανταποκρινόμενων στο ιδιαίτερο σύστημα» (SSRS) αποτελεί μια ολοκληρωμένη και ρητή δήλωση των αρχών ασφαλείας που θα τηρούνται και των λεπτομερών απαιτήσεων ασφαλείας που θα εφαρμόζονται. Βασίζεται στην πολιτική ασφάλειας και στις εκτιμήσεις κινδύνου της Επιτροπής, ή επιβάλλεται από παραμέτρους που αφορούν το επιχειρησιακό περιβάλλον, το χαμηλότερο δυνατό επίπεδο ελέγχων ασφαλείας του προσωπικού, την υψηλότερη

▼B

δυνατή διαβάθμιση των διακινούμενων πληροφοριών, το επίπεδο ασφάλειας της λειτουργίας ή τις απαιτήσεις των χρηστών. Η SSRS αποτελεί αναπόσπαστο μέρος της τεκμηρίωσης του σχεδίου που υποβάλλεται στις αρμόδιες αρχές προς έγκριση από τεχνική άποψη, προϋπολογισμού και ασφάλειας. Στην τελική της μορφή, η SSRS αποτελεί μια ολοκληρωμένη δήλωση περί του τι σημαίνει ο ισχυρισμός ότι το σύστημα είναι ασφαλές.

Ως «ιδιοκτήτης τεχνικών συστημάτων» (TSO) νοείται η αρχή που είναι αρμόδια για τη δημιουργία, τη συντήρηση, τη λειτουργία και το κλείσιμο ενός συστήματος.

Ως αντίμετρα «Tempest» νοούνται τα μέτρα ασφαλείας που αποσκοπούν στην προστασία των μηχανημάτων και της υποδομής των επικοινωνιών από το ενδεχόμενο διαρροής διαβαθμισμένων πληροφοριών λόγω ακούσιων ηλεκτρομαγνητικών εκπομπών και μέσω αγωγιμότητας.

25.3. **Αρμοδιότητες ασφαλείας**

25.3.1. *Γενικά*

Οι γνωμοδοτικές αρμοδιότητες της συμβουλευτικής ομάδας επί θεμάτων πολιτικής ασφάλειας της Επιτροπής, όπως ορίζεται στο τμήμα 12, περιλαμβάνει ζητήματα INFOSEC. Η ομάδα αυτή οργανώνει τις δραστηριότητές της κατά τρόπο ώστε να μπορεί να παρέχει έγκυρες συμβουλές για τα ανωτέρω ζητήματα.

Η ►**M2** Διεύθυνση Ασφαλείας της Επιτροπής ◄είναι αρμόδια για την έκδοση λεπτομερών ρυθμίσεων INFOSEC με βάση τις διατάξεις του παρόντος κεφαλαίου.

Σε περίπτωση προβλημάτων ασφαλείας (επεισόδια, παραβιάσεις κ.λπ.), η ►**M2** Διεύθυνση Ασφαλείας της Επιτροπής ◄ λαμβάνει αμέσως μέτρα.

Η ►**M2** Διεύθυνση Ασφαλείας της Επιτροπής ◄θα διαθέτει διοικητική μονάδα INFOSEC.

25.3.2. *Αρχή διαπίστευσης της ασφάλειας (ΑΔΑ)*

Ο ►**M2** δευθυντής της Διεύθυνσης Ασφαλείας της Επιτροπής ◄ είναι η αρχή διαπίστευσης της ασφάλειας (ΑΔΑ) για την Επιτροπή. Η ΑΔΑ είναι αρμόδια στο γενικό τομέα της ασφάλειας και στους εξειδικευμένους τομείς της INFOSEC, της ασφάλειας επικοινωνιών, της ασφάλειας κρυπτογράφησης και της ασφάλειας Tempest.

Η ΑΔΑ είναι υπεύθυνη για την εξασφάλιση της συμμόρφωσης των συστημάτων με την πολιτική ασφαλείας της Επιτροπής. Ένα από τα καθήκοντά της είναι να εγκρίνει ένα σύστημα για τη διεκπεραίωση διαβαθμισμένων πληροφοριών ΕΕ μέχρις ενός καθοριζόμενου βαθμού ασφαλείας εντός του επιχειρησιακού του περιβάλλοντος.

Η δικαιοδοσία της ΑΔΑ της Επιτροπής καλύπτει όλα τα συστήματα που λειτουργούν στα κτίρια της Επιτροπής. Όταν διάφορα συστατικά στοιχεία ενός συστήματος υπάγονται ταυτόχρονα στη δικαιοδοσία της ΑΔΑ της Επιτροπής και άλλων ΑΔΑ, όλα τα οικεία μέρη διορίζουν κοινό συμβούλιο διαπίστευσης υπό το συντονισμό της ΑΔΑ της Επιτροπής.

25.3.3. *Αρχή INFOSEC (ΙΑ)*

Ο προϊστάμενος του γραφείου ασφαλείας της διοικητικής μονάδας INFOSEC της Επιτροπής είναι η αρχή INFOSEC για την Επιτροπή. Η αρχή INFOSEC είναι αρμόδια για να:

— παρέχει τεχνικές συμβουλές και τεχνική αρωγή στην ΑΔΑ,

— υποβοηθεί στην ανάπτυξη του SSRS,

— επανεξετάζει το SSRS για να εξασφαλίζεται αντιστοιχία προς τους παρόντες κανόνες ασφαλείας και τις πολιτικές και τα έγγραφα αρχιτεκτονικής INFOSEC,

— συμμετέχει στις ομάδες/συμβούλια διαπίστευσης κατά περίπτωση, και διατυπώνει συστάσεις INFOSEC προς την ΑΔΑ όσον αφορά τη διαπίστευση,

— παρέχει στήριξη των δραστηριοτήτων κατάρτισης και εκπαίδευσης INFOSEC,

— παρέχει τεχνικές συμβουλές κατά τη διερεύνηση επεισοδίων που σχετίζονται με την INFOSEC,

— καταρτίζει οδηγίες τεχνικής πολιτικής για να διασφαλίζεται ότι χρησιμοποιείται μόνον εγκεκριμένο λογισμικό.

25.3.4. *Ιδιοκτήτης τεχνικών συστημάτων (TSO)*

Την ευθύνη για την εφαρμογή και τη λειτουργία των ελέγχων και των ειδικών γνωρισμάτων ασφαλείας ενός συστήματος φέρει ο ιδιοκτήτης του συστήματος αυτού, ο ιδιοκτήτης τεχνικών συστημάτων (TSO). Για τα συστήματα συγκεντρωτικής ιδιοκτησίας διορίζεται υπεύθυνος ασφάλειας κεντρικών συστημάτων

▼B

πληροφορικής (CISO). Κάθε τμήμα διορίζει, κατά περίπτωση, ένα υπεύθυνο ασφάλειας τοπικών συστημάτων πληροφορικής (LISO). Η αρμοδιότητα του TSO περιλαμβάνει την εκπόνηση των λειτουργικών διαδικασιών ασφάλειας (SecOPs), εκτείνεται δε σε όλη τη διάρκεια του κύκλου ζωής ενός συστήματος, από το στάδιο του βασικού σχεδιασμού μέχρι την τελική διάθεση.

Ο TSO ορίζει τα πρότυπα και τις πρακτικές ασφαλείας προς τα οποία πρέπει να συμμορφούται ο προμηθευτής του συστήματος.

Ο TSO μπορεί να μεταβιβάζει μέρος των αρμοδιοτήτων του, κατά περίπτωση, σε υπεύθυνο ασφάλειας τοπικών συστημάτων πληροφορικής. Τα διάφορα καθήκοντα INFOSEC είναι δυνατόν να εκτελούνται από το ίδιο άτομο.

25.3.5. *Ιδιοκτήτης πληροφοριών (ΙΠ)*

Ο ιδιοκτήτης πληροφοριών (ΙΠ) είναι αρμόδιος για τις ΔΠΕΕ (και λοιπές πληροφορίες) που πρόκειται να εισέλθουν, υποστούν επεξεργασία και δημιουργηθούν σε τεχνικά συστήματα. Καθορίζει τις απαιτήσεις για την πρόσβαση στις εν λόγω πληροφορίες σε συστήματα. Μπορεί να μεταβιβάζει την αρμοδιότητα αυτή σε διαχειριστή πληροφοριών ή σε διαχειριστή βάσεων δεδομένων εντός του πεδίου ευθύνης του.

25.3.6. *Χρήστες*

Όλοι οι χρήστες πρέπει να φροντίζουν ώστε οι ενέργειές τους να μη θίγουν την ασφάλεια του συστήματος που χρησιμοποιούν.

25.3.7. *Κατάρτιση INFOSEC*

Διατίθεται εκπαίδευση και κατάρτιση INFOSEC σε όλα τα μέλη του προσωπικού που τη χρειάζονται.

25.4. **Μη τεχνικά μέτρα ασφάλειας**

25.4.1. *Ασφάλεια προσωπικού*

Οι χρήστες του συστήματος λαμβάνουν διαβάθμιση και έχουν «ανάγκη γνώσης» ανάλογα με τη διαβάθμιση και το περιεχόμενο των πληροφοριών που διεκπεραιώνουν στο ιδιαίτερο σύστημα τους. Για την πρόσβαση σε ορισμένα είδη εξοπλισμού ή πληροφορίες που σχετίζονται συγκεκριμένα με την ασφάλεια των συστημάτων απαιτείται ειδική διαβάθμιση που χορηγείται σύμφωνα με τις διαδικασίες της Επιτροπής.

Η ΑΔΑ καθορίζει όλες τις ευαίσθητες θέσεις και ορίζει το βαθμό διαβάθμισης και εποπτείας που απαιτείται για το σχετικό προσωπικό.

Τα συστήματα ορίζονται και σχεδιάζονται κατά τρόπο που να διευκολύνει τον καταμερισμό καθηκόντων και αρμοδιοτήτων μεταξύ των μελών του προσωπικού, ώστε ένα άτομο να μην μπορεί να έχει πλήρη γνώση ή έλεγχο των νευραλγικών σημείων ασφαλείας του συστήματος.

Στους χώρους υπολογιστών και απομακρυσμένων τερματικών/σταθμών εργασίας στους οποίους είναι δυνατόν να τροποποιηθεί η ασφάλεια του συστήματος, δεν πρέπει να υπάρχει ένας μόνον εξουσιοδοτημένος υπάλληλος ή μέλος του λοιπού προσωπικού.

Οι ρυθμίσεις ασφαλείας ενός συστήματος αλλάζουν μόνο με τη συνδυασμένη επέμβαση τουλάχιστον δύο εξουσιοδοτημένων προς τούτο μελών του προσωπικού.

25.4.2. *Υλική ασφάλεια*

Οι χώροι υπολογιστών και απομακρυσμένων τερματικών/σταθμών εργασίας (όπως ορίζονται στο τμήμα 25.2), όπου διεκπεραιώνονται, με υπολογιστή, πληροφορίες με διαβάθμιση ►**M1** CONFIDENTIEL UE ◄ και υψηλότερη, ή όπου είναι δυνατή η πρόσβαση σε παρόμοιες πληροφορίες, συγκροτούνται ως ζώνες ασφαλείας ΕΕ κατηγορίας Ι ή ΙΙ, κατά περίπτωση.

25.4.3. *Έλεγχος της πρόσβασης σε ένα σύστημα*

Όλες οι πληροφορίες και το υλικό που επιτρέπουν τον έλεγχο της πρόσβασης σε ένα σύστημα προστατεύονται με ρυθμίσεις που αντιστοιχούν στην υψηλότερη διαβάθμιση και κατηγορία των πληροφοριών στις οποίες παρέχουν πρόσβαση.

Όταν δεν χρησιμοποιούνται πλέον για το σκοπό αυτό, οι πληροφορίες και το υλικό ελέγχου της πρόσβασης καταστρέφονται κατ'εφαρμογή των διατάξεων του τμήματος 25.5.4.

25.5. **Τεχνικά μέτρα ασφάλειας**

25.5.1. *Ασφάλεια πληροφοριών*

Στο συντάκτη των πληροφοριών εναπόκειται να προσδιορίζει και να διαβαθμίζει όλα τα έγγραφα που περιέχουν πληροφορίες, είτε πρόκειται για τυπωμένα έγγραφα είτε για πληροφορικά μέσα αποθήκευσης. Η διαβάθμιση πρέπει να

▼B

αναγράφεται στο άνω και στο κάτω μέρος κάθε σελίδας τυπωμένου εγγράφου. Τα παραγόμενα έγγραφα, είτε είναι τυπωμένα είτε είναι μέσα αποθήκευσης σε υπολογιστή, πρέπει να έχουν την ίδια διαβάθμιση με την ανώτερη διαβάθμιση των πληροφοριών που χρησιμοποιούνται για την παραγωγή τους. Ο τρόπος λειτουργίας ενός συστήματος ενδέχεται να επηρεάζει τη διαβάθμιση των εγγράφων που παράγονται στο σύστημα αυτό.

Εναπόκειται στις υπηρεσίες της Επιτροπής και στους κατόχους πληροφοριών τους να εξετάζουν τα προβλήματα σώρευσης επιμέρους στοιχείων πληροφοριών και των πορισμάτων που είναι δυνατόν να αντληθούν από τα συσχετιζόμενα στοιχεία, και να αποφασίζουν κατά πόσο είναι σκόπιμο να διαβαθμίζεται με υψηλότερο βαθμό ασφαλείας το σύνολο των πληροφοριών.

Το γεγονός ότι οι πληροφορίες ενδέχεται να είναι κωδικός συντομογραφίας, κωδικός διαβίβασης ή οποιαδήποτε άλλη μορφή δυαδικής απεικόνισης δεν προσφέρει καμιά προστασία της ασφάλειας και, συνεπώς, δεν πρέπει να επηρεάζει τη διαβάθμιση των πληροφοριών.

Όταν οι πληροφορίες μεταφέρονται από ένα σύστημα σε άλλο, οι πληροφορίες πρέπει να προστατεύονται κατά τη μεταφορά επίσης στο παραλαμβάνον σύστημα κατά τρόπο ανάλογο προς την αρχική διαβάθμιση και την κατηγορία ασφαλείας των πληροφοριών αυτών.

Ο χειρισμός όλων των πληροφορικών μέσων αποθήκευσης πρέπει να είναι ανάλογος προς την ανώτερη διαβάθμιση των αποθηκευμένων πληροφοριών ή τη σήμανση του μέσου, πρέπει δε να προστατεύονται πάντοτε καταλλήλως.

Τα επαναχρησιμοποιήσιμα μέσα αποθήκευσης σε υπολογιστή που χρησιμοποιούνται για την καταγραφή διαβαθμισμένων πληροφοριών ΕΕ διατηρούν την ανώτερη διαβάθμιση για την οποία ποτέ χρησιμοποιήθηκαν, μέχρις ότου οι πληροφορίες αυτές υποχαρακτηριστούν ή αποχαρακτηριστούν και τα μέσα αναχαρακτηριστούν ανάλογα, ή τα μέσα αποχαρακτηριστούν και καταστραφούν σύμφωνα με εγκεκριμένη από την ΑΔΑ διαδικασία (βλέπε τμήμα 25.5.4).

25.5.2. *Έλεγχος και λογοδότηση πληροφοριών*

Τηρούνται αυτόματα (ίχνη ελέγχου) ή χειρόγραφα μητρώα στα οποία καταγράφεται η πρόσβαση σε πληροφορίες με διαβάθμιση ►**M1** SECRET UE ◄ ή υψηλότερη. Τα μητρώα αυτά φυλάσσονται σύμφωνα με τους παρόντες κανόνες ασφαλείας.

Τα διαβαθμισμένα έγγραφα ΕΕ που διατηρούνται σε χώρο υπολογιστών μπορούν να αντιμετωπίζονται σαν ένα διαβαθμισμένο αντικείμενο και δεν χρειάζεται να καταχωρούνται, εφόσον το υλικό φέρει αναγνωριστικά στοιχεία και σήμανση της διαβάθμισής του και ελέγχεται κατάλληλα.

Όταν από σύστημα που διεκπεραιώνει διαβαθμισμένες πληροφορίες ΕΕ παράγονται έγγραφα που διαβιβάζονται από χώρο υπολογιστών σε απομακρυσμένο τερματικό/σταθμό εργασίας, θεσπίζονται διαδικασίες, εγκεκριμένες από την ΑΔΑ, για τον έλεγχο και την καταχώρηση των παραγόμενων εγγράφων. Για τα υλικά με διαβάθμιση ►**M1** SECRET UE ◄ ή υψηλότερη, οι διαδικασίες αυτές περιλαμβάνουν συγκεκριμένες οδηγίες για τη λογοδότηση των πληροφοριών.

25.5.3. *Χειρισμός και έλεγχος αφαιρετών πληροφορικών μέσων αποθήκευσης*

Όλα τα αφαιρετά πληροφορικά μέσα αποθήκευσης με διαβάθμιση ►**M1** CONFIDENTIEL UE ◄ ή υψηλότερη πρέπει να αντιμετωπίζονται σαν υλικό και υπόκεινται στους γενικούς κανόνες. Οι κατάλληλες σημάνσεις αναγνώρισης και διαβάθμισης πρέπει να είναι προσαρμοσμένες στη συγκεκριμένη υλική εμφάνιση των μέσων, ώστε να είναι δυνατή η σαφής αναγνώρισή τους.

Οι χρήστες φροντίζουν ώστε οι διαβαθμισμένες πληροφορίες ΕΕ αποθηκεύονται σε μέσα με την κατάλληλη σήμανση διαβάθμισης και προστασία. Θα θεσπιστούν διαδικασίες για να διασφαλίζεται ότι, για όλα τα επίπεδα των πληροφοριών ΕΕ, οι πληροφορίες αποθηκεύονται σε πληροφορικά μέσα αποθήκευσης σύμφωνα με τους παρόντες κανόνες ασφαλείας.

25.5.4. *Αποχαρακτηρισμός και καταστροφή πληροφορικών μέσων αποθήκευσης*

Τα πληροφορικά μέσα αποθήκευσης που χρησιμοποιούνται για την καταγραφή διαβαθμισμένων πληροφοριών ΕΕ μπορούν να υποχαρακτηρίζονται ή αποχαρακτηρίζονται εφόσον τηρούνται εγκεκριμένες από την ΑΔΑ διαδικασίες.

Τα πληροφορικά μέσα αποθήκευσης στα οποία είχαν αποθηκευθεί πληροφορίες ►**M1** TRES SECRET UE/EU TOP SECRET ◄ ή ειδικής κατηγορίας δεν αποχαρακτηρίζονται προς επαναχρησιμοποίηση.

Εάν τα πληροφορικά μέσα αποθήκευσης δεν είναι δυνατόν να αποχαρακτηριστούν ή δεν είναι επαναχρησιμοποιήσιμα, καταστρέφονται σύμφωνα με την προαναφερόμενη διαδικασία.

▼**B**

25.5.5. *Ασφάλεια επικοινωνιών*

Ο ►**M2** δευθυντής της Διεύθυνσης Ασφαλείας της Επιτροπής ◄ είναι η αρχή κρυπτογράφησης.

Όταν διαβαθμισμένες πληροφορίες ΕΕ διαβιβάζονται με ηλεκτρομαγνητικά μέσα, λαμβάνονται ειδικά μέτρα για να προστατεύεται η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα των ούτως διαβιβαζόμενων πληροφοριών. Η ΑΔΑ καθορίζει τις απαιτήσεις για την προστασία των διαβιβαζόμενων πληροφοριών από ανίχνευση και υποκλοπή. Οι πληροφορίες που διαβιβάζονται μέσω επικοινωνιακού συστήματος προστατεύονται βάσει των απαιτήσεων εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας.

Όταν απαιτούνται κρυπτογραφικές μέθοδοι για να εξασφαλίζεται η προστασία της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας, οι μέθοδοι αυτές και τα συναφή προϊόντα τους εγκρίνονται ειδικώς για το σκοπό αυτόν από την ΑΔΑ ως την αρχή κρυπτογράφησης.

Κατά τη διαβίβαση, η εμπιστευτικότητα των πληροφοριών με διαβάθμιση ►**M1** SECRET UE ◄ ή υψηλότερη προστατεύεται με κρυπτογραφικές μεθόδους ή προϊόντα εγκεκριμένα από το αρμόδιο επί θεμάτων ασφαλείας μέλος της Επιτροπής μετά από διαβούλευση με τη συμβουλευτική ομάδα επί θεμάτων πολιτικής ασφάλειας της Επιτροπής. Κατά τη διαβίβαση, η εμπιστευτικότητα των πληροφοριών με διαβάθμιση ►**M1** CONFIDENTIEL UE ◄ ή ►**M1** RESTREINT UE ◄ προστατεύεται με κρυπτογραφικές μεθόδους ή προϊόντα εγκεκριμένα από την αρχή κρυπτογράφησης της Επιτροπής μετά από διαβούλευση με τη συμβουλευτική ομάδα επί θεμάτων πολιτικής ασφάλειας της Επιτροπής.

Σε ειδικές οδηγίες ασφαλείας εγκεκριμένες από την►**M2** Διεύθυνση Ασφαλείας της Επιτροπής ◄, μετά από διαβούλευση με τη συμβουλευτική ομάδα επί θεμάτων πολιτικής ασφάλειας της Επιτροπής, καθορίζονται λεπτομερείς κανόνες για τη διαβίβαση διαβαθμισμένων πληροφοριών ΕΕ.

Υπό εξαιρετικές επιχειρησιακές περιστάσεις, πληροφορίες με διαβάθμιση ►**M1** RESTREINT UE ◄, ►**M1** CONFIDENTIEL UE ◄ και ►**M1** SECRET UE ◄ επιτρέπεται να διαβιβάζονται ακρυπτογράφητες, υπό την προϋπόθεση ότι χορηγείται ρητή άδεια για κάθε περίπτωση, η οποία καταχωρείται δεόντως από τον ιδιοκτήτη των πληροφοριών. Οι εξαιρετικές αυτές περιστάσεις είναι οι εξής:

α) κατά τις καταστάσεις επικείμενης ή πραγματικής κρίσης, σύγκρουσης ή πολέμου και

β) όταν η ταχύτητα παράδοσης έχει υπέρτατη σημασία, δεν υπάρχουν μέσα κρυπτογράφησης και κρίνεται ότι οι διαβιβαζόμενες πληροφορίες δεν είναι δυνατόν να αξιοποιηθούν εγκαίρως για να επηρεάσουν αρνητικά τις επιχειρήσεις.

Ένα σύστημα πρέπει να είναι ικανό να απαγορεύει ρητά την πρόσβαση σε διαβαθμισμένες πληροφορίες ΕΕ μέσω οποιουδήποτε ή όλων των απομακρυσμένων σταθμών εργασίας ή τερματικών του, όταν απαιτείται, είτε με υλική αποσύνδεση είτε μέσω εγκεκριμένων από την ΑΔΑ ειδικών χαρακτηριστικών του λογισμικού.

25.5.6. *Εγκατάσταση και ασφάλεια ακτινοβολίας*

Η αρχική εγκατάσταση και τυχόν μείζονες αλλαγές των συστημάτων προδιαγράφονται κατά τρόπο ώστε η εγκατάσταση να πραγματοποιείται από εγκαταστάτες με διαβάθμιση ασφαλείας υπό τη μόνιμη επίβλεψη προσωπικού με τα δέοντα τεχνικά προσόντα, το οποίο είναι διαβαθμισμένο για πρόσβαση σε διαβαθμισμένες πληροφορίες ΕΕ μέχρις επιπέδου που ισοδυναμεί προς την υψηλότερη διαβάθμιση των πληροφοριών που αναμένεται να αποθηκεύει και να διεκπεραιώνει το σύστημα.

Τα συστήματα που χειρίζονται πληροφορίες με διαβάθμιση ►**M1** CONFIDENTIEL UE ◄ ή υψηλότερη προστατεύονται κατά τρόπο ώστε η ασφάλειά τους να μην απειλείται από διαρρέουσες εκπομπές, η μελέτη και ο έλεγχος των οποίων αναφέρονται ως «Tempest».

Τα αντίμετρα «Tempest» επανεξετάζονται και εγκρίνονται από την αρχή Tempest (βλέπε τμήμα 25.3.2).

25.6. **Ασφάλεια κατά το χειρισμό**

25.6.1. *Λειτουργικές διαδικασίες ασφαλείας (SecOPs)*

Στις λειτουργικές διαδικασίες ασφαλείας (SecOP) καθορίζονται οι αρχές που πρέπει να θεσπίζονται για θέματα ασφαλείας, οι ακολουθητέες λειτουργικές διαδικασίες και οι ευθύνες του προσωπικού. Οι SecOPs εκπονούνται υπό την ευθύνη του ιδιοκτήτη τεχνικών συστημάτων (TSO).

▼B

25.6.2. *Διαχείριση της προστασίας/διάταξης λογισμικού*

Η προστασία ασφαλείας των προγραμμάτων εφαρμογών καθορίζεται βάσει μιας αξιολόγησης της διαβάθμισης ασφαλείας του ίδιου του προγράμματος και όχι των πληροφοριών που χειρίζεται. Οι χρησιμοποιούμενες εκδόσεις λογισμικού πρέπει να ελέγχονται κατά τακτά διαστήματα ώστε να εξασφαλίζεται η ακεραιότητά τους και η ορθή λειτουργία τους.

Νέες ή τροποποιημένες εκδόσεις λογισμικού δεν χρησιμοποιούνται για τη διεκπεραίωση διαβαθμισμένων πληροφοριών ΕΕ πριν ελεγχθούν από τον TSO.

25.6.3. *Έλεγχος παρουσίας δόλιου λογισμικού/ών υπολογιστών*

Ο έλεγχος της παρουσίας δόλιου λογισμικού/ών υπολογιστών διενεργείται τακτικά σύμφωνα με τις απαιτήσεις της ΑΔΑ.

Όλα τα πληροφορικά μέσα αποθήκευσης που διαβιβάζονται στην Επιτροπή ελέγχονται για την παρουσία τυχόν δόλιου λογισμικού ή ιών υπολογιστών πριν εισέλθουν σε οποιοδήποτε σύστημα.

25.6.4. *Συντήρηση*

Οι συμβάσεις και οι διαδικασίες για την προγραμματισμένη και την έκτακτη συντήρηση των συστημάτων για τα οποία έχει εκπονηθεί SSRS πρέπει να προδιαγράφουν τις απαιτήσεις και τις ρυθμίσεις για την είσοδο του προσωπικού συντήρησης και του εξοπλισμού του σε χώρο υπολογιστών.

Οι απαιτήσεις πρέπει να αναφέρονται σαφώς στην SSRS, οι δε διαδικασίες πρέπει να αναφέρονται σαφώς στις SecOPs. Η συντήρηση από συμβασιούχο για την οποία απαιτούνται διαγνωστικές διαδικασίες με τηλεπρόσβαση επιτρέπεται μόνον σε εξαιρετικές περιπτώσεις, υπό αυστηρό έλεγχο ασφαλείας, και μόνον με την έγκριση της ΑΔΑ.

25.7. **Προμήθειες**

25.7.1. *Γενικά*

Κάθε προϊόν ασφαλείας, το οποίο πρόκειται να αγοραστεί για να χρησιμοποιηθεί με το σύστημα, είτε θα έχει αξιολογηθεί και πιστοποιηθεί, είτε θα τελεί ήδη υπό αξιολόγηση και έγκριση από αρμόδιο φορέα αξιολόγησης ή πιστοποίησης ενός εκ των κρατών μελών της ΕΕ, βάσει διεθνώς αναγνωρισμένων κριτηρίων (π.χ. των κοινών κριτηρίων για την αξιολόγηση της ασφαλείας της πληροφορικής τεχνολογίας, βλέπε ISO 15408). Απαιτούνται ειδικές διαδικασίες για να ληφθεί έγκριση εκ μέρους της ΣΕΠΣ.

Όταν αποφασίζεται η μίσθωση αντί της αγοράς εξοπλισμού, ιδίως δε πληροφορικών υποθεμάτων αποθήκευσης, λαμβάνεται υπόψη το γεγονός ότι ο εξοπλισμός αυτός, αφού χρησιμοποιηθεί για το χειρισμό διαβαθμισμένων πληροφοριών ΕΕ, δεν μπορεί να αποδεσμεύεται σε μη καταλλήλως ασφαλές περιβάλλον αν δεν αποχαρακτηριστεί προηγουμένως βάσει εγκρίσεως της ΑΔΑ, και ότι η έγκριση αυτή ενδέχεται να μην είναι πάντοτε δυνατή.

25.7.2. *Διαπίστευση*

Πριν χειριστούν διαβαθμισμένες πληροφορίες ΕΕ, όλα τα συστήματα για τα οποία έχει εκπονηθεί SSRS λαμβάνουν διαπίστευση από την ΑΔΑ βάσει των πληροφοριών που περιέχονται στη SSRS, στις SecOPs ή σε κάθε άλλο σχετικό έγγραφο. Τα υποσυστήματα και τα απομακρυσμένα τερματικά/σταθμοί εργασίας λαμβάνουν διαπίστευση ως μέρη όλων των συστημάτων στα οποία συνδέονται. Όταν ένα σύστημα χρησιμοποιείται τόσο από την Επιτροπή όσο και από άλλους οργανισμούς, η Επιτροπή και οι αρμόδιες αρχές ασφαλείας πρέπει να συμφωνούν μεταξύ τους για τη διαπίστευση.

Η διαδικασία διαπίστευσης μπορεί να διεξάγεται σύμφωνα με μια σχετική στρατηγική που είναι κατάλληλη για το συγκεκριμένο σύστημα, που καθορίζεται από την ΑΔΑ.

25.7.3. *Αξιολόγηση και πιστοποίηση*

Σε ορισμένες περιπτώσεις, πριν από τη διαπίστευση, τα χαρακτηριστικά ασφαλείας του υλικού, του υλικολογισμικού και του λογισμικού ενός συστήματος αξιολογούνται και πιστοποιούνται ως ικανά να διασφαλίζουν την απαιτούμενη ασφάλεια για το σκοπούμενο βαθμό διαβάθμισης.

Οι απαιτήσεις αξιολόγησης και πιστοποίησης περιλαμβάνονται στον προγραμματισμό του συστήματος και αναφέρονται ρητά στην SSRS.

Οι διαδικασίες αξιολόγησης και πιστοποίησης διεξάγονται σύμφωνα με εγκεκριμένες κατευθυντήριες γραμμές και από προσωπικό με τα δέοντα τεχνικά προσόντα και την κατάλληλη διαβάθμιση ασφαλείας, που ενεργεί εξ ονόματος του TSO.

▼B

Οι ομάδες μπορούν να προέρχονται από μια οριζόμενη αρχή αξιολόγησης ή πιστοποίησης ενός κράτους μέλους ή από τους οριζόμενους εκπροσώπους της, π.χ. έναν αρμόδιο και διαβαθμισμένο εργολάβο.

Ο βαθμός των εμπλεκόμενων διαδικασιών αξιολόγησης και πιστοποίησης μπορεί να μειώνεται (ώστε να καλύπτουν π.χ. μόνο πτυχές ενοποίησης) όταν τα συστήματα βασίζονται σε υφιστάμενα προϊόντα ασφαλείας υπολογιστών τα οποία αξιολογούνται και πιστοποιούνται σε εθνικό επίπεδο.

25.7.4. *Στερεότυπος έλεγχος των χαρακτηριστικών ασφαλείας για συνεχιζόμενη διαπίστευση*

Ο TSO εκπονεί διαδικασίες στερεότυπου ελέγχου οι οποίες διασφαλίζουν ότι εξακολουθούν να ισχύουν όλα τα χαρακτηριστικά ασφαλείας του συστήματος.

Στην SSRS προσδιορίζεται και αναφέρεται σαφώς το είδος αλλαγών για τις οποίες απαιτείται επαναδιαπίστευση ή προηγούμενη έγκριση της ΑΔΑ. Ύστερα από κάθε τροποποίηση, επισκευή ή αστοχία που ενδέχεται να έχει θίξει τα χαρακτηριστικά ασφαλείας του συστήματος, ο TSO φροντίζει να διενεργείται έλεγχος προκειμένου να εξασφαλίζεται η ορθή λειτουργία των χαρακτηριστικών ασφαλείας. Η διατήρηση της διαπίστευσης του συστήματος εξαρτάται κανονικά από την ικανοποιητική διεξαγωγή των ελέγχων.

Όλα τα συστήματα στα οποία έχουν εφαρμοστεί χαρακτηριστικά ασφαλείας επιθεωρούνται ή εξετάζονται τακτικά από την ΑΔΑ. Για τα συστήματα που διεκπεραιώνουν πληροφορίες ►**M1** TRES SECRET UE/EU TOP SECRET ◄, οι επιθεωρήσεις διεξάγονται τουλάχιστον μία φορά το χρόνο.

25.8. **Προσωρινή ή περιστασιακή χρήση**

25.8.1. *Ασφάλεια μικροϋπολογιστών/προσωπικών υπολογιστών*

Οι μικροϋπολογιστές/προσωπικοί υπολογιστές (PC) με σκληρούς δίσκους (ή άλλα υποθέματα μη πτητικής αποθήκευσης), οι οποίοι λειτουργούν είτε ανεξάρτητα είτε ως μέρος δικτύου, καθώς και οι φορητές υπολογιστικές συσκευές (π.χ. φορητοί PC και ηλεκτρονικά «σημειωματάρια») με σταθερούς σκληρούς δίσκους, θεωρούνται ως μέσα αποθήκευσης πληροφοριών κατά την ίδια έννοια όπως και οι δισκέτες ή τα άλλα αφαιρετά πληροφορικά μέσα αποθήκευσης.

Οι συσκευές αυτές προστατεύονται, όσον αφορά την πρόσβαση, το χειρισμό, την αποθήκευση και τη μεταφορά, ανάλογα με τον ανώτερο βαθμό ασφαλείας των πληροφοριών τις οποίες έχουν ποτέ αποθηκεύσει ή επεξεργαστεί (μέχρις ότου υποχαρακτηριστούν ή αποχαρακτηριστούν σύμφωνα με εγκεκριμένες διαδικασίες).

25.8.2. *Χρήση ιδιωτικού εξοπλισμού πληροφορικής για επίσημη εργασία στους κόλπους της Επιτροπής*

Η χρήση ιδιωτικών αφαιρετών πληροφορικών μέσων αποθήκευσης, λογισμικού και υλικού πληροφορικής (π.χ. PC και φορητών υπολογιστικών συσκευών) με ικανότητα αποθήκευσης απαγορεύεται για το χειρισμό διαβαθμισμένων πληροφοριών ΕΕ.

Απαγορεύεται η είσοδος ιδιωτικού υλικού υπολογιστών, λογισμικού και μέσων αποθήκευσης σε χώρους κατηγορίας I ή II όπου γίνεται χειρισμός διαβαθμισμένων πληροφοριών ΕΕ χωρίς τη γραπτή άδεια του ►**M2** Διευθυντή της Διεύθυνσης Ασφαλείας της Επιτροπής ◄. Η άδεια αυτή μπορεί να χορηγηθεί για τεχνικούς λόγους σε εξαιρετικές περιπτώσεις.

25.8.3. *Χρήση εξοπλισμού πληροφορικής που ανήκει σε εργολάβους ή παρέχεται από εθνικές αρχές, για επίσημη εργασία στους κόλπους της Επιτροπής*

Η χρήση συσκευών πληροφορικής και λογισμικού που ανήκουν σε εργολάβους σε οργανώσεις προς υποστήριξη επίσημων εργασιών της Επιτροπής μπορεί να επιτρέπεται από τον προϊστάμενο της►**M2** Διεύθυνσης Ασφαλείας της Επιτροπής ◄. Είναι δυνατόν επίσης να επιτρέπεται η χρήση εξοπλισμού πληροφορικής και λογισμικού που παρέχονται από αρχή κράτους μέλους· στην περίπτωση αυτήν, ο εξοπλισμός πληροφορικής καταχωρείται στον κατάλληλο κατάλογο της Επιτροπής. Και στις δύο περιπτώσεις, εάν οι συσκευές πληροφορικής πρόκειται να χρησιμοποιηθούν για το χειρισμό διαβαθμισμένων πληροφοριών ΕΕ, πρέπει να ζητείται η γνώμη της ΑΔΑ ώστε να λαμβάνονται δεόντως υπόψη και να εφαρμόζονται τα στοιχεία INFOSEC που ισχύουν για τη χρήση των συσκευών αυτών.

26. ΚΟΙΝΟΠΟΙΗΣΗ ΔΙΑΒΑΘΜΙΣΜΕΝΩΝ ΠΛΗΡΟΦΟΡΙΩΝ ΕΕ ΣΕ ΤΡΙΤΑ ΚΡΑΤΗ Ή ΔΙΕΘΝΕΙΣ ΟΡΓΑΝΙΣΜΟΥΣ

26.1.1. *Αρχές που διέπουν την κοινοποίηση διαβαθμισμένων πληροφοριών ΕΕ*

Η Επιτροπή εν σώματι αποφασίζει για την κοινοποίηση διαβαθμισμένων πληροφοριών ΕΕ σε τρίτα κράτη ή διεθνείς οργανισμούς βάσει:

▼**B**

— της φύσης και του περιεχομένου των πληροφοριών αυτών,

— της ανάγκης γνώσης του αποδέκτη,

— των πλεονεκτημάτων για την ΕΕ.

Ζητείται η συμφωνία του συντάκτη των προς κοινοποίηση διαβαθμισμένων πληροφοριών ΕΕ.

Οι αποφάσεις αυτές λαμβάνονται κατά περίπτωση, ανάλογα με:

— τον επιθυμητό βαθμό συνεργασίας με τα συγκεκριμένα τρίτα κράτη ή διεθνείς οργανισμούς,

— την εμπιστοσύνη που εμπνέουν, η οποία απορρέει από το βαθμό ασφαλείας που θα αποδώσουν στις διαβαθμισμένες πληροφορίες ΕΕ που κοινοποιούνται σε αυτά τα κράτη ή οργανισμούς και από τη συνέπεια μεταξύ των κανόνων ασφαλείας τους και των κανόνων ασφαλείας της ΕΕ· Η Συμβουλευτική Ομάδα της Επιτροπής για την Πολιτική Ασφάλειας παρέχει στην Επιτροπή την τεχνική γνωμοδότησή της στο σημείο αυτό.

Η αποδοχή, από τρίτα κράτη ή διεθνείς οργανισμούς, διαβαθμισμένων πληροφοριών ΕΕ συνεπάγεται την εγγύηση ότι οι πληροφορίες αυτές θα χρησιμοποιηθούν μόνον για τους σκοπούς που αιτιολογούν την κοινοποίηση ή ανταλλαγή πληροφοριών, και ότι τα κράτη ή οι οργανισμοί αυτοί θα παρέχουν την προστασία που απαιτεί η Επιτροπή.

26.1.2. *Επίπεδα*

Όταν η Επιτροπή αποφασίσει ότι επιτρέπεται η κοινοποίηση ή ανταλλαγή διαβαθμισμένων πληροφοριών με συγκεκριμένο κράτος ή διεθνή οργανισμό, αποφασίζει και για το επίπεδο συνεργασίας το οποίο είναι δυνατό. Το επίπεδο αυτό εξαρτάται ιδίως από την πολιτική και τους κανονισμούς ασφαλείας που εφαρμόζει αυτό το κράτος ή οργανισμός.

Προβλέπονται τρία επίπεδα συνεργασίας:

Επίπεδο 1

Συνεργασία με τρίτα κράτη ή με διεθνείς οργανισμούς των οποίων η πολιτική και οι κανονισμοί ασφαλείας είναι πολύ παρόμοιοι με εκείνους της ΕΕ.

Επίπεδο 2

Συνεργασία με τρίτα κράτη ή με διεθνείς οργανισμούς των οποίων η πολιτική και οι κανονισμοί ασφαλείας διαφέρουν σημαντικά από τους κοινοτικούς.

Επίπεδο 3

Περιστασιακή συνεργασία με τρίτα κράτη ή με διεθνείς οργανισμούς των οποίων δεν είναι δυνατόν να αξιολογηθούν η πολιτική και οι κανονισμοί ασφαλείας.

Κάθε επίπεδο συνεργασίας καθορίζει τις διαδικασίες και τις διατάξεις ασφαλείας που αναφέρονται λεπτομερώς στα παραρτήματα 3, 4 και 5.

26.1.3. *Συμφωνίες για την ασφάλεια*

Όταν η Επιτροπή αποφασίσει ότι υπάρχει μόνιμη ή μακροχρόνια ανάγκη ανταλλαγής διαβαθμισμένων πληροφοριών μεταξύ της Επιτροπής και τρίτων κρατών ή άλλων διεθνών οργανισμών, καταρτίζει με αυτούς «συμφωνίες για διαδικασίες ασφαλείας για την ανταλλαγή διαβαθμισμένων πληροφοριών», στις οποίες ορίζονται ο σκοπός της συνεργασίας και οι αμοιβαίοι κανόνες για την προστασία των ανταλλασσόμενων πληροφοριών.

Στην περίπτωση της περιστασιακής συνεργασίας επιπέδου 3, η οποία, εξ ορισμού, έχει περιορισμένη χρονική διάρκεια και σκοπό, αντί της «συμφωνίας για διαδικασίες ασφαλείας για την ανταλλαγή διαβαθμισμένων πληροφοριών», είναι δυνατόν να καταρτίζεται απλό μνημόνιο συμφωνίας στο οποίο ορίζονται η φύση των προς ανταλλαγή διαβαθμισμένων πληροφοριών και οι αμοιβαίες υποχρεώσεις όσον αφορά τις πληροφορίες αυτές, υπό την προϋπόθεση ότι η διαβάθμιση των πληροφοριών αυτών δεν υπερβαίνει το ►**M1** RESTREINT UE ◄.

Πριν υποβληθούν προς έγκριση στην Επιτροπή, τα σχέδια συμφωνιών για τις διαδικασίες ασφαλείας ή τα μνημόνια συμφωνίας συζητούνται στην συμβουλευτική ομάδα της Επιτροπής για την πολιτική ασφάλειας.

▼B

Το αρμόδιο για θέματα ασφαλείας μέλος της Επιτροπής ζητεί από τις ΕΑΑ των κρατών μελών κάθε απαιτούμενη βοήθεια, για να εξασφαλίζεται ότι οι προς κοινοποίηση πληροφορίες θα χρησιμοποιούνται και θα προστατεύονται σύμφωνα με τις διατάξεις των συμφωνιών για τις διαδικασίες ασφαλείας ή των μνημονίων συμφωνίας.

▼M3

27. ΚΟΙΝΕΣ ΣΤΟΙΧΕΙΩΔΕΙΣ ΠΡΟΔΙΑΓΡΑΦΕΣ ΓΙΑ ΤΗ ΒΙΟΜΗΧΑΝΙΚΗ ΑΣΦΑΛΕΙΑ

27.1. **Εισαγωγή**

Το παρόν τμήμα εξετάζει τις πτυχές ασφάλειας βιομηχανικών δραστηριοτήτων που αφορούν αποκλειστικά τη διαπραγμάτευση και ανάθεση συμβάσεων ή τη σύναψη συμφωνιών επιχορήγησης, με τις οποίες ανατίθενται καθήκοντα που αφορούν, συνεπάγονται ή/και περιλαμβάνουν διαβαθμισμένες πληροφορίες ΕΕ, και την υλοποίηση αυτών των συμβάσεων από βιομηχανικούς ή άλλους φορείς, συμπεριλαμβανομένης της διάθεσης διαβαθμισμένων πληροφοριών ΕΕ ή της πρόσβασης σε αυτές κατά τις διαδικασίες ανάθεσης κρατικών συμβάσεων και πρόσκλησης υποβολής προτάσεων (περίοδος υποβολής προσφορών και διαπραγματεύσεις πριν από την ανάθεση της σύμβασης).

27.2. **Ορισμοί**

Για τους σκοπούς αυτών των κοινών στοιχειωδών προδιαγραφών, ισχύουν οι ακόλουθοι ορισμοί:

α) «διαβαθμισμένη σύμβαση»: σύμβαση ή συμφωνία επιχορήγησης για την προμήθεια υλικού, την εκτέλεση έργων, τη διάθεση κτιρίων ή την παροχή υπηρεσιών, της οποίας η υλοποίηση απαιτεί ή περιλαμβάνει την πρόσβαση σε διαβαθμισμένες πληροφορίες ΕΕ ή την παραγωγή τέτοιων πληροφοριών·

β) «διαβαθμισμένη σύμβαση υπεργολαβίας»: σύμβαση που συνάπτεται μεταξύ ενός κύριου εργολάβου ή δικαιούχου επιχορήγησης και ενός υπεργολάβου (επιμέρους συμβαλλόμενου) για την προμήθεια υλικού, την εκτέλεση έργων, τη διάθεση κτιρίων ή την παροχή υπηρεσιών, της οποίας η υλοποίηση απαιτεί ή περιλαμβάνει την πρόσβαση σε διαβαθμισμένες πληροφορίες ΕΕ ή την παραγωγή τέτοιων πληροφοριών·

γ) «εργολάβος»: οικονομικός φορέας ή νομική οντότητα που έχει τη νομική ικανότητα να αναλάβει συμβάσεις ή να είναι δικαιούχος επιχορήγησης·

δ) «καθορισμένη αρχή ασφαλείας (ΚΑΑ)»: αρχή η οποία είναι υπόλογη στην εθνική αρχή ασφαλείας (ΕΑΑ) κράτους μέλους της ΕΕ και έχει καθήκον, αφενός, να ενημερώνει τη βιομηχανία και άλλους φορείς σχετικά με την εθνική πολιτική στα θέματα βιομηχανικής ασφάλειας και, αφετέρου, να τους καθοδηγεί και να τους συνδράμει κατά την εφαρμογή της εν λόγω εθνικής πολιτικής. Η ΕΑΑ μπορεί να ασκεί τα καθήκοντα της ΚΑΑ·

ε) «έλεγχος ασφαλείας φορέα (ΕΑΦ)»: διοικητική απόφαση της ΕΑΑ/ΚΑΑ η οποία πιστοποιεί ότι, από πλευράς ασφάλειας, ο φορέας μπορεί να εξασφαλίσει επαρκώς την προστασία διαβαθμισμένων πληροφοριών ΕΕ ορισμένου βαθμού ασφαλείας και ότι το προσωπικό του, που χρειάζεται να έχει πρόσβαση σε διαβαθμισμένες πληροφορίες ΕΕ, υπόκειται στον δέοντα έλεγχο ασφαλείας και έχει ενημερωθεί για τις απαιτήσεις ασφαλείας που είναι αναγκαίες για την πρόσβαση σε διαβαθμισμένες πληροφορίες ΕΕ και για την προστασία αυτών των πληροφοριών·

στ) «βιομηχανικός ή άλλος φορέας»: κύριος εργολάβος ή υπεργολάβος που ασχολείται με την προμήθεια υλικών αγαθών, την εκτέλεση έργων ή την παροχή υπηρεσιών· ο ορισμός αυτός αφορά βιομηχανικούς, εμπορικούς, επιστημονικούς, ερευνητικούς, εκπαιδευτικούς ή αναπτυξιακούς φορείς καθώς και φορείς παροχής υπηρεσιών·

ζ) «βιομηχανική ασφάλεια»: η εφαρμογή προστατευτικών μέτρων και διαδικασιών ώστε να προλαμβάνεται, να εντοπίζεται και να αποκαθίσταται η απώλεια ή η διαρροή διαβαθμισμένων πληροφοριών ΕΕ τις οποίες διαχειρίζεται ο κύριος εργολάβος ή ο υπεργολάβος κατά τις διαπραγματεύσεις (προ της) ανάθεσης της σύμβασης και κατά την εκτέλεση διαβαθμισμένων συμβάσεων·

η) «εθνική αρχή ασφαλείας (ΕΑΑ)»: η κρατική αρχή κράτους μέλους της ΕΕ που έχει την τελική ευθύνη για την προστασία των διαβαθμισμένων πληροφοριών ΕΕ εντός του εν λόγω κράτους μέλους·

θ) «συνολική διαβάθμιση ασφαλείας της σύμβασης»: καθορισμός της διαβάθμισης ασφαλείας της σύμβασης στο σύνολό της ή της συμφωνίας επιχορήγησης, με βάση τη διαβάθμιση των πληροφοριών ή/και του υλικού που πρόκειται ή ενδέχεται να παραχθούν, να διατεθούν ή να προσπελαθούν δυνάμει οιουδήποτε μέρους της σύμβασης ή της συμφωνίας επιχορήγησης. Η συνολική διαβάθμιση ασφαλείας μιας σύμβασης δεν επιτρέπεται να είναι κατώτερη από την ανώτατη διαβάθμιση οποιουδήποτε μέρους της αλλά μπορεί να είναι ανώτερη λόγω του αθροιστικού αποτελέσματος·

▼**M3**

ι) «έγγραφο θεμάτων ασφαλείας (ΕΘΑ)»: έγγραφο ειδικών συμβατικών όρων, που εκδίδει η αναθέτουσα αρχή, το οποίο αποτελεί αναπόσπαστο μέρος διαβαθμισμένης σύμβασης που συνεπάγεται πρόσβαση σε διαβαθμισμένες πληροφορίες ΕΕ ή παραγωγή συναφών πληροφοριών και το οποίο καθορίζει τις απαιτήσεις ασφαλείας ή τα στοιχεία της διαβαθμισμένης σύμβασης που χρειάζονται προστασία·

ια) «οδηγός διαβάθμισης ασφαλείας (ΟΔΑ)»: έγγραφο στο οποίο περιγράφονται τα στοιχεία προγράμματος, της σύμβασης ή της συμφωνίας επιχορήγησης, τα οποία 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. Ο ΟΔΑ πρέπει να αποτελεί τμήμα του ΕΘΑ.

27.3. **Οργάνωση**

α) Η Επιτροπή μπορεί να αναθέτει με διαβαθμισμένη σύμβαση σε βιομηχανικούς ή άλλους φορείς που έχουν την έδρα τους σε κράτος μέλος, καθήκοντα που αφορούν, συνεπάγονται ή/και περιλαμβάνουν διαβαθμισμένες πληροφορίες ΕΕ.

β) Κατά την ανάθεση διαβαθμισμένων συμβάσεων, η Επιτροπή διασφαλίζει ότι τηρούνται όλες οι απαιτήσεις που απορρέουν από τις στοιχειώδεις προδιαγραφές.

γ) Η Επιτροπή θα συμπεριλάβει τις αντίστοιχες ΕΑΑ ή ΚΑΑ έτσι ώστε να εφαρμόζει τις στοιχειώδεις προδιαγραφές περί βιομηχανικής ασφάλειας. Οι ΕΑΑ δύνανται να αναθέτουν τα εν λόγω καθήκοντα σε μία ή περισσότερες ΚΑΑ.

δ) Την τελική ευθύνη για την προστασία των διαβαθμισμένων πληροφοριών ΕΕ εντός βιομηχανικών ή άλλων φορέων φέρουν οι διευθυντικοί διαχειριστές των εν λόγω οντοτήτων.

ε) Όταν ανατίθεται διαβαθμισμένη σύμβαση ή σύμβαση υπεργολαβίας, η οποία υπόκειται στις στοιχειώδεις προδιαγραφές, η Επιτροπή ή/και οι ΕΑΑ/ΚΑΑ, αναλόγως, ενημερώνουν αμέσως την ΕΑΑ/ΚΑΑ του κράτους μέλους στο οποίο έχει την έδρα του ο κύριος εργολάβος ή ο υπεργολάβος.

27.4. **Διαβαθμισμένες συμβάσεις και αποφάσεις επιχορηγήσεων**

α) Για τη διαβάθμιση ασφαλείας των συμβάσεων ή των συμφωνιών επιχορήγησης πρέπει να λαμβάνονται υπόψη οι ακόλουθες αρχές:

— η Επιτροπή καθορίζει, αναλόγως, τα εν λόγω σημεία της διαβαθμισμένης σύμβασης που πρέπει να προστατευθούν και τη συνεπαγόμενη διαβάθμιση ασφαλείας, λαμβάνοντας υπόψη την αρχική διαβάθμιση ασφαλείας, την οποία έχει καθορίσει η πηγή προέλευσης, για πληροφορίες παραχθείσες πριν από την ανάθεση της διαβαθμισμένης σύμβασης,

— η συνολική διαβάθμιση ασφαλείας της σύμβασης δεν επιτρέπεται να είναι κατώτερη από την ανώτατη διαβάθμιση οποιουδήποτε μέρους της,

— οι διαβαθμισμένες πληροφορίες ΕΕ που παράγονται κατά τη διάρκεια συμβατικής δραστηριότητας διαβαθμίζονται σύμφωνα με τον οδηγό διαβάθμισης ασφαλείας,

— όταν χρειάζεται, η Επιτροπή έχει την αρμοδιότητα να μεταβάλλει τη συνολική διαβάθμιση ασφαλείας της σύμβασης ή τη διαβάθμιση ασφαλείας οιουδήποτε μέρους της σύμβασης, κατόπιν διαβούλευσης με την πηγή προέλευσής της, καθώς και να ενημερώνει όλα τα ενδιαφερόμενα μέρη,

— οι διαβαθμισμένες πληροφορίες που παρέχονται στον κύριο εργολάβο ή τον υπεργολάβο, ή παράγονται κατά τη διάρκεια συμβατικής δραστηριότητας, δεν πρέπει να χρησιμοποιούνται για σκοπούς άλλους από εκείνους που ορίζει η διαβαθμισμένη σύμβαση και δεν πρέπει να κοινολογούνται σε τρίτα μέρη χωρίς προηγούμενη γραπτή συγκατάθεση της πηγής προέλευσης.

β) Η Επιτροπή και οι αρμόδιες ΕΑΑ/ΚΑΑ των κρατών μελών έχουν την ευθύνη να διασφαλίζουν ότι οι κύριοι εργολάβοι και οι υπεργολάβοι στους οποίους έχουν ανατεθεί διαβαθμισμένες συμβάσεις που περιλαμβάνουν πληροφορίες με διαβάθμιση CONFIDENTIEL UE ή ανώτερη, λαμβάνουν όλα τα δέοντα μέτρα για την προστασία των εν λόγω διαβαθμισμένων πληροφοριών ΕΕ που τους παρέχονται ή τις οποίες παράγουν κατά την εκτέλεση των διαβαθμισμένων συμβάσεων, σύμφωνα με τους εθνικούς νόμους και κανόνες. Η μη συμμόρφωση με τις απαιτήσεις ασφαλείας μπορεί να έχει ως συνέπεια την καταγγελία της διαβαθμισμένης σύμβασης.

γ) Όλοι οι βιομηχανικοί ή άλλοι φορείς οι οποίοι συμμετέχουν σε διαβαθμισμένες συμβάσεις που συνεπάγονται πρόσβαση σε πληροφορίες με διαβάθμιση CONFIDENTIEL UE ή ανώτερη, πρέπει να διαθέτουν εθνική πιστοποίηση ελέγχου ασφαλείας φορέα. Η πιστοποίηση αυτή χορηγείται από την

▼**M3**

ΕΑΑ/ΚΑΑ κράτους μέλους και επιβεβαιώνει ότι ένας φορέας μπορεί να εξασφαλίσει επαρκώς την προστασία διαβαθμισμένων πληροφοριών ΕΕ ανάλογα με την εκάστοτε διαβάθμιση ασφαλείας.

δ) Όταν συνάπτεται μια διαβαθμισμένη σύμβαση, ορίζεται από τους διαχειριστές του κύριου εργολάβου ή του υπεργολάβου ένας υπεύθυνος ασφαλείας της εγκατάστασης (ΥΑΕ), που είναι αρμόδιος για να αιτήσει την έκδοση πιστοποιητικού ελέγχου ασφαλείας προσωπικού (ΠΕΑΠ) για όλα τα πρόσωπα τα οποία απασχολούνται σε βιομηχανικούς ή άλλους φορείς που έχουν την έδρα τους σε κράτος μέλος της Ευρωπαϊκής Ένωσης, και τα οποία, λόγω των καθηκόντων τους, απαιτείται να έχουν πρόσβαση σε πληροφορίες ΕΕ με διαβάθμιση CONFIDENTIEL UE ή ανώτερη, στο πλαίσιο διαβαθμισμένης σύμβασης. Το πιστοποιητικό ΠΕΑΠ πρέπει να εκδίδεται από την ΕΑΑ/ΚΑΑ του εν λόγω κράτους μέλους, σύμφωνα με τους εθνικούς κανόνες του.

ε) Οι διαβαθμισμένες συμβάσεις πρέπει να περιλαμβάνουν ΕΘΑ όπως ορίζεται στο σημείο 27 παράγραφος β στοιχείο ι). Το ΕΘΑ πρέπει να περιέχει ΟΔΑ.

στ) Η Επιτροπή, πριν ξεκινήσει τη διαδικασία διαπραγμάτευσης για την ανάθεση διαβαθμισμένης σύμβασης, επικοινωνεί με την ΕΑΑ/ΚΑΑ του κράτους μέλους στο οποίο έχει την έδρα του η βιομηχανική ή άλλη ενδιαφερόμενη οντότητα, ώστε να επιβεβαιώσει ότι διαθέτουν έγκυρη πιστοποίηση ελέγχου ασφαλείας φορέα που ανταποκρίνεται στη διαβάθμιση ασφαλείας της συγκεκριμένης σύμβασης.

ζ) Η αναθέτουσα αρχή δεν αναθέτει διαβαθμισμένη σύμβαση στον επικρατέστερο οικονομικό παράγοντα προτού λάβει έγκυρη πιστοποίηση ελέγχου ασφαλείας φορέα.

η) Δεν απαιτείται πιστοποίηση ελέγχου ασφαλείας φορέα για συμβάσεις που περιλαμβάνουν πληροφορίες με διαβάθμιση RESTREINT UE, εκτός εάν απαιτείται από τους εθνικούς νόμους και κανόνες του κράτους μέλους.

θ) Οι διαγωνισμοί που αφορούν διαβαθμισμένες συμβάσεις πρέπει να περιλαμβάνουν διάταξη που θα υποχρεώνει τον οικονομικό φορέα που τελικά δεν υποβάλλει προσφορά ή δεν επιλέγεται να επιστρέψει όλα τα έγγραφα εντός συγκεκριμένης προθεσμίας.

ι) Οι εργολάβοι ενδέχεται να χρειαστεί να διαπραγματευθούν διαβαθμισμένες συμβάσεις υπεργολαβίας με υπεργολάβους σε διάφορα επίπεδα. Στην περίπτωση αυτή, ο κύριος εργολάβος έχει την ευθύνη να διασφαλίσει ότι όλες οι δραστηριότητες υπεργολαβίας ανατίθενται σύμφωνα με τις κοινές στοιχειώδεις προδιαγραφές που περιέχονται στο παρόν τμήμα. Ωστόσο, ο κύριος εργολάβος δεν πρέπει να παρέχει διαβαθμισμένες πληροφορίες ΕΕ ή διαβαθμισμένο υλικό ΕΕ σε υπεργολάβο χωρίς την προηγούμενη γραπτή συγκατάθεση της πηγής προέλευσης.

ια) Οι όροι βάσει των οποίων ο κύριος εργολάβος μπορεί να συνάπτει σύμβαση υπεργολαβίας πρέπει να καθορίζονται στην προσφορά ή την πρόσκληση υποβολής προτάσεων και στη διαβαθμισμένη σύμβαση. Δεν μπορεί να ανατίθεται σύμβαση υπεργολαβίας σε φορείς οι οποίοι έχουν την έδρα τους σε κράτος που δεν είναι μέλος της ΕΕ, χωρίς ρητή γραπτή εξουσιοδότηση της Επιτροπής.

ιβ) Καθ' όλη τη διάρκεια της διαβαθμισμένης σύμβασης, η συμμόρφωση με όλες τις διατάξεις ασφαλείας που περιέχει η σύμβαση ελέγχεται από την Επιτροπή σε σύμπραξη με την αρμόδια ΕΑΑ/ΚΑΑ. Τυχόν συμβάντα στον τομέα της ασφάλειας πρέπει να αναφέρονται σύμφωνα με τις διατάξεις του μέρους ΙΙ τμήμα 24 των εν λόγω κανονισμών ασφαλείας. Τυχόν μεταβολή ή ανάκληση πιστοποίησης ελέγχου ασφαλείας φορέα αναφέρεται αμέσως στην Επιτροπή και σε όλες τις ΕΑΑ/ΚΑΑ στις οποίες είχε κοινοποιηθεί.

ιγ) Όταν καταγγέλλεται διαβαθμισμένη σύμβαση ή διαβαθμισμένη σύμβαση υπεργολαβίας, η Επιτροπή ή/και οι ΕΑΑ/ΚΑΑ, αναλόγως, ενημερώνουν αμέσως τις ΕΑΑ/ΚΑΑ του κράτους μέλους στο οποίο έχει την έδρα του ο εργολάβος ή ο υπεργολάβος.

ιδ) Μετά την καταγγελία ή την ολοκλήρωση της διαβαθμισμένης σύμβασης ή της διαβαθμισμένης σύμβασης υπεργολαβίας, οι κύριοι εργολάβοι και οι υπεργολάβοι εξακολουθούν να τηρούν τις κοινές στοιχειώδεις προδιαγραφές που περιέχονται στο παρόν τμήμα και το απόρρητο των διαβαθμισμένων πληροφοριών.

ιε) Ειδικοί κανόνες για τη διάθεση των διαβαθμισμένων πληροφοριών μετά τη λήξη της διαβαθμισμένης σύμβασης προβλέπονται στο ΕΘΑ ή σε άλλες σχετικές διατάξεις που αφορούν απαιτήσεις ασφαλείας.

ιστ) Οι υποχρεώσεις και οι όροι που αναφέρονται στο παρόν τμήμα εφαρμόζονται κατ'αναλογία για τις διαδικασίες στις οποίες οι επιχορηγήσεις παρέχονται με απόφαση και συγκεκριμένα στους δικαιούχους των εν λόγω επιχορηγήσεων. Στην απόφαση επιχορήγησης καθορίζονται όλες οι υποχρεώσεις των δικαιούχων.

▼**M3**

27.5. **Επισκέψεις**

Στο πλαίσιο της ανάθεσης διαβαθμισμένων συμβάσεων, πρέπει να οργανώνονται, σε συνεργασία με την αρμόδια ΕΑΑ/ΚΑΑ, επισκέψεις υπαλλήλων της Επιτροπής σε βιομηχανικούς ή άλλους φορείς των κρατών μελών που εκτελούν διαβαθμισμένες συμβάσεις ΕΕ. Επισκέψεις υπαλλήλων βιομηχανικών ή άλλων φορέων στο πλαίσιο διαβαθμισμένων συμβάσεων ΕΕ πρέπει να συμφωνούνται μεταξύ των ενδιαφερόμενων ΕΑΑ/ΚΑΑ. Ωστόσο, οι ΕΑΑ/ΚΑΑ που συμμετέχουν σε διαβαθμισμένη σύμβαση ΕΕ δύνανται να συμφωνήσουν μια διαδικασία απευθείας διοργάνωσης επισκέψεων υπαλλήλων βιομηχανικών ή άλλων φορέων.

27.6. **Διαβίβαση και μεταφορά διαβαθμισμένων πληροφοριών ΕΕ**

α) Όσον αφορά τη διαβίβαση διαβαθμισμένων πληροφοριών ΕΕ, ισχύουν οι διατάξεις του μέρους ΙΙ, τμήμα 21 των παρόντων κανονισμών ασφαλείας. Συμπληρωματικά προς τις διατάξεις αυτές, θα εφαρμόζονται και τυχόν υφιστάμενες διαδικασίες που ισχύουν στα κράτη μέλη.

β) Η διεθνής μεταφορά διαβαθμισμένου υλικού ΕΕ που αφορά διαβαθμισμένες συμβάσεις εκτελείται σύμφωνα με τις εθνικές διαδικασίες των κρατών μελών. Κατά τον έλεγχο των ρυθμίσεων ασφαλείας για τη διεθνή μεταφορά, ισχύουν οι ακόλουθες αρχές:

— η ασφάλεια είναι εγγυημένη σε όλα τα στάδια της μεταφοράς και υπό οιεσδήποτε συνθήκες, από το αρχικό σημείο προέλευσης ως τον τελικό προορισμό,

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

— εάν χρειάζεται, εξασφαλίζεται πιστοποίηση ελέγχου ασφαλείας φορέα για τις εταιρείες που πραγματοποιούν τη μεταφορά. Στις περιπτώσεις αυτές, το προσωπικό που χειρίζεται την αποστολή στοιχείων υπόκειται σε έλεγχο ασφαλείας σύμφωνα με τις κοινές στοιχειώδεις προδιαγραφές του παρόντος τμήματος,

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

— εφόσον είναι εφικτό, τα δρομολόγια πρέπει να διέρχονται μόνον από κράτη μέλη της ΕΕ. Δρομολόγια μέσω κρατών που δεν είναι μέλη της ΕΕ πρέπει να πραγματοποιούνται μόνον κατόπιν εξουσιοδότησης των ΕΑΑ/ΚΑΑ του κράτους τόσο του αποστολέα όσο και του παραλήπτη,

— πριν από οιαδήποτε μεταφορά διαβαθμισμένου υλικού ΕΕ, ο αποστολέας πρέπει να καταρτίζει σχέδιο μεταφοράς το οποίο εγκρίνουν οι ενδιαφερόμενες ΕΑΑ/ΚΑΑ.

▼**M1**

Προσάρτημα 1

ΣΥΓΚΡΙΣΗ ΤΩΝ ΕΘΝΙΚΩΝ ΔΙΑΒΑΘΜΙΣΕΩΝ ΑΣΦΑΛΕΙΑΣ

Διαβάθμιση ΕΕ	TRES SECRET UE/EU TOP SECRET	SECRET UE	CONFIDENTIEL UE	RESTREINT UE
Διαβάθμιση ΔΕΕ	FOCAL TOP SECRET	WEU SECRET	WEU CONFIDENTIAL	WEU RESTRICTED
Διαβάθμιση Ευρατόμ	EURA TOP SECRET	EURA SECRET	EURA CONFIDENTIAL	EURA RESTRICTED
Διαβάθμιση NATO	COSMIC TOP SECRET	NATO SECRET	NATO CONFIDENTIAL	NATO RESTRICTED
Αυστρία	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Βέλγιο	Très Secret Zeer Geheim	Secret Geheim	Confidentiel Vertrouwelijk	Diffusion restreinte Beperkte Verspreiding
Κύπρος	Άκρως Απόρρητο	Απόρρητο	Εμπιστευτικό	Περιορισμένης Χρήσης
Τσεχική Δημοκρατία	Přísne tajné	Tajné	Důvěrné	Vyhrazené
Δανία	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Εσθονία	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Γερμανία	Streng geheim	Geheim	VS [1] – Vertraulich	VS – Nur für den Dienstgebrauch
Ελλάδα	Άκρως Απόρρητο Abr: ΑΑΠ	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Φινλανδία	Erittäin salainen	Erittäin salainen	Salainen	Luottamuksellinen
Γαλλία	Très Secret Défense [2]	Secret Défense	Confidentiel Défense	
Ιρλανδία	Top Secret	Secret	Confidential	Restricted
Ιταλία	Segretissimo	Segreto	Riservatissimo	Riservato
Λεττονία	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Λιθουανία	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
Λουξεμβούργο	Très Secret	Secret	Confidentiel	Diffusion restreinte
Ουγγαρία	Szigorúan titkos !	Titkos !	Bizalmas !	Korlátozott terjesztésű !
Μάλτα	L-Ghola Segretezza	Sigriet	Kunfidenzjali	Ristrett
Κάτω Χώρες	Stg [3]. Zeer Geheim	Stg. Geheim	Stg. Confidentieel	Departementaalvertrouwelijk
Πολωνία	Ściśle Tajne	Tajne	Poufne	Zastrzeżone
Πορτογαλία	Muito Secreto	Secreto	Confidencial	Reservado
Σλοβενία	Strogo tajno	Tajno	Zaupno	SVN Interno
Σλοβακία	Prísne tajné	Tajné	Dôverné	Vyhradené
Ισπανία	Secreto	Reservado	Confidencial	Difusión Limitada
Σουηδία	Kvalificerat hemlig	Hemlig	Hemlig	Hemlig

▼**M1**

Ηνωμένο Βασίλειο	Top Secret	Secret	Confidential	Restricted

([1]) VS = Verschlusssache.
([2]) Η διαβάθμιση «Très Secret Défense», η οποία καλύπτει τις κυβερνητικές προτεραιότητες, μπορεί να αλλάξει μόνο με την έγκριση του πρωθυπουργού.
([3]) Stg = staatsgeheim.

Προσάρτημα 2

ΠΡΑΚΤΙΚΟΣ ΟΔΗΓΟΣ ΔΙΑΒΑΘΜΙΣΗΣ

Ο παρακάτω οδηγός είναι ενδεικτικός και δεν μεταβάλλει τις διατάξεις ουσίας των τμημάτων 16, 17, 20 και 21.

Διαβάθμιση	πότε	ποιος	Επίθεση	Υποχαρακτηρισμός/αποχαρακτηρισμός/καταστροφή	
				ποιος	πότε
►**M1** TRES SECRET UE/EU TOP SECRET ◄: Η διαβάθμιση αυτή εφαρμόζεται μόνο στις πληροφορίες και το υλικό των οποίων η άνευ αδείας κοινολόγηση μπορεί να βλάψει σοβαρότατα τα ζωτικά συμφέροντα της Ευρωπαϊκής Ένωσης ή ενός ή περισσοτέρων κρατών μελών της [16.1].	Όταν η διαρροή στοιχείων με διαβάθμιση ►**M1** TRES SECRET UE/EU TOP SECRET ◄ θα ήταν πιθανό: — να συνιστά άμεση απειλή για την εσωτερική σταθερότητα της ΕΕ ή κράτους μέλους της ή φίλης χώρας — να βλάψει σοβαρότατα τις σχέσεις με φίλα κράτη — να οδηγήσει άμεσα σε μεγάλο αριθμό θανάτων — να βλάψει σοβαρότατα την επιχειρησιακή αποτελεσματικότητα ή την ασφάλεια των δυνάμεων κρατών μελών ή άλλων εισφερόντων, ή τη συνέχιση της αποτελεσματικότητας εξαιρετικά πολύτιμων ενεργειών ασφάλειας ή συλλογής πληροφοριών — να προξενήσει μακροπρόθεσμη σοβαρή βλάβη στην οικονομία της ΕΕ ή των κρατών μελών	Δεόντως εξουσιοδοτημένα πρόσωπα (συντάκτες), γενικοί διευθυντές, προϊστάμενοι υπηρεσίας [17.1] Οι συντάκτες προσδιορίζουν ημερομηνία, προθεσμία ή γεγονός μετά τα οποία μπορεί να υποχαρακτηριστεί ή να αποχαρακτηρισθεί το περιεχόμενο. [16.2] Σε αντίθετη περίπτωση, επανεξετάζουν τα έγγραφα το αργότερο ανά πενταετία, ώστε να επιβεβαιώνεται ότι η αρχική διαβάθμιση εξακολουθεί να είναι αναγκαία [17.3].	Η διαβάθμιση ►**M1** TRES SECRET UE/EU TOP SECRET ◄ επιτίθεται στα έγγραφα ►**M1** TRES SECRET UE/EU TOP SECRET ◄, ενδεχομένως μαζί με ένδειξη ασφαλείας ή/και τη σήμανση άμυνας ESDP, με μηχανικά μέσα και ιδιοχείρως [16.4, 16.5, 16.3]. Οι διαβαθμίσεις ΕΕ και οι ενδείξεις ασφαλείας εμφαίνονται στο κέντρο του άνω και του κάτω μέρους κάθε σελίδας· κάθε σελίδα αριθμείται. Κάθε έγγραφο φέρει αριθμό αναφοράς και ημερομηνία· ο εν λόγω αριθμός αναφοράς εμφαίνεται σε κάθε σελίδα. Εάν τα έγγραφα πρόκειται να διανε- μηθούν σε πολλαπλά αντίτυπα, στην πρώτη σελίδα κάθε αντιτύπου αναγράφεται ο αριθμός αντιτύπου και ο συνολικός αριθμός σελίδων. Όλα τα παραρτήματα και τα συννημμένα απαριθμούνται στην πρώτη σελίδα [21.1].	Αποκλειστικός υπεύθυνος για τον υποχαρακτηρισμό ή αποχαρακτηρισμό είναι ο συντάκτης του εγγράφου, ο οποίος ενημερώνει σχετικά τους μετέπειτα αποδέκτες στους οποίους έχει αποστείλει ή κοινοποιήσει το έγγραφο [17.3]. Τα έγγραφα ►**M1** TRES SECRET UE/EU TOP SECRET ◄ καταστρέφονται από την αρμόδια για τη διαβάθμιση αυτή κεντρική γραμματεία ή υπογραμματεία. Κάθε καταστρεφόμενο έγγραφο πρέπει να καταγράφεται σε πρωτόκολλο καταστροφής το οποίο υπογράφεται από τον ελεγκτικό υπάλληλο ►**M1** TRES SECRET UE/EU TOP SECRET ◄ και από τον υπάλληλο ο οποίος παρίσταται κατά την καταστροφή και ο οποίος πρέπει να έχει διαβάθμιση ►**M1** TRES SECRET UE/EU TOP SECRET ◄. Σχετική σημείωση καταγράφεται στο βιβλίο ημερολογίου. Η γραμματεία διατηρεί τα πρωτόκολλα καταστροφής, μαζί με τα φύλλα διανομής, επί δέκα έτη [22.5].	Καταστρέφονται τα υπεράριθμα αντίτυπα και τα έγγραφα που δεν χρειάζονται πια [22.5]. Τα έγγραφα ►**M1** TRES SECRET UE/EU TOP SECRET ◄, καθώς και η πάσης φύσεως διαβαθμισμένη φύρα που προκύπτει από τη σύνταξη εγγράφων ►**M1** TRES SECRET UE/EU TOP SECRET ◄, όπως κακέκτυπα αντίγραφα, σχέδια εγγράφων, δακτυλογραφημένα σημειώματα και καρμπόν, καταστρέφονται υπό την επίβλεψη ελεγκτικού υπαλλήλου γραμματείας ►**M1** TRES SECRET UE/EU TOP SECRET ◄, με καύση, πολτοποίηση, θρυμματισμό με ψαλίδισμα ή καθ' οιονδήποτε άλλο τρόπο που τα μετατρέπει σε μη αναγνωρίσιμη και μη ανασυστάσιμη μορφή [22.5].
►**M1** SECRET UE ◄:	Όταν η διαρροή στοιχείων με διαβάθμιση ►**M1** SECRET	Εξουσιοδοτημένα πρόσωπα (συντάκτες), Γενικοί Διευ-	Η διαβάθμιση ►**M1** SECRET UE ◄ επιτίθεται στα έγγραφα	Αποκλειστικός υπεύθυνος για τον υποχαρακτηρισμό και	Καταστρέφονται τα υπεράριθμα αντίτυπα και τα έγγραφα που δεν

Διαβάθμιση	πότε	ποιος	Επίθεση	Υποχαρακτηρισμός/αποχαρακτηρισμός/καταστροφή	
				ποιος	πότε
Η διαβάθμιση αυτή εφαρμόζεται μόνο στις πληροφορίες και το υλικό των οποίων η άνευ αδείας κοινολόγηση μπορεί να βλάψει σοβαρότατα τα ζωτικά συμφέροντα της Ευρωπαϊκής Ένωσης ή ενός ή περισσοτέρων κρατών μελών της [16.1].	UE ◄ θα ήταν πιθανό: — να οξύνει διεθνείς εντάσεις — να βλάψει σοβαρότατα τις σχέσεις με φίλα κράτη — να συνιστά άμεσο κίνδυνο ζωής ή να βλάψει σοβαρά τη δημόσια τάξη ή την ατομική ασφάλεια ή ελευθερία — να βλάψει σοβαρά την επιχειρησιακή αποτελεσματικότητα ή την ασφάλεια των δυνάμεων κρατών μελών ή άλλων εισφερόντων, ή τη συνέχιση της αποτελεσματικότητας πολύ πολύτιμων ενεργειών ασφάλειας ή συλλογής πληροφοριών — να προξενήσει αξιόλογη ουσιαστική βλάβη στα οικονομικά, δημοσιονομικά και εμπορικά συμφέροντα της ΕΕ ή των κρατών μελών	θυντές, Προϊστάμενοι Υπηρεσίας [17.1]. Οι συντάκτες προσδιορίζουν ημερομηνία ή προθεσμία μετά την οποία μπορεί να υποχαρακτηριστεί ή να αποχαρακτηριστεί το περιεχόμενο [16.2]. Σε αντίθετη περίπτωση, επανεξετάζουν τα έγγραφα το αργότερο ανά πενταετία, ώστε να επιβεβαιώνεται ότι η αρχική διαβάθμιση εξακολουθεί να είναι αναγκαία [17.3].	►**M1** SECRET UE ◄, ενδεχομένως μαζί με ένδειξη ασφαλείας ή/και τη σήμανση άμυνας ESDP, με μηχανικά μέσα και ιδιοχείρως [16.4, 16.5, 16.3]. Οι διαβαθμίσεις ΕΕ και οι ενδείξεις ασφαλείας εμφαίνονται στο κέντρο του άνω και του κάτω μέρους κάθε σελίδας· κάθε σελίδα αριθμείται. Κάθε έγγραφο φέρει αριθμό αναφοράς και ημερομηνία· ο εν λόγω αριθμός αναφοράς εμφαίνεται σε κάθε σελίδα. Εάν τα έγγραφα πρόκειται να διανεμηθούν σε πολλαπλά αντίτυπα, στην πρώτη σελίδα κάθε αντιτύπου αναγράφεται ο αριθμός αντιτύπου και ο συνολικός αριθμός σελίδων. Όλα τα παραρτήματα και τα συννημμένα απαριθμούνται στην πρώτη σελίδα [21.1].	αποχαρακτηρισμό είναι ο συντάκτης του εγγράφου, ο οποίος ενημερώνει σχετικά τους μετέπειτα αποδέκτες στους οποίους έχει αποστείλει ή κοινοποιήσει το έγγραφο [17.3]. Τα έγγραφα ►**M1** SECRET UE ◄ καταστρέφονται από την αρμόδια για την παραγωγή τους γραμματεία, υπό την εποπτεία προσώπου με κατάλληλη διαβάθμιση ασφαλείας. Τα καταστρεφόμενα έγγραφα ►**M1** SECRET UE ◄ καταγράφονται σε υπογραφόμενο πρωτόκολλο καταστροφής το οποίο διατηρείται από τη γραμματεία, μαζί με τα έντυπα διανομής, επί τρία τουλάχιστον έτη [22.5].	χρειάζονται πια [22.5]. Τα έγγραφα ►**M1** SECRET UE ◄, καθώς και όλα τα διαβαθμισμένα απορρίμματα που προκύπτουν κατά την σύνταξη των εγγράφων ►**M1** SECRET UE ◄, όπως κακέκτυπα αντίγραφα, σχέδια εγγράφων, δακτυλογραφημένα σημειώματα και καρμπόν, καταστρέφονται με καύση, πολτοποίηση, σχίσιμο σε λουρίδες ή καθ' οιονδήποτε άλλο τρόπο που τα μετατρέπει σε μη αναγνωρίσιμη και μη ανασυστάσιμη μορφή [22.5].
►**M1** CONFIDENTIEL UE ◄: Η διαβάθμιση αυτή εφαρμόζεται μόνο στις πληροφορίες και το υλικό των οποίων η άνευ αδείας κοινολόγηση μπορεί να βλάψει σοβαρότατα τα ζωτικά συμφέροντα της Ευρωπαϊκής Ένωσης ή ενός ή περισσοτέρων κρατών μελών της [16.1].	Όταν η διαρροή στοιχείων με διαβάθμιση ►**M1** CONFIDENTIEL UE ◄ θα ήταν πιθανό: — να βλάψει ουσιαστικά τις διπλωματικές σχέσεις, δηλαδή να οδηγήσει σε επίσημες διαμαρτυρίες ή άλλες κυρώσεις — να θέσει σε κίνδυνο την ατομική ασφάλεια ή ελευθερία — να βλάψει την επιχειρη-	Εξουσιοδοτημένα πρόσωπα (συντάκτες), Γενικοί Διευθυντές, Προϊστάμενοι Υπηρεσίας [17.1]. Οι συντάκτες προσδιορίζουν ημερομηνία, προθεσμία ή γεγονός μετά τα οποία μπορεί να υποχαρακτηριστεί ή ν' αποχαρακτηριστθεί το περιεχόμενο. Σε αντίθετη περίπτωση, επανεξετάζουν τα έγγραφα το αργότερο ανά πενταετία, ώστε να επιβεβαιώνεται ότι η αρχική διαβάθμιση εξακολουθεί να	Η διαβάθμιση ►**M1** CONFIDENTIEL UE ◄ επιτίθεται στα έγγραφα ►**M1** CONFIDENTIEL UE ◄, ενδεχομένως μαζί με ένδειξη ασφαλείας ή/και τη σήμανση άμυνας ESDP, με μηχανικά μέσα και ιδιοχείρως ή με εκτύπωση σε ήδη σφραγισμένο και ταξινομημένο χαρτί [16.4, 16.5, 16.3]. Οι διαβαθμίσεις ΕΕ εμφαίνονται στο κέντρο του άνω και του κάτω μέρους κάθε σελίδας· κάθε σελίδα αριθμείται. Κάθε	Αποκλειστικός υπεύθυνος για τον υποχαρακτηρισμό και αποχαρακτηρισμό είναι ο συντάκτης του εγγράφου, ο οποίος ενημερώνει σχετικά τους μετέπειτα αποδέκτες στους οποίους έχει αποστείλει ή κοινοποιήσει το έγγραφο [17.3]. Τα έγγραφα ►**M1** CONFIDENTIEL UE ◄ καταστρέφονται από την αρμόδια για την παραγωγή τους γραμματεία, υπό την εποπτεία προσώπου με	Καταστρέφονται τα υπεράριθμα αντίτυπα και τα έγγραφα που δεν χρειάζονται πια [22.5]. Τα έγγραφα ►**M1** CONFIDENTIEL UE ◄, καθώς και όλα τα διαβαθμισμένα απορρίμματα που προκύπτουν κατά την σύνταξη των εγγράφων ►**M1** CONFIDENTIEL UE ◄, όπως κακέκτυπα αντίγραφα, σχέδια εγγράφων, δακτυλογραφημένα σημειώματα και καρμπόν, καταστρέφονται με καύση, πολτοποίηση, σχίσιμο σε

Διαβάθμιση	πότε	ποιος	Επίθεση	Υποχαρακτηρισμός/αποχαρακτηρισμός/καταστροφή	
				ποιος	πότε
	σιακή αποτελεσματικότητα ή την ασφάλεια των δυνάμεων κρατών μελών ή άλλων εισφερόντων, ή την αποτελεσματικότητα πολύτιμων ενεργειών ασφάλειας ή συλλογής πληροφοριών — να υπονομεύσει ουσιαστικά τη χρηματοοικονομική βιωσιμότητα σημαντικών οργανισμών — να παρεμποδίσει τη διερεύνηση ή να διευκολύνει τη διάπραξη σοβαρών εγκλημάτων — να βλάψει ουσιαστικά τα οικονομικά, νομισματικά, δημοσιονομικά και εμπορικά συμφέροντα της ΕΕ ή των κρατών μελών — να παρεμποδίσει σοβαρά την ανάπτυξη ή λειτουργία σημαντικών ενωσιακών πολιτικών — να διακόψει ή να διαταράξει σημαντικά ουσιαστικές ενωσιακές δραστηριότητες	είναι αναγκαία [17.3].	έγγραφο φέρει αριθμό αναφοράς και ημερομηνία. Όλα τα παραρτήματα και τα συνημμένα απαριθμούνται στην πρώτη σελίδα [21.1].	κατάλληλη διαβάθμιση ασφαλείας. Η καταστροφή τους καταγράφεται σύμφωνα με τους εθνικούς κανονισμούς και, στην περίπτωση της Επιτροπής ή των αποκεντρωμένων οργανισμών της ΕΕ, σύμφωνα με τις οδηγίες του ►**M2** αρμόδιου για θέματα ασφαλείας μέλους της Επιτροπής ◄ [22.5].	λουρίδες ή καθ' οιονδήποτε άλλο τρόπο που τα μετατρέπει σε μη αναγνωρίσιμη και μη ανασυστάσιμη μορφή [22.5].
►**M1** RESTREINT UE ◄: Η διαβάθμιση αυτή εφαρμόζεται στις πληροφορίες και το υλικό των οποίων η άνευ αδείας κοινολόγηση είναι αντίθετη προς τα συμφέροντα της Ευρωπαϊκής Ένωσης ή ενός ή περισσοτέρων κρατών μελών της [16.1].	Όταν η διαρροή στοιχείων με διαβάθμιση ►**M1** RESTREINT UE ◄ θα ήταν πιθανό: — να επηρεάσει δυσμενώς διπλωματικές σχέσεις, — να προξενήσει σημαντική οδύνη σε άτομα — να δυσχεράνει τη διατή-	Εξουσιοδοτημένα πρόσωπα (συντάκτες), γενικοί διευθυντές, προϊστάμενοι υπηρεσίας [17.1]. Οι συντάκτες προσδιορίζουν ημερομηνία, προθεσμία ή γεγονός μετά τα οποία μπορεί να υποχαρακτηριστεί ή να αποχαρακτηριστεί το περιεχόμενο [16.2]. Σε αντίθετη περίπτωση, επανεξετάζουν τα	Η διαβάθμιση ►**M1** RESTREINT UE ◄ επιτίθεται στα έγγραφα ►**M1** RESTREINT UE ◄, ενδεχομένως μαζί με ένδειξη ασφαλείας ή/και τη σήμανση άμυνας ESDP, με μηχανικά μέσα και ιδιοχείρως [16.4, 16.5, 16.3]. Οι διαβαθμίσεις ΕΕ και οι	Αποκλειστικός υπεύθυνος για τον αποχαρακτηρισμό είναι ο συντάκτης του εγγράφου, ο οποίος ενημερώνει σχετικά τους μετέπειτα αποδέκτες στους οποίους έχει αποστείλει ή κοινοποιήσει το έγγραφο [17.3]. Τα έγγραφα ►**M1** RESTREINT UE ◄	Καταστρέφονται τα υπεράριθμα αντίτυπα και τα έγγραφα που δεν χρειάζονται πια [22.5].

▼B

Διαβάθμιση	πότε	ποιος	Επίθεση	Υποχαρακτηρισμός/αποχαρακτηρισμός/καταστροφή	
				ποιος	πότε
	ρηση της επιχειρησιακής αποτελεσματικότητας ή της ασφάλειας των δυνάμεων κρατών μελών ή άλλων εισφερόντων — να προξενήσει χρηματική βλάβη ή να διευκολύνει τον πορισμό αθέμιτων κερδών ή ωφελημάτων από άτομα ή εταιρείες — να συνιστά παράβαση των πρεπουσών δεσμεύσεων τήρησης της εμπιστευτικότητας πληροφοριών που έχουν δοθεί από τρίτους — να συνιστά παράβαση των θεσμοθετημένων περιορισμών ως προς την κοινολόγηση πληροφοριών — να δυσχεράνει τη διερεύνηση ή να διευκολύνει τη διάπραξη σοβαρών εγκλημάτων — να φέρει την ΕΕ ή τα κράτη μέλη σε μειονεκτική θέση στα πλαίσια εμπορικών ή πολιτικών διαπραγματεύσεων με άλλους — να παρεμποδίσει σοβαρά την ανάπτυξη ή λειτουργία των ενωσιακών πολιτικών — να υπονομεύσει την πρέπουσα διαχείριση της ΕΕ ή των δραστηριοτήτων της	έγγραφα το αργότερο ανά πενταετία, ώστε να επιβεβαιώνεται ότι η αρχική διαβάθμιση εξακολουθεί να είναι αναγκαία [17.3].	ενδείξεις ασφαλείας εμφαίνονται στο κέντρο του άνω και του κάτω μέρους κάθε σελίδας κάθε σελίδα αριθμείται. Κάθε έγγραφο φέρει αριθμό αναφοράς και ημερομηνία [21.1].	καταστρέφονται από την αρμόδια για τη διαβάθμιση αυτή γραμματεία ή από το χρήστη, σύμφωνα με τις οδηγίες του ►**M2** αρμόδιου για θέματα ασφαλείας μέλους της Επιτροπής ◄ [22.5].	

▼B

Προσάρτημα 3

Κατευθυντήριες γραμμές για την κοινοποίηση διαβαθμισμένων πληροφορίων ΕΕ σε τρίτα κράτη ή διεθνείς οργανισμούς: Συνεργασία επιπέδου 1

ΔΙΑΔΙΚΑΣΙΕΣ

1. Η επιτροπή εν σώματι είναι αρμόδια για την κοινοποίηση διαβαθμισμένων πληροφοριών ΕΕ σε χώρες που δεν είναι μέλη της Ευρωπαϊκής Ένωσης ή σε άλλους διεθνείς οργανισμούς, των οποίων η πολιτική και οι κανονισμοί ασφαλείας είναι παρόμοιοι προς τους κοινοτικούς.
2. Έως ότου συναφθεί συμφωνία για την ασφάλεια, το αρμόδιο επί θεμάτων ασφαλείας μέλος της Επιτροπής είναι αρμόδιο για την εξέταση αιτημάτων κοινοποίησης διαβαθμισμένων πληροφοριών ΕΕ.
3. Κατά την εξέταση αυτή:
   — ζητεί τις γνώμες των συντακτών των προς κοινοποίηση ΔΠΕΕ·
   — πραγματοποιεί τις απαιτούμενες επαφές με τους φορείς ασφαλείας των δικαιούχων χωρών ή διεθνών οργανισμών για να ελέγξει εάν η πολιτική και οι κανονισμοί τους περί ασφαλείας εξασφαλίζουν ότι οι κοινοποιούμενες διαβαθμισμένες πληροφορίες θα προστατεύονται σύμφωνα με τις προκείμενες διατάξεις ασφαλείας·
   — ζητεί τη γνώμη της συμβουλευτικής ομάδας της Επιτροπής για την πολιτική ασφάλειας όσον αφορά την εμπιστοσύνη που εμπνέουν τα δικαιούχα κράτη ή διεθνείς οργανισμοί.
4. Το αρμόδιο επί θεμάτων ασφαλείας μέλος της Επιτροπής διαβιβάζει το αίτημα και τη γνώμη της συμβουλευτικής ομάδας της Επιτροπής για την πολιτική ασφάλειας στην Επιτροπή για τη λήψη απόφασης.

ΔΙΑΤΑΞΕΙΣ ΑΣΦΑΛΕΙΑΣ ΠΟΥ ΠΡΕΠΕΙ ΝΑ ΕΦΑΡΜΟΖΟΥΝ ΟΙ ΔΙΚΑΙΟΥΧΟΙ

5. Το αρμόδιο για θέματα ασφάλειας μέλος της Επιτροπής γνωστοποιεί στα δικαιούχα κράτη ή διεθνείς οργανισμούς την απόφαση της Επιτροπής σχετικά με την έγκριση της κοινοποίησης των διαβαθμισμένων πληροφοριών ΕΕ.
6. Η απόφαση κοινοποίησης αρχίζει να ισχύει μόνον όταν οι δικαιούχοι εγγυηθούν γραπτώς ότι:
   — θα χρησιμοποιούν τις πληροφορίες μόνον για τους συμφωνημένους σκοπούς,
   — θα προστατεύουν τις πληροφορίες σύμφωνα με τις προκείμενες διατάξεις ασφαλείας, ιδίως δε σύμφωνα με τους παρακάτω ειδικούς κανόνες.
7. Προσωπικό
   α) Ο αριθμός των υπαλλήλων με πρόσβαση στις διαβαθμισμένες πληροφορίες ΕΕ περιορίζεται αυστηρά, βάσει της αρχής της «ανάγκης γνώσης», στα άτομα των οποίων τα καθήκοντα απαιτούν την πρόσβαση αυτή.
   β) Όλοι οι υπάλληλοι ή πολίτες που έχουν εξουσιοδοτημένη πρόσβαση σε πληροφορίες με διαβάθμιση τουλάχιστον ►**M1** CONFIDENTIEL UE ◄ πρέπει να διαθέτουν είτε πιστοποιητικό ασφαλείας κατάλληλου επιπέδου ή ισοδύναμη διαβάθμιση ασφαλείας είτε τα αντίστοιχα που έχουν εκδοθεί από την κυβέρνηση του κράτους τους.
8. Διαβίβαση εγγράφων
   α) Οι πρακτικές διαδικασίες για τη διαβίβαση των εγγράφων αποφασίζονται με συμφωνία. Έως ότου συναφθεί συμφωνία, εφαρμόζονται οι διατάξεις του τμήματος 21. Η συμφωνία πρέπει να ορίζει, ιδίως, τις γραμματείες στις οποίες πρέπει να διαβιβάζονται οι διαβαθμισμένες πληροφορίες ΕΕ.
   β) Εάν οι διαβαθμισμένες πληροφορίες των οποίων την κοινοποίηση ενέκρινε η Επιτροπή περιλαμβάνουν πληροφορίες ►**M1** TRES SECRET UE/EU TOP SECRET ◄, το δικαιούχο κράτος ή διεθνής οργανισμός συγκροτεί κεντρική γραμματεία ΕΕ και, ενδεχομένως, υπογραμματείες ΕΕ. Οι γραμματείες αυτές εφαρμόζουν διατάξεις αυστηρά ισοδύναμες με του τμήματος XXII των παρουσών διατάξεων ασφαλείας.
9. Καταχώρηση

   Μόλις μια γραμματεία παραλάβει έγγραφο ΕΕ με διαβάθμιση τουλάχιστον ►**M1** CONFIDENTIEL UE ◄, το καταχωρεί σε ειδικό μητρώο που τηρεί ο οργανισμός, στις στήλες του οποίου αναγράφονται η ημερομηνία παραλαβής, τα στοιχεία του εγγράφου (ημερομηνία, αριθμός αναφοράς και αριθμός αντιτύπου), η διαβάθμισή του, ο τίτλος του, το ονοματεπώνυμο ή ο

▼B

τίτλος του αποδέκτη, η ημερομηνία επιστροφής της απόδειξης και η ημερομηνία επιστροφής του εγγράφου στον συντάκτη ΕΕ ή η ημερομηνία καταστροφής του.

10. Καταστροφή

α) Τα διαβαθμισμένα έγγραφα ΕΕ καταστρέφονται σύμφωνα με τις οδηγίες του τμήματος 22 των παρουσών διατάξεων ασφαλείας. Αντίγραφα των πρωτοκόλλων καταστροφής των εγγράφων ►**M1** SECRET UE ◄ και ►**M1** TRES SECRET UE/EU TOP SECRET ◄ αποστέλλονται στη γραμματεία ΕΕ που είχε διαβιβάσει τα έγγραφα.

β) Τα διαβαθμισμένα έγγραφα ΕΕ περιλαμβάνονται στα σχέδια καταστροφής σε περίπτωση έκτακτης ανάγκης τα οποία αφορούν τα διαβαθμισμένα έγγραφα των δικαιούχων οργανισμών.

11. Προστασία των εγγράφων

Πρέπει να λαμβάνεται κάθε μέτρο για να αποτρέπεται η πρόσβαση μη εξουσιοδοτημένων ατόμων στις διαβαθμισμένες πληροφορίες ΕΕ.

12. Αντίγραφα, μεταφράσεις και αποσπάσματα

Απαγορεύονται να παράγονται φωτοαντίγραφα, μεταφράσεις ή αποσπάσματα εγγράφων ►**M1** CONFIDENTIEL UE ◄ ή ►**M1** SECRET UE ◄ χωρίς την άδεια του προϊσταμένου ασφαλείας του οργανισμού, ο οποίος καταχωρεί και ελέγχει αυτά τα αντίγραφα, μεταφράσεις ή αποσπάσματα και τα σφραγίζει, εφόσον απαιτείται.

Η αναπαραγωγή ή μετάφραση εγγράφου ►**M1** TRES SECRET UE/EU TOP SECRET ◄ μπορεί να επιτρέπεται μόνον από την συντάκτρια αρχή, η οποία και ορίζει τον αριθμό επιτρεπόμενων αντιτύπων· εάν είναι αδύνατο να προσδιοριστεί η συντάκτρια αρχή, το αίτημα παραπέμπεται στη►**M2** Διεύθυνση Ασφαλείας της Επιτροπής ◄.

13. Παραβιάσεις των κανόνων ασφαλείας

Όταν έχουν παραβιαστεί οι κανόνες ασφαλείας για ένα διαβαθμισμένο έγγραφο ΕΕ ή όταν υπάρχουν σχετικές υπόνοιες, λαμβάνονται αμέσως τα ακόλουθα μέτρα, υπό την προϋπόθεση ότι έχει συναφθεί συμφωνία ασφαλείας:

α) διεξάγεται έρευνα για να διαπιστωθούν οι περιστάσεις υπό τις οποίες παραβιάστηκαν οι κανόνες ασφαλείας,

β) ειδοποιείται η►**M2** Διεύθυνση Ασφαλείας της Επιτροπής ◄, η εθνική αρχή ασφαλείας και η συντάκτρια αρχή ή δηλώνεται σαφώς ότι η συντάκτρια αρχή δεν ειδοποιήθηκε εάν αυτό δεν κατέστη δυνατόν,

γ) λαμβάνονται μέτρα για να ελαχιστοποιηθούν οι επιπτώσεις της παραβίασης,

δ) επανεξετάζονται και εφαρμόζονται μέτρα για να αποφευχθεί επανάληψη παρόμοιων συμβάντων,

ε) εφαρμόζονται τα μέτρα που συνιστά η►**M2** Διεύθυνση Ασφαλείας της Επιτροπής ◄ για να αποφευχθεί επανάληψη παρόμοιων συμβάντων.

14. Επιθεωρήσεις

Η►**M2** Διεύθυνση Ασφαλείας της Επιτροπής ◄ έχει το δικαίωμα, βάσει συμφωνίας με τα ενδιαφερόμενα κράτη ή διεθνείς οργανισμούς, να αξιολογεί την αποτελεσματικότητα των μέτρων προστασίας των κοινοποιούμενων διαβαθμισμένων πληροφοριών ΕΕ.

15. Εκθέσεις

Υπό την προϋπόθεση ότι έχει συναφθεί συμφωνία ασφαλείας, καθ' όλο το διάστημα κατά το οποίο το κράτος ή ο διεθνής οργανισμός διατηρούν στην κατοχή τους διαβαθμισμένες πληροφορίες ΕΕ, υποβάλλουν ετήσια έκθεση, σε ημερομηνία που καθορίζεται όταν χορηγείται η άδεια κοινοποίησης των πληροφοριών, με την οποία επιβεβαιώνεται ότι έχουν τηρηθεί οι προκείμενες διατάξεις ασφαλείας.

▼B

Προσάρτημα 4

Κατευθυντήριες γραμμές για τη διαβίβαση διαβαθμισμένων πληροφοριών ΕΕ σε τρίτες χώρες ή διεθνείς οργανισμούς: Συνεργασία επιπέδου 2

ΔΙΑΔΙΚΑΣΙΕΣ

1. Αρμόδιος για την κοινοποίηση διαβαθμισμένων πληροφοριών ΕΕ σε τρίτα κράτη ή διεθνείς οργανισμούς, των οποίων η πολιτική και οι διατάξεις ασφαλείας διαφέρουν σημαντικά από εκείνους της ΕΕ, είναι ο αρχικός συντάκτης. Την αρμοδιότητα για την κοινοποίηση ΔΠΕΕ που δημιουργήθηκαν εντός της Επιτροπής, έχει η Επιτροπή εν σώματι.

2. Κατά κανόνα, η κοινοποίηση περιορίζεται σε διαβαθμισμένες πληροφορίες με βαθμό ασφαλείας έως ►**M1** SECRET UE ◄· αποκλείονται οι διαβαθμισμένες πληροφορίες που προστατεύονται από ειδικές σημάνσεις ή ενδείξεις ασφαλείας.

3. Εν αναμονή της σύναψης συμφωνίας στον τομέα της ασφάλειας, το αρμόδιο για θέματα ασφαλείας μέλος της Επιτροπής, έχει την αρμοδιότητα να εξετάζει αιτήσεις για την κοινοποίηση διαβαθμισμένων πληροφοριών ΕΕ.

4. Προς το σκοπό αυτό:

   — ζητεί τις γνώμες των συντακτών των προς κοινοποίηση ΔΠΕΕ·

   — πραγματοποιεί τις απαραίτητες επαφές με τους φορείς ασφαλείας των δικαιούχων κρατών ή διεθνών οργανισμών, για να λάβει πληροφορίες σχετικά με την πολιτική και τους κανονισμούς ασφαλείας τους, ιδίως δε για να καταρτίσει πίνακα στον οποίο συγκρίνονται οι διαβαθμίσεις που ισχύουν στην ΕΕ, με εκείνες που ισχύουν στο συγκεκριμένο κράτος ή οργανισμό·

   — διοργανώνει συνεδρίαση της συμβουλευτικής ομάδας επί θεμάτων πολιτικής ασφαλείας της Επιτροπής ή, εφόσον απαιτείται, με τη διαδικασία σιωπηρής συναίνεσης, απευθύνει ερωτήματα στις εθνικές αρχές ασφαλείας των κρατών μελών, προκειμένου να λάβει τη γνώμη της συμβουλευτικής ομάδας επί θεμάτων πολιτικής ασφαλείας της Επιτροπής.

5. Η γνώμη της συμβουλευτικής ομάδας επί θεμάτων πολιτικής ασφαλείας της Επιτροπής, θα αφορά:

   — την εμπιστοσύνη που εμπνέουν τα δικαιούχα κράτη ή διεθνείς οργανισμοί ενόψει της αξιολόγησης των κινδύνων ασφαλείας που διατρέχουν η ΕΕ ή τα κράτη μέλη της·

   — αξιολόγηση της ικανότητας των δικαιούχων να προστατεύουν τις διαβαθμισμένες πληροφορίες που τους κοινοποιεί η ΕΕ·

   — προτάσεις πρακτικών διαδικασιών για το χειρισμό των διαβιβαζόμενων διαβαθμισμένων πληροφοριών ΕΕ (π.χ. κοινοποίηση κειμένου από το οποίο έχουν αφαιρεθεί τα ευαίσθητα στοιχεία) και εγγράφων (διατήρηση ή διαγραφή των ενδείξεων διαβάθμισης ΕΕ, ειδικών επισημάνσεων κ.λπ.)·

   — τον υποχαρακτηρισμό ή αποχαρακτηρισμό των πληροφοριών, πριν από την κοινοποίηση στις δικαιούχες χώρες ή διεθνείς οργανισμούς.

6. Το αρμόδιο για θέματα ασφαλείας μέλος της Επιτροπής διαβιβάζει στην Επιτροπή για τη λήψη της σχετικής απόφασης, το αίτημα, καθώς και τη γνώμη της συμβουλευτικής ομάδας επί θεμάτων πολιτικής ασφαλείας της Επιτροπής.

ΚΑΝΟΝΕΣ ΑΣΦΑΛΕΙΑΣ ΠΟΥ ΠΡΕΠΕΙ ΝΑ ΕΦΑΡΜΟΖΟΥΝ ΟΙ ΔΙΚΑΙΟΥΧΟΙ

7. Το αρμόδιο για θέματα ασφάλειας μέλος της Επιτροπής κοινοποιεί στα δικαιούχα κράτη ή τους διεθνείς οργανισμούς, την απόφαση της Επιτροπής να επιτρέψει τη διαβίβαση διαβαθμισμένων πληροφοριών ΕΕ, καθώς και τους σχετικούς περιορισμούς.

8. Η απόφαση κοινοποίησης αρχίζει να ισχύει μόνον όταν οι δικαιούχοι εγγυηθούν γραπτώς ότι:

   — θα χρησιμοποιήσουν τις πληροφορίες μόνον για τους συμφωνημένους σκοπούς·

   — θα προστατεύουν τις πληροφορίες σύμφωνα με τις διατάξεις που έχουν θεσπιστεί από την Επιτροπή.

9. Οι ακόλουθοι κανόνες προστασίας ισχύουν εκτός εάν η Επιτροπή, αφού λάβει την τεχνικής φύσεως γνώμη της συμβουλευτικής ομάδας επί θεμάτων πολιτικής ασφαλείας της Επιτροπής, αποφασίσει μια ειδική διαδικασία για το χειρισμό των διαβαθμισμένων εγγράφων ΕΕ (διαγραφή των ενδείξεων διαβάθμισης ΕΕ, ειδικών επισημάνσεων κ.λπ.).

▼B

10. Προσωπικό

α) Ο αριθμός υπαλλήλων με πρόσβαση στις διαβαθμισμένες πληροφορίες ΕΕ πρέπει να περιορίζεται αυστηρά, βάσει της αρχής «ανάγκη γνώσης», στα άτομα των οποίων τα καθήκοντα απαιτούν την πρόσβαση αυτή.

β) Όλοι οι υπάλληλοι ή πολίτες που έχουν εξουσιοδοτημένη πρόσβαση στις διαβαθμισμένες πληροφορίες που κοινοποιούνται από την ΕΕ, πρέπει να διαθέτουν εθνική διαβάθμιση ασφαλείας ή άδεια πρόσβασης, κατάλληλου επιπέδου που θα ισοδυναμεί με εκείνο της ΕΕ, όπως ορίζεται στο συγκριτικό πίνακα·

γ) Οι εν λόγω εθνικές διαβαθμίσεις ή εξουσιοδοτήσεις ασφαλείας διαβιβάζονται προς ενημέρωση στον ►M2 διευθυντή της Διεύθυνσης Ασφαλείας της Επιτροπής ◄.

11. Διαβίβαση εγγράφων

Οι πρακτικές διαδικασίες για τη διαβίβαση εγγράφων, αποφασίζονται κατόπιν συμφωνίας. Εν αναμονή της σύναψης της εν λόγω συμφωνίας, θα εφαρμόζονται οι διατάξεις του τμήματος 21. Στη συμφωνία αυτή διευκρινίζονται ιδίως οι γραμματείες στις οποίες πρέπει να διαβιβαστούν οι διαβαθμισμένες πληροφορίες ΕΕ και η ακριβής διεύθυνση στην οποία θα αποσταλούν τα έγγραφα, καθώς και οι υπηρεσίες μεταφορέων ή ταχυδρομείου που χρησιμοποιούνται για τη διαβίβαση των διαβαθμισμένων πληροφοριών ΕΕ.

12. Καταχώρηση κατά την άφιξη

Η εθνική αρχή ασφαλείας του κράτους παραλαβής ή ο ανάλογος φορέας του κράτους που παραλαμβάνει, εξ ονόματος της κυβέρνησής του, τις διαβαθμισμένες πληροφορίες που κοινοποιούνται από την ΕΕ, ή το γραφείο ασφαλείας του παραλήπτη διεθνούς οργανισμού, θα τηρεί ειδικό μητρώο για την καταχώρηση των διαβαθμισμένων πληροφοριών ΕΕ κατά την παραλαβή τους. Στις στήλες του μητρώου αυτού αναγράφονται η ημερομηνία παραλαβής, τα στοιχεία του εγγράφου (ημερομηνία, αριθμός αναφοράς και αριθμός αντιτύπου), η διαβάθμισή του, ο τίτλος του, το ονοματεπώνυμο και η ιδιότητα του παραλήπτη, η ημερομηνία επιστροφής της απόδειξης και η ημερομηνία επιστροφής του εγγράφου στην ΕΕ, ή της καταστροφής του.

13. Επιστροφή εγγράφων

Όταν ο αποδέκτης επιστέφει ένα διαβαθμισμένο έγγραφο στην Επιτροπή, ακολουθεί τη διαδικασία που αναφέρεται στην παράγραφο «Διαβίβαση εγγράφων» ανωτέρω.

14. Προστασία

α) Όταν τα έγγραφα δεν χρησιμοποιούνται, αποθηκεύονται σε ασφαλή περιέκτη εγκεκριμένο για την αποθήκευση εθνικού διαβαθμισμένου υλικού της ίδιας διαβάθμισης. Ο περιέκτης δεν φέρει ένδειξη του περιεχομένου του, στο οποίο έχουν πρόσβαση μόνον άτομα εξουσιοδοτημένα να χειρίζονται διαβαθμισμένες πληροφορίες ΕΕ. Όταν χρησιμοποιούνται κλειδαριές με συνδυασμό, ο συνδυασμός πρέπει να είναι γνωστός μόνον στους υπαλλήλους του κράτους ή του οργανισμού που έχει εξουσιοδοτημένη πρόσβαση στις διαβαθμισμένες πληροφορίες ΕΕ που είναι αποθηκευμένες στον φωριαμό και πρέπει να αλλάζει ανά εξάμηνο, ή συχνότερα όταν μετατίθεται ο υπάλληλος, όταν ανακαλείται η διαβάθμιση ασφαλείας ενός από τους υπαλλήλους που γνωρίζουν το συνδυασμό, ή όταν υπάρχει κίνδυνος διαρροής.

β) Τα διαβαθμισμένα έγγραφα ΕΕ αφαιρούνται από τον φωριαμό ασφαλείας μόνον από τους υπαλλήλους που έχουν εξουσιοδότηση πρόσβασης στα διαβαθμισμένα έγγραφα ΕΕ και έχουν «ανάγκη γνώσης». Οι υπάλληλοι αυτοί φέρουν την ευθύνη για την ασφαλή φύλαξη των εγγράφων αυτών καθ' όλο το διάστημα που τα έγγραφα παραμένουν στην κατοχή τους, ιδίως δε, για να εξασφαλίζουν ότι τα μη εξουσιοδοτημένα άτομα δεν έχουν πρόσβαση στα έγγραφα. Οι υπάλληλοι εξασφαλίζουν επίσης ότι τα έγγραφα αποθηκεύονται σε φωριαμό ασφαλείας όταν δεν τα χρησιμοποιούν πλέον και εκτός ωρών εργασίας.

γ) Από τα έγγραφα με διαβάθμιση τουλάχιστον ►M1 CONFIDENTIEL UE ◄, απαγορεύεται να παράγονται φωτοαντίγραφα ή να λαμβάνονται αποσπάσματα χωρίς την άδεια της ►M2 Διεύθυνσης Ασφαλείας της Επιτροπής ◄.

δ) Πρέπει να καθορίζεται η διαδικασία για την ταχεία και πλήρη καταστροφή των εγγράφων σε κατάσταση έκτακτης ανάγκης, και να επιβεβαιώνεται σε συμφωνία με την ►M2 Διεύθυνση Ασφαλείας της Επιτροπής ◄.

▼**B**

15. Υλική ασφάλεια

α) Όταν δεν χρησιμοποιούνται, οι φωριαμοί ασφαλείας που χρησιμοποιούνται για την αποθήκευση διαβαθμισμένων εγγράφων ΕΕ, διατηρούνται πάντα κλειδωμένοι.

β) Όταν το προσωπικό συντήρησης ή καθαρισμού πρέπει να εισέλθει ή να εργαστεί σε μια αίθουσα όπου υπάρχουν οι εν λόγω φωριαμοί ασφαλείας, το προσωπικό αυτό πρέπει να συνοδεύεται πάντοτε από ένα μέλος της υπηρεσίας ασφαλείας του κράτους ή του οργανισμού, ή από υπάλληλο που είναι ειδικά επιφορτισμένος με την εποπτεία της ασφάλειας της αίθουσας.

γ) Εκτός κανονικών ωρών εργασίας (τη νύχτα, κατά τα σαββατοκύριακα ή τις αργίες), οι φωριαμοί ασφαλείας που περιέχουν διαβαθμισμένα έγγραφα ΕΕ προστατεύονται είτε από φρουρό είτε από αυτόματο σύστημα συναγερμού.

16. Παραβάσεις των κανόνων ασφαλείας

Όταν έχουν παραβιαστεί οι κανόνες ασφαλείας για ένα διαβαθμισμένο έγγραφο ΕΕ, ή όταν υπάρχουν σχετικές υπόνοιες, λαμβάνονται αμέσως τα ακόλουθα μέτρα:

α) διαβιβάζεται αμέσως σχετική έκθεση στην ►**M2** Διεύθυνση Ασφαλείας της Επιτροπής ◄ ή στην εθνική αρχή ασφαλείας του κράτους μέλους που έλαβε την πρωτοβουλία να διαβιβάσει τα έγγραφα (με αντίγραφο προς την ►**M2** Διεύθυνση Ασφαλείας της Επιτροπής ◄)·

β) διεξάγεται έρευνα, κατά το πέρας της οποίας υποβάλλεται πλήρης έκθεση στην υπηρεσία ασφαλείας [βλέπε σημείο α) ανωτέρω]. Στη συνέχεια πρέπει να ληφθούν τα απαραίτητα μέτρα για την αντιμετώπιση της κατάστασης.

17. Επιθεωρήσεις

Η ►**M2** Διεύθυνση Ασφαλείας της Επιτροπής ◄ έχει το δικαίωμα, κατόπιν συμφωνίας με τα ενδιαφερόμενα κράτη ή διεθνείς οργανισμούς, να προβαίνει στην αξιολόγηση της αποτελεσματικότητας των μέτρων προστασίας των κοινοποιούμενων διαβαθμισμένων πληροφοριών ΕΕ.

18. Εκθέσεις

Υπό την προϋπόθεση ότι έχει συναφθεί συμφωνία στον τομέα της ασφαλείας, καθ' όλο το διάστημα κατά το οποίο το κράτος ή ο διεθνής οργανισμός διατηρούν στην κατοχή τους διαβαθμισμένες πληροφορίες ΕΕ, υποβάλλουν ετήσια έκθεση, μέχρι μια ημερομηνία που καθορίζεται όταν χορηγείται η άδεια κοινοποίησης των πληροφοριών, με την οποία επιβεβαιώνεται ότι τηρούνται οι προκείμενοι κανονισμοί ασφαλείας.

▼**B**

Προσάρτημα 5

Κατευθυντήριες γραμμές για τη διαβίβαση διαβαθμισμένων πληροφοριών ΕΕ σε τρίτες χώρες ή διεθνείς οργανισμούς: Συνεργασία επιπέδου 3

ΔΙΑΔΙΚΑΣΙΕΣ

1. Ενίοτε, η Επιτροπή ενδέχεται να θελήσει να συνεργαστεί, υπό ορισμένες ειδικές περιστάσεις, με κράτη ή οργανισμούς που δεν μπορούν μεν να παράσχουν τις εγγυήσεις που απαιτούνται βάσει των προκειμένων κανόνων ασφαλείας, η συνεργασία όμως με τα οποία μπορεί να απαιτήσει την κοινοποίηση διαβαθμισμένων πληροφοριών ΕΕ.

2. Αρμόδιος για την κοινοποίηση διαβαθμισμένων πληροφοριών ΕΕ σε τρίτα κράτη ή διεθνείς οργανισμούς, των οποίων η πολιτική και οι διατάξεις ασφαλείας διαφέρουν σημαντικά από εκείνους της ΕΕ, είναι ο αρχικός συντάκτης. Την αρμοδιότητα για την κοινοποίηση ΔΠΕΕ που δημιουργήθηκαν εντός της Επιτροπής, έχει η Επιτροπή εν σώματι.

   Κατά κανόνα, η κοινοποίηση περιορίζεται σε διαβαθμισμένες πληροφορίες με βαθμό ασφαλείας έως ►**M1** SECRET UE ◄· αποκλείονται οι διαβαθμισμένες πληροφορίες που προστατεύονται από ειδικές σημάνσεις ή ενδείξεις ασφαλείας.

3. Η Επιτροπή εξετάζει εάν είναι σκόπιμο να κοινοποιηθούν διαβαθμισμένες πληροφορίες, εκτιμά την «ανάγκη γνώσης» των δικαιούχων, και αποφαίνεται ως προς τη φύση των διαβαθμισμένων πληροφοριών που επιτρέπεται να κοινοποιηθούν.

4. Εάν η Επιτροπή έχει θετική γνώμη, το αρμόδιο για θέματα ασφαλείας Μέλος της Επιτροπής

   — ζητεί τις γνώμες των συντακτών των προς κοινοποίηση ΔΠΕΕ·

   — διοργανώνει συνεδρίαση της συμβουλευτικής ομάδας επί θεμάτων πολιτικής ασφαλείας της Επιτροπής ή, εφόσον απαιτείται, με τη διαδικασία σιωπηρής συναίνεσης, απευθύνει ερωτήματα στις εθνικές αρχές ασφαλείας των κρατών μελών, προκειμένου να λάβει τη γνώμη της συμβουλευτικής ομάδας επί θεμάτων πολιτικής ασφαλείας της Επιτροπής.

5. Η γνώμη της συμβουλευτικής ομάδας επί θεμάτων πολιτικής ασφαλείας της Επιτροπής, θα αφορά:

   α) την αξιολόγηση των κινδύνων ασφαλείας που διατρέχουν η ΕΕ ή τα κράτη μέλη της·

   β) το επίπεδο διαβάθμισης των πληροφοριών που ενδέχεται να κοινοποιηθούν·

   γ) τον υποχαρακτηρισμό ή τον αποχαρακτηρισμό πριν από την κοινοποίηση των πληροφοριών·

   δ) τις διαδικασίες για το χειρισμό των προς κοινοποίηση εγγράφων (βλέπε παράγραφο κατωτέρω)·

   ε) τις πιθανές μεθόδους διαβίβασης (χρήση δημόσιων ταχυδρομικών υπηρεσιών, δημόσια ή ασφαλή τηλεπικοινωνιακά συστήματα, διπλωματικοί σάκοι, διαβαθμισμένοι μεταφορείς κ.λπ.).

6. Τα έγγραφα που κοινοποιούνται στα κράτη ή τους οργανισμούς που καλύπτονται από το παρόν παράρτημα συντάσσονται, κατά κανόνα, χωρίς αναφορά της πηγής ή της διαβάθμισης ΕΕ. Η συμβουλευτική ομάδα επί θεμάτων πολιτικής ασφάλειας της Επιτροπής ενδέχεται να προτείνει:

   — τη χρήση ειδικής σήμανσης ή κωδικής ονομασίας·

   — τη χρήση ειδικού συστήματος διαβάθμισης, με το οποίο η ευαισθησία των πληροφοριών συνδέεται με τα μέτρα ελέγχου που πρέπει να τηρούνται κατά την εφαρμογή των μεθόδων διαβίβασης των εγγράφων από τους δικαιούχους.

7. Το►**M2** αρμόδιο για θέματα ασφαλείας μέλος της Επιτροπής ◄ διαβιβάζει στην Επιτροπή για τη λήψη της σχετικής απόφασης, τη γνώμη της συμβουλευτικής ομάδας επί θεμάτων πολιτικής ασφαλείας της Επιτροπής.

8. Από τη στιγμή που η Επιτροπή εγκρίνει την κοινοποίηση διαβαθμισμένων πληροφοριών ΕΕ και τις διαδικασίες πρακτικής εφαρμογής, η ►**M2** Διεύθυνση Ασφαλείας της Επιτροπής ◄ πραγματοποιεί τις απαιτούμενες επαφές με τον φορέα ασφαλείας του ενδιαφερόμενου κράτους ή οργανισμού, για να διευκολύνει την εφαρμογή των προτεινόμενων μέτρων ασφαλείας.

▼B

9. Το αρμόδιο για θέματα ασφαλείας μέλος της Επιτροπής ενημερώνει τα κράτη μέλη σχετικά με τη φύση και τη διαβάθμιση των πληροφοριών, παραθέτοντας κατάλογο των οργανισμών και των χωρών στις οποίες μπορεί να κοινοποιηθούν, όπως αποφασίστηκε από την Επιτροπή.

10. Η ►**M2** Διεύθυνση Ασφαλείας της Επιτροπής ◄ λαμβάνει όλα τα απαραίτητα μέτρα για να διευκολυνθεί η τυχόν επακόλουθη αξιολόγηση της ζημίας και η αναθεώρηση των διαδικασιών.

Σε περίπτωση μεταβολής των όρων συνεργασίας, η Επιτροπή θα επανεξετάζει το θέμα.

ΔΙΑΤΑΞΕΙΣ ΑΣΦΑΛΕΙΑΣ ΠΟΥ ΠΡΕΠΕΙ ΝΑ ΕΦΑΡΜΟΖΟΥΝ ΟΙ ΔΙΚΑΙΟΥΧΟΙ

11. Το αρμόδιο για θέματα ασφάλειας μέλος της Επιτροπής κοινοποιεί στα δικαιούχα κράτη ή τους διεθνείς οργανισμούς, την απόφαση της Επιτροπής να επιτρέψει την κοινοποίηση διαβαθμισμένων πληροφοριών ΕΕ, καθώς και τους λεπτομερείς κανόνες προστασίας που έχει προτείνει η συμβουλευτική ομάδα επί θεμάτων πολιτικής ασφάλειας της Επιτροπής και έχουν εγκριθεί από την Επιτροπή.

12. Η απόφαση αρχίζει να ισχύει μόνον όταν οι δικαιούχοι εγγυηθούν γραπτώς ότι:

— θα χρησιμοποιούν τις πληροφορίες μόνον για τη συνεργασία που αποφάσισε η Επιτροπή·

— θα προστατεύουν τις πληροφορίες όπως απαιτεί η Επιτροπή.

13. Διαβίβαση εγγράφων

α) Οι πρακτικές διαδικασίες για τη διαβίβαση των εγγράφων συμφωνούνται μεταξύ της ►**M2** Διεύθυνσης Ασφαλείας της Επιτροπής ◄ και των φορέων ασφαλείας των παραληπτών κρατών ή διεθνών οργανισμών. Στις διαδικασίες αυτές πρέπει ιδίως να προσδιορίζονται οι ακριβείς διευθύνσεις στις οποίες πρέπει να αποσταλούν τα έγγραφα.

β) Τα έγγραφα με διαβάθμιση τουλάχιστον ►**M1** CONFIDENTIEL UE ◄ διαβιβάζονται εντός διπλού φακέλου. Ο εσωτερικός φάκελος φέρει την ειδική σφραγίδα ή την κωδική ονομασία που έχουν αποφασιστεί και αναφέρει την ειδική διαβάθμιση που έχει εγκριθεί για το συγκεκριμένο έγγραφο. Μέσα στο φάκελο, κάθε διαβαθμισμένο έγγραφο συνοδεύεται από έντυπο απόδειξης παραλαβής. Στο έντυπο απόδειξης παραλαβής, το οποίο δεν είναι διαβαθμισμένο, αναγράφονται μόνον τα στοιχεία του εγγράφου (αριθμός αναφοράς, ημερομηνία, αριθμός αντιτύπου) και η γλώσσα του, αλλά όχι ο τίτλος.

γ) Ο εσωτερικός φάκελος τοποθετείται εντός του εξωτερικού φακέλου ο οποίος φέρει αριθμό δέματος για να είναι δυνατόν να χορηγηθεί απόδειξη παραλαβής. Ο εξωτερικός φάκελος δεν φέρει διαβάθμιση ασφαλείας.

δ) Στους μεταφορείς χορηγείται πάντοτε απόδειξη, στην οποία αναγράφεται ο αριθμός του δέματος.

14. Καταχώρηση κατά την άφιξη

Η Εθνική Αρχή Ασφαλείας του κράτους παραλαβής ή ο ανάλογος φορέας του κράτους που παραλαμβάνει, εξ ονόματος της κυβέρνησής του, τις διαβαθμισμένες πληροφορίες που κοινοποιούνται από την ΕΕ, ή το γραφείο ασφαλείας του παραλήπτη διεθνούς οργανισμού, θα τηρεί ειδικό μητρώο για την καταχώρηση των διαβαθμισμένων πληροφοριών ΕΕ κατά την παραλαβή τους. Στις στήλες του μητρώου αυτού αναγράφονται η ημερομηνία παραλαβής, τα στοιχεία του εγγράφου (ημερομηνία, αριθμός αναφοράς και αριθμός αντιτύπου), η διαβάθμισή του, ο τίτλος του, το ονοματεπώνυμο ή ο τίτλος του παραλήπτη, η ημερομηνία επιστροφής της απόδειξης και η ημερομηνία επιστροφής της απόδειξης στην ΕΕ ή καταστροφής του εγγράφου.

15. Χρήση και προστασία των ανταλλασσόμενων διαβαθμισμένων πληροφοριών

α) Οι πληροφορίες με βαθμό ασφαλείας ►**M1** SECRET UE ◄ διεκπεραιώνονται από ειδικά εξουσιοδοτημένους υπαλλήλους που έχουν πρόσβαση σε πληροφορίες με τη διαβάθμιση αυτή. Οι πληροφορίες αυτές αποθηκεύονται σε καλής ποιότητας φωριαμούς ασφαλείας, τους οποίους μπορούν να ανοίξουν μόνον τα άτομα που έχουν εξουσιοδότηση πρόσβασης στις πληροφορίες που περιέχουν. Οι χώροι όπου ευρίσκονται οι φωριαμοί αυτοί πρέπει να φρουρούνται συνεχώς, πρέπει δε να εφαρμόζεται ένα σύστημα ελέγχου προκειμένου να εξασφαλίζεται ότι η είσοδος επιτρέπεται μόνον σε δεόντως εξουσιοδοτημένα άτομα. Οι πληροφορίες με βαθμό ασφαλείας ►**M1** SECRET UE ◄ διαβιβάζονται με διπλωματικό σάκο, ασφαλείς ταχυδρομικές υπηρεσίες και ασφαλείς τηλεπικοινωνιακές υπηρεσίες. Ένα έγγραφο ►**M1** SECRET UE ◄ μπορεί να αντιγράφεται μόνον με τη γραπτή συγκατάθεση της συντάκτριας αρχής. Όλα

▼**B**

τα αντίτυπα πρέπει να καταχωρούνται και να παρακολουθούνται. Για όλες τις εργασίες που αφορούν έγγραφα με βαθμό ασφαλείας ►**M1** SECRET UE ◄ εκδίδεται απόδειξη παραλαβής.

β) Οι πληροφορίες ►**M1** CONFIDENTIEL UE ◄ διεκπεραιώνονται από δεόντως οριζόμενους υπαλλήλους που είναι εξουσιοδοτημένοι να λαμβάνουν γνώση του θέματος. Τα έγγραφα αποθηκεύονται σε κλειδωμένους φωριαμούς ασφαλείας, σε ελεγχόμενους χώρους·

Οι πληροφορίες ►**M1** CONFIDENTIEL UE ◄ διαβιβάζονται με διπλωματικό σάκο, υπηρεσίες στρατιωτικού ταχυδρομείου και ασφαλείς τηλεπικοινωνιακές υπηρεσίες. Ο παραλήπτης φορέας μπορεί να παράγει αντίγραφα, των οποίων ο αριθμός και οι παραλήπτες καταχωρούνται σε ειδικά μητρώα·

γ) Οι πληροφορίες ►**M1** RESTREINT UE ◄ διεκπεραιώνονται σε χώρους στους οποίους δεν επιτρέπεται η πρόσβαση μη εξουσιοδοτημένων προσώπων, αποθηκεύονται δε σε κλειδωμένους περιέκτες. Τα έγγραφα αυτά μπορούν να διαβιβάζονται μέσω των δημόσιων ταχυδρομικών υπηρεσιών ως συστημένα εντός διπλού φακέλου και, σε επείγουσες καταστάσεις κατά τη διάρκεια επιχειρήσεων, μέσω των μη προστατευόμενων δημόσιων τηλεπικοινωνιακών συστημάτων. Οι αποδέκτες μπορούν να παράγουν αντίγραφα·

δ) Για τις μη διαβαθμισμένες πληροφορίες δεν απαιτούνται ειδικά μέτρα προστασίας, οι δε πληροφορίες αυτές μπορούν να διαβιβάζονται ταχυδρομικώς και μέσω των δημόσιων τηλεπικοινωνιακών συστημάτων. Οι αποδέκτες μπορούν να παράγουν αντίγραφα.

16. Καταστροφή

Τα έγγραφα που δεν χρειάζονται πλέον πρέπει να καταστρέφονται. Για τα έγγραφα ►**M1** RESTREINT UE ◄ και ►**M1** CONFIDENTIEL UE ◄, πραγματοποιείται σχετική εγγραφή στα ειδικά μητρώα. Για τα έγγραφα ►**M1** SECRET UE ◄, συντάσσονται πρωτόκολλα καταστροφής τα οποία υπογράφονται από δύο άτομα που παρίστανται κατά την καταστροφή τους.

17. Παραβιάσεις των κανόνων ασφαλείας

Όταν έχουν διαρρεύσει πληροφορίες βαθμού ασφαλείας ►**M1** CONFIDENTIEL UE ◄ ή ►**M1** SECRET UE ◄, ή εφόσον υπάρχουν σχετικές υπόνοιες, η εθνική αρχή ασφαλείας του κράτους ή ο προϊστάμενος ασφαλείας του οργανισμού, ερευνούν τις περιστάσεις της διαρροής. Τα αποτελέσματα της έρευνας κοινοποιούνται στην ►**M2** Διεύθυνση Ασφαλείας της Επιτροπής ◄. Λαμβάνονται τα απαιτούμενα μέτρα για τη διόρθωση των ακατάλληλων διαδικασιών ή μεθόδων αποθήκευσης, εάν η διαρροή οφείλεται σε αυτές.

▼**B**

Προσάρτημα 6

ΚΑΤΑΛΟΓΟΣ ΣΥΝΤΟΜΟΓΡΑΦΙΩΝ

ΣΕΑΣ	Συμβουλευτική Επιτροπή Αγορών και Συμβάσεων
CrA	Αρχή Κρυπτογράφησης
CISO	Υπεύθυνος Ασφαλείας Κεντρικών Συστημάτων Πληροφορικής
COMPUSEC	Ασφάλεια Υπολογιστή
COMSEC	Ασφάλεια Επικοινωνιών
CSO	►**M2** Διεύθυνση Ασφαλείας της Επιτροπής ◄
ESDP	Ευρωπαϊκή Πολιτική Ασφάλειας και Άμυνας
EUCI	Διαβαθμισμένες Πληροφορίες ΕΕ
IA	Αρχή INFOSEC
INFOSEC	Ασφάλεια Πληροφοριών
IO	Ιδιοκτήτης των πληροφοριών
ISO	Διεθνής Οργανισμός Τυποποίησης
IT	Τεχνολογία των Πληροφοριών
LISO	Υπεύθυνος Ασφαλείας Τοπικών Συστημάτων Πληροφορικής
LSO	Τοπικός Υπεύθυνος Ασφαλείας
MSO	Υπάλληλος Ασφαλείας της Συνεδρίασης
NSA	Εθνική Αρχή Ασφαλείας
PC	Προσωπικός Υπολογιστής
RCO	Ελεγκτικός Υπάλληλος Γραμματείας
SAA	Αρχή Διαπίστευσης της Ασφάλειας
SecOP	Ασφαλείς Διαδικασίες Λειτουργίας
SSRS	Δήλωση Απαιτήσεων Ασφαλείας Ανταποκρινόμενων στο Ιδιαίτερο Σύστημα
TA	Αρχή Tempest
TSO	Ιδιοκτήτης Τεχνικών Συστημάτων

▼**M3**

ΚΑΑ	Καθορισμένη Αρχή Ασφάλειας
ΕΑΦ	Έλεγχος Ασφαλείας Φορέα
ΥΑΕ	Υπεύθυνος Ασφαλείας της Εγκατάστασης
ΠΕΑΠ	Πιστοποιητικό Ελέγχου Ασφαλείας Προσωπικού
ΕΘΑ	Έγγραφο Θεμάτων Ασφαλείας
ΟΔΑ	Οδηγός Διαβάθμισης Ασφαλείας