Ο περί Κανονισμών Ασφαλείας Διαβαθμισμένων Πληροφοριών, Εγγράφων και Υλικού και για Συναφή Θέματα Νόμος του 2002, εκδίδεται με δημοσίευση στην Επίσημη Εφημερίδα της Κυπριακής Δημοκρατίας σύμφωνα με το Άρθρο 52 του Συντάγματος.

Αριθμός 216(Ι) του 2002

ΝΟΜΟΣ ΠΟΥ ΠΡΟΝΟΕΙ ΓΙΑ ΤΟΥΣ ΚΑΝΟΝΙΣΜΟΥΣ ΑΣΦΑΛΕΙΑΣ ΔΙΑΒΑΘΜΙΣΜΕΝΩΝ ΠΛΗΡΟΦΟΡΙΩΝ, ΕΓΓΡΑΦΩΝ ΚΑΙ ΥΛΙΚΟΥ ΚΑΙ ΓΙΑ ΣΥΝΑΦΗ ΘΕΜΑΤΑ ΤΟΥ 2002

Επειδή καθίσταται αναγκαία η λήψη των κατάλληλων μέτρων από μέρους της Δημοκρατίας ως συμμετέχουσας στην Κοινή Εξωτερική Πολιτική και Πολιτική Ασφάλειας και στην Κοινή Πολιτική Ασφάλειας και Άμυνας της Ευρωπαϊκής Ένωσης, για τη διευκόλυνση υλοποίησης και τήρησης ενός ολοκληρωμένου συστήματος ασφαλείας το οποίο θα καλύπτει το Συμβούλιο της Ευρωπαϊκής Ένωσης, τη Γενική Γραμματεία του Συμβουλίου και τα κράτη μέλη και προκειμένου να αναπτυχθούν οι δραστηριότητες του Συμβουλίου σε τομείς που απαιτείται εμπιστευτικότητα και ειδικότερα, για σκοπούς άμεσης εφαρμογής της πράξης της Ευρωπαϊκής Κοινότητας με τίτλο-

«Απόφαση 2001/264/ΕΚ του Συμβουλίου, της 19ης Μαρτίου 2001, για την έγκριση των κανονισμών ασφαλείας του Συμβουλίου (ΕΕ L 101 της 11.04.2001, σ. 1)»,

Η Βουλή των Αντιπροσώπων ψηφίζει ως ακολούθως:

Συνοπτικός τίτλος.

1. Ο παρών Νόμος θα αναφέρεται ως ο περί Κανονισμών Ασφαλείας Διαβαθμισμένων Πληροφοριών, Εγγράφων και Υλικού και για Συναφή Θέματα Νόμος του 2002.

Ερμηνεία.

2. Στον παρόντα Νόμο, εκτός αν από το κείμενο προκύπτει διαφορετική έννοια-

«Απόφαση 2001/264/ΕΚ» σημαίνει την πράξη της Ευρωπαϊκής Ένωσης με τίτλο «Απόφαση 2001/264/ΕΚ του Συμβουλίου, της 19ης Μαρτίου 2001, για την έγκριση των κανονισμών ασφαλείας του Συμβουλίου (ΕΕ L 101 της 11.04.2001, σ.1)»·

«Αρχή Ασφαλείας Πληροφοριών Τεχνικής Φύσεως (INFOSEC)» σημαίνει το Υπουργείο Άμυνας/Γενικό Επιτελείο Εθνικής Φρουράς (ΥΠΑΜ/ ΓΕΕΦ) όταν ασκεί τις αρμοδιότητες που του ανατίθενται από το άρθρο 8·

«Αρχή Διαπίστευσης Ασφαλείας» σημαίνει το Υπουργείο Άμυνας/ Γενικό Επιτελείο Εθνικής Φρουράς (ΥΠΑΜ/ΓΕΕΦ), όταν ασκεί τις αρμοδιότητες που του ανατίθενται από το άρθρο 6·

«Γενικός Γραμματέας/Ύπατος Εκπρόσωπος» σημαίνει το Γενικό Γραμματέα του Συμβουλίου, όταν ασκεί τα καθήκοντα του Υπάτου Εκπροσώπου για την Κοινή Εξωτερική Πολιτική και Πολιτική Ασφάλειας, σύμφωνα με το Άρθρο 18 της Συνθήκης για την Ευρωπαϊκή Ένωση·

«Δημοκρατία» σημαίνει την Κυπριακή Δημοκρατία·

«διαβαθμισμένη πληροφορία ΕΕ» σημαίνει κάθε πληροφορία έγγραφο ή υλικό των οποίων η άνευ άδειας κοινολόγηση μπορεί να βλάψει σε ποικίλο βαθμό τα συμφέροντα της Ευρωπαϊκής Ένωσης (ΕΕ) ή ενός ή περισσότερων κρατών μελών της, ασχέτως του εάν η πληροφορία αυτή προέρχεται από την Ευρωπαϊκή Ένωση (ΕΕ) ή έχει ληφθεί από κράτος μέλος, τρίτο κράτος ή διεθνή οργανισμό·

«έγγραφο» σημαίνει κάθε επιστολή, σημείωμα, κείμενο πρακτικών, έκθεση, υπόμνημα, σήμα/μήνυμα, σκαρίφημα, φωτογραφία, διαφάνεια,

φιλμ, χάρτη, 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-

«Εθνική Αρχή Ασφαλείας» ή «ΕΕΑ» σημαίνει το Υπουργείο Άμυνας Επιτελείο Υπουργού Άμυνας (ΥΠΑΜ/ΕΠΥΠΑΜ) όταν ασκεί τις αρμοδιότητες που του ανατίθενται από το άρθρο 5-

«Εθνικός Οργανισμός Ασφαλείας» ή «ΕΟΑ» σημαίνει την Κεντρική Υπηρεσία Πληροφοριών όταν ασκεί τις αρμοδιότητες που της ανατίθενται από το άρθρο 7·

«Κεντρική Γραμματεία ΑΚΡΩΣ ΑΠΟΡΡΗΤΩΝ ΕΕ (EU TOP SECRET)» ή «Κεντρική Γραμματεία ΑΚΡΩΣ ΑΠΟΡΡΗΤΩΝ ΕΕ» σημαίνει την Υπηρεσία Κοινής Εξωτερικής Πολιτικής και Πολιτικής Ασφαλείας (ΚΕΠΠΑ) του Υπουργείου Εξωτερικών όταν ασκεί τις αρμοδιότητες που της ανατίθενται από το άρθρο 9·

«κράτος μέλος» σημαίνει κράτος μέλος της Ευρωπαϊκής Ένωσης(ΕΕ) και ως κράτος μέλος λογίζεται και η Δημοκρατία·

«Συμβούλιο» σημαίνει το Συμβούλιο της Ευρωπαϊκής Ένωσης (ΕΕ)·

Παράρτημα.

«ΣΥΣΤΗΜΑΤΑ», σημαίνει τα συστήματα και δίκτυα επικοινωνιών και πληροφορικής που προβλέπονται στο Κεφάλαιο Ι, του Τμήματος ΧΙ, του Μέρους ΙΙ, του Παραρτήματος·

«τρίτο κράτος» σημαίνει οποιοδήποτε κράτος δεν είναι κράτος μέλος·

«υλικό» σημαίνει κάθε έγγραφο καθώς και κάθε στοιχείο μηχανισμού ή όπλου που έχει ήδη κατασκευασθεί ή βρίσκεται υπό κατασκευή.

Σκοπός.

3. Σκοπός του παρόντος Νόμου είναι—

(α) Ο καθορισμός των θεμελιωδών αρχών και προδιαγραφών ασφαλείας που πρέπει να τηρούνται από τη Δημοκρατία, προκειμένου να διασφαλίζεται ότι εφαρμόζεται ένας ενιαίος βαθμός προστασίας των διαβαθμισμένων πληροφοριών, εγγράφων και υλικού από το Συμβούλιο, τη Γενική Γραμματεία του Συμβουλίου, τα κράτη μέλη και τους αποκεντρωμένους οργανισμούς της Ευρωπαϊκής Ένωσης· και

(β) η λήψη των κατάλληλων μέτρων για τη διευκόλυνση υλοποίησης και τήρησης ενός ολοκληρωμένου συστήματος ασφαλείας διαβαθμισμένων πληροφοριών, εγγράφων και υλικού, το οποίο θα καλύπτει το Συμβούλιο της Ευρωπαϊκής Ένωσης, τη Γενική Γραμματεία του Συμβουλίου και τα κράτη μέλη, προκειμένου να αναπτυχθούν οι δραστηριότητες του Συμβουλίου σε τομείς που απαιτείται εμπιστευτικότητα:

Νοείται ότι με τον όρο ασφάλεια εξυπηρετούνται οι εξής στόχοι:

(α) Η προστασία διαβαθμισμένων πληροφοριών ΕΕ από την κατασκοπεία, τη διαρροή, ή την κοινολόγηση χωρίς άδεια·

(β) η προστασία διαβαθμισμένων πληροφοριών ΕΕ που διακινούνται στα συστήματα και στα δίκτυα επικοινωνιών και πληροφορικής·

(γ) η προστασία των χώρων και των εγκαταστάσεων εντός της Δημοκρατίας, όπου αποθηκεύονται διαβαθμισμένες πληροφορίες ΕΕ από το ενδεχόμενο δολιοφθοράς και κακόβουλης ζημιάς-

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

Υποχρέωση τήρησης των κανονισμών ασφαλείας.

4. Όλα τα πρόσωπα που χειρίζονται διαβαθμισμένες πληροφορίες, έγγραφα ή υλικό ή τα μέσα επεξεργασίας διαβαθμισμένων πληροφοριών, εγγράφων ή υλικού, και ειδικότερα—

(α) Τα μέλη της Μόνιμης Αντιπροσωπείας της Δημοκρατίας στην Ευρωπαϊκή Ένωση καθώς και τα μέλη των αντιπροσωπειών της Δημοκρατίας, που συμμετέχουν σε συνόδους του Συμβουλίου ή συνεδριάσεις των επιτροπών και ομάδων του ή λαμβάνουν μέρος σε άλλες δραστηριότητες του Συμβουλίου-

(β) άλλα μέλη της δημόσιας υπηρεσίας της Δημοκρατίας τα οποία χειρίζονται διαβαθμισμένες πληροφορίες ΕΕ, ασχέτως του αν υπηρετούν στο έδαφος της Δημοκρατίας ή στο έδαφος κρατών μελών ή σε τρίτα κράτη· και

(γ) οι εξωτερικοί συμβασιούχοι της Δημοκρατίας και το αποσπασμένο προσωπικό που χειρίζεται διαβαθμισμένες πληροφορίες ΕΕ,

οφείλουν να τηρούν τις διατάξεις του παρόντος Νόμου και των Κανονισμών και Διαταγμάτων που εκδίδονται δυνάμει αυτού και τους Κανονισμούς Ασφαλείας του Συμβουλίου που εγκρίθηκαν με την Απόφαση 2001/264/ΕΚ του Συμβουλίου, το κείμενο των οποίων, στο ελληνικό πρωτότυπο, εκτίθενται στο Παράρτημα του παρόντος Νόμου.

Παράρτημα.

Αρμοδιότητες Εθνικής Αρχής Ασφαλείας.

5.—(1) Το Υπουργείο Άμυνας/Επιτελείο Υπουργού Άμυνας (ΥΠΑΜ/ ΕΠΥΠΑΜ) ορίζεται ως Εθνική Αρχή Ασφαλείας. Η Εθνική Αρχή Ασφαλείας (ΕΑΑ) έχει την ευθύνη για την ασφάλεια των διαβαθμισμένων πληροφοριών ΕΕ και ειδικότερα είναι υπεύθυνη για—

(α) Την τήρηση της ασφάλειας των διαβαθμισμένων πληροφοριών που βρίσκονται στην κατοχή και /ή φύλαξη των διάφορων φορέων, οργανισμών και υπηρεσιών της Δημοκρατίας, τόσο εντός της Δημοκρατίας όσο και στο εξωτερικό, όπως σε πρεσβείες και μόνιμες αντιπροσωπείες·

(β) τον έλεγχο περιοδικά των ρυθμίσεων ασφαλείας για την προστασία διαβαθμισμένων πληροφοριών ΕΕ·

(γ) να διασφαλίζει ότι όλοι οι εργαζόμενοι σε φορείς, οργανισμούς και υπηρεσίες της Δημοκρατίας, οι οποίοι μπορούν να έχουν πρόσβαση σε πληροφορίες της ΕΕ που έχουν διαβάθμιση ΑΚΡΩΣ ΑΠΟΡΡΗΤΟΝ ΕΕ, ΑΠΟΡΡΗΤΟΝ ΕΕ και ΕΜΠΙΣΤΕΥΤΙΚΟ ΕΕ, έχουν υποστεί έλεγχο ασφαλείας·

(δ) την πρόληψη διαρροής διαβαθμισμένων πληροφοριών σε μη εξουσιοδοτημένα άτομα- και

(ε) την έγκριση της δημιουργίας υπογραμματειών σύμφωνα με τις διατάξεις του άρθρου 9.

(2) Η ΕΑΑ δύναται να διενεργεί περιοδικές επιθεωρήσεις των ρυθμίσεων ασφαλείας για την προστασία των διαβαθμισμένων πληροφοριών ΕΕ σε χώρους όπου φυλάσσεται τέτοιας φύσης υλικό. Η ΕΑΑ συνεργάζεται με το Γραφείο Ασφαλείας της Γενικής Γραμματείας του Συμβουλίου, για τη διενέργεια από κοινού επιθεωρήσεων.

(3) Η ΕΑΑ έχει επίσης την ευθύνη να διαβιβάζει τα αποτελέσματα των ετήσιων απογραφών που διεξάγονται στην Κεντρική Γραμματεία ΑΚΡΩΣ ΑΠΟΡΡΗΤΩΝ ΕΕ στο Γενικό Γραμματέα/Ύπατο Εκπρόσωπο, πριν από την 1η Απριλίου κάθε έτους.

Αρμοδιότητες Αρχής Διαπίστευσης Ασφάλειας.

6. Το Υπουργείο Άμυνας/Γενικό Επιτελείο Εθνικής Φρουράς (ΥΠΑΜ/ ΓΕΕΦ) ορίζεται ως η Αρχή Διαπίστευσης Ασφαλείας. Στο πλαίσιο των αρμοδιοτήτων του συγκροτεί κατά περίπτωση επιτροπές για τη διαπίστευση των «ΣΥΣΤΗΜΑΤΩΝ» και ειδικότερα, για την εξασφάλιση της συμμόρφωσης των «ΣΥΣΤΗΜΑΤΩΝ» εντός του επιχειρησιακού τους περιβάλλοντος, με την πολιτική ασφαλείας του Συμβουλίου.

Εξουσίες Εθνικού Οργανισμού Ασφαλείας.

7. Η Κεντρική Υπηρεσία Πληροφοριών (ΚΥΠ) ορίζεται ως Εθνικός Οργανισμός Ασφαλείας και είναι υπεύθυνη σύμφωνα με τις διατάξεις του Παραρτήματος και για σκοπούς προσαρμογής με τις διατάξεις της Αποφάσεως 2001/264/ΕΚ για—

(α) Τη συγκέντρωση και καταγραφή στοιχείων για περιπτώσεις κατασκοπείας, δολιοφθορών, τρομοκρατίας και άλλες ανατρεπτικές δραστηριότητες· και

(β) την παροχή πληροφοριών και συμβουλών στην Κυβέρνηση της Δημοκρατίας και μέσω αυτής στο Συμβούλιο σχετικά με τη φύση των απειλών κατά της ασφαλείας και τα μέσα για την προστασία από αυτές.

Αρμοδιότητες Αρχής Ασφάλειας Πληροφοριών Τεχνικής Φύσης (INFOSEC). Παράρτημα.

8. Το Υπουργείο Άμυνας/Γενικό Επιτελείο Εθνικής Φρουράς (ΥΠΑΜ/ ΓΕΕΦ) ορίζεται ως η Αρχή Ασφαλείας Πληροφοριών Τεχνικής Φύσεως (INFOSEC), η οποία ως τέτοια, εκτός των άλλων αρμοδιοτήτων που έχει σύμφωνα με τις διατάξεις του Παραρτήματος, είναι υπεύθυνη για τη συνεργασία με την Εθνική Αρχή Ασφαλείας προκειμένου να παρέχει πληροφορίες και συμβουλές σχετικά με τις τεχνικής φύσεως απειλές κατά της ασφάλειας και τα μέσα για την προστασία από αυτές.

Αρμοδιότητες Κεντρικής Γραμματείας Άκρως Απορρήτων ΕΕ και Υπογραμματειών.

9.—(1) Στην Υπηρεσία Κοινής Εξωτερικής Πολιτικής και Πολιτικής Ασφαλείας (ΚΕΠΠΑ) του Υπουργείου Εξωτερικών ιδρύεται η Κεντρική Γραμματεία ΑΚΡΩΣ ΑΠΟΡΡΗΤΩΝ ΕΕ (EU TOP SECRET), η οποία λειτουργεί ως η κύρια αρχή παραλαβής και αποστολής ΑΚΡΩΣ ΑΠΟΡΡΗΤΩΝ ΕΕ, από τη Δημοκρατία προς τα κράτη μέλη και αντίστροφα και η οποία συνεργάζεται με τις Υπογραμματείες που ορίζονται σύμφωνα με τα εδάφια (3) και (5).

Παράρτημα.

(2) Η Κεντρική Γραμματεία ΑΚΡΩΣ ΑΠΟΡΡΗΤΩΝ ΕΕ αναλαμβάνει το έργο της καταγραφής, διεκπεραίωσης, διανομής και διαφύλαξης όλων των ΑΚΡΩΣ ΑΠΟΡΡΗΤΩΝ ΕΕ εγγράφων, σύμφωνα με τις διατάξεις του Τμήματος VII του Παραρτήματος και τηρεί κατάλογο όλων των εξαρτώμενων Υπογραμματειών που ιδρύονται σύμφωνα με το εδάφιο (3) για να την υποβοηθήσουν στην τακτική διεκπεραίωση του έργου της, και διατηρεί αρχείο διατηρούμενων και διανεμόμενων ΑΚΡΩΣ ΑΠΟΡΡΗΤΩΝ ΕΕ εγγράφων:

Νοείται ότι, η προσωρινή και περιστασιακή πρόσβαση σε ΑΚΡΩΣ ΑΠΟΡΡΗΤΑ ΕΕ έγγραφα, δύναται να γίνεται χωρίς τη σύσταση υπογραμματειών.

(3) Στο Υπουργείο Άμυνας, στο ΓΕΕΦ και στη Μόνιμη Αντιπροσωπεία της Δημοκρατίας στην Ευρωπαϊκή Ένωση ιδρύονται Υπογραμματείες ΑΚΡΩΣ ΑΠΟΡΡΗΤΩΝ ΕΕ (EU TOP SECRET), οι οποίες εξαρτώνται από την Κεντρική Γραμματεία και εγκρίνονται σύμφωνα με το εδάφιο (5). Οι Υπογραμματείες δε δύνανται να διαβιβάζουν ΑΚΡΩΣ ΑΠΟΡΡΗΤΑ ΕΕ έγγραφα, σε άλλες Υπογραμματείες εκτός της Δημοκρατίας.

(4) Η Κεντρική Γραμματεία και κάθε Υπογραμματεία ΑΚΡΩΣ ΑΠΟΡΡΗΤΩΝ ΕΕ διεξάγει αναλυτική απογραφή όλων των εγγράφων ΑΚΡΩΣ ΑΠΟΡΡΗΤΩΝ ΕΕ για τα οποία είναι υπεύθυνη, πριν την 1η Μαρτίου κάθε έτους.

Τα αποτελέσματα της ετήσιας απογραφής διαβιβάζονται από τις Υπογραμματείες στην Κεντρική Γραμματεία και στη συνέχεια συγκεντρωτικά στην Εθνική Αρχή Ασφαλείας. Η Εθνική Αρχή Ασφαλείας διαβιβάζει τα αποτελέσματα των ετήσιων απογραφών στο Γενικό Γραμματέα/Ύπατο Εκπρόσωπο, πριν την 1η Απριλίου κάθε έτους.

(5) Η ίδρυση και λειτουργία Υπογραμματειών ΑΚΡΩΣ ΑΠΟΡΡΗΤΩΝ ΕΕ (EU TOP SECRET) σε Υπουργεία, Τμήματα, Υπηρεσίες ή άλλους Κρατικούς Φορείς εγκρίνεται από την Εθνική Αρχή Ασφαλείας σύμφωνα και με τις διατάξεις της παραγράφου (ε), του εδαφίου (1), του άρθρου 5.

Μέτρα ασφαλείας.

10.—(1) Οι αρχές της Δημοκρατίας που αναφέρονται στα άρθρα 5 έως 9, λαμβάνουν όλα τα κατάλληλα μέτρα ασφαλείας και μεριμνούν ώστε να γίνεται ορθή αξιολόγηση των πληροφοριών και του υλικού που πρέπει να προστατεύεται, ώστε να διασφαλίζεται ο μέγιστος βαθμός προστασίας κατά τον προγραμματισμό και τη διοργάνωση τρόπων αντιμετώπισης της κατασκοπείας, των δολιοφθορών της τρομοκρατίας και άλλων απειλών, σύμφωνα με τις σχετικές πρόνοιες του Παραρτήματος.

Παράρτημα.

(2) Τα μέτρα ασφαλείας καλύπτουν όλα τα πρόσωπα που έχουν πρόσβαση σε διαβαθμισμένες πληροφορίες όλα τα μέσα επεξεργασίας τους και τους χώρους, τα κτίρια και τις εγκαταστάσεις στα οποία αποθηκεύονται. Τα μέτρα ασφαλείας σχεδιάζονται κατά τέτοιο τρόπο, ώστε να αποκλείεται η πρόσβαση σε μη εξουσιοδοτημένο προσωπικό, να επισημαίνεται έγκαιρα οποιαδήποτε διαρροή και να προβλέπεται η απομάκρυνση και ο αποκλεισμός προσώπων που δεν πληρούν τους κανόνες ασφαλείας, με απώτερο στόχο να εξασφαλίζεται η αξιοπιστία και η διαθεσιμότητα όλων των πληροφοριών.

(3) Οι αρχές της Δημοκρατίας που αναφέρονται στα άρθρα 5 έως 9 συνεργάζονται σε τακτική βάση με το Συμβούλιο και τις αντίστοιχες υπηρεσίες των κρατών μελών, ώστε να διασφαλίζεται ότι τηρούνται οι κοινές στοιχειώδεις προδιαγραφές ασφαλείας σε όλες τις αρμόδιες αρχές.

Υλική ασφάλεια.

11. Όσον αφορά την υλική ασφάλεια, οι αρχές της Δημοκρατίας που αναφέρονται στα άρθρα 5 έως 9 μεριμνούν ώστε η αυστηρότητα των μέτρων υλικής ασφάλειας που εφαρμόζονται να είναι ανάλογη με τη διαβάθμιση, τον όγκο των πληροφοριών και του υλικού και την υφιστάμενη απειλή. Προς τούτο διενεργούνται έλεγχοι σε όλους τους χώρους όπου αποθηκεύονται διαβαθμισμένες πληροφορίες ΕΕ, ώστε να βεβαιώνεται ότι προστατεύονται επαρκώς τα κτίρια από το ενδεχόμενο εισόδου μη εξουσιοδοτημένων προσώπων και σχετικά, εκπονούνται σχέδια έκτακτης ανάγκης για την προστασία των διαβαθμισμένων πληροφοριών από το ενδεχόμενο να θιγεί τυχαία ή εσκεμμένα η εμπιστευτικότητα, η διαθεσιμότητα ή η ακεραιότητά τους, τηρουμένων

Παράρτημα.

και των σχετικών διατάξεων του Παραρτήματος.

Έλεγχος προσωπικού.

12.—(1) Ο έλεγχος των προσώπων που απαιτείται να έχουν πρόσβαση σε πληροφορίες με διαβάθμιση «ΕΜΠΙΣΤΕΥΤΙΚΟ ΕΕ» (EU CONFIDENTIAL), ή ανώτερη, διενεργείται σύμφωνα με τις σχετικές διατάξεις του Παραρτήματος, τηρουμένων των Συνταγματικών διατάξεων που προστατεύουν τα δικαιώματά τους:

Παράρτημα.

Νοείται ότι, κάθε πρόσωπο το οποίο πρόκειται να επιλεγεί για να έχει πρόσβαση σε σχετικές πληροφορίες ενημερώνεται από την οικεία υπηρεσία επί τούτου, καθώς και για τους σχετικούς ελέγχους και δίδει τη συναίνεσή του για τη διενέργειά τους.

(2) Όλα τα πρόσωπα που απαιτείται να έχουν πρόσβαση σε διαβαθμισμένες πληροφορίες υπόκεινται σε έλεγχο ώστε να εξακριβώνεται κατά πόσο τα πρόσωπα αυτά είναι έμπιστα, διαθέτουν χαρακτήρα και σύνεση που να μη δημιουργούν ερωτηματικά για την αξιοπιστία τους και δεν είναι ευάλωτα σε πιέσεις από ξένους παράγοντες ή άλλες πηγές που θα μπορούσαν να συνιστούν απειλή για την ασφάλεια, τηρουμένων των διατάξεων του Συντάγματος και των διατάξεων του περί Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του Ατόμου) Νόμου του 2001. 138(Ι) του 2001.

(3) Ο έλεγχος αυτός γίνεται πιο προσεκτικός ανάλογα με την εμπιστευτικότητα, τον όγκο και την ειδική πρόσβαση σε διαβαθμισμένες πληροφορίες. Σχετικά τηρούνται αρχεία των ελέγχων ασφάλειας που έχουν πραγματοποιηθεί για το προσωπικό. Το προσωπικό ενημερώνεται για τους κανονισμούς ασφαλείας που ισχύουν κατά την εργασία του και εκπαιδεύεται ανάλογα. Τα διευθυντικά στελέχη των υπηρεσιών και φορέων της Δημοκρατίας οφείλουν να έχουν πλήρη εικόνα για το ποια μέλη του προσωπικού τους χειρίζονται διαβαθμισμένες πληροφορίες ΕΕ, σύμφωνα και με τις σχετικές πρόνοιες του Παραρτήματος. Παράρτημα.

(4) Ο έλεγχος και η έγκριση διαβαθμίσεως «ΕΜΠΙΣΤΕΥΤΙΚΟ ΕΕ» (EU CONFIDENTIAL), ή ανώτερη, για τα πρόσωπα που αναφέρονται στο εδάφιο (1) γίνεται ως ακολούθως:

(α) Για τους δημόσιους υπαλλήλους (ένστολο και πολιτικό προσωπικό), από τις οικείες υπηρεσίες και φορείς της Δημοκρατίας που χειρίζονται διαβαθμισμένες πληροφορίες ΕΕ· και

(β) για το λοιπό προσωπικό, από την Εθνική Αρχή Ασφαλείας.

13.—(1)Τα «ΣΥΣΤΗΜΑΤΑ» στα οποία διακινούνται πληροφορίες με διαβάθμιση ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ ΕΕ και ανώτερη, απαιτείται να καλύπτονται από μέτρα ασφαλείας, ώστε να προστατεύονται η εμπιστευτικότητα, αυθεντικότητα, ακεραιότητα και διαθεσιμότητα αυτών των συστημάτων και των πληροφοριών που περιέχουν. Συστήματα.

(2) Η αναφερόμενη στο άρθρο 8 Αρχή Ασφαλείας Πληροφοριών Τεχνικής Φύσεως (INFOSEC), δύναται να μεταβιβάζει την αρμοδιότητα για την εφαρμογή και τη λειτουργία των ελέγχων και των ειδικών μέτρων ασφαλείας ενός συστήματος στην καθ' ύλην αρμόδια υπηρεσία ή φορέα της Δημοκρατίας, που χειρίζεται τις πληροφορίες που αναφέρονται στο εδάφιο (1), και να ορίζει την εν λόγω υπηρεσία ή φορέα ως Επιχειρησιακή Αρχή Συστημάτων Πληροφορικής IT SYSTEM OPERATIONAL AUTHORITY (ITSOA). Η αρμοδιότητα αυτή ισχύει καθ' όλην τη διάρκεια του κύκλου ζωής του συστήματος, από το στάδιο του βασικού σχεδιασμού μέχρι την τελική του απόσυρση.

14. Κοινοποίηση διαβαθμισμένων πληροφοριών ΕΕ σε τρίτα κράτη ή διεθνείς οργανισμούς, γίνεται μόνο με απόφαση του Συμβουλίου σύμφωνα με τις σχετικές διατάξεις του Παραρτήματος. Κοινοποίηση διαβαθμισμένων πληροφοριών.

15. Παράβαση των προνοιών του παρόντος Νόμου λογίζεται ως παράβαση «υποχρέωσης και καθήκοντος δημοσίου υπαλλήλου» για σκοπούς εφαρμογής των πειθαρχικών διατάξεων των άρθρων 73 έως 86 των περί Δημόσιας Υπηρεσίας Νόμων του 1990 έως 2001. Παράρτημα. Πειθαρχικά παραπτώματα.
1 του 1990
71 του 1991
211 του 1991
27(Ι) του 1994
83(1) του 1995
60(Ι) του 1996
109(Ι) του 1996
69(Ι) του 2000
156(Ι) του 2000
4(Ι) του 2001.

Αδικήματα και ποινές.

16.—(1) Οποιοσδήποτε—

(α) Διαδίδει ή αφήνει να διαρρεύσουν καθ' οποιοδήποτε τρόπο διαβαθμισμένες πληροφορίες, έγγραφα ή υλικό κατά παράβαση των διατάξεων του παρόντος Νόμου, και των Κανονισμών ή Διαταγμάτων που εκδίδονται δυνάμει αυτού· ή

(β) παραλείπει να συμμορφωθεί προς οποιαδήποτε οδηγία ή εντολή που του επιβάλλεται με βάση τον παρόντα Νόμο και τους Κανονισμούς και Διατάγματα που εκδίδονται βάσει αυτού,

είναι ένοχος αδικήματος και υπόκειται, σε περίπτωση καταδίκης του, σε φυλάκιση που δεν υπερβαίνει τα δύο χρόνια ή σε χρηματική ποινή που δεν υπερβαίνει τις Λ.Κ. 2.000, ή και στις δύο ποινές της φυλάκισης και της χρηματικής ποινής.

(2) Οποιοσδήποτε παραλείπει να συμμορφωθεί με οποιαδήποτε διάταξη του παρόντος Νόμου ή των Κανονισμών ή Διαταγμάτων για την οποία δεν προβλέπεται διαφορετικά, υπόκειται, σε περίπτωση καταδίκης του, σε φυλάκιση που δεν υπερβαίνει τον ένα χρόνο ή σε χρηματική ποινή που δεν υπερβαίνει τις Λ.Κ. 1.000 ή και στις δύο ποινές της φυλάκισης και της χρηματικής ποινής.

Εξουσία έκδοσης Κανονισμών.

17.—(1) Το Υπουργικό Συμβούλιο δύναται να εκδίδει Κανονισμούς σχετικά με τους κανόνες του διαβαθμισμένου υλικού καθώς και για την καλύτερη εφαρμογή του Νόμου και για οτιδήποτε πρέπει ή είναι δεκτικό καθορισμού στον παρόντα Νόμο.

(2) Χωρίς επηρεασμό της γενικότητας του εδαφίου (1), Κανονισμοί που εκδίδονται με βάση τον παρόντα Νόμο μπορούν να προβλέπουν ειδικότερα για—

(α) Τον καθορισμό των λεπτομερειών των όρων άσκησης των αρμοδιοτήτων, εξουσιών και υποχρεώσεων των αρμόδιων φορέων που αναφέρονται στα άρθρα 5 έως 9, και την υλοποίηση των διατάξεων της Απόφασης 2001/264/ΕΚ· και

(β) την τήρηση των αρχών που καθορίζονται στην Απόφαση 2001/264/ΕΚ καθώς και για οτιδήποτε εμπίπτει στο πεδίο εφαρμογής του παρόντος Νόμου, με σκοπό την προσαρμογή με το κοινοτικό κεκτημένο και ευρύτερα το ευρωπαϊκό δίκαιο.

Εξουσία έκδοσης διαταγμάτων. Παράρτημα.

18. Το Υπουργικό Συμβούλιο δύναται να εκδίδει διατάγματα για:

(α) Την πρακτική εφαρμογή και υλοποίηση στην επικράτεια της Δημοκρατίας των Κανονισμών Ασφαλείας που αναφέρονται στο Παράρτημα· και

Παράρτημα.

(β) την τροποποίηση του Παραρτήματος, για σκοπούς άμεσης προσαρμογής με το κοινοτικό κεκτημένο και την ευρωπαϊκή νομοθεσία γενικότερα.

ΠΑΡΑΡΤΗΜΑ (άρθρα 2, 4, 8-12, 14,18)

ΚΑΝΟΝΙΣΜΟΙ ΑΣΦΑΛΕΙΑΣ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

Προσαρτήματα

Προσάρτημα 1

Κατάλογος των εθνικών αρχών ασφαλείας.

Προσάρτημα 2

Πίνακας των εθνικών διαβαθμίσεων ασφαλείας

Προσάρτημα 3

Πρακτικός οδηγός διαβάθμισης .

Προσάρτημα 4

Κατευθυντήριες γραμμές για την κοινοποίηση διαβαθμισμένων πληροφοριών ΕΕ σε τρίτα κράτη ή διεθνείς οργανισμούς — συνεργασία επιπέδου

Προσάρτημα 5

Κατευθυντήριες γραμμές για την κοινοποίηση διαβαθμισμένων πληροφοριών ΕΕ σε τρίτα κράτη ή διεθνείς οργανισμούς — συνεργασία επιπέδου 2 .

Προσάρτημα 6

Κατευθυντήριες γραμμές για την κοινοποίηση διαβαθμισμένων πληροφοριών ΕΕ *σε* τρίτα κράτη ή διεθνείς οργανισμούς — συνεργασία επιπέδου 3

ΜΕΡΟΣ Ι

ΘΕΜΕΛΙΩΣΕΙΣ ΑΡΧΕΣ ΚΑΙ ΣΤΟΙΧΕΙΩΔΕΣ ΠΡΟΔΙΑΓΡΑΦΕΣ ΑΣΦΑΛΕΙΑΣ

ΕΙΣΑΓΩΓΗ

1. Με τις παρούσες διατάξεις καθορίζονται οι θεμελιώδεις αρχές και οι στοιχειώδεις προδιαγραφές ασφαλείας που πρέπει να τηρούνται από το Συμβούλιο, τη Γενική Γραμματεία του Συμβουλίου («ΓΤΣ»), τα κράτη μέλη και τους αποκεντρωμένους οργανισμούς της Ευρωπαϊκής Ένωσης (εφεξής «αποκεντρωμένοι οργανισμοί ΕΕ>>) προκειμένου να διασφαλίζεται η ασφάλεια και να είναι όλοι βέβαιοι ότι εφαρμόζεται ένας ενιαίος βαθμός προστασίας.

2 Με τον όρο «διαβαθμισμένη πληροφορία ΕΕ» 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

3. Σε ολόκληρο των κείμενο των παρόντων κανονισμών:

α) 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,

β) ως <υλικό> νοείται κάθε «έγγραφο» όπως ορίζεται στο στοιχείο α) καθώς και κάθε στοιχείο μηχανισμού ή όπλου που έχει ήδη κατασκευασθεί ή βρίσκεται υπό κατασκευή.

4 Η ασφάλεια εξυπηρετεί τους παρακάτω κύριους στόχους:

α) την προστασία των διαβαθμισμένων πληροφοριών ΕΕ 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 αξιοπιστία και τη διαθεσιμότητα τους

γ) την προστασία των εγκαταστάσεων 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.

5. Η ορθή διαχείριση της ασφαλείας στηρίζεται στα εξής στοιχεία:

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

i) τη συγκέντρωση και καταγραφή στοιχείων για περιπτώσεις κατασκοπείας, δολιοφθορών, τρομοκρατίας και άλλες ανατρεπτικές δραστηριότητες, και

ii) την παροχή πληροφοριών και συμβουλών στην κυβέρνηση της χώρας του και, μέσω αυτής, στο Συμβούλιο 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 ΓΤΣ, 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 κρατικών υπηρεσιών και οργανισμών και των αρμόδιων υπηρεσιών της ΓΤΣ προκειμένου να καθορίζονται και ενδεχομένως να υποδεικνύονται:

i) συγκεκριμένες πληροφορίες, πηγές πληροφοριών και εγκαταστάσεις που χρήζουν προστασίας και

ii) κοινές προδιαγραφές προστασίας.

6. 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 την ομαλή ροή των πληροφοριών, λαμβάνονται μέτρα για την αποφυγή κατάχρησης των διαβαθμίσεων ασφαλείας. Το σύστημα διαβάθμισης αποτελεί το μέσο με το οποίο υλοποιούνται οι αρχές αυτές παρόμοιο σύστημα διαβάθμισης θα 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.

ΘΕΜΕΛΙΩΔΕΙΣ ΑΡΧΕΣ

7. **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 την 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 ότου αποθηκεύονται αυτές,

δ) εξασφαλίζουν ότι οι διαβαθμισμένες πληροφορίες διανέμονται μόνο στα πρόσωπα που απαιτείται να έχουν γνώση αυτών, 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.

Η ΟΡΓΑΝΩΣΗ ΤΗΣ ΑΣΦΑΛΕΙΑΣ

Κοινές στοιχειώδεις προδιαγραφές

8. Το Συμβούλιο και κάθε κράτος μέλος εξασφαλίζουν ότι τηρούνται οι κοινές στοιχειώδεις προδιαγραφές ασφαλείας σε όλες τις διοικητικές και/ή κρατικές υπηρεσίες καθώς και στα άλλα θεσμικά όργανα, τους οργανισμούς και τους συμβασιούχους της ΕΕ, ούτως ώστε οι διαβαθμισμένες πληροφορίες ΕΕ να μπορούν να διαβιβάζονται με τη βεβαιότητα ότι τυγχάνουν ανάλογης μέριμνας. Στις εν λόγω στοιχειώδεις προδιαγραφές περιλαμβάνονται κριτήρια για τον έλεγχο ασφαλείας του προσωπικού και ρυθμίσεις για την προστασία των διαβαθμισμένων πληροφοριών ΕΕ.

ΑΞΙΟΠΙΣΤΙΑ ΤΟΥ ΠΡΟΣΩΠΙΚΟΥ

Έλεγχος ασφαλείας (διαβάθμιση) του προσωπικού

9. Όλα τα πρόσωπα που απαιτείται να έχουν πρόσβαση σε πληροφορίες με διαβάθμιση 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 εξακρίβωνα κατά πόσον τα πρόσωπα αυτά:

α) είναι αναμφιβόλως έμπιστα,

β) διαθέτουν χαρακτήρα και σύνεση που να μην 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, πχ. λόγω παλαιότερης διαμονής ή προηγούμενων σχέσεων που θα μπορούσαν να συνιστούν απειλή για την ασφάλεια.

Ιδιαίτερα προσεκτικός έλεγχος γίνεται επί προσώπων τα οποία:

δ) πρόκειται να έχουν πρόσβαση σε πληροφορίες TRÈS SECRET UE/EU TOP SECRET,

ε) καταλαμβάνουν θέσεις που συνεπάγονται τακτική πρόσβαση σε σημαντικό όγκο πληροφοριών SECRET UE,

στ) έχουν καθήκοντα τέτοια που τους παρέχουν ειδική πρόσβαση σε συστήματα επικοινωνιών και επεξεργασίας πληροφοριών τα οποία είναι καίριας σημασίας για την επίτευξη συγκεκριμένης αποστολής 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.

10. 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, προσωπικά ασφαλώς, συντήρησης μηχανημάτων, καθαριότητας, κλπ.), πρέπει προηγουμένως να υφίστανται τον δέοντα έλεγχο ασφαλείας.

Αρχεία ελέγχων ασφαλείας του προσωπικού

11 Κάθε υπηρεσία, φορέας ή εγκατάσταση που χειρίζεται διαβαθμισμένες πληροφορίες ΕΕ, ή στεγάζει συστήματα επικοινωνιών ή επεξεργασίας πληροφοριών τα οποία είναι καίριας σημασίας για την επίτευξη συγκεκριμένης αποστολής, τηρεί αρχεία των ελέγχων ασφαλείας που έχουν πραγματοποιηθεί για το προσωπικό του/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. Τα αρχεία των ελέγχων ασφαλείας τηρούνται από τον προϊστάμενο ασφαλείας της υπηρεσίας, του φορέα ή της εγκατάστασης.

Εκπαίδευση του προσωπικού σε θέματα ασφαλείας

12. 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. Θεωρείται χρήσιμο να απαιτείται από όλους τους εν λόγω υπαλλήλους να πιστοποιούν γραπτώς ότι κατανοούν πλήρως τους κανονισμούς ασφαλείας που ισχύουν για την εργασία τους

Ευθύνες της διεύθυνσης

13. Τα διευθυντικά στελέχη πρέπει να γνωρίζουν ποιοι από το προσωπικό τους εργάζονται σε περιβάλλον διαβαθμισμένων πληροφοριών ή έχουν πρόσβαση σε συστήματα επικοινωνιών ή επεξεργασίας πληροφοριών καίριας σημασίας για την επίτευξη συγκεκριμένης αποστολής καθώς και να καταγράφουν και να αναφέρουν όλα τα περιστατικά ή τα εμφανή τρωτά σημεία που ενδέχεται να έχουν επιπτώσεις στην ασφάλεια.

Καθεστώς ασφαλείας που εφαρμόζεται στο προσωπικό

14. 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 συστήματα επικοινωνιών ή επεξεργασίας πληροφοριών καίριας σημασίας για την επίτευξη μιας αποστολής και ενημερώνεται η αρμόδια αρχή. Εάν διαπιστωθεί άτι 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.

ΥΛΙΚΗ ΑΣΦΑΛΕΙΑ

Ανάγκη προστασίας

15 Η αυστηρότητα των μέτρων υλικής ασφαλείας που εφαρμόζονται για την προστασία των διαβαθμισμένων πληροφοριών ΕΕ είναι ανάλογος με τη διαβάθμιση, τον όγκο των πληροφοριών και του υλικού και την υφισταμένη απειλή. Κατά συνέπεια, λαμβάνεται μέριμνα για την αποφυγή τόσο της υπερβολικά υψηλής όσο και της υπερβολικά χαμηλής διαβάθμισης οι δε διαβαθμίσεις υπόκεινται σε τακτική αναθεώρηση. 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.

Έλεγχος

16 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, κλπ). Διεξάγονται και περαιτέρω έλεγχοι μετά το πέρας των κανονικών ωρών εργασίας

Ασφάλεια των κτιρίων

17 Τα κτίρια όπου στεγάζονται διαβαθμισμένες πληροφορίες ΕΕ ή συστήματα επικοινωνιών και επεξεργασίας στοιχείων καίριας σημασίας για την επίτευξη μιας αποστολής 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 καν 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.

18. 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.

Σχέδια έκτακτης ανάγκης

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

ΑΣΦΑΛΕΙΑ ΤΩΝ ΠΛΗΡΟΦΟΡΙΩΝ (INFOSEC)

20. Η ασφάλεια των πληροφοριών αναφέρεται στον προσδιορισμό και στην εφαρμογή μέτρων ασφαλείας για την προστασία των πληροφοριών 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 διαθεσιμότητα τους Λαμβάνονται επαρκή μέτρα κατά της πρόσβασης μη εξουσιοδοτημένων χρηστών σε πληροφορίες ΕΕ, κατά της άρνησης πρόσβασης εξουσιοδοτημένων χρηστών σε πληροφορίες ΕΕ, και κατά της αλλοίωσης ή της άνευ αδείας τροποποίησης ή εξάλειψης πληροφοριών ΕΕ.

ΠΡΟΛΗΨΗ ΤΩΝ ΔΟΛΙΟΦΘΟΡΩΝ ΚΑΙ ΑΛΛΩΝ ΜΟΡΦΩΝ ΚΑΚΟΒΟΥΛΗΣ ΦΘΟΡΑΣ ΕΚ ΠΡΟΘΕΣΕΩΣ

21. 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 συγκεντρώνει στοιχεία για το ενδεχόμενο πράξεων κατασκοπείας δολιοφθοράς τρομοκρατίας και άλλων ανατρεπτικών δραστηριοτήτων.

ΚΟΙΝΟΠΟΙΗΣΗ ΔΙΑΒΑΘΜΙΣΜΕΝΩΝ ΠΛΗΡΟΦΟΡΙΩΝ ΣΕ ΤΡΙΤΑ ΚΡΑΤΗ΄Η ΔΙΕΘΝΕΙΣ ΟΡΓΑΝΙΣΜΟΥΣ

22. Η απόφαση για την κοινοποίηση διαβαθμισμένων πληροφοριών ΕΕ προελεύσεως Συμβουλίου σε τρίτο κράτος ή σε διεθνή οργανισμό λαμβάνεται από το Συμβούλιο. Εάν πηγή των πληροφοριών των οποίων ζητείται η κοινοποίηση δεν είναι το Συμβούλιο, τότε το Συμβούλιο ζητά πρώτα τη συγκατάθεση της εν λόγω πηγής Εάν δεν είναι δυνατόν να καθοριστεί συγκεκριμένη πηγή, τότε το Συμβούλιο αναλαμβάνει αυτό την ευθύνη κοινοποίησης.

23 Στην περίπτωση που το Συμβούλιο 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 στους προκείμενους κανονισμούς 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 ελέγχων από κοινού

24 Οι ανωτέρω αρχές εφαρμόζονται σύμφωνα με τις λεπτομερείς ρυθμίσεις που προβλέπονται στο μέρος 13.

ΜΕΡΟΣ ΙΙ

ΤΜΗΜΑ Ι

Η ΟΡΓΑΝΩΣΗ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΣΤΟ ΣΥΜΒΟΥΛΙΟ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ

Ο Γενικός Γραμματέας/Υπατος Εκπρόσωπος

1. Ο Γενικός Γραμματέας/Υπατος Εκπρόσωπος

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

β) εξετάζει τα προβλήματα ασφαλείας που του αναφέρονται από το Συμβούλιο ή τα αρμόδια κλιμάκιά του,

γ) μελετά τα θέματα που συνεπάγονται μεταβολές στην πολιτική ασφαλείας του Συμβουλίου, σε στενή συνεργασία με τις Εθνικές Αρχές Ασφαλείας («ΕΑΑ>>) ή άλλες αρμόδιες αρχές των κρατών μελών. Κατάλογος των εν λόγω αρχών περιλαμβάνει στο προσάρτημα Ι.

2. Ειδικότερα, ο Γενικός Γραμματέας/Υπάτος Εκπρόσωπος οφείλει:

α) να συντονίζει όλα τα θέματα ασφαλείας που αφορούν δραστηριότητες του Συμβουλίου,

β) να απαιτεί από κάθε κράτος μέλος τη δημιουργία μιας κεντρικής γραμματείας πληροφοριών TRE SECRET UE/EU TOP SECRET και να επιβάλλει τη δημιουργία τέτοιας γραμματείας στους αποκεντρωμένους οργανισμούς ΕΕ, όπου ενδείκνυται.

γ) να απευθύνει στις καθορισμένες για τον σκοπό αυτά αρχές των κρατών μελών αιτήματα παροχής εκ μέρους των ΕΑΑ εγκρίσεων ελέγχου ασφαλείας για το προσωπικό που εργάζεται στη ΓΤΣ σύμφωνα με το τμήμα VI,

δ) να διερευνά ή να διατάσσει τη διερεύνηση κάθε διαρροής διαβαθμισμένων πληροφοριών ΕΕ η οποία, κατά τα φαινόμενα, έχει προέλθει από τη ΓΤΣ ή από κάποιο αποκεντρωμένο οργανισμό ΕΕ,

ε) να ζητά από τις αρμόδιες αρχές ασφαλείας να διερευνούν τις διαρροές διαβαθμισμένων πληροφοριών ΕΕ που φαίνεται να έχουν προέλθει εκτός της ΓΤΣ ή των αποκεντρωμένων οργανισμών ΕΕ, και να συντονίζει τις έρευνες στην περίπτωση που συμμετέχουν σε αυτές περισσότερες της μίας αρχές ασφαλείας,

στ) να πραγματοποιεί κατά διαστήματα, από κοινού και σε συμφωνία με την ενεχόμενη ΕΑΑ, έλεγχο των ρυθμίσεων ασφαλείας στα κράτη μέλη για την προστασία των διαβαθμισμένων πληροφοριών ΕΕ,

ζ) να διατηρεί στενό σύνδεσμο με όλες τις ενεχόμενες αρχές ασφαλώς για γενικότερο συντονισμό της ασφαλείας

η) να επανεξετάζει τακτικά την πολιτική ασφαλείας του Συμβουλίου και τις σχετικές ρυθμίσεις και, εφόσον απαιτείται, να προβαίνει στις κατάλληλες συστάσεις. Στο πλαίσιο αυτό, υποβάλλει στο Συμβούλιο το ετήσιο πρόγραμμα επιθεωρήσεων που εκπονεί το Γραφείο Ασφαλείας της ΓΤΣ.

Η Επιτροπή Ασφαλείας του Συμβουλίου

3. Δημιουργείται Επιτροπή Ασφαλείας αποτελούμενη από αντιπροσώπους των ΕΑΑ όλων των κρατών μελών, υπό την προεδρία του Γενικού Γραμματέα/Υπατου Εκπροσώπου ή του εξουσιοδοτημένου εκπροσώπου του. Οι αντιπρόσωποι των αποκεντρωμένων οργανισμών ΕΕ επίσης μπορούν να καλούνται να συμμετάσχουν στις εργασίες όταν συζητούνται δέματα που τους αφορούν

4. Η Επιτροπή Ασφαλείας συνέρχεται σύμφωνα με τις οδηγίες του Συμβουλίου, κατόπιν αιτήματος του Γενικού Γραμματέα/Υπατου Εκπροσώπου ή κάποιας ΕΑΑ. Η Επιτροπή Ασφαλείας δύναται να εξετάζει και να αξιολογεί όλα τα θέματα ασφαλείας που αφορούν τις εργασίες του Συμβουλίου και να υποβάλλει τις κατάλληλες συστάσεις στο Συμβούλιο. Όσον αφορά τις δραστηριότητες της ΓΤΣ, η Επιτροπή Ασφαλείας δύναται να προβαίνει σε συστάσεις για θέματα ασφαλείας προς τον Γενικό Γραμματέα/Υπατο Εκπρόσωπο.

Το Γραφείο Ασφαλείας της Γενικής Γραμματείας του Συμβουλίου

5. Για την εκπλήρωση των καθηκόντων του κατά τις παραγράφους 1 και 2, ο Γενικός Γραμματέας/Υπατος Εκπρόσωπος έχει στη διάθεσή του το Γραφείο Ασφαλείας της ΓΤΣ για τον συντονισμό, την εποπτεία και την εφαρμογή των μέτρων ασφαλείας

6. Ο Προϊστάμενος του Γραφείου Ασφαλείας της ΓΤΣ είναι ο κύριος σύμβουλος του Γενικού Γραμματέα/Ύπατου Εκπροσώπου σε θέματα ασφαλείας και ενεργεί ως γραμματέας της Επιτροπής 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 το Συμβούλιο με συμφωνίες σε θέματα ασφαλείας. Για τον σκοπό αυτά, ενεργεί ως αξιωματικός-σύνδεσμος

7. Ο Προϊστάμενος του Γραφείου Ασφαλείας της ΓΤΣ είναι υπεύθυνος για την έγκριση των συστημάτων και δικτύων τεχνολογίας των πληροφοριών στη ΓΤΣ Ο Προϊστάμενος του Γραφείου Ασφαλείας της ΓΤΣ και η αρμόδια ΕΑΑ αποφασίζουν από κοινού, όπου απαιτείται, για την έγκριση των συστημάτων και δικτύων τεχνολογίας των πληροφοριών στα οποία συμμετέχουν η ΓΤΣ, τα κράτη μέλη, οι αποκεντρωμένοι οργανισμοί ΕΕ και/ή τρίτα μέρη (κράτη ή διεθνείς οργανισμοί).

Αποκεντρωμένοι οργανισμοί ΕΕ

8. Κάθε διευθυντής αποκεντρωμένου οργανισμού ΕΕ είναι υπεύθυνος για την εφαρμογή των κανονισμών ασφαλείας στην υπηρεσία του, διορίζει δε κανονικά ένα μέλος του προσωπικού του ως υπόλογο έναντι του για θέματα ασφαλείας Το εν λόγω μέλος του προσωπικού ορίζεται ως υπεύθυνος ασφαλείας

Κράτη μέλη

9. Κάθε κράτος μέλος ορίζει μια ΕΑΑ ως υπεύθυνη για την ασφάλεια των διαβαθμισμένων πληροφοριών ΕΕ ([1]).

10. Εντός κάθε διοίκησης κράτους μέλους η αντίστοιχη ΕΑΑ είναι, υπεύθυνη:

α) να τηρεί την ασφάλεια των διαβαθμισμένων πληροφοριών ΕΕ εις χείρας των Εθνικών φορέων, οργανισμών ή υπηρεσιών, δημόσιων ή ιδιωτικών, εντός της χώρας ή στο εξωτερικό,

β) να παρέχει έγκριση για τη δημιουργία γραμματειών πληροφοριών TRÈS SECRET UE/EU TOP SECRET (η εξουσία αυτή μπορεί να μεταβιβαστεί στον υπεύθυνο ελέγχου των πληροφοριών TRÈS SECRET UE/EU TOP SECRET μιας κεντρικής γραμματείας),

γ) να ελέγχει κατά διαστήματα τις ρυθμίσεις ασφαλείας για την προστασία των διαβαθμισμένων πληροφοριών ΕΕ,

δ) να εξασφαλίζει ότι όλοι οι υπήκοοι μιας χώρος καθώς και οι αλλοδαποί που εργάζονται σε εθνικούς φορείς οργανισμούς και υπηρεσίες οι οποίοι μπορούν να έχουν πρόσβαση σε πληροφορίες ΕΕ που έχουν διαβαθμιστεί ως TRÈS SECRET UE/EU TOP SECRET, SECRET UE και CONFIDENTIEL UE, έχουν υποστεί έλεγχο ασφαλείας

ε) να λαμβάνει τα αναγκαία μέτρα ασφαλείας ώστε να προλαμβάνεται η διαρροή διαβαθμισμένων πληροφοριών σε μη εξουσιοδοτημένα πρόσωπα.

Αμοιβαίες επιθεωρήσεις ασφαλείας

11. Το Γραφείο Ασφαλείας της ΓΤΣ και η αντίστοιχη ΕΑΑ, από κοινού και κατόπιν συμφωνίας ([2]), διενεργούν περιοδικές επιθεωρήσεις των ρυθμίσεων ασφαλείας για την προστασία των διαβαθμισμένων πληροφοριών ΕΕ στη ΓΤΣ και στις Μόνιμες Αντιπροσωπείες των κρατών μελών στην Ευρωπαϊκή Ένωση, καθώς και στους χώρους των κρατών μελών στα κτίρια του Συμβουλίου

12. Το Γραφείο Ασφαλείας της ΓΤΣ ή, κατόπιν αιτήματος του Γενικού Γραμματέα, η ΕΑΑ του κράτους μέλους υποδοχής, διενεργούν περιοδικές επιθεωρήσεις των ρυθμίσεων ασφαλείας για την προστασία των διαβαθμισμένων πληροφοριών ΕΕ στους αποκεντρωμένους οργανισμούς ΕΕ.

([1]) Για τον κατάλογο των Εθνικών Αρχών Ασφαλείας που είναι υπεύθυνες για την ασφάλεια των διαβαθμισμένων πληροφοριών ΕΕ, βλέπε προσάρτημα 1.
([2]) Με την επιφύλαξη της σύμβασης της Βιέννης του 1961 για τις διπλωματικές σχέσεις.

ΤΜΗΜΑ ΙΙΙ

ΔΙΑΧΕΙΡΙΣΗ ΤΩΝ ΔΙΑΒΑΘΜΙΣΕΩΝ

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

2. Αποκλειστικός υπεύθυνος για τη διαβάθμιση των πληροφοριών και για τον τυχόν μεταγενέστερο υποχαρακτηρισμό ή αποχαρακτηρισμό τους ([1]) είναι ο συντάκτης του εγγράφου.

   Οι υπάλληλοι και το λοιπό προσωπικό της ΓΤΣ διαβαθμίζουν, υποχαρακτηρίζουν ή αποχαρακτηρίζουν πληροφορίες κατόπιν εντολής του Γενικού Διευθυντή τους ή σε συμφωνία μαζί του.

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

4. Ο αριθμός των προσώπων που επιτρέπεται να συντάσσουν έγγραφα TRÈS SECRET UE/EU TOP SECRET περιορίζεται στο απολύτως αναγκαίο, τα δε ονόματά τους συμπεριλαμβάνονται σε κατάλογο που καταρτίζεται από τη ΓΤΣ, κάθε κράτος μέλος και, ενδεχομένως, από κάθε αποκεντρωμένο οργανισμό EL

ΕΦΑΡΜΟΓΗ ΤΩΝ ΔΙΑΒΑΘΜΙΣΕΩΝ

5. Η διαβάθμιση ενός εγγράφου καθορίζεται από το επίπεδο ευαισθησίας του περιεχομένου του κατά τα οριζόμενα στο τμήμα ΙΙ, παράγραφοι 1 έως 4. Είναι σημαντικό η διαβάθμιση να χρησιμοποιείται σωστά και με φειδώ. Αυτό ισχύει ιδίως για τη διαβάθμιση TRÈS SECRET UE/EU TOP SECRET.

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

   Αν και μια υψηλή διαβάθμιση μπορεί εκ πρώτης όψεως να φαίνεται ότι εγγυάται την αυξημένη προστασία ενός εγγράφου, η εκ συστήματος υπερβολικά υψηλή διαβάθμιση ενδέχεται να επιφέρει απώλεια της εμπιστοσύνης στην αξία του συστήματος διαβάθμισης.

   Από την άλλη πλευρά, τα έγγραφα δεν πρέπει να λαμβάνουν υπερβολικά χαμηλή διαβάθμιση με στόχο να αποφεύγονται οι περιορισμοί που συνδέονται με την προστασία τον έγγραφων υψηλής διαβάθμισης.

   Ένας πρακτικός οδηγός για τις διαβαθμίσεις περιλαμβάνεται στο προσάρτημα 3.

7. Επί μέρους σελίδες, παράγραφοι, τμήματα, παραρτήματα και προσαρτήματα ενός εγγράφου καθώς και τα επισυναπτόμενα σε αυτό έγγραφα ενδέχεται να απαιτούν διαφορετικές διαβαθμίσεις, οι οποίες επισημαίνονται αναλόγως. Η διαβάθμιση του όλου εγγράφου αντίστοιχα σε εκείνη του τμήματος του με την υψηλότερη διαβάθμιση.

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

ΥΠΟΧΑΡΑΚΤΗΡΙΣΜΟΣ ΚΑΙ ΑΠΟΧΑΡΑΚΤΗΡΙΣΜΟΣ

9. 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. Το θεσμικά όργανο, το κράτος μέλος, το γραφείο, ο διάδοχος οργανισμός ή η υψηλότερη αρχή προέλευσης του εγγράφου 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.

10. Ει δυνατόν, οι συντάκτες αναγράφουν επί των διαβαθμισμένων εγγράφων την ημερομηνία ή την προθεσμία μετά την 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.

([1]) Ως υποχαρακτηρισμός (déclassement) νοείται η μείωση του βαθμού ασφαλείας . Ως αποχαρακτηρισμός (déclassification) νοείται η άρση οποιασδήποτε διαβάθμισης.

ΤΜΗΜΑ IV

ΥΛΙΚΗ ΑΣΦΑΛΕΙΑ

ΓΕΝΙΚΑ

1. Ο κύριος στόχος των μέτρων υλικής ασφάλειας είναι να εμποδίζεται η πρόσβαση μη εξουσιοδοτημένων προσώπων σε διαβαθμισμένες πληροφορίες ή/και υλικό ΕΕ.

ΑΠΑΙΤΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ

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

3. 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,

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

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

4. Τα εφαρμοζόμενα μέτρα υλικής ασφάλειας αποσκοπούν:

α) στην εμπόδιση της λαθραίας ή βιαίας εισόδου αναρμόδιων,

β) στην αποτροπή, παρεμπόδιση και ανίχνευση ενεργειών τυχόν αναξιόπιστου προσωπικού (κατάσκοποι «εντός των τειχών»),

γ) στο να εμποδίζεται η πρόσβαση στις διαβαθμισμένες πληροφορίες της ΕΕ στους υπαλλήλους και το λοιπό προσωπικό της ΓΤΣ, των κρατικών υπηρεσιών των κρατών μελών ή/και των άλλων θεσμικών οργάνων ή τρίτων μερών που δεν χρειάζεται να λαμβάνουν γνώση των πληροφοριών αυτών.

ΜΕΤΡΑ ΥΛΙΚΗΣ ΑΣΦΑΛΕΙΑΣ

Χώροι ασφαλείας

5 Οι χώροι στους οποίους γίνεται χειρισμός και αποθήκευση πληροφοριών με βαθμό διαβάθμισης 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 CONFIDENTIEL UE ή υψηλότερη κατά τρόπο ώστε η είσοδος στο συγκεκριμένο χώρο να αποτελεί, ουσιαστικά, πρόσβαση σε διαβαθμισμένες πληροφορίες Για έναν τέτοιο χώρο απαιτούνται.

i) μια συγκεκριμένη 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 οδική 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 ασφαλώς κατηγορίας ΙΙ χώρος στον οποίο γίνεται χειρισμός και η αποθήκευση πληροφοριών με διαβάθμιση 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 περιλαμβάνονται γραφεία στα οποία γίνεται τακτικά χειρισμός και αποθήκευση πληροφοριών με διαβάθμιση CONFIDENTIEL UE ή υψηλότερη Για έναν τέτοιο χώρο απαιτούντα:

i) μια συγκεκριμένη 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

Διοικητικός χώρος

6. Γύρω από τους χώρους ασφαλείας κατηγορίας Ι ή κατηγορίας ΙΙ καθώς και στις προσβάσεις τους, είναι δυνατόν να υπάρξει 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 διοικητικούς χώρους γίνεται χειρισμός και αποθήκευση μόνο πληροφοριών RESTREINT UE

Έλεγχοι εισόδου και εξόδου

7. Η είσοδος στους χώρους ασφαλείας κατηγορίας Ι και κατηγορίας ΙΙ ελέγχεται με σύστημα ειδικής ταυτότητας ή προσωπικής αναγνώρισης που ισχύει για το μόνιμο προσωπικό. Θα εγκαθιδρυθεί 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 αξιολόγησης κινδύνου μπορεί να συνεπάγεται την ενίσχυση των μέτρων ελέγχου εισόδου/ εξόδου, για παράδειγμα κατά τη διάρκεια της επίσκεψης σημαντικών προσωπικοτήτων

Περιπολίες των φυλάκων

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

Φωριαμοί ασφαλείας και θωρακισμένες αίθουσες

9. Για την αποθήκευση των διαβαθμισμένων πληροφοριών ΕΕ χρησιμοποιούνται φωριαμοί τριών κατηγοριών.

— Κατηγορία Α: φωριαμοί που έχουν εγκριθεί σε εθνικά επίπεδο για την αποθήκευση πληροφοριών TRÈS SE GIET 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 SECRET UE και CONFIDENTIEL UE σε χώρους ασφαλείας κατηγορίας Ι ή κατηγορίας ΙΙ,

— Κατηγορία Γ: έπιπλα γραφείου κατάλληλα μόνο για την αποθήκευση πληροφοριών RESTREINT UE

10. Για τις θωρακισμένες αίθουσες που κατασκευάζονται εντός χώρου ασφαλείας κατηγορίας Ι ή κατηγορίας ΙΙ, και για όλες τους χώρους ασφαλείας κατηγορίας Ι όπου διαβαθμισμένες πληροφορίες με χαρακτηρισμό CONFIDENTIEL UE αποθηκεύονται σε ανοικτά ράφια ή επιδεικνύονται σε σχεδιαγράμματα, χάρτες κλπ., οι τοίχοι, τα πατώματα και οι οροφές καθώς και οι θύρες που κλειδώνουν πιστοποιούνται από Εθνική Αρχή Ασφαλείας ότι προσφέρουν ισοδύναμη προστασία με την κατηγορία του φωριαμού ασφαλείας που έχει εγκριθεί για την αποθήκευση πληροφοριών ίδιας διαβάθμισης

Κλειδαριές

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

— Ομάδα Α εγκεκριμένες σε εθνικά επίπεδο για φωριαμούς κατηγορίας Α,

— Ομάδα Β. εγκεκριμένες σε εθνικά επίπεδο για φωριαμούς κατηγορίας Β,

— Ομάδα Γ. κατάλληλες μόνο για έπιπλα γραφείου κατηγορίας Γ.

Έλεγχος των κλειδιών και των συνδυασμών

12 Τα κλειδιά των φωριαμών ασφαλείας δεν πρέπει να βγαίνουν από το κτίριο των γραφείων Οι συνδυασμοί των φωριαμών ασφαλείας απομνημονεύονται από τα πρόσωπα που πρέπει να τους γνωρίζουν. Για χρήση σε επείγουσα ανάγκη, ο Υπεύθυνος Ασφαλείας του οικείου καταστήματος είναι υπεύθυνος να κατέχει αντικλείδια καθώς και, γραπτώς όλους τους συνδυασμούς 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 ισχύει προστασία ασφαλείας τουλάχιστον ισοδύναμη προς το υλικό στο οποίο παρέχουν πρόσβαση

13. 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 πάντως τουλάχιστον ανά δωδεκάμηνο.

Συσκευές ανίχνευσης εισόδου αναρμόδιων

14. 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 σήμαινα συναγερμός ή να ειδοποιείται με άλλον αξιόπιστο τρόπο το προσωπικό επιτήρησης όποτε σημειώνεται βλάβη των εν λόγω συστημάτων ή επιχειρείται παρέμβαση σ' αυτά.

Εγκεκριμένος εξοπλισμός

15. Οι ΕΑΑ διατηρούν, με δικούς τους ή με διμερείς πόρους ενημερωμένους καταλόγους ανά τύπο και μοντέλο του εξοπλισμού ασφαλείας που έχουν εγκρίνει για την άμεση ή την έμμεση προστασία των διαβαθμισμένων πληροφοριών υπό διάφορες συγκεκριμένες περιστάσεις και συνθήκες. Το Γραφείο Ασφαλείας της ΓΤΣ τηρεί παρόμοιο κατάλογο, με βάση, μεταξύ άλλων, πληροφορίες που παρέχονται από τις ΕΑΑ. Προτού αγοράσουν τον σχετικό εξοπλισμό, οι αποκεντρωμένοι οργανισμοί της ΕΕ συμβουλεύονται το Γραφείο Ασφαλείας της ΓΤΣ και, ενδεχομένως την ΕΑΑ του κράτος μέλους που τις φιλοξενεί

Υλική προστασία των φωτοαντιγραφικών συσκευών και συσκευών (φαξ)

16. Οι φωτοαντιγραφικές συσκευές Kat οι συσκευές φαξ προστατεύονται υλικώς όσο απαιτείται ώστε να διασφαλίζεται ότι χρησιμοποιούνται μόνο από εγκεκριμένα πρόσωπα και ότι όλο το διαβαθμισμένο υλικό ελέγχεται δεόντως

ΠΡΟΣΤΑΣΙΑ ΚΑΤΑ ΤΗΣ ΛΑΘΡΟΒΛΕΨΙΑΣ ΚΑΙ ΤΗΣ ΛΑΘΡΑΚΡΟΑΣΗΣ

Λαθροβλεψία

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

Λαθρακρόαση

18. Τα γραφεία ή οι χώροι όπου συζητούνται ταχτικά πληροφορίες με διαβάθμιση SECRET UE ή υψηλότερη προστατεύονται από κρούσματα παθητικής ή ενεργητικής λαθρακρόασης εφόσον υφίσταται σχετικός κίνδυνος Υπεύθυνη για την αξιολόγηση αυτού του κινδύνου είναι η αρμόδια αρχή ασφαλείας έπειτα από διαβούλευση, εφόσον χρειάζεται, με τις ΕΑΑ.

19. Για την καθορισμό των ληπτέων 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), το Γραφείο Ασφαλείας της ΓΤΣ μπορεί να ζητά τη συνδρομή εμπειρογνωμόνων των ΕΑΑ. Οι υπάλληλοι ασφαλείας των αποκεντρωμένων οργανισμών της ΕΕ μπορούν να ζητούν τη διενέργεια τεχνικών επιθεωρήσεων από το Γραφείο Ασφαλείας της ΓΤΣ ή/και τη συνδρομή εμπειρογνωμόνων των ΕΑΑ

20. Ομοίως, όταν το απαιτούν οι περιστάσεις, ο κάθε είδους τηλεπικοινωνιακός εξοπλισμός και ηλεκτρικός ή ηλεκτρονικός εξοπλισμός γραφείου που χρησιμοποιείται κατά τις συνεδριάσεις σε επίπεδο SECRET UE ή υψηλότερο μπορεί να ελέγχεται από ειδικούς τεχνικούς ασφαλείας των ΕΑΑ έπειτα από αίτηση του αρμόδιου υπαλλήλου ασφαλείας

ΤΕΧΝΙΚΟΣ ΑΣΦΑΛΕΙΣ ΧΩΡΟΙ

21. Ορισμένοι χώροι μπορούν να χαρακτηρισθούν ως τεχνικώς ασφαλώς 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.

22. 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 γενικό κανόνα, θα πρέπει να αποφεύγεται η εγκατάσταση τηλεπικοινωνιακών γραμμών σε τεχνικώς ασφαλείς χώρους

ΤΜΗΜΑ V

ΓΕΝΙΚΟΙ ΚΑΝΟΝΕΣ ΓΙΑ ΤΗΝ ΑΡΧΗ ΤΗΣ «ΑΝΑΓΚΑΙΑΣ ΓΝΩΣΗΣ» ΚΑΙ ΓΙΑ ΤΟΝ ΕΛΕΓΧΟ ΑΣΦΑΛΕΙΑΣ

1. Η πρόσβαση στις διαβαθμισμένες πληροφορίες ΕΕ επιτρέπεται μόνο στα πρόσωπα που όντως χρειάζεται να τις γνωρίζουν για να εκτελούν τα καθήκοντα ή την αποστολή τους Η πρόσβαση στις πληροφορίες TRÈS SECRET UE/EU TOP SECRET, SECRET UE και CONFIDENTIEL UE επιτρέπεται μόνο στα πρόσωπα που έχουν υποστεί με επιτυχία τον ενδεδειγμένο έλεγχο ασφαλείας

2. Αρμόδιοι για τον καθορισμό των προσώπων που πρέπει να έχουν την «αναγκαία γνώση» είναι η ΓΤΣ, οι αποκεντρωμένοι οργανισμοί της ΕΕ και οι υπηρεσίες ή τα τμήματα των κρατών μελών όπου πρόκειται να εργασθεί το οικείο πρόσωπο, ανάλογα με τις απαιτήσει; της σχετικής αποστολής

3. Αρμόδιος για τον έλεγχο ασφαλείας του προσωπικού είναι ο εργοδότης του υπαλλήλου, βάσει των σχετικών ισχυουσών διαδικασιών Σε ότι αφορά τους υπαλλήλους και το λοιπό προσωπικά της ΓΤΣ, η διαδικασία του ελέγχου ασφαλείας προβλέπεται στο τμήμα VI

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

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

4. Πρόσωπα άλλα πλην των υπαλλήλων ή του λοιπού προσωπικού της ΓΤΣ ή των κρατών μελών, π.χ. μέλη, υπάλληλοι ή προσωπικό των θεσμικών οργάνων της ΕΕ, με τα οποία χρειάζεται ενδεχομένως να συζητηθούν ή στα οποία χρειάζεται ενδεχομένως να επιδειχθούν διαβαθμισμένες πληροφορίες ΕΕ, πρέπει να έχουν υποστεί επιτυχώς έλεγχο ασφαλείας όσον αφορά τις διαβαθμισμένες πληροφορίες ΕΕ και να ενημερώνονται για την ευθύνη τους όσον αφορά την ασφάλεια. Ο ίδιος κανόνας ισχύει, σε παρόμοιες περίσταση, για τους εξωτερικούς συμβασιούχους εμπειρογνώμονες ή συμβούλους

ΕΙΔΙΚΟΙ ΚΑΝΟΝΕΣ ΓΙΑ ΤΗΝ ΠΡΟΣΒΑΣΗ ΣΕ ΠΛΗΡΟΦΟΡΙΕΣ TRÊS SECRET UE/EU TOP SECRET

5. Όλα τα πρόσωπα που πρόκειται να έχουν πρόσβαση σε πληροφορίες TRÈS SECRET UE/EU TOP SECRET υποβάλλονται προηγουμένως στον αντίστοιχο έλεγχο ασφαλείας

6. Όλα τα πρόσωπα που πρέπει να έχουν πρόσβαση σε πληροφορίες TRÈS SECRET UE/EU TOP SECRET ορίζονται από τον προϊστάμενο του τμήματος τους και τα ονόματα τους καταχωρούνται στην οικεία γραμματεία TRÈS SECRET UE/EU TOP SECRET.

7. Προτού αποκτήσουν πρόσβαση σε πληροφορίες TRÈS SECRET UE/EU TOP SECRET, όλα τα πρόσωπα υπογράφουν βεβαίωση ότι έχουν ενημερωθεί για τις διαδικασίες ασφαλείας του Συμβουλίου και ότι κατανοούν πλήρως την ειδική τους ευθύνη για τη διασφάλιση των πληροφοριών TRÈS 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 ΕΕ περιέρχονται σε μη εξουσιοδοτημένα πρόσωπα, είτε εκ προθέσεως είτε εξ αμελείας

8. Στην περίπτωση προσώπων τα οποία έχουν πρόσβαση σε πληροφορίες TRÈS SECRET UE/EU TOP SECRET σε συνεδριάσεις κλπ, ο αρμόδιος υπάλληλος ελέγχου της υπηρεσίας ή του οργάνου στο οποίο απασχολείται το εν λόγω πρόσωπο γνωστοποιεί στο όργανο το οποίο διοργανώνει τη συνεδρίαση ότι τα οικεία πρόσωπα διαθέτουν τη σχετική άδεια.

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

ΕΙΔΙΚΟΙ ΚΑΝΟΝΕΣ ΓΙΑ ΤΗΝ ΠΡΟΣΒΑΣΗ ΣΕ ΠΛΗΡΟΦΟΡΙΕΣ SECRET UE ΚΑΙ CONFIDENTIEL UE

10. Όλα τα πρόσωπα που πρόκειται να έχουν πρόσβαση σε πληροφορίες SECRET UE και CONFIDENTIEL UE υφίστανται προηγουμένως τον έλεγχο ασφαλείας στον, ενδεδειγμένο βαθμό.

11. Όλα τα πρόσωπα που πρόκειται να έχουν πρόσβαση σε πληροφορίες SECRET UE και CONFIDENTIEL UE ενημερώνονται για τους κανονισμούς ασφαλώς καθώς και για τις συνέπειες τυχόν αμέλειας.

12 Στην περίπτωση προσώπων που έχουν πρόσβαση σε πληροφορίες SECRET UE και CONFIDENTIEL UE κατά τη διάρκεια συνεδριάσεων κλπ., ο Υπεύθυνος Ασφαλώς του οργάνου όπου εργάζεται το εν λόγω πρόσωπο γνωστοποιεί στο όργανο που οργανώνει τη συνεδρίαση άτι τα σχετικά πρόσωπα διαθέτουν τη σχετική άδεια.

ΕΙΔΙΚΟΙ ΚΑΝΟΝΕΣ ΠΑ ΤΗΝ ΠΡΟΣΒΑΣΗ ΣΕ ΠΛΗΡΟΦΟΡΙΕΣ RESTREINT UE

13. Οι έχοντες πρόσβαση σε πληροφορίες RESTREINT UE ενημερώνονται για τους προκείμενους κανονισμούς ασφαλείας καθώς και για τις συνέπειες τυχόν αμέλειας.

ΜΕΤΑΘΕΣΕΙΣ

14. 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 στον νέο υπάλληλο.

ΕΙΔΙΚΕΣ ΕΝΤΟΛΕΣ

15. Τα πρόσωπα τα οποία απαιτείται να χειρίζονται διαβαθμισμένες πληροφορίες ΕΕ θα πρέπει, για πρώτη φόρα 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 λαμβάνουν κατά τις σχέσεις τους με τον τύπο,

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.

16. 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 ότι αφορά διαβαθμισμένες πληροφορίες και δραστηριότητες ΕΕ, ενημερώνονται για τις τεχνικές που είναι γνωστά ότι χρησιμοποιούνται από τις διάφορες υπηρεσίες πληροφοριών.

17. Δεν υπάρχουν κανονισμοί ασφαλείας του Συμβουλίου σχετικά με τα ιδιωτικά ταξίδια του προσωπικού που έχει άδεια πρόσβασης σε διαβαθμισμένες πληροφορίες ΕΕ, ασχέτως προορισμού. Ωστόσο, οι αρμόδιες αρχές ασφαλείας γνωστοποιούν στους υπαλλήλους και το λοιπό προσωπικά που υπάγονται στην αρμοδιότητα τους σχετικά με τους ταξιδιωτικούς κανονισμούς οι οποίοι ενδέχεται να ισχύουν γι' αυτούς. Οι υπεύθυνοι ασφαλείας μεριμνούν για επιμορφωτικές συναντήσεις για τα μέλη του προσωπικού όσον αφορά τις εν λόγω ειδικές οδηγίες.

ΤΜΗΜΑ VI

ΔΙΑΔΙΚΑΣΙΑ ΕΛΕΓΧΟΥ ΑΣΦΑΛΕΙΑΣ ΤΩΝ ΥΠΑΛΛΗΛΩΝ ΚΑΙ ΤΟΥ ΛΟΙΠΟΥ ΠΡΟΣΩΠΙΚΟΥ ΤΗΣ ΓΤΣ

1. Μόνο οι υπάλληλοι και το λοιπό προσωπικό της ΓΤΣ ή πρόσωπα τα οποία εργάζονται στα πλαίσια της ΓΤΣ και τα οποία, λόγω των καθηκόντων τους και για τις ανάγκες της υπηρεσίας χρειάζεται να γνωρίζουν ή να χρησιμοποιούν διαβαθμισμένες πληροφορίες που έχει στην κατοχή του το Συμβούλιο, έχουν πρόσβαση στις πληροφορίες αυτές.

2. Για την πρόσβαση στις πληροφορίες TRÊS SECRET UE/EU TOP SECRET, SECRET UE και CONFIDENTIEL UE, τα πρόσωπα που μνημονεύονται στην παράγραφο 1 πρέπει να έχουν λάβει σχετική άδεια, σύμφωνα με τη διαδικασία των παραγράφων 4 και 5.

3. 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 6 έως 10.

4. Η αρμόδια για τους διορισμούς αρχή, κατά την έννοια του άρθρου 2, πρώτο εδάφιο του Κανονισμού Υπηρεσιακής Κατάστασης είναι αρμόδια για τη χορήγηση των αδειών που μνημονεύονται στα σημεία 1, 2 και 3.

   Η αρμόδια για τους διορισμούς αρχή χορηγεί την άδεια αφού λάβει τη γνώμη των αρμόδιων εθνικών αρχών των κρατών μελών βάσει του ελέγχου ασφαλείας που διενεργείται σύμφωνα με τα σημεία 6 έως 12. -

5. Η άδεια, η οποία έχει πενταετή ισχύ, δεν μπορεί να υπερβεί τη διάρκεια των καθηκόντων βάσει των οποίων χορηγείται. Μπορεί να ανανεωθεί από την αρμόδια για τους διορισμούς αρχή με τη διαδικασία της παραγράφου 4.

   Η αρμόδια για τους διορισμούς αρχή ανακαλεί την άδεια όταν κρίνει ότι συντρέχει λόγος προς τούτο Τυχόν ανακλητική απόφαση κοινοποιείται στο ενδιαφερόμενο πρόσωπο, το οποίο μπορεί να ζητήσει ακρόαση από την αρμόδια για τους διορισμούς καθώς και στην αρμόδια εθνική αρχή.

6. Στόχος του ελέγχου ασφαλείας είναι να εξακριβωθεί ότι δεν υπάρχουν αντιρρήσεις στο να επιτραπεί στο συγκεκριμένο πρόσωπο να έχει πρόσβαση σε διαβαθμισμένες πληροφορίες που έχει στην κατοχή του το Συμβούλιο.

7. Ο έλεγχος ασφαλείας διενεργείται, με τη συνδρομή του ενδιαφερομένου προσώπου και έπειτα από αίτηση της αρμόδιας για τους διορισμούς αρχής από τις αρμόδιες εθνικές αρχές του κράτους μέλους του οποίου είναι υπήκοος το πρόσωπο που χρειάζεται την άδεια. Εάν ο ενδιαφερόμενος διαμένει στο έδαφος άλλου κράτους μέλους, οι ενδιαφερόμενες εθνικές αρχές μπορούν να διασφαλίζουν τη συνεργασία των αρχών του κρότους διαμονής

8. Ως μέρος της διαδικασίας ελέγχου, μπορεί να ζητηθεί από τον ενδιαφερόμενο να συμπληρώσει έντυπο με προσωπικές πληροφορίες.

9. Η αρμόδια για τους διορισμούς αρχή προσδιορίζει στην αίτησή της 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.

10. Το σύνολο της διαδικασίας ελέγχου ασφαλείας μαζί με το πόρισμά της υπόκειται στους κανόνες και τις ρυθμίσεις που ισχύουν εν προκειμένω στο οικείο κράτος μέλος περιλαμβανομένων των κανόνων και ρυθμίσεων που αφορούν τις ενστάσεις και προσφυγές

11. Όταν οι αρμόδιες εθνικές αρχές του κράτους μέλους δίνουν θετική γνώμη, η αρμόδια για τους διορισμούς αρχή μπορεί να χορηγεί την άδεια στο ενδιαφερόμενο πρόσωπο.

12. Η αρνητική γνώμη των αρμόδιων εθνικών αρχών γνωστοποιείται στον ενδιαφερόμενο, ο οποίος μπορεί να ζητήσει ακρόαση από την αρμόδια για τους διορισμούς αρχή Εφόσον τα κρίνα αναγκαίο, η τελευταία μπορεί να ζητήσει από τις αρμόδιες εθνικές αρχές οιαδήποτε περαιτέρω διευκρίνιση μπορούν να παράσχουν Εάν επιβεβαιωθεί η αρνητική γνώμη, η άδεια δεν χορηγείται.

13. Όλα τα πρόσωπα που έχουν άδεια κατά την έννοια των παραγράφων 4 και 5 λαμβάνουν, κατά τη χορήγηση της άδειας και στη συνέχεια σε τακτικά διαστήματα, τις τυχόν αναγκαίες οδηγίες σχετικά με την προστασία διαβαθμισμένων πληροφοριών και με τα μέσο για τη διασφάλιση της προστασίας αυτής. Τα πρόσωπα αυτά υπογράφουν δήλωση με την οποία βεβαιώνουν ότι έλαβαν τις οδηγίες και αναλαμβάνουν *να* τις τηρούν.

14. Η αρμοδία για τους διορισμούς αρχή λαμβάνει *τα* τυχόν αναγκαία μέτρα *για* την εφαρμογή του παρόντος τμήματος, ιδίως όσον αφορά τους κανόνες που διέπουν την πρόσβαση στον κατάλογο των προσώπων στα οποία έχει χορηγηθεί η σχετική άδεια.

15. Κατ' εξαίρεση, εφόσον απαιτείται από την υπηρεσία, η αρμόδια για τους διορισμούς αρχή 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 στο σημείο 7.

16. Οι ούτως χορηγούμενες προσωρινές και υπό αίρεση άδειες δεν επιτρέπουν την πρόσβαση σε πληροφορίες TRÈS SECRET UE/EU TOP SECRET. Η πρόσβαση στις πληροφορίες αυτές περιορίζεται στους υπαλλήλους που έχουν όντως υποστεί έλεγχο επιτυχώς, σύμφωνα με την παράγραφο 7. Εν αναμονή του πορίσματος του ελέγχου, οι υπάλληλοι για τους οποίους έχει ζητηθεί πρόσβαση TRÈS SECRET UE/EU TOP SECRET μπορούν να λαμβάνουν προσωρινή και υπό αίρεση άδεια πρόσβασης σε πληροφορίες έως και SECRET UE.

ΤΜΗΜΑ VII

ΚΑΤΑΡΤΙΣΜΟΣ, ΔΙΑΝΟΜΗ, ΔΙΑΒΙΒΑΣΗ, ΑΠΟΘΗΚΕΥΣΗ ΚΑΙ ΚΑΤΑΣΤΡΟΦΗ ΔΙΑΒΑΘΜΙΣΜΕΝΩΝ ΥΛΙΚΩΝ ΕΕ

Περιεχόμενα

Γενικές διατάξεις

Το παρόν τμήμα πραγματεύεται τα μέτρα για τον καταρτισμό, τη διανομή, τη διαβίβαση, την αποθήκευση και την καταστροφή των διαβαθμισμένων εγγράφων ΕΕ όπως ορίζονται στην παράγραφο 3 σημείο α) των Βασικών Αρχών και Στοιχειωδών Κανόνων Ασφαλείας του μέρους 1 του παρόντος παραρτήματος, πρέπει δε να χρησιμοποιείται ως αναφορά για την προσαρμογή των μέτρων αυτών για άλλα διαβαθμισμένα υλικά ΕΕ, ανάλογα με το είδος τους και κατά περίπτωση

Κεφάλαιο I

Καταρτισμός και διανομή διαβαθμισμένων *εγγράφων* ΕΕ

ΚΑΤΑΡΤΙΣΜΟΣ

1. Η διαβάθμιση και οι επισημάνσεις ΕΕ εφαρμόζονται όπως ορίζεται στο τμήμα ΙΙ, εμφαίνονται δε στο κέντρο του άνω και του κάτω μέρους κάθε σελίδας· κάθε σελίδα αριθμείται Κάθε διαβαθμισμένο έγγραφο ΕΕ φέρει αριθμό αναφοράς και ημερομηνία Στα έγγραφα TRÈS SECRET UE/EU TOP SECRET και SECRET UE, ο αριθμός αυτός εμφαίνεται σε κάθε σελίδα Εάν τα έγγραφα πρόκειται να διανεμηθούν σε πολλαπλά αντίτυπα, στην πρώτη σελίδα κάθε αντιτύπου αναγράφεται ο αριθμός αντιτύπου και ο ολικός αριθμός σελίδων. Στην πρώτη σελίδα των εγγράφων που είναι διαβαθμισμένα τουλάχιστον ως CONFIDENTIEL UE πρέπει να αναφέρονται όλα τα παραρτήματα και τα επισυναπτόμενα έγγραφα.

2. Τα έγγραφα που διαβαθμίζονται τουλάχιστον ως 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, εκτός από την ειδική περίπτωση *στην* παράγραφο 27 του παρόντος τμήματος.

   Οι διατάξεις για την αναπαραγωγή διαβαθμισμένων εγγράφων μέσω υπολογιστή περιέχονται στο τμήμα XI.

ΔΙΑΝΟΜΗ

3. 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 συντάκτη.

4. Τα έγγραφα TRÈS SECRET UE/EU TOP SECRET κυκλοφορούν μέσω γραμματειών ΑΚΡΩΣ ΑΠΟΡΡΗΤΟΝ ΕΕ (βλέπε τμήμα VIII). Όσον αφορά τα μηνύματα τα TRÈS 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.

5. Τα έγγραφα με διαβάθμιση το πολύ SECRET UE επιτρέπεται να αναδιανέμονται από τον αρχικό παραλήπτη σε άλλους παραλήπτες ανάλογα με την ανάγκη γνώσης. Ωστόσο, οι συντάκτριες αρχές αναφέρουν σαφώς τις τυχόν προειδοποιήσεις που επιθυμούν να επιβάλουν. Όταν επιβάλλονται παρόμοιες προειδοποιήσεις οι παραλήπτες αναδιανέμουν τα έγγραφα μόνον με την άδεια των συντακτριών αρχών

6. Κατά την είσοδο του σε ή την έξοδό του από μια υπηρεσία, κάθε έγγραφο τουλάχιστον CONFIDENTIEL UE καταγράφεται από τη γραμματεία 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 προστατευμένο υπόθεμα πληροφορικής

Κεφάλαιο II

Διαβίβαση διαβαθμισμένων *εγγράφων* ΕΕ

ΣΥΣΚΕΥΑΣΙΑ

7. Τα έγγραφα τουλάχιστον CONFIDENTIEL UE διαβιβάζονται εντός ανθεκτικών και αδιαφανών διπλών φακέλων Στον εσωτερικό φάκελο αναγράφεται η πρέπουσα διαβάθμιση ασφαλείας EU καθώς και, εφόσον είναι δυνατόν, η πλήρης υπηρεσιακή ιδιότητα και διεύθυνση του αποδέκτη.

8. Μόνον ένας Ελεγκτικός Υπάλληλος Γραμματείας 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 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.

9. 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

10. Ο εσωτερικός φάκελος περικλείεται σε εξωτερικό φάκελο, ο οποίος φέρει αριθμό δέματος για να είναι δυνατόν να χορηγείται απόδειξη . Ο βαθμός ασφαλείας δεν αναγράφεται ποτέ στον εξωτερικό φάκελο.

11. Για τα έγγραφα με διαβάθμιση τουλάχιστον CONFIDENTIEL UE, οι μεταφορείς και οι αγγελιαφόροι λαμβάνουν αποδείξεις με τον αριθμό δέματος

ΔΙΑΒΙΒΑΣΗ ΣΤΟ ΕΣΩΤΕΡΙΚΟ ΕΝΟΣ ΚΤΙΡΙΟΥ Ή ΜΙΑΣ ΟΜΑΔΑΣ ΚΤΙΡΙΩΝ

12. 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.

ΔΙΑΒΙΒΑΣΗ ΕΓΓΡΑΦΩΝ ΕΕ ΕΝΤΟΣ ΜΙΑΣ ΧΩΡΑΣ

13. Εντός μιας χώρας, τα έγγραφα TRÈS SECRET UE/EU TOP SECRET πρέπει να αποστέλλονται μέσω επίσημης υπηρεσίας αγγελιοφόρων ή μέσω ατόμων τα οποία έχουν εξουσιοδοτημένη πρόσβαση σε πληροφορίες TRES SECRET UE/EU TOP SECRET.

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

15. Κατ' εξαίρεση, υπάλληλοι πλην των αγγελιοφόρων, επιτρέπεται να μεταφέρουν έγγραφα TRÈS SECRET UE/EU TOP SECRET στο εσωτερικό ενός κτιρίου ή ομάδας κτιρίων, προκειμένου να τα χρησιμοποιούν επιτόπου σε συνεδριάσεις και συζητήσεις, εφόσον;

A) ο κομιστής έχει εξουσιοδότηση πρόσβασης στα εν λόγω έγγραφα TRÈS SECRET UE/EU TOP SECRET,

β) ο τρόπος μεταφοράς τηρεί τους εθνικούς κανόνες περί διαβίβασης εθνικών εγγράφων TOP SECRET,

γ) ο υπάλληλος δεν εγκαταλείπει ποτέ αφύλακτα τα έγγραφα TRÈS SECRET UE/EU TOP SECRET,

δ) λαμβάνονται μέτρα ώστε να τηρείται κατάλογος των μεταφερόμενων εγγράφων και να καταχωρείται σε βιβλίο στην Γραμματεία TRÈS SECRET UE/EU TOP SECRET, και να αντιπαραβάλλεται προς την εγγραφή αυτήν κατά την επιστροφή τους

16. Εντός μιας και της αυτής χώρας τα έγγραφα SECRET UE και CONFIDENTIEL UE επιτρέπεται να αποστέλλονται είτε με το ταχυδρομείο, εφόσον τούτο επιτρέπεται από τους εθνικούς κανονισμούς και διενεργείται σύμφωνα με τις διατάξεις τους, είτε από υπηρεσία αγγελιοφόρων ή από άτομα με έγκριση πρόσβασης σε διαβαθμισμένες πληροφορίες ΕΕ

17. Βάσει των κανονισμών αυτών, κάθε κράτος μέλος ή αποκεντρωμένος οργανισμός της ΕΕ πρέπει να καταρτίσει οδηγίες για την αυτοπρόσωπη 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) εγκαταλείπουν την κατοχή του κομιστή, εκτός εάν φυλάσσονται ασφαλώς σύμφωνα με τις διατάξεις του τμήματος IV,

β) εγκαταλείπονται αφύλακτα σε συγκοινωνιακά μέσα ή ιδιωτικά οχήματα ή σε μέρη 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.

ΔΙΑΒΙΒΑΣΗ ΜΕΤΑΞΥ ΚΡΑΤΩΝ ΜΕΛΩΝ

18. Τα υλικά που είναι διαβαθμισμένα τουλάχιστον CONFIDENTIEL UE πρέπει να μεταφέρονται μεταξύ κρατών μελών μέσω υπηρεσιών διπλωματικών ή στρατιωτικών μεταφορών.

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

20. Οι Εθνικές Αρχές Ασφαλείας μπορούν να επιτρέπουν την αυτοπρόσωπη μεταφορά όταν δεν υπάρχουν διπλωματικοί ή στρατιωτικοί μεταφοράς ή όταν η χρήση των μεταφορέων αυτών θα οδηγούσε σε καθυστέρηση που θα έβλαπτε τις επιχειρήσεις της ΕΕ και ο παραλήπτης χρειάζεται επειγόντως το συγκεκριμένο υλικό. Κάθε κράτος μέλος πρέπει να εκπονήσει οδηγίες για την αυτοπρόσωπη μεταφορά, διεθνώς, υλικού διαβαθμισμένου μέχρι και SECRET UE από άτομα άλλα πλην των διπλωματικών και στρατιωτικών μεταφορέων. Βάσει των οδηγιών αυτών πρέπει να απαιτείται

α) να διαθέτει ο κομιστής την κατάλληλη διαβάθμιση ασφαλείας που χορηγείται από τα κράτη μέλη,

β) να καταγράφονται, στο κατάλληλο γραφείο ή γραμματεία, όλα τα υλικά που μεταφέρονται κατ' αυτόν τον τρόπο,

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

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

ε) να μην πραγματοποιείται διέλευση εξωκοινοτικού κράτους ή των συνόρων του κατά τη χερσαία μεταφορά, εκτός εάν το κράτος αποστολής έχει λάβει συγκεκριμένη εξασφάλιση από το κράτος αυτό,

στ) να είναι οι ταξιδιωτικές ρυθμίσεις του κομιστή όσον αφορά τους προορισμούς, τα ακολουθούμενα δρομολόγια και τα χρησιμοποιούμενα μεταφορικά μέσα σύμφωνες προς τους κανονισμούς της ΕΕ ή — εάν οι σχετικοί εθνικοί κανονισμοί είναι αυστηρότεροι — σύμφωνες προς αυτούς,

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

η) να μην εγκαταλείπεται το υλικό αφύλακτο σε δημόσια ή ιδιωτικά οχήματα ή σε μέρη 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 κλπ.)

Το άτομο στο οποίο ανατίθεται η μεταφορά διαβαθμισμένου υλικού πρέπει να διαβάζει και να υπογράφει οδηγίες ασφαλείας οι οποίες να 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.

ΔΙΑΒΙΒΑΣΗ ΕΓΓΡΑΦΩΝ RESTREINT UE

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

ΑΣΦΑΛΕΙΑ ΜΕΤΑΦΟΡΕΩΝ

22. Όλοι οι μεταφορείς και αγγελιοφόροι που χρησιμοποιούνται για τη μεταφορά εγγράφων SECRET UE και CONFIDENTIEL UE πρέπει να διαθέτουν την κατάλληλη διαβάθμιση ασφαλείας.

Κεφάλαιο III

Ηλεκτρικά και *άλλα* μέσα τεχνικής διαβίβασης

23. Τα μέτρα ασφαλείας επικοινωνιών αποσκοπούν στην εξασφάλιση της ασφαλούς διαβίβασης διαβαθμισμένων πληροφοριών ΕΕ. Οι λεπτομερείς κανόνες για την διαβίβαση αυτών των διαβαθμισμένων πληροφοριών ΕΕ περιέχονται στο τμήμα XI.

24. Μόνον δεόντως διαπιστευμένα κέντρα επικοινωνιών και δίκτυα ή/και τερματικά και συστήματα Επιτρέπεται να διαβιβάζουν πληροφορίες διαβαθμισμένες ως CONFIDENTIEL UE και SECRET UE.

Κεφάλαιο IV

Πρόσθετα αντίγραφα, μεταφράσεις και αποσπάσματα διαβαθμισμένων εγγράφων ΕΕ

25. Μόνον ο συντάκτης μπορεί να επιτρέπει την αντιγραφή ή τη μετάφραση εγγράφων TRÈS SECRET UE/EU TOP SECRET.

26. Εάν άτομα χωρίς διαβάθμιση TRÈS SECRET UE/EU TOP SECRET χρειάζονται πληροφορίες οι οποίες, μολονότι περιέχονται σε έγγραφο TRÈS SECRET UE/EU TOP SECRET, δεν έχουν την διαβάθμιση αυτήν, είναι δυνατόν να επιτρέπεται στον προϊστάμενο της Γραμματείας TRÈS SECRET UE/EU TOP SECRET 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.

27. Τα έγγραφα με διαβάθμιση το πολύ 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. Οι αποκεντρωμένοι οργανισμοί της ΕΕ πρέπει να ακολουθούν τους προκείμενους κανονισμούς ασφαλείας.

Κεφάλαιο V

Απογραφές και *έλεγχοι*, αποθήκευση και καταστροφή διαβαθμισμένων εγγράφων ΕΕ

ΑΠΟΓΡΑΦΕΣ ΚΑΙ ΕΛΕΓΧΟΙ

28. Κάθε χρόνο, κάθε Γραμματεία TRÈS SECRET UE/EU TOP SECRET που αναφέρεται στο τμήμα VIII πραγματοποιεί αναλυτική απογραφή των εγγράφων TRÈS SECRET UE/EU TOP SECRET σύμφωνα με τους κανονισμούς του τμήματος VIII, παράγραφοι 9 έως 11. Τα έγγραφα με διαβάθμιση ΕΕ κατώτερη του TRÈS SECRET UE/EU TOP SECRET υποβάλλονται σε εσωτερικά έλεγχο σύμφωνα με τις εθνικές κατευθυντήριες γραμμές και, στην περίπτωση της ΓΤΣ ή των αποκεντρωμένων οργανισμών της ΕΕ, σύμφωνα με τις οδηγίες του Γενικού Γραμματέα/Υπατου Εκπροσώπου.

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.

ΑΡΧΕΙΟΘΕΤΗΣΗ ΔΙΑΒΑΘΜΙΣΜΕΝΩΝ ΠΛΗΡΟΦΟΡΙΩΝ ΕΕ

29. Προκειμένου να ελαχιστοποιηθούν τα προβλήματα αποθήκευσης, Επιτρέπεται στους ελεγκτικούς υπαλλήλους όλων των υπηρεσιών να αναπαράγουν σε μικροφίλμ ή να αποθηκεύουν και άλλο τρόπο σε μαγνητικό ή οπτικό υπόθεμα προς αρχειοθέτηση έγγραφα TRÈS SECRET 'UE/EU TOP SECRET, SECRET UE και CONFIDENTIEL UE, εφόσον:

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

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

γ) η παραγωγή μικροφίλμ/αποθήκευση των εγγράφων TRÈS SECRET UE/EU TOP SECRET γνωστοποιείται στο συντάκτη,

δ) τα ρολά φιλμ ή οι άλλοι τύποι υποθέματος περιέχουν μόνον έγγραφα με την ίδια διαβάθμιση TRÈS SECRET UE/EU TOP SECRET, SECRET UE ή CONFIDENTIEL UE,

ε) η παραγωγή μικροφίλμ/αποθήκευση ενός εγγράφου TRÈS SECRET UE/EU TOP SECRET ή 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 κανονισμούς των παρακάτω παραγράφων 31 έως 36.

30. Οι κανόνες αυτοί εφαρμόζονται και σε κάθε άλλη μορφή αποθήκευσης που επιτρέπεται από την Εθνική Αρχή Ασφαλείας, όπως ηλεκτρομαγνητικά υποθέματα και οπτικοί δίσκοι.

ΣΥΝΗΘΗΣ ΚΑΤΑΣΤΡΟΦΗ ΔΙΑΒΑΘΜΙΣΜΕΝΩΝ ΕΓΓΡΑΦΩΝ ΕΕ

31. Για να αποφευχθεί η περιττή συσσώρευση διαβαθμισμένων εγγράφων ΕΕ, τα έγγραφα τα οποία, κατά τη γνώμη του προϊσταμένου της υπηρεσίας στην κατοχή της οποίας ευρίσκονται, είναι πεπαλαιωμένα και περισσεύουν καταστρέφονται το συντομότερο δυνατόν ως εξής:

α) τα έγγραφα TRÈS SECRET UE/EU TOP SECRET καταστρέφονται μόνον από την αρμόδια Κεντρική Γραμματεία Κάθε καταστρεφόμενο έγγραφο πρέπει να καταγράφεται σε πρωτόκολλο καταστροφής, το οποίο υπογράφεται από τον ελεγκτικά υπάλληλο TRÈS SECRET UE/EU TOP SECRET και από τον υπάλληλο ο οποίος παρίσταται κατά την καταστροφή και ο οποίος πρέπει να έχει διαβάθμιση TRÈS 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 στον συντάκτη ή την αρμόδια κεντρική γραμματεία μόνον όταν ζητούνται ρητά,

γ) τα έγγραφα TRÈS SECRET UE/EU TOP SECRET, καθώς και όλα τα διαβαθμισμένα απορρίμματα που προκύπτουν κατά την σύνταξη των εγγράφων TRÈS SECRET UE/EU TOP SECRET, όπως κακέκτυπα αντίγραφα, σχέδια - εγγράφων, δακτυλογραφημένα σημειώματα και καρμπόν, καταστρέφονται υπό την επίβλεψη υπαλλήλου TRÈS SECRET UE/EU TOP SECRET, με καύση, πολτοποίηση, σχίσιμο σε λεπτές λουρίδες ή καθ' οιονδήποτε άλλο τρόπο που τα μετατρέπει σε μη αναγνωρίσιμη και μη ανασυστάσιμη μορφή.

32. Τα έγγραφα SECRET UE καταστρέφονται από την αρμόδια γραμματεία, υπό την επίβλεψη άτομου με διαβάθμιση ασφαλείας, με μια από τις μεθόδους που αναφέρονται στην παράγραφο 31 στοιχείο γ). Τα καταστρεφόμενα έγγραφα SECRET UE καταγράφονται σε υπογραφόμενο πρωτόκολλο καταστροφής το οποίο διατηρείται από τη γραμματεία, μαζί με τα έντυπα διανομής, επί τρία τουλάχιστον έτη.

33. Τα έγγραφα CONFIDENTIEL UE καταστρέφονται από την αρμόδια γραμματεία, υπό την επίβλεψη ατόμου με διαβάθμιση ασφαλείας και με μια από τις μεθόδους της παραγράφου 31 στοιχείο γ). Η καταστροφή τους καταγράφεται σύμφωνα με τους εθνικούς κανονισμούς και στην περίπτωση της ΓΤΣ ή των αποκεντρωμένων οργανισμών της ΕΕ, σύμφωνα με τις οδηγίες του Γενικού Γραμματέα/Ύπατου Εκπροσώπου.

34. Τα έγγραφα RESTREINT UE καταστρέφονται από την αρμόδια γραμματεία ή από το χρήστη, σύμφωνα με τους εθνικούς κανονισμούς και στην περίπτωση της ΓΤΣ ή των αποκεντρωμένων οργανισμών της ΕΕ, σύμφωνα με τις οδηγίες του Γενικού Γραμματέα/Ύπατου Εκπροσώπου.

ΚΑΤΑΣΤΡΟΦΗ ΣΕ ΠΕΡΙΠΤΩΣΗ ΕΚΤΑΚΤΗΣ ΑΝΑΓΚΗΣ

35. Η ΓΤΣ, τα κράτη μέλη και οι αποκεντρωμένοι οργανισμοί της ΕΕ καταρτίζουν σχέδια βάσει των τοπικών συνθηκών για τη διαφύλαξη του διαβαθμισμένου υλικού ΕΕ σε περίπτωση χρίσης τα οποία περιλαμβάνουν, εφόσον απαιτείται, σχέδια καταστροφής και εκκένωσης σε περίπτωση έκτακτης ανάγκης, εκδίδουν δε, εντός των αντίστοιχων οργανώσεών τους τις οδηγίες που κρίνονται αναγκαίες ώστε να μην περιπέσουν διαβαθμισμένες πληροφορίες ΕΕ στα χέρια μη εξουσιοδοτημένων ατόμων.

36. Οι ρυθμίσεις για τη διαφύλαξη ή/και την καταστροφή του υλικού SECRET UE και CONFIDENTIEL UE σε περίπτωση κρίσης δεν πρέπει ποτέ να επηρεάζουν αρνητικά τη διαφύλαξη ή την καταστροφή υλικού TRÈS SECRET UE/EU TOP SECRET, συμπεριλαμβανομένου του κρυπτογραφικού εξοπλισμού, του οποίου η διαφύλαξη ή καταστροφή πρέπει να έχουν προτεραιότητα έναντι κάθε άλλης εργασίας. Τα ληπτέα μέτρα για τη διαφύλαξη και την καταστροφή του κρυπτογραφικού εξοπλισμού σε περίπτωση έκτακτης ανάγκης καλύπτονται από ειδικές οδηγίες

Κεφάλαιο VI

Ειδικοί κανόνες για τα έγγραφα που προορίζονται για το Συμβούλιο

37. Εντός της ΓΤΣ, ένα «Γραφείο Διαβαθμισμένων Πληροφοριών» παρακολουθεί τις πληροφορίες που διαβαθμίζονται ως SECRET UE ή CONFIDENTIEL UE οι οποίες περιέχονται σε έγγραφα που προορίζονται για το Συμβούλιο.

Υπό την εποπτεία του Γενικού Διευθυντή Προσωπικού και Διοίκησης, το Γραφείο αυτό:

α) διαχειρίζεται τις εργασίες καταχώρησης αναπαραγωγής, μετάφρασης, διαβίβασης αποστολής και καταστροφής των πληροφοριών αυτών,

β) ενημερώνει το μητρώο για τις διαβαθμισμένες πληροφορίες

γ) ερωτά περιοδικώς τους εκδότες των πληροφοριών ως προς την ανάγκη διατήρησης του χαρακτηρισμού τους

δ) καθορίζει, σε συνεργασία με την Υπηρεσία Ασφαλείας τις πρακτικές λεπτομέρειες χαρακτηρισμού και αποχαρακτηρισμού των πληροφοριών,

38. Το Γραφείο Διαβαθμισμένων Πληροφοριών τηρεί μητρώο των ακόλουθων στοιχείων:

α) ημερομηνία παραγωγής των διαβαθμισμένων πληροφοριών,

β) βαθμός ασφαλείας

γ) λήξη του χαρακτηρισμού.

δ) ονοματεπώνυμο και υπηρεσία του εκδότη,

ε) αποδέκτης ή αποδέκτες με ένδειξη του αύξοντα αριθμού,

στ) θέμα,

ζ) αριθμός

η) αριθμός αντιτύπων,

θ) απογραφή των διαβαθμισμένων πληροφοριών που υποβάλλονται στο Συμβούλιο,

ι) μητρώο αποχαρακτηρισμού και υποχαρακτηρισμού διαβαθμισμένων πληροφοριών.

39. Οι γενικοί κανόνες των κεφαλαίων Ι έως V του παρόντος τμήματος ισχύουν για το Γραφείο Διαβαθμισμένων Πληροφοριών της ΓΤΣ, εκτός εάν τροποποιούνται από τους ειδικούς κανόνες του παρόντος κεφαλαίου.

ΤΜΗΜΑ VIII

ΓΡΑΜΜΑΤΕΙΕΣ TRÈS SECRET UE/EU TOP SECRET

1. Οι γραμματείες TRÈS SECRET UE/EU TOP SECRET εξασφαλίζουν την καταγραφή, τη διεκπεραίωση και τη διανομή των εγγράφων TRÈS SECRET UE/EU TOP SECRET σύμφωνα με τους κανονισμούς περί ασφαλείας. Ο προϊστάμενος της γραμματείας TRÈS SECRET UE/EU TOP SECRET, αντίστοιχα σε κάθε κράτος μέλος στη ΓΤΣ και, ανάλογα με την περίπτωση, στους αποκεντρωμένους οργανισμούς της ΕΕ, είναι ο ελεγκτικός υπάλληλος TRÈS SECRET UE/EU TOP SECRET.

2. Οι κεντρικές γραμματείες λειτουργούν ως η κύρια αρχή παραλαβής και αποστολής στα κράτη μέλη, τη ΓΤΣ και τους αποκεντρωμένους οργανισμούς της ΕΕ, όπου έχουν συσταθεί παρόμοιες γραμματείες, καθώς και, ανάλογα με την περίπτωση, σε άλλα θεσμικά όργανα της ΕΕ, διεθνείς οργανισμούς και τρίτα κράτη με τα οποία το Συμβούλιο έχει συμφωνίες για διαδικασίες ασφαλείας για την ανταλλαγή διαβαθμισμένων πληροφοριών.

3. Εφόσον απαιτείται, συγκροτούνται υπογραμματείες αρμόδιες για την εσωτερική διαχείριση των εγγράφων TRÈS SECRET UE/EU TOP SECRET οι υπογραμματείες τηρούν ενημερωμένα αρχεία της κυκλοφορίας κάθε εγγράφου για το οποίο είναι υπεύθυνες

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

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

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

ΚΕΝΤΡΙΚΕΣ ΓΡΑΜΜΑΤΕΙΕΣ TRÈS SECRET UE/EU TOP SECRET

7. Ως ελεγκτικός υπάλληλος ο προϊστάμενος μιας γραμματείας TRÈS SECRET UE/EU TOP SECRET είναι αρμόδιος για,

α) τη διαβίβαση εγγράφων TRÈS SECRET UE/EU TOP SECRET σύμφωνα με τους κανονισμούς του τμήματος VII,

β) την τήρηση καταλόγου όλων των εξαρτωμένων από αυτόν υπογραμματειών TRÈS 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 TRÈS SECRET UE/EU TOP SECRET που διανέμει η κεντρική γραμματεία,

δ) τη διατήρηση αρχείου των διατηρούμενων και διανεμόμενων εγγράφων TRÈS SECRET UE/EU TOP SECRET,

ε) την τήρηση ενημερωμένου καταλόγου όλων των κεντρικών γραμματειών TRÈS 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 TRÈS SECRET UE/EU TOP SECRET που φυλάγει η γραμματεία σύμφωνα με τους κανονισμούς του τμήματος IV.

ΥΠΟΓΡΑΜΜΑΤΕΙΕΣ TRÈS SECRET UE/EU TOP SECRET

8. Ως ελεγκτικός υπάλληλος, ο προϊστάμενος μιας υπογραμματείας TRÈS SECRET UE/EU TOP SECRET είναι αρμόδιος για

α) τη διαβίβαση εγγράφων TRÈS SECRET UE/EU TOP SECRET σύμφωνα με τους κανονισμούς του τμήματος VII και των παραγράφων 5 και 6 του τμήματος VIII,

ΤΜΗΜΑ IX

ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ ΠΟΥ ΠΡΕΠΕΙ ΝΑ ΕΦΑΡΜΟΖΟΝΤΑΙ ΣΕ ΕΙΔΙΚΕΣ ΣΥΝΕΔΡΙΑΣΕΙΣ ΟΙ ΟΠΟΙΕΣ ΔΙΕΞΑΓΟΝΤΑΙ ΕΚΤΟΣ ΤΩΝ ΚΤΙΡΙΩΝ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ ΚΑΙ ΚΑΤΑ ΤΙΣ ΟΠΟΙΕΣ ΣΥΖΗΤΟΥΝΤΑΙ ΙΔΙΑΙΤΕΡΑ ΕΥΑΙΣΘΗΤΑ ΘΕΜΑΤΑ

ΓΕΝΙΚΑ

1. Όταν σύνοδοι του Ευρωπαϊκού Συμβουλίου ή του Συμβουλίου ή υπουργικές ή άλλες σημαντικές συνεδριάσεις πραγματοποιούνται εκτός των κτιρίων του Συμβουλίου στις Βρυξέλλες και το Λουξεμβούργο, και όταν δικαιολογείται από ιδιαίτερες απαιτήσεις ασφαλείας λόγω της ιδιαίτερης ευαισθησίας των προς συζήτηση θεμάτων ή πληροφοριών, λαμβάνονται τα παρακάτω μέτρα ασφαλείας Τα μέτρα αυτά αφορούν μόνον την προστασία των διαβαθμισμένων πληροφοριών ΕΕ· για τα λοιπά θέματα ασφαλείας ενδέχεται να απαιτείται ιδιαίτερος προγραμματισμός.

ΕΥΘΥΝΕΣ

Κράτος μέλος υποδοχής

2. Το κράτος μέλος όπου διοργανώνεται μια συνεδρίαση (κράτος μέλος υποδοχής) είναι υπεύθυνο, σε συνεργασία με την υπηρεσία ασφαλείας της ΓΤΣ, για την ασφάλεια των συνόδων του Ευρωπαϊκού Συμβουλίου ή του Συμβουλίου ή των υπουργικών ή άλλων σημαντικών συνεδριάσεων και για την υλική ασφάλεια των κυριότερων αντιπροσώπων και του προσωπικού τους.

Όσον αφορά την προστασία της ασφάλειας, το κράτος μέλος υποδοχής εξασφαλίζει ιδίως ότι:

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

β) λαμβάνονται μέτρα για να παρέχεται πρόσβαση στο σύστημα επικοινωνιών του Συμβουλίου για την παραλαβή και τη διαβίβαση διαβαθμισμένων μηνυμάτων ΕΕ. Επίσης το κράτος μέλος υποδοχής πρέπει να παρέχει πρόσβαση σε ασφαλή τηλεφωνικά συστήματα

Κράτη μέλη

3. Οι αρχές των κρατών μελών εξασφαλίζουν ότι.

α) παρέχεται κατάλληλη πιστοποίηση της διαβάθμισης ασφαλείας για τους εθνικούς τους αντιπροσώπους εν ανάγκη με σήμα ή φαξ, είτε απευθείας στον υπάλληλο ασφαλείας της συνεδρίασης είτε μέσω της Υπηρεσίας Ασφαλείας της ΓΤΣ,

β) κάθε συγκεκριμένη απειλή γνωστοποιείται στις αρχές του κρότους μέλους υποδοχής και, ανάλογα με την περίπτωση, στην Υπηρεσία Ασφαλείας της ΓΤΣ, ώστε να είναι δυνατόν να ληφθούν τα κατάλληλα μέτρα.

Υπάλληλος Ασφαλείας της Συνεδρίασης

4. Ορίζεται υπάλληλος ασφαλείας υπεύθυνος για τη γενική προετοιμασία και τον έλεγχο των γενικών εσωτερικών μέτρων ασφαλείας και για το συντονισμό με τις λοιπές ενδιαφερόμενες υπηρεσίες ασφαλείας Τα μέτρα που λαμβάνει, κατά κανόνα, αφορούν:

α) i) προστατευτικά μέτρα στον τόπο της συνεδρίασης ώστε να εξασφαλίζεται ότι η συνεδρίαση διεξάγεται χωρίς συμβάντα ικανά να θίξουν την ασφάλεια των διαβαθμισμένων πληροφοριών ΕΕ που ενδέχεται να χρησιμοποιηθούν κατά τη συνεδρίαση αυτήν,

ii) 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.

iii) συνεχή συντονισμό με τις αρμόδιες αρχές του κράτους μέλους υποδοχής και με την Υπηρεσία Ασφαλείας της ΓΤΣ.

β) την προσθήκη οδηγιών ασφαλείας στο φάκελο της συνεδρίασης λαμβανομένων δεόντως υπόψη των απαιτήσεων που προβλέπονται από τους παρόντες κανονισμούς ασφαλείας και κάθε άλλης οδηγίας που κρίνεται αναγκαία

Υπηρεσία Ασφαλείας της ΓΤΣ

5. Η Υπηρεσία Ασφαλείας της ΓΤΣ λειτουργεί ως σύμβουλος ασφαλείας κατά την προετοιμασία της συνεδρίασης, στην οποία πρέπει να εκπροσωπείται για να επικουρεί και να παρέχει συμβουλές προς τον υπάλληλο ασφαλείας της συνεδρίασης και τις αντιπροσωπείες εφόσον απαιτείται

6. Κάθε αντιπροσωπεία που συμμετέχει στη συνεδρίαση ορίζει έναν υπάλληλο ασφαλείας ο οποίος θα είναι υπεύθυνος για την αντιμετώπιση θεμάτων ασφαλώς εντός της αντιπροσωπείας του και για τη διασύνδεση με τον υπάλληλο ασφαλείας της συνεδρίασης, καθώς και με την Υπηρεσία Ασφαλείας της ΓΤΣ εφόσον απαιτείται.

ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ

Περιοχές ασφαλείας

7. Πρέπει να δημιουργούνται οι ακόλουθοι χώροι ασφαλείας

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

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 χώρου της συνεδρίασης τα οποία χρησιμοποιούνται για διοικητικές εργασίες, εστίαση και κατάλυμα, και το χώρο που γειτνιάζει άμεσα με το Κέντρο Τύπου και το χώρο της συνεδρίασης

Άδειες κυκλοφορίας

8. Ο υπάλληλος ασφαλείας της συνεδρίασης 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

9. Οι οδηγίες ασφαλείας της συνεδρίασης 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

10 Εκτός από τους συμμετέχοντες με ειδική ταυτότητα, στο χώρο της συνεδρίασης πρέπει να επιτρέπεται η είσοδος σε όσο το δυνατόν λιγότερα άτομα Οι εθνικές αντιπροσωπείες που επιθυμούν να δεχθούν επισκέπτες κατά τη διάρκεια της συνεδρίασης πρέπει να ενημερώνουν τον υπάλληλο ασφαλείας της συνεδρίασης. Στους επισκέπτες πρέπει να χορηγείται ειδική ταυτότητα επισκέπτη. Προς τούτο, πρέπει να συμπληρώνεται ειδικά έντυπο με το ονοματεπώνυμό του και το ονοματεπώνυμο του ατόμου που επισκέπτεται. Οι επισκέπτες πρέπει να συνοδεύονται πάντα από φύλακα ή από το άτομο του επισκέπτονται. Το έντυπο εισόδου του επισκέπτη πρέπει να φέρεται από το άτομο που επισκέπτεται, το οποίο και το επιστρέφει, μαζί με την ειδική ταυτότητα του επισκέπτη, στο προσωπικό ασφαλείας κατά την αναχώρηση του επισκέπτη από το χώρο της συνεδρίασης

Έλεγχος φωτογραφικού και ακουστικού εξοπλισμού

11. Στο χώρο ασφαλείας κατηγορίας Ι απαγορεύεται να εισάγονται φωτογραφικές μηχανές ή ηχογραφικές συσκευές, πλην του εξοπλισμού των φωτογράφων και των μηχανικών ήχου που είναι δεόντως εξουσιοδοτημένοι από τον υπάλληλο ασφαλείας της συνεδρίασης

Έλεγχος χαρτοφυλάκων, φορητών υπολογιστών και δεμάτων

12. Οι κάτοχοι άδειας κυκλοφορίας 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 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 ανοιχτούν προς επιθεώρηση από το προσωπικό ασφαλείας Εάν ο υπάλληλος ασφαλείας της συνεδρίασης το κρίνει αναγκαίο, είναι δυνατόν να λαμβάνονται αυστηρότερα μέτρα για την επιθεώρηση των χαρτοφυλάκων και των δεμάτων.

Τεχνική ασφάλεια

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

Έγγραφα των αντιπροσωπειών

14. 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 εγγράφων αυτών κατά τη χρήση τους στους διατεθέντες χώρους. Είναι δυνατόν να ζητείται η βοήθεια του κράτους μέλους υποδοχής για τη μεταφορά διαβαθμισμένων εγγράφων από και προς το χώρο της συνεδρίασης.

Ασφαλής φύλαξη των εγγράφων

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

Επιθεώρηση γραφείων

16. Ο υπάλληλος ασφαλείας της συνεδρίασης πρέπει να λαμβάνει μέτρα για την επιθεώρηση των γραφείων της ΓΤΣ και των αντιπροσωπειών στο τέλος κάθε ημέρας εργασίας προκειμένου να βεβαιώνεται ότι όλα τα διαβαθμισμένα έγγραφα ΕΕ διατηρούνται σε ασφαλή χώρο σε διαφορετική περίπτωση, μπορεί να λαμβάνει τα δέοντα μέτρα.

Διάθεση διαβαθμισμένων απορριμμάτων ΕΕ

17. Όλα τα απορρίμματα πρέπει να αντιμετωπίζονται ως διαβαθμισμένα ΕΕ, οι δε κάλαθοι ή σάκοι αχρήστων πρέπει να παραδίδονται στη ΓΤΣ και τις αντιπροσωπείες προς διάθεση. Πριν εγκαταλείψουν τους διατεθέντες χώρους, η ΓΤΣ και οι αντιπροσωπείες πρέπει να παραδίδουν τα απορρίμματά τους στον υπάλληλο ασφαλείας της συνεδρίασης, ο οποίος φροντίζει για την καταστροφή τους σύμφωνα με τους κανονισμούς

18. Μετά το πέρας της συνεδρίασης όλα τα έγγραφα που βρίσκονται στην κατοχή της ΓΤΣ 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 ΓΤΣ και των αντιπροσωπειών. Τα έγγραφα για τα οποία έχει χορηγηθεί υπογεγραμμένη απόδειξη πρέπει, στο μέτρο του εφικτού, να καταστρέφονται σύμφωνα με το τμήμα VII.

ΤΜΗΜΑ X

ΠΑΡΑΒΙΑΣΕΙΣ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΔΙΑΡΡΟΗ ΔΙΑΒΑΘΜΙΣΜΕΝΩΝ ΠΛΗΡΟΦΟΡΙΩΝ ΕΕ

1. Παραβίαση της ασφάλειας προκύπτει ως αποτέλεσμα μιας πράξης ή μιας παράλειψης αντίθετης προς συγκεκριμένο κανονισμό ασφαλώς του Συμβουλίου ή κράτους μέλους, με την οποία τίθενται σε κίνδυνο ή διαρρέουν διαβαθμισμένες πληροφορίες ΕΕ

2. Διαρροή διαβαθμισμένων πληροφοριών ΕΕ προκύπτει όταν αυτές καταλήγουν εξ ολοκλήρου ή εν μέρει σε χέρια μη εξουσιοδοτημένων προσώπων, δηλαδή προσώπων που είτε δεν έχουν υποστεί επιτυχώς τον πρέποντα έλεγχο ασφαλείας είτε δεν δικαιολογείται να γνωρίζουν, ή όταν θεωρείται πιθανό να έχει συμβεί κάτι τέτοιο.

3. 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.

4. Είναι σημαντικό όλα τα πρόσωπα τα οποία απαιτείται να χειρίζονται διαβαθμισμένες πληροφορίες ΕΕ να έχουν ενημερωθεί αναλυτικά για τις ρυθμίσεις ασφαλείας, τους κινδύνους τυχόν ακριτομυθιών και τις σχέσεις τους με τον τύπο. Πρέπει να έχουν συνείδηση ότι είναι σημαντικό να αναφέρεται αμέσως στην αρχή ασφαλείας του κράτους μέλους του θεσμικού οργάνου ή του οργανισμού για τον οποίο εργάζονται κάθε παραβίαση της ασφάλειας που τυχόν υποπέσει στην αντίληψη τους.

5. Όταν μια αρχή ασφαλείας ανακαλύπτει ή πληροφορείται παραβίαση της ασφάλειας σχετικά με διαβαθμισμένες πληροφορίες ΕΕ ή απώλεια ή εξαφάνιση διαβαθμισμένου υλικού ΕΕ, λαμβάνει εγκαίρως μέτρα προκειμένου:

   α) να διαπιστώσει τα πραγματικά περιστατικά,

   β) να εκτιμήσει και να ελαχιστοποιήσει την επελθούσα ζημία,

   γ) να αποτρέψει επανάληψη του συμβάντος

   δ) να ειδοποιήσει τις δέουσες αρχές για τις συνέπειες της παραβίασης της ασφάλειας

   Στα πλαίσια αυτά, 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 ο τομέας 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.

6. Αποτελεί καθήκον της κάθε αρχής ασφαλείας, μόλις ειδοποιηθεί για μια τέτοια παραβίαση της ασφάλειας να αναφέρει το γεγονός αμέσως με την ακόλουθη διαδικασία· οι υπεύθυνοι της συγκεκριμένης υπογραμματείας TRÈS SECRET UE/EU TOP SECRET ειδοποιούν **ΤΟ** Γραφείο Ασφαλείας της ΓΤΣ μέσω της κεντρικής γραμματείας TRES SECRET UE/EU TOP SECRET· στην περίπτωση διαρροής διαβαθμισμένων πληροφοριών ΕΕ εντός της επικράτειας κράτους μέλους αυτή αναφέρεται στο Γραφείο Ασφαλείας της ΓΤΣ όπως ορίζεται στην παράγραφο 5, μέσω της αρμόδιας ΕΕΑ.

7. Οι περιπτώσει που αφορούν πληροφορίες RESTREINT UE αναφέρονται μόνο όταν παρουσιάζουν ασυνήθιστα χαρακτηριστικά.

8. Ο Γενικός Γραμματέας/Ύπατος Εκπρόσωπος, μόλις πληροφορηθεί μια παραβίαση της ασφάλειας·

   α) ενημερώνει την αρχή από όπου προήλθαν οι εν λόγω διαβαθμισμένες πληροφορίες.

   β) δίνει εντολή στις αρμόδιες αρχές ασφαλείας να διεξαγάγουν έρευνες

   γ) συντονίζει τις έρευνες όταν ενέχονταν πλείονες αρχές ασφαλείας

δ) λαμβάνει έκθεση για τα πραγματικά περιστατικά της παραβίασης, την ημερομηνία ή το διάστημα κατά το οποίο ενδέχεται να συνέβη και την ανακάλυψη της ρε λεπτομερή περιγραφή του περιεχομένου και της διαβάθμισης του σχετικού υλικού, καθώς επίσης και έκθεση της ζημίας που υπέστησαν τα συμφέροντα της ΕΕ ή ενός ή περισσοτέρων κρατών μελών της και των ενεργειών που έγιναν για την αποτροπή επανάληψης του συμβάντος

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

10. Κάθε υπεύθυνος για τη διαρροή διαβαθμισμένων πληροφοριών ΕΕ υπόκειται σε πειθαρχικές κυρώσεις σύμφωνα με τους οικείους κανόνες και κανονισμούς. Οι κυρώσεις επιβάλλονται με την επιφύλαξη των τυχόν περαιτέρω δικαστικών ενεργειών.

ΤΜΗΜΑ XI

ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΠΛΗΡΟΦΟΡΙΩΝ ΣΤΑ ΣΥΣΤΗΜΑΤΑ ΤΕΧΝΟΛΟΓΙΑΣ ΤΩΝ ΠΛΗΡΟΦΟΡΙΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ

Πίνακας περιεχομένων

Κεφάλαιο I

Εισαγωγή

ΓΕΝΙΚΕΣ ΠΤΥΧΕΣ

1. Η πολιτική και οι απαιτήσεις ασφαλείας που προβλέπονται στο παρόν τμήμα ισχύουν για όλα τα συστήματα και δίκτυα επικοινωνιών και πληροφορικής (εφεξής συστήματα) στα οποία διακινούνται πληροφορίες με διαβάθμιση CONFIDENTIEL UE ή υψηλότερη

2. Τα συστήματα στα οποία διακινούνται πληροφορίες RESTREINT UE επίσης απαιτείται να καλύπτονται από μέτρα ασφαλείας ώστε να προστατεύεται η εμπιστευτικότητα 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. Τα μέτρα ασφαλείας των συστημάτων αυτών καθορίζονται από την καθορισμένη Αρχή Πιστοποίησης της Ασφάλειας (ΑΠΑ) και είναι ανάλογα προς τον εκτιμώμενο κίνδυνο και σύμφωνα με την πολιτική που χαράσσεται στους παρόντες κανονισμούς ασφαλείας.

3. Η προστασία των συστημάτων ανίχνευσης στα οποία έχουν ενσωματωθεί συστήματα πληροφορικής καθορίζεται και διευκρινίζεται στο γενικότερο πλαίσιο των συστημάτων στα οποία ανήκουν, με τη χρήση των εφαρμοστέων διατάξεων του παρόντος τμήματος κατά το μέτρο του δυνατού.

ΑΠΕΙΛΕΣ ΚΑΤΑ ΤΩΝ ΣΥΣΤΗΜΑΤΩΝ ΚΑΙ ΤΡΩΤΑ ΣΗΜΕΙΑ ΑΥΤΩΝ

4. Σε γενικές γραμμές ως απειλή ορίζεται κάθε δυνατότητα, τυχαίας ή εσκεμμένης αποδυνάμωση, άμβλυνση της ασφάλειας Στην περίπτωση των συστημάτων, η εν λόγω αποδυνάμωση της ασφάλειας συνεπάγεται απώλεια εμπιστευτικότητας ακεραιότητας, διαθεσιμότητας, ή δύο περισσότερων από τις ιδιότητες αυτές Ως τρωτό σημείο ορίζεται μια αδυναμία των ελέγχων ή έλλειψη αυτών που διευκολύνει ή καθιστά δυνατή την ενεργοποίηση μιας απειλής εις βάρος συγκεκριμένου περιουσιακού στοιχείου ή στόχου. Ένα τρωτό σημείο μπορεί να οφείλεται σε κάποια παράλειψη ή να απορρέει από κάποια ανεπάρκεια όσον αφορά την αυστηρότητα, την πληρότητα ή τη σταθερότητα των ελέγχων, μπορεί δε να *είναι* τεχνικής, διαδικαστικής η επιχειρησιακής φύσεως

5. Οι διαβαθμισμένες ή αδιαβάθμητες πληροφορίες ΕΕ που διακινούνται στα συστήματα υπό συμπυκνωμένη μορφή που αποσκοπεί στην ταχεία ανάκτηση, κοινοποίηση και χρήση είναι ευάλωτες σε πολλούς κινδύνους Σε αυτούς περιλαμβάνεται η πρόσβαση μη εξουσιοδοτημένων χρηστών σε αυτές ή, αντίθετα, η άρνηση πρόσβασης στους εξουσιοδοτημένους χρήστες Υπάρχουν επίσης οι κίνδυνοι κοινολόγησης άνευ αδείας, αλλοίωσης τροποποίησης ή εξάλειψης των πληροφοριών. Επιπλέον, τα χρησιμοποιούμενα πολύπλοκα και ορισμένες φορές εύθραυστα μηχανήματα είναι ακριβά και συχνά είναι δύσκολο να επιδιορθωθούν ή να αντικατασταθούν γρήγορα. Τα συστήματα αυτά αποτελούν επομένως ελκυστικούς στόχους για κατασκοπευτικές δραστηριότητες και πράξεις δολιοφθοράς ιδίως εάν υπάρχει η εντύπωση ότι τα μέτρα ασφαλείας είναι αναποτελεσματικά.

ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ

6. Ο κύριος σκοπός των μέτρων ασφαλείας που αναφέρονται στο παρόν τμήμα συνίσταται στην παροχή προστασίας από το ενδεχόμενο κοινολόγησης πληροφοριών άνευ αδείας (απώλεια εμπιστευτικότητας) καθώς και απώλειας της ακεραιότητας και της διαθεσιμότητας των πληροφοριών Για την επίτευξη επαρκούς προστασίας της ασφάλειας των συστημάτων που περιέχουν διαβαθμισμένες πληροφορίες ΕΕ, καθορίζονται κατάλληλες προδιαγραφές συμβατικής ασφάλειας καθώς και κατάλληλες ρυθμίσεις και τεχνικές ασφαλείας ειδικά για το κάθε σύστημα.

7. Αποφασίζεται και τίθεται σε εφαρμογή ένα ισορροπημένο σύνολο μέτρων ασφαλείας για τη δημιουργία ασφαλούς περιβάλλοντος εντός του οποίου λειτουργεί ένα σύστημα. Τα πεδία εφαρμογής των μέτρων αυτών καλύπτουν τα υλικά στοιχεία, το προσωπικό, τις μη τεχνικές διαδικασίες και τις διαδικασίες λειτουργίας των υπολογιστών και των επικοινωνιών

8. Στα μέτρα ασφαλείας των υπολογιστών (τόσο των μηχανημάτων όσο και των προγραμμάτων) πρέπει να ενσωματώνεται η εφαρμογή της αρχής της πρόσβασης μόνον όσων έχουν ανάγκη να γνωρίζουν καθώς και η πρόληψη και ανίχνευση της κοινολόγησης πληροφοριών άνευ αδείας. Ο βαθμός στον οποίο τα μέτρα ασφαλείας των υπολογιστών μπορούν να θεωρούνται αξιόπιστα καθορίζεται κατά τη διαδικασία θέσπισης των απαιτήσεων ασφάλειας Κατά τη διαδικασία έγκρισης της λειτουργίας εξακριβώνεται η ύπαρξη επαρκούς βεβαιότητας όσον αφορά την αξιοπιστία των μέτρων ασφαλείας των υπολογιστών

ΔΗΛΩΣΗ ΓΙΑ ΤΙΣ ΕΙΔΙΚΕΣ ΓΙΑ ΤΟ ΚΑΘΕ ΣΥΣΤΗΜΑ ΑΠΑΙΤΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ (SSRS)

9. Για όλα τα συστήματα στα οποία διακινούνται πληροφορίες με διαβάθμιση EU CONFIDENTIAL και υψηλότερες διαβαθμίσεις, απαιτείται να εκδίδεται μια δήλωση για τις ειδικές για το κάθε σύστημα απαιτήσεις ασφαλείας (SSRS) από την ITSOA, με εισηγήσεις και βοήθεια από το προσωπικό του σχεδίου και την Αρχή INFOSEC Η δήλωση αυτή εγκρίνεται από την ΑΠΑ. Απαιτείται μια SSRS και στις περιπτώσεις *όπου* η διαθεσιμότητα και ακεραιότητα των πληροφοριών με διαβάθμιση RESTREINT UE ή χωρίς διαβάθμιση κρίνεται καίριας σημασίας από την ΑΠΑ

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

11. Η SSRS συνιστά δεσμευτική συμφωνία μεταξύ της Επιχειρησιακής Αρχής του συστήματος πληροφορικής και της ΑΠΑ από την οποία το σύστημα λαμβάνει την έγκριση λειτουργίας.

12. Η 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 σης εκτιμήσεις κινδύνου του Συμβουλίου, ή επιβάλλεται από παραμέτρους που αφορούν το επιχειρησιακό περιβάλλον, το χαμηλότερο δυνατό επίπεδο ελέγχων ασφαλείας του προσωπικού, την υψηλότερη δυνατή διαβάθμιση των πληροφοριών, το συγκεκριμένο 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 άποψη τεχνικής, προϋπολογισμού και ασφάλειας Στην τελική της μορφή, η SSRS αποτελεί μια ολοκληρωμένη δήλωση περί του τι σημαίνει ο ισχυρισμός ότι το σύστημα είναι ασφαλές

ΕΠΙΠΕΔΑ ΑΣΦΑΛΕΙΑΣ ΤΗΣ ΛΕΙΤΟΥΡΓΙΑΣ

13. Όλα τα συστήματα στα οποία διακινούνται πληροφορίες με διαβάθμιση EU CONFIDENTIAL ή υψηλότερη πρέπει να έχουν λάβει πιστοποίηση 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

γ) πολλαπλό.

Κεφάλαιο II

Ορισμοί

ΠΡΟΣΘΕΤΕΣ ΣΗΜΑΝΣΕΙΣ

14. Στις περιπτώσεις που υπάρχει ανάγκη περιορισμένης διανομής και ειδικής μεταχείρισης πέραν των όσων απαιτούνται βάσει της διαβάθμισης ασφαλείας τίθενται πρόσθετες σημάνσεις όπως CRYPTO ή άλλες αναγνωρισμένες από την ΕΕ σημάνσεις ειδικής μεταχείρισης

15. Ως «ΑΠΟΛΥΤΟ» επίπεδο ασφαλείας νοείται το επίπεδο λειτουργίας στο οποίο ΟΛΑ τα πρόσωπα που έχουν πρόσβαση στο σύστημα. Ελέγχονται σύμφωνα με τον υψηλότερο βαθμό διαβάθμισης των πληροφοριών που περιέχονται στο σύστημα, ενώ παράλληλα έχουν και τον ίδιο βαθμό ανάγκης να γνωρίζουν ΟΛΕΣ τις πληροφορίες που περιέχονται 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 απαίτησης της υψηλότερης διαβάθμισης και όλων των κατηγοριών πληροφοριών που περιέχονται στο σύστημα.

16 Ως «ΥΨΗΛΟ» επίπεδο ασφαλείας νοείται το επίπεδο λειτουργίας στο οποίο ΟΛΑ τα πρόσωπα που έχουν πρόσβαση στο σύστημα ελέγχονται σύμφωνα με τον υψηλότερο βαθμό διαβάθμισης των πληροφοριών που περιέχονται στο σύστημα, αλλά μεταξύ αυτών ΔΕΝ ΕΧΟΥΝ ΟΛΑ τον ίδιο βαθμό ανάγκης να γνωρίζουν τις πληροφορίες που περιέχονται στο σύστημα.

Σημειώσεις

1. Η μη ύπαρξη «ίδιου βαθμού ανάγκης να γνωρίζουν» σημαίνει ότι τα χαρακτηριστικά ασφαλείας των υπολογιστών πρέπει οπωσδήποτε να παρέχουν τη δυνατότητα επιλεκτικής πρόσβασης στο σύστημα και διαχωρισμού των πληροφοριών που περιέχονται σε αυτό.

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 περιέχονται στο σύστημα.

3. Όλες οι πληροφορίες που διακινούνται ή καθίστανται προσιτές σε ένα σύστημα σύμφωνα με αυτό το επίπεδο ασφαλείας 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 λειτουργίες επισήμανσης υπάρχουν.

17. Ως «ΠΟΛΛΑΠΛΟ» επίπεδο ασφαλείας νοείται το επίπεδο λειτουργίας στο οποίο ΟΡΙΣΜΕΝΑ ΜΟΝΟ από τα πρόσωπα που έχουν πρόσβαση στο σύστημα έχουν υποστεί έλεγχο ασφαλείας και λάβει άδεια χειρισμού του υψηλότερου βαθμού διαβάθμισης των πληροφοριών που περιέχονται στο σύστημα και παράλληλα ΟΡΙΣΜΕΝΑ ΜΟΝΟ από τα πρόσωπα που έχουν πρόσβαση έχουν τον ίδιο βαθμό ανάγκης να γνωρίζουν τις πληροφορίες που περιέχονται στο σύστημα.

Σημειώσεις:

1. Αυτός ο τρόπος λειτουργίας πρέπει, τη στιγμή αυτή, τον χειρισμό πληροφοριών διαφορετικής διαβάθμισης και διαφόρων κατηγοριών, και

2. Το γεγονός *ότι* δεν έχουν όλα τα πρόσωπα υποστεί έλεγχο και λάβει άδεια στο υψηλότερο επίπεδο, σε συνδυασμό με την μη ύπαρξη ίδιου βαθμού ανάγκης να γνωρίζουν, σημαίνει ότι τα χαρακτηριστικά ασφαλείας των υπολογιστών πρέπει οπωσδήποτε να παρέχουν τη δυνατότητα επιλεκτικής πρόσβασης και διαχωρισμού τον πληροφοριών που περιέχονται *στο* σύστημα.

18. Ως 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 συστημάτων αυτών καθεαυτών. 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.

19. Ως ΑΣΦΑΛΕΙΑ ΤΩΝ ΥΠΟΛΟΓΙΣΤΩΝ (COMPUSEC) νοείται η εφαρμογή μέτρων προστασίας του υλικού, του υλικολογισμικού και του λογισμικού σε σύστημα υπολογιστών ώστε να υπάρχει προστασία έναντι, ή πρόληψη, κοινολόγησης άνευ αδείας, αλλοίωσης, τροποποίησης/εξάλειψης πληροφοριών ή άρνησης εξυπηρέτησης.

20. Ως ΠΡΟΪΟΝ ΑΣΦΑΛΕΙΑΣ ΥΠΟΛΟΓΙΣΤΩΝ 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 πληροφοριών που περιέχονται σε αυτό.

21. Ως ΑΣΦΑΛΕΙΑ ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ (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, τον υλικού, του προσωπικού, των εγγράφων και των υπολογιστών.

22. Ως ΑΞΙΟΛΟΓΗΣΗ νοείται η λεπτομερής τεχνική εξέταση, από αρμόδια αρχή, των πτυχών ασφαλείας ενός συστήματος ή ενός προϊόντος κρυπτογράφησης η ασφαλείας των υπολογιστών.

Σημειώσεις

1. Με την αξιολόγηση διερευνάται η ύπαρξη των απαιτούμενων λειτουργιών ασφάλειας και η απουσία επικίνδυνων παρενεργειών από τις λειτουργίες αυτές και εκτιμάται το απρόσβλητο αυτών των λειτουργιών και

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.

23. Ως ΠΙΣΤΟΠΟΙΗΣΗ νοείται η έκδοση επίσημης δήλωσης, βασισμένης σε ανεξάρτητη εξέταση της διεξαγωγής και των αποτελεσμάτων μιας αξιολόγησης για τον βαθμό στον οποίο ένα σύστημα ανταποκρίνεται στις απαιτήσεις ασφαλείας ή ένα προϊόν ασφάλειας των υπολογιστών στις προκαθορισμένες προδιαγραφές ασφαλείας.

24. Ως ΕΓΚΡΙΣΗ ΛΕΙΤΟΥΡΓΙΑΣ νοείται η άδεια και η έγκριση που χορηγείται σε ένα σύστημα να επεξεργάζεται διαβαθμισμένες πληροφορίες ΕΕ στο λειτουργικό του περιβάλλον.

Σημείωση.

Η έγκριση λειτουργίας πρέπει να παρέχεται αφού πρώτα εφαρμοστούν όλες οι ενδεδειγμένες διαδικασίες ασφάλειας και έχει επιτευχθεί ικανοποιητικό επίπεδο προστασίας των πόρων του συστήματος . Η έγκριση λειτουργίας παρέχεται κανονικά βάσει της SSRS στην οποία συμπεριλαμβάνονται και τα εξής:

α) μια δήλωση για τον στόχο της έγκρισης λειτουργίας του συστήματος συγκεκριμένα, ποια επίπεδα διαβάθμισης πληροφοριών πρόκειται να εφαρμοστούν σε αυτό και ποιο είναι το προτεινόμενο επίπεδο ασφάλειας της λειτουργίας του συστήματος ή του δικτύου,

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

γ) οι λειτουργικές διαδικασίες ασφάλειας σης οποίες περιλαμβάνονται μια αναλυτική περιγραφή των προτεινόμενων λειτουργιών (π.χ. τρόποι λειτουργίας, υπηρεσίες) και μια περιγραφή των χαρακτηριστικών ασφαλείας του συστήματος βάση των οποίων παρέχεται η έγκριση λειτουργίας,

δ) το σχέδιο εφαρμογής και συντήρησης των χαρακτηριστικών ασφαλείας,

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

στ) την πιστοποίηση, όπου απαιτείται, από κοινού με άλλα στοιχεία της έγκρισης λειτουργίας

25. Ως ΣΥΣΤΗΜΑ ΤΕΧΝΟΛΟΓΙΑΣ ΤΩΝ ΠΛΗΡΟΦΟΡΙΩΝ νοείται ο συνδυασμός μηχανημάτων, μεθόδων και διαδικασιών, και ενδεχομένως προσωπικού, οργανωμένων κατά τρόπο που να εκπληρούν λειτουργίες επεξεργασίας πληροφοριών

Σημειώσεις:

1. Αυτό θεωρείται ότι σημαίνει σύνολο εγκαταστάσεων που έχει δημιουργηθεί για τον 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.

3 Τα όρια ενός συστήματος καθορίζονται σε γενικές γραμμές ως τα στοιχεία που βρίσκονται υπό τον έλεγχο μιας και της αυτής λειτουργικής αρχής ενός συστήματος πληροφορικής και

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

26. Ως ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΑΣΦΑΛΕΙΑΣ ενός συστήματος τεχνολογίας των πληροφοριών νοούνται όλες οι λειτουργίες οι ιδιαιτερότητες και τα χαρακτηριστικά του υλικού, του υλικολογισμικού και του λογισμικού, οι διαδικασίες λειτουργίας οι διαδικασίες λογοδοσίας οι έλεγχοι πρόσβασης ο χώρος πληροφορικής ο χώρος ανεξάρτητων τερματικών/σταθμών εργασίας καθώς και οι διαχειριστικοί περιορισμοί, η υλική δομή και οι συσκευές, το προσωπικό και οι έλεγχοι των επικοινωνιών που απαιτούνται για την εξασφάλιση αποδεκτού επιπέδου προστασίας των διαβαθμισμένων πληροφοριών που εμπεριέχονται σε ένα σύστημα πληροφορικής.

27. Ως ΔΙΚΤΥΟ 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 για τη διασύνδεση και 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 στο ίδιο μέρος.

28. Ως ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΑΣΦΑΛΕΙΑΣ ΕΝΟΣ ΔΙΚΤΥΟΥ 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 επισήμανσης της ασφάλειας έλεγχοι πρόσβασης προγράμματα και αυτόματες καταγραφές ενεργειών) τα οποία απαιτούνται για την παροχή αποδεκτού επιπέδου προστασίας των διαβαθμισμένων πληροφοριών.

29. Ως ΧΩΡΟΣ ΠΛΗΡΟΦΟΡΙΚΗΣ νοείται ο χώρος ο οποίος περιλαμβάνει έναν ή περισσότερους υπολογιστές τα επί τόπου ανεξάρτητα περιφερειακά και μονάδες αποθήκευσης τους τις μονάδες ελέγχου και ειδικό για τον σκοπό αυτό δίκαιο και εξοπλισμό επικοινωνιών.

Σημείωση.

Δεν συμπεριλαμβάνεται ο τυχόν ξεχωριστός χώρος στον οποίο βρίσκονται εγκατεστημένα τα ανεξάρτητα περιφερειακά ή τερματικά/σταθμοί εργασίας ακόμα κι αν τα τερματικά αυτά είναι συνδεδεμένα με μηχανήματα του χώρου πληροφορικής.

30. Ως ΧΩΡΟΣ ΑΝΕΞΑΡΤΗΤΩΝ ΤΕΡΜΑΤΙΚΩΝ/ΣΤΑΘΜΩΝ ΕΡΓΑΣΙΑΣ νοείται ένας χώρος ο οποίος περιλαμβάνει μια ποσότητα πληροφορικού εξοπλισμού, τα επί τόπου περιφερειακά ή τερματικά/σταθμούς εργασίας και τα τυχόν συνδεδεμένα με αυτά μηχανήματα επικοινωνιών, χωριστά από τον χώρο πληροφορικής

31. 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

Κεφάλαιο III

Αρμοδιότητες ασφαλείας

ΓΕΝΙΚΑ

32. Οι αρμοδιότητες της Επιτροπής Ασφαλείας, που ορίζεται στο τμήμα 1, παράγραφος 4, περιλαμβάνουν θέματα INFOSEC. Η Επιτροπή Ασφαλείας οργανώνει τις δραστηριότητές της κατά τρόπο ώστε να μπορεί να παρέχει έγκυρες συμβουλές για τα θέματα αυτά.

33. Σε περίπτωση προβλημάτων ασφαλείας (συμβάντα, παραβιάσεις κλπ.), η αρμόδια Εθνική Αρχή ή/και η Υπηρεσία Ασφαλείας της ΓΤΣ λαμβάνουν αμέσως μέτρα. Όλα τα προβλήματα πρέπει να αναφέρονται στην Υπηρεσία Ασφαλείας της ΓΤΣ.

34. Ο Γενικός Γραμματέας/Ύπατος Εκπρόσωπος ή, κατά περίπτωση, ο προϊστάμενος ενός αποκεντρωμένου οργανισμού της ΕΕ, συνιστά Γραφείο INFOSEC για να παρέχει οδηγίες στην αρχή ασφαλείας όσον αφορά την εφαρμογή και τον έλεγχο ειδικών μέτρων ασφαλείας που είναι σχεδιασμένα ως μέρη συστημάτων.

ΑΡΧΗ ΠΙΣΤΟΠΟΙΗΣΗΣ ΑΣΦΑΛΕΙΑΣ (ΑΠΑ)

35. Η ΑΠΑ είναι:

— είτε μια ΕΑΑ,

— είτε η Αρχή που ορίζεται από το Γενικό Γραμματέα/Ύπατο Εκπρόσωπο,

— είτε η αρχή ασφαλείας ενός αποκεντρωμένου οργανισμού της ΕΕ,

— είτε οι διαπιστευμένοι/διορισμένοι εκπρόσωποί τους ανάλογα με το σύστημα που πρέπει να λάβει έγκριση λειτουργίας.

36. Η ΑΠΑ είναι υπεύθυνη για την εξασφάλιση της συμμόρφωσης των συστημάτων με την πολιτική ασφαλείας του Συμβουλίου. Ένα από τα καθήκοντα της είναι να εγκρίνει ένα σύστημα για τη διεκπεραίωση διαβαθμισμένων πληροφοριών ΕΕ μέχρις ενός καθοριζόμενου βαθμού ασφαλείας εντός τον επιχειρησιακού του περιβάλλοντος Όσον αφορά τη ΓΤΣ και, κατά περίπτωση, τους αποκεντρωμένους οργανισμούς της ΕΕ, η ΑΠΑ ασκεί την ευθύνη για ασφάλεια εξ ονόματος του Γενικού Γραμματέα/Ύπατου Εκπροσώπου ή των προϊσταμένων των αποκεντρωμένων οργανισμών.

Η δικαιοδοσία της ΑΠΑ της ΓΤΣ καλύπτει όλα τα συστήματα που λειτουργούν στα κτίρια της ΓΤΣ. Τα συστήματα και τα στοιχεία συστημάτων που λειτουργούν στο εσωτερικό κράτους μέλους παραμένουν στη δικαιοδοσία του κράτους μέλους αυτού. Όταν διάφορα στοιχεία ενός συστήματος υπάγονται ταυτόχρονα στη δικαιοδοσία της ΑΠΑ της ΓΤΣ και άλλων ΑΠΑ, όλα τα μέρη διορίζουν κοινό συμβούλιο πιστοποίησης υπό το συντονισμό της ΑΠΑ της ΓΤΣ.

ΑΡΧΗ INFOSEC (ΙΑ)

37. Η αρχή INFOSEC είναι αρμόδια για τις δραστηριότητες του γραφείου INFOSEC. Όσον αφορά τη ΓΤΣ και, κατά περίπτωση, τους αποκεντρωμένους οργανισμούς της ΕΕ, η Αρχή INFOSEC είναι υπεύθυνη για τα εξής:

— παροχή τεχνικών συμβουλών και τεχνικής επικουρίας στην ΑΠΑ,

— συμβολή στην ανάπτυξη του SSRS,

— επανεξέταση του SSRS για να εξασφαλίζεται αντιστοιχία προς τους παρόντες κανονισμούς ασφαλείας και τις πολιτικές και τα έγγραφα αρχιτεκτονικής INFOSEC

— συμμετοχή στις ομάδες/συμβούλια διαπίστευσης κατά περίπτωση, και διατύπωση συστάσεων INFOSEC προς την ΑΠΑ όσον αφορά τη διαπίστευση,

— υποστήριξη των δραστηριοτήτων κατάρτισης και εκπαίδευσης INFOSEC,

— παροχή τεχνικών συμβουλών κατά τη διερεύνηση περιστατικών που σχετίζονται με την INFOSEC,

— κατάρτιση οδηγιών τεχνικής πολιτικής για να εξασφαλίζεται ότι χρησιμοποιείται μόνον εγκεκριμένο λογισμικό.

ΕΠΙΧΕΙΡΗΣΙΑΚΗ ΑΡΧΗ ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ (ITSOA)

38. Η Αρχή INFOSEC μεταβιβάζει, το συντομότερο δυνατόν, την αρμοδιότητα για την εφαρμογή και τη λειτουργία των ελέγχων και των ειδικών μέτρων ασφαλείας του συστήματος στην επιχειρησιακή αρχή συστημάτων πληροφορικής (ITSOA). Η αρμοδιότητα αυτή ισχύει καθ' όλη τη διάρκεια του κύκλου ζωής του συστήματος, από το στάδιο του βασικού σχεδιασμού μέχρι την τελική διάθεση.

39. Η ITSOA είναι υπεύθυνη για όλα τα μέτρα ασφαλείας που σχεδιάζονται ως μέρη του συνολικού συστήματος Η ευθύνη αυτή περιλαμβάνει την εκπόνηση των SecOP. Η ITSOA ορίζει τα πρότυπα και τις πρακτικές ασφαλείας προς τα οποία πρέπει να συμμορφούται ο προμηθευτής του συστήματος.

40. Η ITSOA μπορεί, να μεταβιβάζει μέρος της αρμοδιότητας της, κατά περίπτωση, π.χ. στον υπάλληλο ασφαλείας INFOSEC και στον επιτόπου υπάλληλο ασφαλείας INFOSEC Τα διάφορα καθήκοντα INFOSEC είναι δυνατόν να εκτελούνται από το ίδιο άτομο.

ΧΡΗΣΤΕΣ

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

ΚΑΤΑΡΤΙΣΗ INFOSEC

42. Εντός της ΓΤΣ, των αποκεντρωμένων οργανισμών της ΕΕ ή των υπουργείων των κρατών μελών, κατά περίπτωση, παρέχονται εκπαίδευση και κατάρτιση INFOSEC σε διάφορα επίπεδα και για διάφορες βαθμίδες προσωπικού.

Κεφάλαια IV

Μη τεχνικά μέτρα ασφάλειας

ΑΣΦΑΛΕΙΑ ΠΡΟΣΩΠΙΚΟΥ

43. Οι χρήστες του συστήματος διαβαθμίζονται και έχουν «ανάγκη γνώσης» ανάλογα με τη διαβάθμιση και το περιεχόμενο των πληροφοριών που διεκπεραιώνουν στο 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 του Συμβουλίου

44. Η ΑΠΑ καθόριζα όλες τις ευαίσθητες θέσεις και ορίζει το βαθμό διαβάθμισης και εποπτείας που απαιτείται για το σχετικό προσωπικό.

45. 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 βασικών σημείων ασφαλείας του συστήματος ούτως ώστε να απαιτείται η συνεργία δύο ή περισσότερων ατόμων για την αλλοίωση ή τη σκόπιμη υποβάθμιση του συστήματος ή του δικτύου.

ΥΛΙΚΗ ΑΣΦΑΛΕΙΑ

46. Οι χώροι υπολογιστών και ανεξάρτητων τερματικών/σταθμών εργασίας (όπως ορίζονται στις παραγράφους 29 και 30), όπου διεκπεραιώνονται, με υπολογιστή, πληροφορίες με διαβάθμιση τουλάχιστον CONFIDENTIEL UE, ή όπου είναι δυνατή η πρόσβαση σε παρόμοιες πληροφορίες συγκρατούνται ως ζώνες ασφαλείας κατηγορίας Ι ή ΙΙ ΕΕ ή ισοδύναμης εθνικής κατηγορίας κατά περίπτωση

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

ΕΛΕΓΧΟΣ ΤΗΣ ΠΡΟΣΒΑΣΗΣ ΣΕ ΕΝΑ ΣΥΣΤΗΜΑ

48. 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.

49. Όταν δεν χρησιμοποιούνται πλέον για το σκοπό αυτόν, οι πληροφορίες και το υλικό ελέγχου της πρόσβασης καταστρέφονται σύμφωνα με τις παραγράφους 61 έως 63

Κεφάλαιο V

Τεχνικά μέτρα ασφάλειας

ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΩΝ

50. Ο συντάκτης των πληροφοριών πρέπει να προσδιορίζει και να διαβαθμίζει τα έγγραφα που περιέχουν πληροφορίες, είτε πρόκειται για τυπωμένα έγγραφα είτε για πληροφορικά υποθέματα αποθήκευσης. Η διαβάθμιση πρέπει να αναγράφεται στο άνω και το κάτω μέρος κάθε σελίδας τυπωμένου εγγράφου Τα παραγόμενα έγγραφα, είτε είναι τυπωμένα είτε είναι υποθέματα αποθήκευσης υπολογιστή, πρέπει να έχουν την ίδια διαβάθμιση με την ανώτερη διαβάθμιση των πληροφοριών που χρησιμοποιούνται για την παραγωγή τους. Ο τρόπος λειτουργίας ενός ΣΥΣΤΗΜΑΤΟΣ ενδέχεται να επηρεάζει τη διαβάθμιση των εγγράφων που παράγονται με αυτό.

51. Ένας οργανισμός και οι κάτοχοι πληροφοριών του πρέπει να εξετάζουν τα προβλήματα σώρευσης επιμέρους στοιχείων πληροφοριών και των συμπερασμάτων που είναι δυνατόν να αντληθούν από τα συσχετιζόμενα στοιχεία, και να αποφασίζουν εάν είναι σκόπιμα να διαβαθμίζεται το σύνολο πληροφοριών με υψηλότερο βαθμό ασφαλείας.

52 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

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

54. Ο χειρισμός όλων των πληροφορικών υποθεμάτων αποθήκευσης πρέπει να είναι ανάλογος προς την ανώτερη διαβάθμιση των αποθηκευμένων πληροφοριών ή την ετικέτα του υποθέματος, πρέπει δε να προστατεύονται πάντοτε καταλλήλως

55. Τα επαναχρησιμοποιήσιμα υποθέματα αποθήκευσης υπολογιστών που χρησιμοποιούνται για την αποθήκευση διαβαθμισμένων πληροφοριών ΕΕ διατηρούν την ανώτερη διαβάθμιση για την οποία χρησιμοποιήθηκαν ποτέ μέχρις ότου οι πληροφορίες αυτές υποχαρακτηριστούν ή αποχαρακτηριστούν και τα υποθέματα αναχαρακτηριστούν ανάλογα, ή τα υποθέματα αποχαρακτηριστούν και καταστραφούν σύμφωνα με εγκεκριμένη διαδικασία της ΙΤΣ ή εθνική διαδικασία (βλέπε παραγράφους 61 έως 63).

ΕΛΕΓΧΟΣ ΠΛΗΡΟΦΟΡΙΩΝ ΚΑΙ ΣΧΕΤΙΚΕΣ ΕΥΘΥΝΕΣ

56. Η πρόσβαση σε πληροφορίες με διαβάθμιση τουλάχιστον SECRET UE καταχωρείται σε αυτόματα (ίχνη ελέγχου) ή χειρόγραφα μητρώα. Τα μητρώα αυτά διατηρούνται σύμφωνα με τους προκειμένους κανονισμούς ασφαλείας.

57. 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 διαβάθμισης του και ελέγχεται κατάλληλα.

58. Όταν από σύστημα που διεκπεραιώνει διαβαθμισμένες πληροφορίες ΕΕ παράγονται έγγραφα που διαβιβάζονται σε ανεξάρτητο τερματικό/σταθμό εργασίας σε χώρο υπολογιστών, θεσπίζονται διαδικασίες εγκεκριμένες από την ΑΠΑ, για τον έλεγχο των εγγράφων που παράγονται στο ανεξάρτητο τερματικό/σταθμό εργασίας Για τα υλικά με διαβάθμιση τουλάχιστον SECRET UE, οι διαδικασίες αυτές περιλαμβάνουν συγκεκριμένες οδηγίες για το άτομο που είναι υπεύθυνο για τις πληροφορίες αυτές.

ΧΕΙΡΙΣΜΟΣ ΚΑΙ ΕΛΕΓΧΟΣ ΑΦΑΙΡΕΤΩΝ ΠΛΗΡΟΦΟΡΙΚΩΝ ΥΠΟΘΕΜΑΤΩΝ ΑΠΟΘΗΚΕΥΣΗΣ

59. Όλα τα αφαιρετά πληροφορικά υποθέματα αποθήκευσης με διαβάθμιση τουλάχιστον CONFIDENTIEL UE πρέπει να αντιμετωπίζονται σαν υλικό και υπόκεινται στους γενικούς κανόνες Οι κατάλληλες επισημάνσεις αναγνώρισης και διαβάθμισης πρέπει να είναι προσαρμοσμένες στη συγκεκριμένη υλική μορφή των υποθεμάτων, ώστε να είναι δυνατή η σαφής αναγνώρισή τους

60. Οι χρήστες πρέπει να φροντίζουν ότι οι διαβαθμισμένες πληροφορίες ΕΕ αποθηκεύονται σε υποθέματα με την κατάλληλη επισήμανση διαβάθμισης και προστασία. Θα θεσπιστούν διαδικασίες για να εξασφαλίζεται ότι, για όλα τα επίπεδα των πληροφοριών ΕΕ, οι πληροφορίες αποθηκεύονται σε πληροφορικά υποθέματα αποθήκευσης σύμφωνα με τους προκείμενους κανονισμούς ασφαλείας

ΑΠΟΧΑΡΑΚΤΗΡΙΣΜΟΙ ΚΑΙ ΚΑΤΑΣΤΡΟΦΗ ΥΠΟΘΕΜΑΤΩΝ ΑΠΟΘΗΚΕΥΣΗΣ ΥΠΟΛΟΓΙΣΤΩΝ

61. Τα πληροφορικά υποθέματα αποθήκευσης που χρησιμοποιούνται για την καταγραφή διαβαθμισμένων πληροφοριών ΕΕ μπορούν να υποχαρακτηρίζονται ή να αποχαρακτηρίζονται εφόσον εφαρμόζονται εγκεκριμένες διαδικασίες της ΓΤΣ ή εθνικές διαδικασίες

62. Τα πληροφορικά υποθέματα αποθήκευσης στα οποία είχαν αποθηκευθεί πληροφορίες TRÈS SECRET UE/EU TOP SECRET ή ειδικής κατηγορίας δεν αποχαρακτηρίζονται προς επαναχρησιμοποίηση

63. Εάν τα πληροφορικά υποθέματα αποθήκευσης δεν είναι δυνατόν να αποχαρακτηριστούν ή δεν είναι επαναχρησιμοποιήσιμα, καταστρέφονται σύμφωνα με εγκεκριμένη διαδικασία της ΓΤΣ ή εθνική διαδικασία.

ΑΣΦΑΛΕΙΑ ΕΠΙΚΟΙΝΩΝΙΩΝ

64. Όταν διαβαθμισμένες πληροφορίες ΕΕ διαβιβάζονται με ηλεκτρομαγνητικά μέσα, λαμβάνονται ειδικά μέτρα για να προστατεύεται η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα των διαβιβαζόμενων πληροφοριών. Η ΑΠΑ 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.

65. Όταν απαιτούνται κρυπτογραφικές μέθοδοι για να εξασφαλίζεται η προστασία της εμπιστευτικότητας της ακεραιότητας και της διαθεσιμότητας οι μέθοδοι αυτές ή τα σχετικά προϊόντα εγκρίνονται ειδικά για το σκοπό αυτόν από την ΑΠΑ.

66. Κατά τη διαβίβαση, η εμπιστευτικότητα των πληροφοριών με διαβάθμιση τουλάχιστον SECRET UE προστατεύεται με κρυπτογραφικές μεθόδους ή προϊόντα που εγκρίνει το Συμβούλιο βάσει σχετικής συστάσεως της Επιτροπής Ασφαλείας του Συμβουλίου. Κατά τη διαβίβαση, η εμπιστευτικότητα των πληροφοριών με διαβάθμιση CONFIDENTIEL UE ή RESTREINT UE προστατεύεται με κρυπτογραφικές μεθόδους ή προϊόντα που εγκρίνονται, είτε από τον ΓΤ/ΥΕ βάσει σχετικής συστάσεως της Επιτροπής Ασφαλείας του Συμβουλίου είτε από κράτος μέλος

67. Σε ειδικές οδηγίες ασφαλείας που εγκρίνονται από το Συμβούλιο βάση σχετικής συστάσεως της Επιτροπής Ασφαλείας του Συμβουλίου καθορίζονται λεπτομερείς κανόνες για τη διαβίβαση διαβαθμισμένων πληροφοριών ΕΕ.

68. Υπό εξαιρετικές επιχειρησιακές περιστάσεις πληροφορίες με διαβάθμιση RESTREINT UE, CONFIDENTIEL UE και SECRET UE επιτρέπεται να διαβιβάζονται ακρυπτογράφητες υπό την προϋπόθεση ότι χορηγείται ρητή άδεια για κάθε περίπτωση. Οι εξαιρετικές αυτές περιστάσεις είναι οι εξής:

α) κατά τις καταστάσεις επικείμενης ή πραγματικής κρίσης σύγκρουσης ή πολφού και

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

69. Ένα σύστημα πρέπει να έχει τη δυνατότητα να απαγορεύει ρητά την πρόσβαση σε διαβαθμισμένες πληροφορίες ΕΕ μέσω οποιουδήποτε ή όλων των ανεξάρτητων σταθμών εργασίας ή τερματικών του, όταν απαιτείται, είτε με υλική αποσύνδεση είτε μέσω ειδικών χαρακτηριστικών του λογισμικού που εγκρίνονται από την ΑΠΑ.

ΕΓΚΑΤΑΣΤΑΣΗ ΚΑΙ ΑΣΦΑΛΕΙΑ ΑΚΤΙΝΟΒΟΛΙΩΝ

70. Η αρχική εγκατάσταση και οι σημαντικές αλλαγές των συστημάτων καθορίζονται κατά τρόπον ώστε η εγκατάσταση να πραγματοποιείται από εγκαταστάτες με διαβάθμιση ασφαλείας υπό τη συνεχή εποπτεία προσωπικού με τα δέοντα τεχνικά προσόντα το οποίο είναι διαβαθμισμένα για πρόσβαση σε διαβαθμισμένες πληροφορίες ΕΕ μέχρις επιπέδου που ισοδυναμεί προς την ανώτερη διαβάθμιση των πληροφοριών που θα αποθηκεύει και θα χειρίζεται το σύστημα.

71. Όλος ο εξοπλισμός εγκαθίσταται σύμφωνα με την τρέχουσα πολιτική περί ασφαλείας του Συμβουλίου.

72. Τα συστήματα που χειρίζονται πληροφορίες με διαβάθμιση τουλάχιστον CONFIDENTIEL UE προστατεύονται κατά τρόπον ώστε η ασφάλειά τους να μην απειλείται από διαρρέουσες εκπομπές, η μελέτη και ο έλεγχος των οποίων αναφέρονται ως «TEMPEST»

73. Τα αντίμετρα TEMPEST της ΓΤΣ και των αποκεντρωμένων οργανισμών της ΕΕ εξετάζονται και εγκρίνονται από αρχή TEMPEST που ορίζεται από την Αρχή Ασφαλείας της ΓΤΣ Για τις εθνικές εγκαταστάσεις οι οποίες χειρίζονται διαβαθμισμένες πληροφορίες ΕΕ, εγκρίνουσα αρχή είναι η αναγνωρισμένη εθνική εγκρίνουσα αρχή TEMPEST.

Κεφάλαιο *VI*

Ασφάλεια κατά το χειρισμό

ΑΣΦΑΛΕΙΣ ΔΙΑΔΙΚΑΣΙΕΣ ΛΕΙΤΟΥΡΓΙΑΣ

74. Οι SecOP καθορίζουν τις αρχές που πρέπει να θεσπίζονται για θέματα ασφαλείας, τις ακολουθητέες διαδικασίες λειτουργίας και τις ευθύνες του προσωπικού. Οι SecOP εκπονούνται υπό την ευθύνη της Αρχής Λειτουργίας του Συστήματος Πληροφορικής.

ΠΡΟΣΤΑΣΙΑ ΛΟΓΙΣΜΙΚΟΥ/ΔΙΑΧΕΙΡΙΣΗ ΔΙΑΜΟΡΦΩΣΗΣ

75. 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 τακτικά για να εξασφαλίζεται η ακεραιότητά τους και η ορθή λειτουργία τους

76. Νέες ή τροποποιημένες εκδόσεις λογισμικού δεν πρέπει να χρησιμοποιούνται για το χειρισμό διαβαθμισμένων πληροφοριών ΕΕ πριν ελεγχθούν από την ΙΤSOA.

ΕΛΕΓΧΟΣ ΠΑΡΟΥΣΙΑΣ ΔΟΛΙΟΥ ΛΟΓΙΣΜΙΚΟΥ/ΠΛΗΡΟΦΟΡΙΚΩΝ ΙΩΝ

77. Ο έλεγχος της παρουσίας δόλιου λογισμικού/πληροφορικών ιών διενεργείται τακτικά σύμφωνα με τις απαιτήσεις της ΑΠΑ.

78. Πριν εισαχθούν σε οποιοδήποτε σύστημα, όλα τα πληροφορικά υποθέματα αποθήκευσης που διαβιβάζονται στη ΓΤΣ ή στους αποκεντρωμένους οργανισμούς της ΕΕ πρέπει να ελέγχονται για την παρουσία τυχόν δόλιου λογισμικού ή πληροφορικών ιών.

ΣΥΝΤΗΡΗΣΗ

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

80. Οι απαιτήσεις πρέπει να αναφέρονται σαφώς στην SSRS, οι δε διαδικασίες πρέπει να αναφέρονται σαφώς στις SecOP. 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 ΑΠΑ.

Κεφάλαιο VII

ΠΡΟΜΗΘΕΙΕΣ

81. Κάθε προϊόν ασφαλείας, το οποίο πρόκειται να αγοραστεί για να χρησιμοποιηθεί με το σύστημα, πρέπει είτε να έχει αξιολογηθεί και πιστοποιηθεί , είτε να τελεί ήδη υπό αξιολόγηση και έγκριση από αρμόδιο φορέα αξιολόγησης ή πιστοποίησης βάσει διεθνώς αναγνωρισμένων κριτηρίων (π.χ. των Κοινών Κριτηρίων για την Αξιολόγηση της Ασφαλείας της Πληροφορικής Τεχνολογίας βλέπε ISO 15408).

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

ΕΓΚΡΙΣΗ ΛΕΙΤΟΥΡΓΙΑΣ

83. Πριν χειριστούν διαβαθμισμένες πληροφορίες ΕΕ, όλα το συστήματα για τα οποία έχει εκπονηθεί SSRS λαμβάνουν έγκριση λειτουργίας από την ΑΠΑ βάσει των πληροφοριών που περιέχονται στη SSRS, στις SecOP ή σε κάθε άλλο σχετικό έγγραφο. Τα υποσυστήματα και τα ανεξάρτητα τερματικά/σταθμοί εργασίας λαμβάνουν έγκριση λειτουργίας ως μέρη όλων των συστημάτων με τα οποία συνδέονται. Όταν ένα σύστημα χρησιμοποιείται τόσο από το Συμβούλιο όσο και από άλλους οργανισμούς η ΓΤΣ και οι αρμόδιες Αρχές Ασφαλείας πρέπει να συμφωνούν μεταξύ τους για την έγκριση λειτουργίας.

84. Η διαδικασία έγκρισης λειτουργίας μπορεί να διεξάγεται σύμφωνα με μια σχετική στρατηγική που είναι κατάλληλη για το συγκεκριμένο ΣΥΣΤΗΜΑ, που καθορίζεται από την ΑΠΑ.

ΑΞΙΟΛΟΓΗΣΗ ΚΑΙ ΠΙΣΤΟΠΟΙΗΣΗ

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

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

87. 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 της ΙΤSOA.

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

89. Ο βαθμός των συγκεκριμένων διαδικασιών αξιολόγησης και πιστοποίησης μπορεί να μειώνεται (ώστε να καλύπτουν π χ. μόνον θέματα συνολοκλήρωσης) όταν τα συστήματα βασίζονται σε υφιστάμενα προϊόντα ασφαλείας υπολογιστών τα οποία αξιολογούνται και πιστοποιούνται σε εθνικό επίπεδο.

ΤΑΚΤΙΚΟΣ ΕΛΕΓΧΟΣ ΤΩΝ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ ΓΙΑ ΤΗ ΔΙΑΤΗΡΗΣΗ ΤΗΣ ΕΓΚΡΙΣΗΣ ΛΕΙΤΟΥΡΓΙΑΣ

90. Η ΙΤSOA εκπονεί διαδικασίες τακτικού ελέγχου οι οποίες εξασφαλίζουν ότι εξακολουθούν να ισχύουν όλα τα χαρακτηριστικά ασφαλείας του συστήματος.

91. Το είδος αλλαγών για τις οποίες απαιτείται νέα έγκριση λειτουργίας ή προηγούμενη έγκριση της ΑΠΑ, προσδιορίζεται και αναφέρεται σαφώς στην SSRS. Ύστερα από κάθε τροποποίηση, επισκευή ή βλάβη που ενδέχεται να έχει θίξει τα χαρακτηριστικά ασφαλείας του συστήματος, η ΙΤSOA φροντίζει να διενεργείται έλεγχος προκειμένου να εξασφαλίζεται η ορθή λειτουργία των χαρακτηριστικών ασφαλείας Η διατήρηση της έγκρισης λειτουργίας του συστήματος **εξαρτάται** κανονικά από την ικανοποιητική διεξαγωγή των ελέγχων.

92. Όλα τα συστήματα στα οποία λειτουργούν χαρακτηριστικά ασφαλείας επιθεωρούνται ή εξετάζονται τακτικά από την ΑΠΑ. Για τα συστήματα που χαρίζονται πληροφορίες TRES SECRET UE/EU TOP SECRET ή πληροφορίες με πρόσθετες επισημάνσεις, οι επιθεωρήσεις διεξάγονται τουλάχιστον μια φορά το χρόνο.

Κεφάλαιο VIII

Προσωρινή ή περιστασιακή χρήση

ΑΣΦΑΛΕΙΑ ΜΚΡΟΫΠΟΛΟΓΙΣΤΩΝ/ΠΡΟΣΩΠΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

93. 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 (πχ. φορητοί PC και ηλεκτρονικά «σημειωματάρια») με σταθερούς σκληρούς δίσκους θεωρούνται ως υποθέματα αποθήκευσης πληροφοριών όπως και οι δισκέτες ή τα άλλα αφαιρετά υποθέματα αποθήκευσης

94. 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 υπό-χαρακτηριστούν ή αποχαρακτηριστούν σύμφωνα με εγκεκριμένες διαδικασίες).

ΧΡΗΣΗ ΙΔΙΩΤΙΚΩΝ ΣΥΣΚΕΥΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΠΑ ΕΠΙΣΗΜΕΣ ΕΡΓΑΣΙΕΣ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ

95. Απαγορεύεται η χρήση ιδιωτικών αφαιρετών πληροφορικών υποθεμάτων αποθήκευσης, λογισμικού και υλικού πληροφορικής (π χ PC και φορητών υπολογιστικών συσκευών) με δυνατότητα αποθήκευσης για το χειρισμό διαβαθμισμένων πληροφοριών ΕΕ.

96. Απαγορεύεται η εισαγωγή ιδιωτικού υλικού υπολογιστών, λογισμικού και υποθεμάτων σε χώρους κατηγορίας I ή II όπου γίνεται χειρισμός διαβαθμισμένων πληροφοριών ΕΕ χωρίς την άδεια του προϊσταμένου της υπηρεσίας Ασφαλείας της ΓΤΣ ή ενός υπουργείου κράτους μέλους ή του αντίστοιχου αποκεντρωμένου οργανισμού της ΕΕ.

ΧΡΗΣΗ ΣΥΣΚΕΥΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΠΟΥ ΑΝΗΚΟΥΝ ΣΕ ΕΡΓΟΛΑΒΟΥΣ Ή ΠΟΥ ΠΑΡΕΧΟΝΤΑΙ ΑΠΟ ΕΘΝΙΚΕΣ ΑΡΧΕΣ ΠΑ ΕΠΙΣΗΜΕΣ ΕΡΓΑΣΙΕΣ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ

97. Η χρήση συσκευών πληροφορικής και λογισμικού που ανήκουν σε εργολάβους σε οργανώσεις προς υποστήριξη επίσημων εργασιών του Συμβουλίου μπορεί να επιτρέπεται από τον προϊστάμενο της Υπηρεσίας Ασφαλείας της ΓΤΣ ή ενός υπουργείου κράτους μέλους ή του αντίστοιχου αποκεντρωμένου οργανισμού της ΕΕ. Είναι δυνατόν επίσης να επιτρέπεται η χρήση, από υπαλλήλους της ΓΤΣ ή ενός αποκεντρωμένου οργανισμού της ΕΕ, συσκευών πληροφορικής και λογισμικού που παρέχονται από αρχή κράτους μέλους στην περίπτωση αυτήν, οι συσκευές πληροφορικής καταχωρούνται στον κατάλληλο κατάλογο της ΓΤΣ. Και στις δύο περιπτώσεις, εάν οι συσκευές πληροφορικής πρόκειται να χρησιμοποιηθούν για το χειρισμό διαβαθμισμένων πληροφοριών ΕΕ, πρέπει να ζητείται η γνώμη της αρμόδιας ΑΠΑ ώστε να λαμβάνονται δεόντως υπόψη και να εφαρμόζονται τα στοιχεία INFOSEC του ισχύουν για τη χρήση των συσκευών αυτών.

ΤΜΗΜΑ XII

ΚΟΙΝΟΠΟΙΗΣΗ ΔΙΑΒΑΘΜΙΣΜΕΝΩΝ ΠΛΗΡΟΦΟΡΙΩΝ ΕΕ ΣΕ ΤΡΙΤΑ ΚΡΑΤΗ Ή ΔΙΕΘΝΕΙΣ ΟΡΓΑΝΙΣΜΟΥΣ

ΑΡΧΕΣ ΠΟΥ ΔΙΕΠΟΥΝ ΤΗΝ ΚΟΙΝΟΠΟΙΗΣΗ ΔΙΑΒΑΘΜΙΣΜΕΝΩΝ ΠΛΗΡΟΦΟΡΙΩΝ ΕΕ

1. Η κοινοποίηση διαβαθμισμένων πληροφοριών ΕΕ σε τρίτα κράτη ή διεθνείς οργανισμούς αποφασίζεται από το Συμβούλιο βάσει.

   — της φύσης και του περιεχομένου των πληροφοριών αυτών,

   — της ανάγκης γνώσης του αποδέκτη,

   — των πλεονεκτημάτων για την ΕΕ.

   Ζητάται η συμφωνία του κράτους μέλους που συνέταξε τις προς κοινοποίηση διαβαθμισμένες πληροφορίες ΕΕ

2. 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 συνεπή εφαρμογή των κανόνων ασφαλείας τους και των κανόνων ασφαλείας της ΕΕ η Επιτροπή Ασφαλείας του Συμβουλίου δίνει στο Συμβούλιο τεχνική γνώμη για το θέμα αυτό.

3. 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 το Συμβούλιο.

ΕΠΙΠΕΔΑ

4. Όταν το Συμβούλιο αποφασίσει άτι 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.

5. 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.

6. Σε κάθε επίπεδο συνεργασίας καθορίζονται οι κανονισμοί ασφαλείας αναδιατυπωμένοι στις επιμέρους περιπτώσεις βάσει της τεχνικής γνώμης της Επιτροπής Ασφαλείας του Συμβουλίου, τους οποίους θα πρέπει να εφαρμόζουν οι δικαιούχοι για την προστασία των διαβαθμισμένων πληροφοριών που τους κοινοποιούνται. Αυτές οι διαδικασίες και κανονισμοί ασφαλείας εκτίθενται στα προσαρτήματα 4, 5 και 6

ΣΥΜΦΩΝΙΕΣ

7. Όταν το Συμβούλιο αποφασίσει ότι υπάρχει μόνιμη ή μακροχρόνια ανάγκη ανταλλαγής διαβαθμισμένων πληροφοριών μεταξύ της ΕΕ 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.

8. Στην περίπτωση της συνεργασίας επιπέδου 3, η οποία, εξ ορισμού, έχει περιορισμένη χρονική διάρκεια και σκοπό, αντί της «συμφωνίας για διαδικασίες ασφαλώς 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 RESTREINT UE.

9. Πριν υποβληθούν προς έγκριση στο Συμβούλιο, τα σχέδια συμφωνιών για τις διαδικασίες ασφαλώς ή τα μνημόνια συμφωνίας εγκρίνονται από την Επιτροπή Ασφαλείας.

10. Οι εθνικές αρχές ασφαλείας παρέχουν στο Γενικό Γραμματέα/Ύπατο Εκπρόσωπο κάθε απαιτούμενη βοήθεια ώστε 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.

Προσάρτημα 1

Κατάλογος των εθνικών αρχών ασφάλειας

ΒΕΛΓΙΟ

Ministère des Affaires Etrangères, du Commerce Extérieur et de la Coopération au Développement
Direction de la sécurité — A 01
Rue des Petits Cannes, 15
B-1000 Bruxelles
Τηλέφωνο: 32-2-501 85 14
Φαξ 32-2-501 80 58
Τέλεξ. 21376
Τηλεγραφική διεύθυνση: Direction de Sécunté A01 — MINAFET

ΔΑΝΙΑ

Politiets Efterretningstjeneste
Borups Alle 266
DK-2400 Copenhagen NV
Τηλέφωνο: 45 33 14 88 88
Φαξ: 45 38 19 07 05

Forsvarsministeriet
Forsvarets Efterretningstjeneste
Kastellet 30
DK-2100 Copenhagen Ø
Τηλέφωνο 45 33 32 55 66
Φαξ: 45 33 93 13 20

ΓΕΡΜΑΝΙΑ

Bundesministenum des Innern
Referat IS 4
Alt-Moabit 101D
D-10559 Berlin
Τηλέφωνο 49-30-39 81 15 28
Φαξ: 49-30-39 81 16 10

ΕΛΛΑΣ

Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ)
Υπηρεσία Στρατιωτικών Πληροφοριών (ΥΣΠ - Β' Κλάδος)
Γραφείο Ασφάλειας
ΣΤΓ 1020 Χολαργός (Αθήνα)
Ελλάδα
Τηλέφωνα. 00 30-1-655 22 03 (ώρες γραφείου)
00 30-1-655 22 05 (εικοσιτετράωρο)
Φαξ 00 30-1-642 69 40

Hellenic National Defence
General Staff (HNDGS)
Intelligence Branch/Security
(INT. BR./SEC)
STG 1020, Holargos — Athens
Greece
Telephone. 00 30-1-655 22 03 (office hours)
00 30-1-655 22 05 (24 hours)
Fax: 00 30-1-642 69 40

ΙΣΠΑΝΙΑ

Autoridad Nacional de Segundad
Oficina Nacional de Seguridad
Avenida Padre Huidobro s/n
Carretera Nacional Radial VI, km 8,500
E-28023 Madnd
Τηλέφωνο 34-91-372 57 07
Φαξ 34-91-372 58 08
E-mail: nsa-sp@areatec.com

ΓΑΛΛΙΑ

Secrétariat général de la Défense Nationale
Service de Sécurité de Défense (SGDN/SSD)
51 Boulevard de la Tour-Maubourg
F-75700 Paris 07 SP
Τηλέφωνο: 33-0-144 18 81 80
Φαξ. 33-0-144 18 82 00
Τέλεξ: SEGEDEFNAT 200019
Τηλεγραφική διεύθυνση SEGEDEFNAT PARIS

ΙΡΛΑΝΔΙΑ

National Security Authority
Department of Foreign Affairs
80 St Stephens Green
Dublin 2
Τηλέφωνο: 353-1-478 08 22
Φαξ: 353-1-478 14 84

ΙΤΑΛΙΑ

Presidenza del Consiglio dei Ministri
Autorità Nazionale per la Sicurezza
Ufficio Centrale per la Sicurezza
Via della Pineta Sacchetti, 216
1-00168 Roma
Τηλέφωνο: 39-06-627 47 75
Φαξ: 39-06-614 33 97
Τέλεξ: 623376 AQUILA 1
Τηλεγραφική διεύθυνση: ess: PCM-ANS-UCSI-ROMA

ΛΟΥΞΕΜΒΟΥΡΓΟ

Autorité Nationale de Sécurité
Ministère d'Etat
Boîte Postale 2379
L-1023 Luxembourg
Τηλέφωνο: 352-478 22 10 (κέντρο)
352-478 22 35 (απευθείας γραμμή)
Φαξ. 352-478 22 43 352-478 22 71
Τέλεξ: 3481 SERET LU
Τηλεγραφική διεύθυνση· MIN D'ETAT — ANS

ΚΑΤΩ ΧΩΡΕΣ

Ministerie van Binnenlandse Zaken
Postbus 20010
NL-2500 EA Den Haag
Τηλέφωνο: 31-70-320 44 00
Φαξ: 31-70-320 07 33
Τελεξ: 32166 SYTH NL

Ministene van Defensie
Militaire Inlichtingendienst (MID)
Postbus 20701
NL-2500 ES Den Haag
Τηλέφωνο: 31-70-318 70 60
Φαξ: 31-70-318 79 51

ΑΥΣΤΡΙΑ

Bundesministerium fur auswärtige Angelegenheiten
Abteilung I 9
Ballhausplatz 2
A-1014 Wien
Τηλέφωνο: 43-1-531 15 34 64
Φαξ. 43-1-531 8 52 19

ΠΟΡΤΟΓΑΛΙΑ

Presidência do Conselho de Ministros
Autoridade Nacional de Segurança
Avenida Ilha da Madeira, 1
P-1449-004 Lisboa
Τηλέφωνο: 351-21-301 55 10
351-21-301 00 01, εσωτερικό 20 45 37
Φαξ: 351-21-302 03 50

ΦΙΝΛΑΝΔΙΑ

Alivaltiosihteeri (Hallinto)/Understatssekreteraren (Administration)
Ulkoasiainministenö/Utrikesmmisteniet
Laivastokatu/Maringatan 22
PL/PB 176
FIN-00161 Helsinki/Helsingfors
Τηλέφωνο 358-9-13 41 53 38
Φαξ: 358-9-13 41 53 03

ΣΟΥΗΔΙΑ

Utrikesdepartementet
SSSB
S-103 39 Stockholm
Τηλέφωνο: 46-8-405 54 44
Φαξ: 46-8-723 11 76

ΗΝΩΜΕΝΟ ΒΑΣΙΛΕΙΟ

The Secretary (for DIR/5)
PO Box 5656
London ECIA 1 AH
Τηλέφωνα 44-20-72 70 87 51
Φαξ: 44-20-76 30 14 28
Τηλεγραφική διεύθυνση: UK Delegation to Security Policy Dept FCO, marked (in Box 5656 for DIR/5).

Προσάρτημα 2

Πίνακας των εθνικών διαβαθμίσεων ασφάλειας

Διαβάθμιση ΕΕ	Très secret UE/ EU TOP SECRET	Secret UE	Confidentiel UE	Restreint UE
Διαβάθμιση NATO (1)				
Διαβάθμιση WEU	Focal Top Secret	WEU Secret	WEU Confidentia	WEU Restricted
Γερμανία	STRENG GEHEIM	GEHEIM	VS(2) — VERTRAULICH	VS — NUR FÜR DEN DIENSTGEBRAUCH
Αυστρία	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Βέλγιο	Très Secret Zeer Geheim	Secret Geheum	Confidentiel Vertrouwelijk	Diffusion restreinte Beperkte Verspreiding
Δανία	Yderst Hemmeligt	Hemmeligt	Fortroligt	Til Tjenestebrug
Ισπανία	Secreto	Reservado	Confidencial	Difusion limitada
Φινλανδία	Erittain salainen	Erittäin salainen	Salainen	Luottamuksellinen
Γαλλία	Très Secret Défense (3)	Secret Defense	Confidentiel Défense	Diffusion restreinte
Ελλάδα	Άκρως Απόρρητο	Απόρρητο	Εμπιστευτικό	Περιορισμένης χρήσης
Ιρλανδία	Top Secret	Secret	Confidential	Restricted
Ιταλία	Segretissimo	Segreto	Riservatissimo	Riservato
Λουξεμβούργο	Très Secret	Secret	Confidentiel	Diffusion restreinte
Κάτω Χώρες	STG Zeer Geheim	STG Geheim	STG Confidentieel	
Πορτογαλία	Muito Secreto	Secreto	Confidencial	Reservado
Ηνωμένο Βασίλειο	Top Secret	Secret	Confidential	Restricted
Σουηδία	Kvalificerat hemlig	Hemlig	Hemlig	Hemlig

(1) NATO, η αντιστοιχία με τα επίπεδα διαβάθμισης του NATO θα καθοριστεί κατά τη διαπραγμάτευση της συμφωνίας ασφαλείας μεταξύ της Ευρωπαϊκής Ένωσης και *του* NATO
(2) Γερμανία VS = Verschlusssache.
(3) Γαλλία, η διαβάθμιση «Très Secret Defense», η οποία καλύπτει τις κυβερνητικές προτεραιότητες, μπορεί να αλλάξει μόνο με την έγκριση του Πρωθυπουργού

Προσάρτημα 3

Πρακτικός οδηγός διαβάθμισης

Ο παρακάτω οδηγός είναι απλώς ενδεικτικός και δεν μεταβάλλει τις διατάξεις ουσίας των τμημάτων II και III

Διαβάθμιση	πότε	πώς	επισημάνσεις	υποχαρακτηρισμός/αποχαρακτηρισμός/καταστροφή	
				ποιος	πότε
TRÈS SECRET UE/ EU TOP SECRET: Η διαβάθμιση αυτή εφαρμόζεται μόνο στις πληροφορίες και το υλικό, η άνευ αδείας κοινολόγηση των οποίων μπορεί να βλάψει σοβαρότατα τα ζωτικά συμφέροντα της Ευρωπαϊκής Ένωσης ή ενός ή περισσοτέρων κρατών μελών της. [Τμήμα II, § 1]	Όταν η διαρροή στοιχείων με διαβάθμιση TRÈS SECRET UE/EU TOP SECRET θα ήταν πιθανά. — να συνιστά άμεση απειλή για την εσωτερική σταθερότητα της ΟΕ ή κράτους μέλους της ή φίλης χώρας — να βλάψει σοβαρότατα τις σχέσης 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	Κράτη μέλη δεόντως εξουσιοδοτημένα πρόσωπα (συντάκτες) [Τμήμα III], § 4] ΓΤΣ. δεόντως εξουσιοδοτημένα πρόσωπα (συντάκτες) [Τμήμα III, § 4], ΓΤ/ΥΕ. Οι συντάκτες προσδιορίζουν ημερομηνία ή προθεσμία μετά την οποία μπορεί να υποχαρακτηριστεί ή να αποχαρακτηριστεί το περιεχόμενο Σε αντίθετη περίπτωση, επανεξετάζουν τα έγγραφα το αργότερο ανά πενταετία, ώστε να επιβεβαιώνεται ότι εξακολουθεί να είναι αναγκαία η αρχική διαβάθμιση [Τμήμα III, §10]	Η διαβάθμιση TRÈS SECRET UE/EU TOP SECRET επιτίθεται στα έγγραφα TRÈS SECRET UE/EU TOP SECRET, ενδεχομένως μαζί με την επισήμανση ESDP, με μηχανικά μέσα και ιδιοχείρως. [Τμήμα II. § 8] Οι διαβαθμίσεις EU εμφαίνονται στο κέντρο του άνω και του κάτω μέρους κάθε σελίδας κάθε σελίδα αριθμείται Κάθε έγγραφο φέρει αριθμό αναφοράς και ημερομηνία , ο δε αριθμός εμφαίνεται σε κάθε σελίδα. Εάν τα έγγραφα πρόκειται να διανεμηθούν σε πολλαπλά αντίτυπα, στην πρώτη σελίδα κάθε αντίτυπου αναγράφεται ο αριθμός αντιτύπου και ο ολικός αριθμός σελίδων και απαριθμούνται όλα τα παραρτήματα και τα συνημμένα. [Τμήμα VII § 1]	Αποκλειστικός υπεύθυνος για τον υποχαρακτηρισμό ή αποχαρακτηρισμό είναι ο συντάκτης του εγγράφου, ή ο ΙΤ/VE, οι οποίοι ενημερώνουν σχετικά τους μετέπειτα αποδέκτες στους οποίους έχουν απόστειλα ή κοινοποιήσει το έγγραφο. [Τμήμα VIII § 9] Τα έγγραφα TRÈS SECRET UE/EU TOP SECRET καταστρέφονται από την αρμόδια Κεντρική Γραμματεία ή υπογραμματεία. Κάθε καταστρεφόμενο έγγραφο πρέπει να καταγράφεται σε πρωτόκολλο καταστροφής, το οποίο υπογράφεται από τον ελεγκτικό υπάλληλο TRÈS SECRET UE/EU TOP SECRET και από τον υπάλληλο ο οποίος παρίσταται κατά την καταστροφή και ο οποίος πρέπει να έχει διαβάθμιση TRÈS 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. [Τμήμα VII § 31]	Καταστρέφονται τα υπεράριθμα αντίτυπα και τα έγγραφα που δεν χρειάζονται πια. [Τμήμα VII § 31] Τα έγγραφα TRÈS SECRET UE/EU TOP SECRET, καθώς και όλα τα διαβαθμισμένα απορρίμματα που προκύπτουν κατά τη σύνταξη των εγγράφων TRÈS SECRET UE/EU TOP SECRET, όπως κακέκτυπα αντίγραφα, σχέδια εγγράφων, δακτυλογραφημένα σημειώματα και καρμπόν, καταστρέφονται υπό την επίβλεψη υπάλληλου TRÈS SECRET UE/EU TOP SECRET, με καύση, πολτοποίηση, σχίσιμο σε λουρίδες ή καθ' οιονδήποτε άλλο τρόπο που τα μετατρέπει σε μη αναγνωρίσιμη και μη ανασυστάσιμη μορφή. [Τμήμα VII § 31]

Διαβάθμιση	πότε	πώς	επισημάνσεις	υποχαρακτηρισμός/αποχαρακτηρισμός/καταστροφή	
				ποιος	πότε
SECRET Η διαβάθμιση αυτή εφαρμόζεται μόνο στις πληροφορίες και το υλικό, η άνευ αδείας κοινολόγηση των οποίων μπορεί να βλάψει σοβαρά τα ζωτικά συμφέροντα της Ευρωπαϊκής Ένωσης ή ενός ή περισσοτέρων κρατών μελών της. [Τμήμα II, § 2]	Όταν η διαρροή στοιχείων με διαβάθμιση SECRET UE θα ήταν πιθανό — να οξύνει διεθνείς εντάσεις — να βλάψει σοβαρά 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, νομισματικά, δημοσιονομικά και εμπορικά συμφέροντα της ΕΕ ή των κρατών μελών	Κράτη μέλη: δεόντως εξουσιοδοτημένα πρόσωπα (συντάκτες) [Τμήμα III, § 2], ΓΤΣ και αποκεντρωμένοι οργανισμοί ΕΕ. δεόντως εξουσιοδοτημένα πρόσωπα (συντάκτες) (Τμήμα III § 2], Γενικοί Διευθυντές και ΙΤ/ΥΕ. Οι συντάκτες προσδιορίζουν ημερομηνία ή προθεσμία μετά την οποία μπορεί να υποχαρακτηριστεί ή να αποχαρακτηριστεί το περιεχόμενο. Σε αντίθετη περίπτωση, επανεξετάζουν τα έγγραφα το αργότερο ανά πενταετία, ώστε να επιβεβαιώνεται ότι εξακολουθεί να είναι αναγκαία η αρχική διαβάθμιση. [Τμήμα VII, §1]	Η διαβάθμιση SECRET UE επιτίθεται στα έγγραφα SECRET UE, ενδεχομένως μαζί με την επισήμανση ESDP με μηχανικά μέσα και ιδιοχείρως. [Τμήμα III, §8] Οι διαβαθμίσεις EU εμφαίνονται στο κέντρο του άνω και του κάτω μέρους κάθε σελίδας κάθε σελίδα αριθμείται Κάθε έγγραφο φέρει αριθμό αναφοράς και ημερομηνία, ο δε αριθμός εμφαίνεται σε κάθε σελίδα. Εάν τα έγγραφα πρόκειται να διανεμηθούν σε πολλαπλά αντίτυπα, στην πρώτη σελίδα κάθε αντιτύπου αναγράφεται ο αριθμός αντιτύπου και ο ολικός αριθμός σελίδων, και απαριθμούνται όλα τα παραρτήματα και τα συνημμένα. [Τμήμα VII § 1]	Αποκλειστικός υπεύθυνος για τον υποχαρακτηρισμό ή αποχαρακτηρισμό είναι ο συντάκτης του εγγράφου, ή ο ΓΤ/ΥΕ, οι οποίοι ενημερώνουν σχετικά τους μετέπειτα αποδέκτες στους οποίους έχουν αποστείλει ή κοινοποιήσει το έγγραφο [Τμήμα VII § 9] Τα έγγραφα **S**ecret UE καταστρέφονται από την αρμόδια για την παραγωγή τους γραμματεία, υπό την εποπτεία προσώπου με κατάλληλη διαβάθμιση ασφαλείας . Τα καταστρεφόμενα έγγραφα SECRET UE πρέπει να καταγράφονται σε υπογεγραμμένα πρωτόκολλα καταστροφής, τα οποία διατηρεί η Γραμματεία, μαζί με τα φύλλα διανομής επί τρία τουλάχιστον έτη. [Τμήμα VII § 3 2]	Καταστρέφονται τα υπεράριθμα αντίτυπα και τα έγγραφα που δεν χρειάζονται πια. [Τμήμα VII § 31] Τα έγγραφα SECRET UE, καθώς και όλα τα διαβαθμισμένα απορρίμματα που προκύπτουν κατά την σύνταξη των εγγράφων 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. [Τμήμα VII §§ 31,32]

Διαβάθμιση	πότε	πώς	επισημάνσεις	υποχαρακτηρισμός/αποχαρακτηρισμός/καταστροφή	
				ποιος	πότε
CONFIDENTIEL UE Η διαβάθμιση αυτή εφαρμόζεται μόνο στις πληροφορίες και το υλικό, η άνευ αδείας κοινολόγηση των οποίων μπορεί να βλάψει τα ζωτικά συμφέροντα της Ευρωπαϊκής Ένωσης ή ενός ή περισσοτέρων κρατών μελών της. [Τμήμα II, §3]	Όταν η διαρροή στοιχείων με διαβάθμιση 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 επιχειρησιακή αποτελεσματικότητα ή την ασφάλεια των δυνάμεων κρατών μελών ή άλλων εισφερόντων, ή την αποτελεσματικότητα πολύτιμων ενεργειών ασφαλείας 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	Κράτη μέλη: δεόντως εξουσιοδοτημένα πρόσωπα (συντάκτες) [Τμήμα III, § 2], ΓΤΣ και αποκεντρωμένοι οργανισμοί ΕΕ: δεόντως εξουσιοδοτημένα πρόσωπα (συντάκτες) [Τμήμα III, § 2], Γενικοί Διευθυντές και ΙΤ/ΥΕ. Οι συντάκτες προσδιορίζουν ημερομηνία ή προθεσμία μετά την οποία μπορεί να υποχαρακτηριστεί ή να αποχαρακτηριστεί το περιεχόμενο. Σε αντίθετη περίπτωση, επανεξετάζουν τα έγγραφα το αργότερο ανά πενταετία, ώστε να επιβεβαιώνεται ότι εξακολουθώ να είναι αναγκαία η αρχική διαβάθμιση [Τμήμα III, §10]	Η διαβάθμιση CONFIDENTIEL UE επιτίθεται στα *έγγραφα* CONFIDENTIEL UE. ενδεχομένως μαζί με την επισήμανση ESDP, με μηχανικά μέσα και ιδιοχείρως, ή με εκτύπωση σε ήδη σφραγισμένο και πρωτοκολλημένο χαρτί [Τμήμα II, § 8] Οι διαβαθμίσεις EU εμφαίνονται στο κέντρο του άνω και του κάτω μέρους κάθε σελίδας κάθε σελίδα αριθμείται. Κάθε έγγραφο φέρει αριθμό αναφοράς και ημερομηνία. Όλα τα παραρτήματα και τα συνημμένα απαριθμούνται στην πρώτη σελίδα. [Τμήμα VII § 1]	Αποκλειστικός υπεύθυνος για τον υποχαρακτηρισμό ή αποχαρακτηρισμό είναι ο συντάκτης του εγγράφου, ή ο ΓΤ/ΥΕ, οι οποίοι ενημερώνουν σχετικά τους μετέπειτα αποδέκτες στους οποίους έχουν αποστείλει ή κοινοποιήσει το έγγραφο. [Τμήμα VIII § 31] Τα *έγγραφα* CONFIDENTIEL UE καταστρέφονται από την αρμόδια για την παραγωγή τους γραμματεία, υπό την εποπτεία προσώπου με κατάλληλη διαβάθμιση ασφαλείας. Η καταστροφή τους καταγράφεται σύμφωνα με τους εθνικούς κανονισμούς και, στην περίπτωση της ΓΤΣ των αποκεντρωμένων υπηρεσιών της ΕΕ, σύμφωνα με τις οδηγίες του Γενικού Γραμματέα/Υπατου Εκπροσώπου. [Τμήμα VII § 33]	Καταστρέφονται *τα* υπεράριθμα αντίτυπα και τα *έγγραφα* που δεν χρειάζονται πια. [Τμήμα VII § 31] Τα *έγγραφα* CONFIDENTIEL UE, καθώς και όλα τα διαβαθμισμένα απορρίμματα που προκύπτουν κατά την σύνταξη των *εγγράφων* CONFIDENTIEL 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 [Τμήμα VII §§ 31,33]

Διαβάθμιση	πότε	πως	επισημάνσεις	υποχαρακτηρισμός/αποχαρακτηρισμός/καταστροφή	
				ποιος	πότε
RESTREINT UE Η διαβάθμιση αυτή εφαρμόζεται στις πληροφορίες και το υλικό, η άνευ αδείας κοινολόγηση των οποίων μπορεί να βλάψει τα συμφέροντα της Ευρωπαϊκής Ένωσης ή ενός ή περισσοτέρων κρατών μελών της [Τμήμα II, § 4]	Όταν η διαρροή στοιχείων με διαβάθμιση RESTREINT UE θα ήταν πιθανό — να επηρεάσει δυσμενώς διπλωματικές σχέσεις, — να προξενήσει σημαντική οδύνη σε άτομα — να δυσχεράνει τη διατήρηση 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	Κράτη μέλη δεόντως εξουσιοδοτημένα πρόσωπα (συντάκτες). [Τμήμα III,§ 2], ΓΤΣ και αποκεντρωμένοι οργανισμοί ΕΕ: δεόντως εξουσιοδοτημένα πρόσωπα (συντάκτες) [Τμήμα III, § 2], Γενικοί Διευθυντές, ΓΤ/ΥΕ. Οι συντάκτες προσδιορίζουν ημερομηνία ή προθεσμία μετά την οποία μπορεί να υποχαρακτηριστεί ή να αποχαρακτηριστεί το περιεχόμενο. Σε αντίθετη περίπτωση, επανεξετάζουν τα έγγραφα το αργότερο ανά πενταετία, ώστε να επιβεβαιώνεται ότι εξακολουθεί να είναι αναγκαία η αρχική διαβάθμιση. [Τμήμα III, §10]	Η διαβάθμιση RESTREINT UE επιτίθεται στα έγγραφα RESTREINT UE, ενδεχομένως μαζί με την επισήμανση ESDP, με μηχανικά ή ηλεκτρονικά μέσα. [Τμήμα II § 8] Οι διαβαθμίσεις EU εμφαίνονται στο κέντρο του άνω και του κάτω μέρους κάθε σελίδας κάθε σελίδα αριθμείται. Κάθε έγγραφο φέρει αριθμό αναφοράς και ημερομηνία. [Τμήμα VII § 1]	Αποκλειστικός υπεύθυνος για τον υποχαρακτηρισμό ή αποχαρακτηρισμό είναι ο συντάκτης του εγγράφου, ή ο ΓΤ/ΥΕ, οι οποίοι ενημερώνουν σχετικά τους μετέπειτα αποδέκτες στους οποίους έχουν αποστείλει ή κοινοποιήσει το έγγραφο [Τμήμα III §9] Τα έγγραφα RESTREINT UE καταστρέφονται από την αρμόδια γραμματεία σύμφωνα με τους εθνικούς κανονισμούς και, στην περίπτωση της ΓΤΣ ή των αποκεντρωμένων υπηρεσιών της ΕΕ, σύμφωνα με τις οδηγίες του ΓΤ/ΥΕ. [Τμήμα VII § 34]	Καταστρέφονται τα υπεράριθμα αντίτυπα και τα έγγραφα που δεν χρειάζονται πια. [Τμήμα VII § 31]

Προσάρτημα 4

Κατευθυντήριες γραμμές για την κοινοποίηση διαβαθμισμένων πληροφοριών ΕΕ σε τρίτο κράτη ή διεθνείς οργανισμούς

Συνεργασία επιπέδου 1

ΔΙΑΔΙΚΑΣΙΕΣ

1. Το Συμβούλιο είναι αρμόδιο για την κοινοποίηση διαβαθμισμένων πληροφοριών ΕΕ σε χώρες που δεν έχουν υπογράψει τη συνθήκη για την Ευρωπαϊκή Ένωση ή σε άλλους διεθνείς οργανισμούς, των οποίων η πολιτική και οι κανονισμοί ασφαλείας είναι παρόμοιοι προς τους κοινοτικούς.

2 Το Συμβούλιο μπορεί να μεταβιβάζει την αρμοδιότητα για τη λήψη απόφασης για την κοινοποίηση διαβαθμισμένων πληροφοριών Στην πράξη μεταβίβασης πρέπει να αναφέρονται η φύση των πληροφοριών που επιτρέπεται να κοινοποιηθούν και ο βαθμός διαβάθμισης τους, ο οποίος κατά κανόνα, δεν πρέπει να υπερβαίνει το CONFIDENTIEL UE.

3. Υπό την προϋπόθεση ότι έχει συναφθεί συμφωνία ασφαλείας οι αιτήσεις κοινοποίησης διαβαθμισμένων πληροφοριών ΕΕ υποβάλλονται στο Γενικά Γραμματέα/Υπατο Εκπρόσωπο από τους φορείς ασφαλείας των ενδιαφερόμενων κρατών ή διεθνών οργανισμών, οι οποίοι πρέπει να δηλώνουν τους σκοπούς για τους οποίους προορίζεται η κοινοποίηση αυτή και τη φύση των προς κοινοποίηση διαβαθμισμένων πληροφοριών.

Αιτήσεις είναι δυνατόν να υποβάλλονται και από κράτος μέλος ή αποκεντρωμένο οργανισμό της ΕΕ που κρίνουν επιθυμητή την κοινοποίηση διαβαθμισμένων πληροφοριών ΕΕ· στις αιτήσεις αυτές πρέπει να αναφέρονται οι στόχοι και τα πλεονεκτήματα της κοινοποίησης αυτής για την ΕΕ, και να προσδιορίζεται η φύση και η διαβάθμιση των προς κοινοποίηση πληροφοριών.

4. Η αίτηση εξετάζεται από τη ΓΤΣ, η οποία:

— ζητά τις γνώμες του κράτους μέλους ή, ανάλογα με την περίπτωση, του αποκεντρωμένου οργανισμού της ΕΕ από τους οποίους προέρχονται οι προς κοινοποίηση πληροφορίες

— 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 τους προκείμενους κανονισμούς ασφαλείας

— ζητά τις τεχνικές γνώμες των Εθνικών Αρχών Ασφαλείας των κρατών μελών όσον αφορά την εμπιστοσύνη που εμπνέουν τα δικαιούχα κράτη ή διεθνείς οργανισμοί.

5. Η ΓΤΣ διαβιβάζει την αίτηση και τη σύσταση της Υπηρεσίας Ασφαλείας στο Συμβούλιο προκειμένου να ληφθεί σχετική απόφαση.

ΚΑΝΟΝΙΣΜΟΙ ΑΣΦΑΛΕΙΑΣ ΠΟΥ ΠΡΕΠΕΙ ΝΑ ΕΦΑΡΜΟΖΟΥΝ ΟΙ ΔΙΚΑΙΟΥΧΟΙ

6. Ο Γενικός Γραμματέας/Υπατος Εκπρόσωπος ενημερώνει τα δικαιούχα κράτη ή διεθνείς οργανισμούς για την απόφαση του Συμβουλίου να επιτρέψει την κοινοποίηση διαβαθμισμένων πληροφοριών ΕΕ, διαβιβάζοντας ταυτόχρονα τα απαιτούμενα αντίγραφα των προκειμένων κανονισμών ασφαλείας Εάν η αίτηση έχει υποβληθεί από κράτος μέλος το κράτος αυτό ενημερώνει το δικαιούχο της επιτρεπόμενης κοινοποίησης

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 τους προκείμενους κανονισμούς ασφαλείας ιδίως δε σύμφωνα με τις παρακάτω ειδικές διατάξεις.

7. Προσωπικό

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

β) Όλοι οι υπάλληλοι ή πολίτες που έχουν εξουσιοδοτημένη πρόσβαση σε πληροφορίες με διαβάθμιση τουλάχιστον CONFIDENTIEL UE πρέπει να διαθέτουν πιστοποιητικό ασφαλείας κατάλληλου επιπέδου ή ισοδύναμη διαβάθμιση ασφαλείας, που έχουν εκδοθεί από την κυβέρνηση του κράτους τους.

8. Διαβίβαση εγγράφων

α) Οι πρακτικές διαδικασίες για τη διαβίβαση των εγγράφων αποφασίζονται με συμφωνία βάσει των διατάξεων του τμήματος VII των προκείμενων κανονισμών ασφαλείας. Στις διαδικασίες αυτές πρέπει να ορίζονται, ιδίως, οι γραμματείες στις οποίες πρέπει να διαβιβάζονται οι διαβαθμισμένες πληροφορίες ΕΕ

β) Εάν οι διαβαθμισμένες πληροφορίες των οποίων την κοινοποίηση ενέκρινε το Συμβούλιο περιλαμβάνουν πληροφορίες TRES SECRET UE/EU TOP SECRET, το δικαιούχο κράτος ή διεθνής οργανισμός συγκροτεί κεντρική γραμματεία ΕΕ και, ενδεχομένως, υπογραμματείες ΕΕ. Οι γραμματείες αυτές διέπονται από τις διατάξεις του τμήματος VIII των προκείμενων κανονισμών ασφαλείας.

9. Καταχώρηση

Μόλις μια γραμματεία παραλάβει έγγραφο ΕΕ με διαβάθμιση τουλάχιστον 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 διαβάθμιση του, ο τίτλος του, το ονοματεπώνυμο και ο 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 VI των κανονισμών περί ασφαλείας του Συμβουλίου. Αντίγραφα των πρωτοκόλλων καταστροφής των εγγράφων SECRET UE και TRES SECRET UE/EU TOP SECRET αποστέλλονται στη γραμματεία ΕΕ που είχε διαβιβάσει το έγγραφο.

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 αποσπ*άσματα*

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

Η αναπαραγωγή ή μετάφραση εγγράφου TRÈS 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 στην Υπηρεσία Ασφαλείας της ΓΤΣ.

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 Υπηρεσία Ασφαλείας της ΓΤΣ, 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 Υπηρεσία Ασφαλείας της ΓΤΣ για να αποφευχθεί επανάληψη παρόμοιων συμβάντων.

14. Επιθεωρήσεις

Η Υπηρεσία Ασφαλείας της ΓΤΣ 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 τηρούνται οι προκείμενοι κανονισμοί ασφαλείας

Προσάρτημα 5

Κατευθυντήριες γραμμές για την κοινοποίηση διαβαθμισμένων πληροφοριών ΕΕ σε τρίτα κράτη ή διεθνείς οργανισμούς

Συνεργασία επιπέδου 2

ΔΙΑΔΙΚΑΣΙΕΣ

1. Η αρμοδιότητα για την κοινοποίηση διαβαθμισμένων πληροφοριών ΕΕ σε τρίτα κράτη ή διεθνείς οργανισμούς, των οποίων η πολιτική και οι κανονισμοί ασφαλείας διαφέρουν σημαντικά από τους κοινοτικούς, ανήκει στο Συμβούλιο. Κατ' αρχήν, επιτρέπεται να κοινοποιούνται μόνον πληροφορίες με διαβάθμιση το πολύ SECRET UE, αλλά απαγορεύεται η κοινοποίηση εθνικών πληροφοριών που προορίζονται αποκλειστικά για τα κράτη μέλη καθώς και κατηγοριών διαβαθμισμένων πληροφοριών ΕΕ που προστατεύονται με ειδική επισήμανση.

2. Το Συμβούλιο μπορεί να μεταβιβάζει την αρμοδιότητα για τη λήψη απόφασης. Κατά τη μεταβίβαση, το Συμβούλιο, υπό την προϋπόθεση ότι τηρούνται οι όροι της παραγράφου 1, αναφέρει τη φύση των πληροφοριών που επιτρέπεται να κοινοποιηθούν και το βαθμό διαβάθμισής τους, ο οποίος, κατά κανόνα, δεν πρέπει να υπερβαίνει το RESTREINT UE.

3. Υπό την προϋπόθεση ότι έχει συναφθεί συμφωνία ασφαλείας οι αιτήσεις κοινοποίησης διαβαθμισμένων πληροφοριών ΕΕ υποβάλλονται στο Γενικό Γραμματέα/Ύπατο Εκπρόσωπο από τους φορείς ασφαλείας των ενδιαφερόμενων κρατών ή διεθνών οργανισμών, οι οποίοι πρέπει να δηλώνουν τους σκοπούς για τους οποίους προορίζεται η κοινοποίηση αυτή καθώς και τη φύση και τη διαβάθμιση των προς κοινοποίηση πληροφοριών.

   Αιτήσεις είναι δυνατόν να υποβάλλονται και από κράτος μέλος ή αποκεντρωμένο οργανισμό της ΕΕ που επιθυμούν την κοινοποίηση διαβαθμισμένων πληροφοριών ΕΕ· στις αιτήσεις αυτές πρέπει να αναφέρονται οι στόχοι και τα πλεονεκτήματα της κοινοποίησης αυτής για την ΕΕ, και να προσδιορίζεται η φύση και διαβάθμιση των προς κοινοποίηση πληροφοριών.

4. Η αίτηση εξετάζεται από τη ΓΤΣ η οποία:

   — ζητά τις γνώμες του κράτους μέλους ή, κατά περίπτωση, του αποκεντρωμένου οργανισμού της ΕΕ από τους οποίους προέρχονται οι προς κοινοποίηση πληροφορίες.

   — πραγματοποιεί προκαταρκτικές 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 εκείνους που ισχύουν στο συγκεκριμένο κράτος ή οργανισμό,

   — διοργανώνει συνεδρίαση της Επιτροπής Ασφαλείας του Συμβουλίου ή, εφόσον απαιτείται, με τη διαδικασία σιωπηρής συναίνεσης απευθύνει ερωτήματα στις Εθνικές Αρχές Ασφαλείας των κρατών μελών προκειμένου να λάβει την τεχνική γνώμη της Επιτροπής Ασφαλείας.

5. Η τεχνική γνώμη της Επιτροπής Ασφαλείας του Συμβουλίου αφορά τα εξής

   — 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 κλπ.),

   — τον υποχαρακτηρισμό ή αποχαρακτηρισμό των πληροφοριών από τη συντάκτρια αρχή πριν από την κοινοποίηση στις δικαιούχες χώρες ή διεθνείς οργανισμούς ([1]).

([1]) Πράγμα το οποίο σημαίνει ότι η συντάκτρια αρχή εφαρμόζει τη διαδικασία της παραγράφου 9 του τμήματος ΙΙΙ για όλα τα αντίτυπα που κυκλοφορούν εντός της ΕΕ.

6. Ο Γενικός Γραμματέας/Ύπατος Εκπρόσωπος διαβιβάζει, προκειμένου να ληφθεί απόφαση, στο Συμβούλιο τόσο την αίτηση όσο και την τεχνική γνώμη της Επιτροπής Ασφαλείας του Συμβουλίου που έχει λάβει η Υπηρεσία Ασφαλείας της ΓΤΣ.

ΚΑΝΟΝΙΣΜΟΙ ΑΣΦΑΛΕΙΑΣ ΠΟΥ ΠΡΕΠΕΙ ΝΑ ΕΦΑΡΜΟΖΟΥΝ ΟΙ ΔΙΚΑΙΟΥΧΟΙ

7. Η απόφαση του Συμβουλίου να επιτρέψει την κοινοποίηση διαβαθμισμένων πληροφοριών ΕΕ ανακοινώνεται στις δικαιούχες χώρες ή διεθνείς οργανισμούς από το Γενικό Γραμματέα/Ύπατο Εκπρόσωπο, μαζί με πίνακα στον οποίον συγκρίνονται οι διαβαθμίσεις που ισχύουν στην ΕΕ με εκείνους που ισχύουν στα συγκεκριμένα κράτη ή οργανισμούς. Εάν η αίτηση έχει υποβληθεί από κράτος μέλος, το κράτος αυτό ενημερώνει το δικαιούχο της επιτρεπόμενης κοινοποίησης.

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 τους κανονισμούς περί ασφαλείας του Συμβουλίου, ιδίως δε σύμφωνα με τις παρακάτω ειδικές διατάξεις

8. Οι ακόλουθοι κανόνες προστασίας θεσπίζονται εκτός εάν το Συμβούλιο, αφού λάβει την τεχνική γνώμη της Επιτροπής Ασφαλείας του Συμβουλίου, αποφασίσει ειδική διαδικασία για το χειρισμό των διαβαθμισμένων εγγράφων ΕΕ (διαγραφή των ενδείξεων διαβάθμισης ΕΕ, ειδικών επισημάνσεων κλπ.).

Στην περίπτωση αυτή, οι κανόνες προσδιορίζονται αναλόγως

9. Προσωπικό

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

β) Όλοι οι υπάλληλοι ή πολίτες που έχουν εξουσιοδοτημένη πρόσβαση στις διαβαθμισμένες πληροφορίες που κοινοποιεί η ΕΕ πρέπει να διαθέτουν εθνική διαβάθμιση ασφαλείας κατάλληλου επιπέδου ή εξουσιοδότηση πρόσβασης στην περίπτωση των εθνικών διαβαθμισμένων πληροφοριών, κατάλληλου επιπέδου ισοδύναμου προς το κοινοτικό, όπως ορίζεται στο συγκριτικό πίνακα.

γ) Αυτές οι εθνικές διαβαθμίσεις ή εξουσιοδοτήσεις ασφαλείας διαβιβάζονται προς ενημέρωση στο Γενικό Γραμματέα/Ύπατο Εκπρόσωπο

10. Διαβίβαση εγγράφων

α) Οι πρακτικές διαδικασίες για τη διαβίβαση των εγγράφων συμφωνούνται μεταξύ της Υπηρεσίας Ασφαλείας της ΓΤΣ και των φορέων ασφαλείας των παραληπτών κρατών ή διεθνών οργανισμών βάσει των κανόνων της που περιέχονται στο τμήμα VII των παρόντων κανονισμών Στις διαδικασίες αυτές πρέπει ιδίως να προσδιορίζονται οι ακριβείς διευθύνσεις στις οποίες πρέπει να αποσταλούν τα έγγραφα, καθώς και οι υπηρεσίες μεταφορέων ή ταχυδρομείου που χρησιμοποιούνται για τη διαβίβαση διαβαθμισμένων πληροφοριών ΕΕ.

β) Τα έγγραφα με διαβάθμιση τουλάχιστον CONFIDENTIEL UE διαβιβάζονται εντός διπλού φακέλου. Ο εσωτερικός φάκελος φέρει την επισήμανση «EU» καθώς και τη διαβάθμιση ασφαλείας Μέσα στο φάκελο, κάθε διαβαθμισμένο έγγραφο συνοδεύεται από έντυπο απόδειξης. Στο έντυπο απόδειξης, 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 λόγους χορήγησης απόδειξης. Ο εξωτερικός φάκελος δεν φέρει διαβάθμιση ασφαλείας

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

11. Καταχώρηση κατά *την* άφιξη

Η Εθνική Αρχή Ασφαλείας του παραλήπτη κράτους ή ο ομόλογος φορέας του κράτους που παραλαμβάνει, εξ ονόματος της κυβέρνησής του τις διαβαθμισμένες πληροφορίες που κοινοποιεί η ΕΕ, ή το γραφείο ασφαλείας του παραλήπτη διεθνούς οργανισμού, 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 διαβάθμιση του, ο τίτλος του, το ονοματεπώνυμο και ο τίτλος του παραλήπτη, η ημερομηνία επιστροφής της απόδειξης και η ημερομηνία επιστροφής του εγγράφου στην ΕΕ ή καταστροφής του

12 Επιστροφή *εγγράφων*

Όταν ο αποδέκτης επιστρέφει ένα διαβαθμισμένο έγγραφο στο Συμβούλιο ή στο κράτος μέλος το οποίου του το κοινοποίησε, ακολουθεί τη διαδικασία της παραγράφου 10.

13. 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 εξουσιοδότηση πρόσβασης στις διαβαθμισμένες πληροφορίες ΕΕ που είναι αποθηκευμένες στον περιέκτη και πρέπει να αλλάζει ανά εξάμηνο, ή συχνότερα όταν μετατίθεται ο υπάλληλος, ανακαλείται η διαβάθμιση ασφαλείας ενός από τους υπαλλήλους που γνωρίζουν το συνδυασμό, ή υπάρχει κίνδυνος διαρροής.

β) Τα διαβαθμισμένα έγγραφα ΕΕ αφαιρούνται από τον περιέκτη 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 περιέκτη ασφαλείας όταν δεν τα χρησιμοποιούν πλέον και εκτός ωρών εργασίας.

γ) Από τα έγγραφα με διαβάθμιση τουλάχιστον CONFIDENTIEL UE, απαγορεύεται να παράγονται φωτοαντίγραφα ή αποσπάσματα χωρίς την άδεια της Υπηρεσίας Ασφαλείας της ΓΤΣ.

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 Υπηρεσία Ασφαλείας της ΓΤΣ.

14. Υλική ασφάλεια

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

β) Όταν το προσωπικό συντήρησης ή καθαρισμού πρέπει να εισέλθει σε ένα δωμάτιο όπου υπάρχουν τέτοιοι περιέκτες ασφαλείας, το προσωπικό αυτό πρέπει να συνοδεύεται πάντοτε από μέλος της υπηρεσίας ασφαλείας του κράτους ή του οργανισμού ή από υπάλληλο που είναι ειδικά επιφορτισμένος με την εποπτεία της ασφάλειας του δωματίου.

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

15. 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 Υπηρεσία Ασφαλείας της ΓΤΣ ή στην Εθνική Αρχή Ασφαλείας του κράτους μέλους που έλαβε την πρωτοβουλία να διαβιβάσει τα έγγραφα (με αντίγραφο προς την Υπηρεσία Ασφαλείας της ΓΤΣ),

β) διεξάγεται έρευνα, μετά την ολοκλήρωση της οποίας υποβάλλεται πλήρης έκθεση στο φορέα ασφαλείας [βλέπε στοιχείο α) παραπάνω], στη συνέχεια δε λαμβάνονται τα μέτρα που απαιτούνται για την επανόρθωση της κατάστασης.

16. Επιθεωρήσεις

Η Υπηρεσία Ασφαλείας της ΓΤΣ έχει το δικαίωμα, βάσει συμφωνίας με τα ενδιαφερόμενα κράτη ή διεθνείς οργανισμούς να αξιολογεί την αποτελεσματικότητα των μέτρων προστασίας των κοινοποιούμενων διαβαθμισμένων πληροφοριών ΕΕ.

17. Εκθέσεις

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 οι προκείμενοι κανονισμοί ασφαλείας τηρήθηκαν.

Προσάρτημα 6

Κατευθυντήριες γραμμές για την κοινοποίηση διαβαθμισμένων πληροφοριών ΕΕ σε τρίτα κράτη ή διεθνείς οργανισμούς

Συνεργασία επιπέδου 3

ΔΙΑΔΙΚΑΣΙΕΣ

1. Ενίοτε, το Συμβούλιο ενδέχεται να συνεργαστεί, υπό ορισμένες συγκεκριμένες περιστάσεις, με κράτη ή οργανισμούς που δεν μπορούν μεν να παράσχουν τις εγγυήσεις που απαιτούνται βάσει των προκειμένων κανονισμών ασφαλείας, η συνεργασία όμως με τα οποία απαιτεί την κοινοποίηση διαβαθμισμένων πληροφοριών ΕΕ. Από την κοινοποίηση αυτήν αποκλείονται οι εθνικές πληροφορίες που προορίζονται αποκλειστικά για τα κράτη μέλη.

2. Στις ειδικές αυτές περιστάσεις, οι αιτήσεις συνεργασίας με την ΕΕ, είτε προέρχονται από τρίτα κράτη ή διεθνείς οργανισμούς είτε προτείνονται από κράτη μέλη ή, ανάλογα με την περίπτωση, αποκεντρωμένους οργανισμούς της ΕΕ, εξετάζονται κατ' αρχάς ως προς την ουσία τους από το Συμβούλιο, το οποίο, εφόσον απαιτείται, ζητά τη "γνώμη του κράτους μέλους η του αποκεντρωμένου οργανισμού από τον οποίο προέρχονται οι πληροφορίες. Το Συμβούλιο 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.

3. Εάν το Συμβούλιο λάβει θετική απόφαση, ο Γενικός Γραμματέας/Ύπατος Εκπρόσωπος συγκαλεί την Επιτροπή Ασφαλείας του Συμβουλίου ή να ζητεί τη γνώμη των Αρχών Εθνικής Ασφαλείας των κρατών μελών, ενδεχομένως μέσω της διαδικασίας σιωπηρής συναίνεσης προκειμένου να λάβει την τεχνική γνώμη της Επιτροπής Ασφαλείας

4. Η τεχνική γνώμη της Επιτροπής Ασφαλείας του Συμβουλίου αφορά τα εξής:

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

β) τη διαβάθμιση των πληροφοριών που επιτρέπεται να κοινοποιηθούν, ενδεχομένως ανάλογα με τη φύση τους

γ) τον υποχαρακτηρισμό ή αποχαρακτηρισμό των πληροφοριών από τη συντάκτρια αρχή πριν από την κοινοποίηση τους σης δικαιούχες χώρες ή διεθνείς οργανισμούς([1]),

δ) τις διαδικασίες για το χειρισμό των προς κοινοποίηση εγγράφων (βλέπε παράγραφο 5 παρακάτω),

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

5. Τα έγγραφα που κοινοποιούνται στα κράτη ή οργανισμούς που καλύπτονται από το παρόν προσάρτημα συντάσσονται, κάτ' αρχήν, χωρίς αναφορά της πηγής ή της διαβάθμισης EU. Η Επιτροπή Ασφαλείας του Συμβουλίου μπορεί να συνιστά:

— τη χρήση ειδικής σήμανσης ή κωδικού ονόματος

— τη χρήση οδικού συστήματος διαβάθμισης με το οποίο η ευαισθησία των πληροφοριών συνδέεται με τα μέτρα ελέγχου που πρέπει να τηρούν οι μέθοδοι διαβίβασης των εγγράφων τις οποίες εφαρμόζει ο δικαιούχος (βλέπε παραδείγματα στην παράγραφο 14)

6. Η Υπηρεσία Ασφαλείας της ΓΤΣ υποβάλλει την τεχνική γνώμη της Επιτροπής Ασφαλείας στο Συμβούλιο, επισυνάπτοντας εφόσον απαιτείται, τις προτεινόμενες μεταβιβάσεις αρμοδιότητας που απαιτούνται για την εκτέλεση του συγκεκριμένου έργου, ιδίως σε επείγουσες περιστάσεις

7. Όταν το Συμβούλιο εγκρίνει την κοινοποίηση των διαβαθμισμένων πληροφοριών ΕΕ και τις διαδικασίες πρακτικής εφαρμογής, η Υπηρεσία Ασφαλείας της ΓΤΣ πραγματοποιεί τις απαιτούμενες επαφές με τον φορέα ασφαλείας του ενδιαφερόμενου κράτους ή οργανισμού για να διευκολύνει την εφαρμογή των προτεινόμενων μέτρων ασφαλείας

([1]) Πράγμα το οποίο σημαίνει ότι η συντάκτρια αρχή εφαρμόζει τη διαδικασία της παραγράφου 9 του τμήματος ΙΙΙ για όλα τα αντίτυπα που κυκλοφορούν εντός της ΕΕ.

8. Ως έγγραφο αναφοράς, η Υπηρεσία Ασφαλείας της ΓΤΣ κυκλοφορεί, σε όλα τα κράτη μέλη και, ανάλογα με την περίπτωση, του ενδιαφερόμενου αποκεντρωμένου οργανισμού της ΕΕ, πίνακα στον οποίον συνοψίζονται η φύση και η διαβάθμιση των πληροφοριών και αναφέρονται οι οργανισμοί και οι χώρες στις οποίες επιτρέπεται να κοινοποιηθούν, σύμφωνα με τη σχετική απόφαση του Συμβουλίου.

9. Η Εθνική Αρχή Ασφαλείας του κοινοποιούντος κράτους μέλους ή η Υπηρεσία Ασφαλείας της ΓΤΣ λαμβάνουν όλα τα απαιτούμενα μέτρα για να διευκολύνουν την μετέπειτα αξιολόγηση τυχόν ζημιών και την επανεξέταση των διαδικασιών.

10. Όποτε τροποποιούνται οι συνθήκες συνεργασίας, το θέμα παραπέμπεται εκ νέου στο Συμβούλιο.

ΚΑΝΟΝΙΣΜΟΙ ΑΣΦΑΛΕΙΑΣ ΠΟΥ ΠΡΕΠΕΙ ΝΑ ΕΦΑΡΜΟΖΟΥΝ ΟΙ ΔΙΚΑΙΟΥΧΟΙ

11. Η απόφαση του Συμβουλίου να επιτρέψει την κοινοποίηση διαβαθμισμένων πληροφοριών ΕΕ ανακοινώνεται στις δικαιούχες χώρες ή διεθνείς οργανισμούς από το Γενικό Γραμματέα/Ύπατο Εκπρόσωπο, μαζί με τους λεπτομερείς κανόνες προστασίας που προτείνει η Επιτροπή Ασφαλείας του Συμβουλίου. Εάν η αίτηση έχει υποβληθεί από κράτος μέλος το κράτος αυτό ενημερώνει το δικαιούχο της επιτρεπόμενης κοινοποίησης

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

— θα χρησιμοποιούν τις πληροφορίες μόνον για τη συνεργασία που αποφάσισε το Συμβούλιο,

— θα προστατεύουν τις πληροφορίες όπως απαιτεί το Συμβούλιο.

12. Διαβίβαση εγγράφων

α) Οι πρακτικές διαδικασίες για τη διαβίβαση των εγγράφων συμφωνούνται μεταξύ της Υπηρεσίας Ασφαλείας της ΓΤΣ 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 CONFIDENTIEL UE και υψηλότερη διαβιβάζονται εντός διπλού φακέλου. Ο εσωτερικός φάκελος φέρει την ειδική σφραγίδα ή κωδικό όνομα που έχουν αποφασιστεί και αναφέρει την ειδική διαβάθμιση που εγκρίνεται για το συγκεκριμένο έγγραφο. Μέσα στο φάκελο, κάθε διαβαθμισμένο έγγραφο συνοδεύεται από έντυπο απόδειξης Στο έντυπο απόδειξης 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 λόγους χορήγησης απόδειξης. Ο εξωτερικός φάκελος δεν φέρει διαβάθμιση ασφαλείας

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

13. Καταχώρηση κατά την άφιξη

Η Εθνική Αρχή Ασφαλείας του παραλήπτη κράτους ή ο ομόλογος φορέας του κρότους που παραλαμβάνει, εξ ονόματος της κυβέρνησης του τις διαβαθμισμένες πληροφορίες που κοινοποιεί η ΕΕ, ή το γραφείο ασφαλείας του παραλήπτη διεθνούς οργανισμού, 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 διαβάθμιση 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 έγγραφου

14. Χρήση και προστασία *των* ανταλλασσόμενων διαβαθμισμένων πληροφοριών

α) Οι πληροφορίες SECRET UE διεκπεραιώνονται από ειδικά οριζόμενους υπαλλήλους που έχουν εξουσιοδότηση πρόσβασης σε πληροφορίες ρε αυτή τη διαβάθμιση. 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 SECRET UE διαβιβάζονται με διπλωματικό σάκο, ασφαλείς ταχυδρομικές υπηρεσίες και ασφαλείς τηλεπικοινωνιακές υπηρεσίες. Ένα έγγραφο SECRET UE μπορεί να αντιγράφεται μόνον με τη γραπτή συγκατάθεση της συντάκτριας αρχής Όλα τα αντίτυπα πρέπει να καταχωρούνται και να παρακολουθούνται. Για όλες τις εργασίες που αφορούν έγγραφα SECRET UE εκδίδεται απόδειξη.