ΑΠΟΦΑΣΕΙΣ

ΑΠΟΦΑΣΗ (ΕΕ, Ευρατόμ) 2017/46 ΤΗΣ ΕΠΙΤΡΟΠΗΣ

της 10ης Ιανουαρίου 2017

σχετικά με την ασφάλεια των συστημάτων επικοινωνίας και πληροφοριών στην Ευρωπαϊκή Επιτροπή

Η ΕΥΡΩΠΑΪΚΗ ΕΠΙΤΡΟΠΗ,

Έχοντας υπόψη τη Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης, και ιδίως το άρθρο 249,

Έχοντας υπόψη τη Συνθήκη για την ίδρυση της Ευρωπαϊκής Κοινότητας Ατομικής Ενέργειας,

Εκτιμώντας τα ακόλουθα:

(1) Τα συστήματα επικοινωνίας και πληροφοριών της Επιτροπής αποτελούν αναπόσπαστο μέρος της λειτουργίας της Επιτροπής και τα συμβάντα ασφαλείας στον τομέα της τεχνολογίας των πληροφοριών (ΤΠ) μπορεί να έχουν σοβαρό αντίκτυπο στις δραστηριότητες της Επιτροπής καθώς και σε τρίτους όπως, μεταξύ άλλων, ιδιώτες, επιχειρήσεις και κράτη μέλη.

(2) Υπάρχουν πολλές απειλές που μπορούν να επηρεάσουν δυσμενώς την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των συστημάτων επικοινωνίας και πληροφοριών της Επιτροπής, καθώς και των πληροφοριών που υποβάλλονται σε επεξεργασία μέσω αυτών. Οι απειλές αυτές περιλαμβάνουν ατυχήματα, σφάλματα, εσκεμμένες επιθέσεις και φυσικά φαινόμενα και πρέπει να αναγνωρίζονται ως λειτουργικοί κίνδυνοι.

(3) Τα συστήματα επικοινωνίας και πληροφοριών πρέπει να διαθέτουν επίπεδο προστασίας που να είναι ανάλογο της πιθανότητας, του αντίκτυπου και της φύσης των κινδύνων στους οποίους εκτίθενται.

(4) Η ασφάλεια ΤΠ στην Επιτροπή θα πρέπει να διασφαλίζει ότι τα συστήματα επικοινωνίας και πληροφοριών προστατεύουν τις πληροφορίες που επεξεργάζονται και ότι λειτουργούν όπως και όποτε χρειάζεται υπό τον έλεγχο των νομίμων χρηστών.

(5) Η πολιτική ασφάλειας ΤΠ της Επιτροπής θα πρέπει να εφαρμόζεται κατά τρόπο που συνάδει με τις πολιτικές σχετικά με την ασφάλεια στην Επιτροπή.

(6) Η Διεύθυνση Ασφάλειας της Γενικής Διεύθυνσης Ανθρωπίνων Πόρων και Ασφάλειας έχει τη γενική ευθύνη της ασφάλειας στην Επιτροπή υπό την εξουσία και την ευθύνη του αρμόδιου για την ασφάλεια μέλους της Επιτροπής.

(7) Η προσέγγιση της Επιτροπής θα πρέπει να λαμβάνει υπόψη τις πρωτοβουλίες πολιτικής και τη νομοθεσία της ΕΕ σχετικά με την ασφάλεια δικτύων και πληροφοριών, τα πρότυπα και τις ορθές πρακτικές του κλάδου, ώστε να συμμορφώνεται με όλες τις σχετικές νομοθετικές διατάξεις και να εξασφαλίζει διαλειτουργικότητα και συμβατότητα.

(8) Τα τμήματα της Επιτροπής που είναι αρμόδια για τα συστήματα επικοινωνίας και πληροφοριών θα πρέπει να αναπτύσσουν και να εφαρμόζουν κατάλληλα μέτρα, και θα πρέπει να υπάρχει συντονισμός των μέτρων ασφάλειας ΤΠ για την προστασία των συστημάτων επικοινωνίας και πληροφοριών σε όλα τα επίπεδα της Επιτροπής ώστε να εξασφαλίζεται αποδοτικότητα και αποτελεσματικότητα.

(9) Οι κανόνες και οι διαδικασίες που ισχύουν για την πρόσβαση σε πληροφορίες στο πλαίσιο της ασφάλειας ΤΠ, όπως, μεταξύ άλλων, κατά τον χειρισμό συμβάντων ασφαλείας ΤΠ, θα πρέπει να έχουν χαρακτήρα ανάλογο προς την απειλή που υφίσταται για την Επιτροπή ή το προσωπικό της, να συμμορφώνονται με τις αρχές που παρατίθενται στον κανονισμό (ΕΚ) αριθ. 45/2001 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου [1] σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα όργανα και τους οργανισμούς της Ένωσης και σχετικά με την ελεύθερη κυκλοφορία των δεδομένων αυτών, και να λαμβάνουν υπόψη την αρχή του επαγγελματικού απορρήτου που κατοχυρώνεται στο άρθρο 339 της ΣΛΕΕ.

[1] Κανονισμός (ΕΚ) αριθ. 45/2001 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 18ης Δεκεμβρίου 2000, σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα όργανα και τους οργανισμούς της Κοινότητας και σχετικά με την ελεύθερη κυκλοφορία των δεδομένων αυτών (ΕΕ L 8 της 12.1.2001, σ. 1).

(10) Οι πολιτικές και οι κανόνες για τα συστήματα επικοινωνίας και πληροφοριών που επεξεργάζονται διαβαθμισμένες πληροφορίες της ΕΕ (ΔΠΕΕ), ευαίσθητες μη διαβαθμισμένες πληροφορίες και αδιαβάθμητες πληροφορίες πρέπει να συνάδουν πλήρως με τις αποφάσεις της Επιτροπής (ΕΕ, Ευρατόμ) 2015/443 ([1]) και (ΕΕ, Ευρατόμ) 2015/444 ([2]).

(11) Η Επιτροπή πρέπει να αναθεωρήσει και να επικαιροποιήσει τις διατάξεις για την ασφάλεια των συστημάτων επικοινωνίας και πληροφοριών που χρησιμοποιεί.

(12) Ως εκ τούτου, η απόφαση C(2006) 3602 της Επιτροπής θα πρέπει να καταργηθεί,

ΕΞΕΔΩΣΕ ΤΗΝ ΠΑΡΟΥΣΑ ΑΠΟΦΑΣΗ:

ΚΕΦΑΛΑΙΟ 1

ΓΕΝΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Άρθρο 1

Αντικείμενο και πεδίο εφαρμογής

1. Η παρούσα απόφαση εφαρμόζεται σε όλα τα συστήματα επικοινωνίας και πληροφοριών (CIS) η κυριότητα, προμήθεια, διαχείριση ή εκμετάλλευση των οποίων ανήκει στην Επιτροπή ή πραγματοποιείται από την Επιτροπή ή για λογαριασμό της, καθώς και σε κάθε χρήση των εν λόγω CIS από την Επιτροπή.

2. Η παρούσα απόφαση καθορίζει τις βασικές αρχές, τους στόχους, την οργάνωση και τις αρμοδιότητες που σχετίζονται με την ασφάλεια των εν λόγω CIS, ειδικότερα δε για τα τμήματα της Επιτροπής στα οποία ανήκει η κυριότητα ή από τα οποία πραγματοποιείται η προμήθεια, διαχείριση ή εκμετάλλευση CIS, περιλαμβανομένων CIS που παρέχονται από εσωτερικό πάροχο υπηρεσιών ΤΠ. Στην περίπτωση που η κυριότητα, προμήθεια, διαχείριση ή εκμετάλλευση ενός CIS ανήκει σε ή πραγματοποιείται από εξωτερικό φορέα βάσει διμερούς συμφωνίας ή σύμβασης με την Επιτροπή, οι όροι της συμφωνίας ή της σύμβασης συμμορφώνονται με την παρούσα απόφαση.

3. Η παρούσα απόφαση εφαρμόζεται σε όλα τα τμήματα της Επιτροπής και τους εκτελεστικούς οργανισμούς. Στην περίπτωση που CIS της Επιτροπής χρησιμοποιείται από άλλους οργανισμούς και θεσμικά όργανα βάσει διμερούς συμφωνίας με την Επιτροπή, οι όροι της συμφωνίας συμμορφώνονται με την παρούσα απόφαση.

4. Με την επιφύλαξη τυχόν ειδικών ενδείξεων που αφορούν συγκεκριμένες ομάδες προσωπικού, η παρούσα απόφαση εφαρμόζεται στα μέλη της Επιτροπής, στο προσωπικό της Επιτροπής που εμπίπτει στο πεδίο εφαρμογής του κανονισμού υπηρεσιακής κατάστασης των υπαλλήλων της Ευρωπαϊκής Ένωσης (ο «κανονισμός υπηρεσιακής κατάστασης») και του καθεστώτος που εφαρμόζεται στο λοιπό προσωπικό της Ένωσης ([3]), στους εθνικούς εμπειρογνώμονες που είναι αποσπασμένοι στην Επιτροπή («ΑΕΕ») ([4]), στους εξωτερικούς παρόχους υπηρεσιών και στο προσωπικό τους, στους ασκουμένους και σε κάθε πρόσωπο που έχει πρόσβαση σε CIS στο πλαίσιο του πεδίου εφαρμογής της παρούσας απόφασης.

5. Η παρούσα απόφαση εφαρμόζεται στην Ευρωπαϊκή Υπηρεσία Καταπολέμησης της Απάτης (OLAF) στον βαθμό που αυτό είναι συμβατό με τη νομοθεσία της Ένωσης και την απόφαση 1999/352/ΕΚ, ΕΚΑΧ, Ευρατόμ της Επιτροπής ([5]). Ειδικότερα, μέτρα που προβλέπονται στην παρούσα απόφαση, όπως μεταξύ άλλων οδηγίες, επιθεωρήσεις, έρευνες και ισοδύναμα μέτρα, ενδέχεται να μην εφαρμόζονται σε CIS της Υπηρεσίας σε περίπτωση που αυτό δεν είναι συμβατό με την ανεξαρτησία των ερευνητικών καθηκόντων της Υπηρεσίας και/ή με την εμπιστευτικότητα των πληροφοριών που συλλέγει η Υπηρεσία κατά την άσκηση αυτών των καθηκόντων.

Άρθρο 2

Ορισμοί

Για τους σκοπούς της παρούσας απόφασης ισχύουν οι ακόλουθοι ορισμοί:

1) «υπόλογος»: πρόσωπο που λογοδοτεί για ενέργειες, αποφάσεις και επιδόσεις·

([1]) Απόφαση (ΕΚ, Ευρατόμ) 2015/443 της Επιτροπής, της 13ης Μαρτίου 2015, σχετικά με την ασφάλεια στην Επιτροπή (ΕΕ L 72 της 17.3.2015, σ. 41).

([2]) Απόφαση (ΕΚ, Ευρατόμ) 2015/444 της Επιτροπής, της 13ης Μαρτίου 2015, σχετικά με τους κανόνες ασφαλείας για την προστασία των διαβαθμισμένων πληροφοριών της ΕΕ (ΕΕ L 72 της 17.3.2015, σ. 53).

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

([4]) Απόφαση της Επιτροπής της 12ης Νοεμβρίου 2008 περί του καθεστώτος των αποσπασμένων και των εκπαιδευόμενων στις υπηρεσίες της Επιτροπής εθνικών εμπειρογνωμόνων [C(2008) 6866 τελικό].

([5]) Απόφαση 1999/352/ΕΚ, ΕΚΑΧ, Ευρατόμ της Επιτροπής, της 28ης Απριλίου 1999, για την ίδρυση της Ευρωπαϊκής Υπηρεσίας Καταπολέμησης της Απάτης (ΕΕ L 136 της 31.5.1999, σ. 20).

2) «CERT-ΕΕ»: ομάδα αντιμετώπισης έκτακτων αναγκών στην πληροφορική για τα θεσμικά όργανα και τους οργανισμούς της ΕΕ. Αποστολή της είναι να παρέχει υποστήριξη στα ευρωπαϊκά θεσμικά όργανα ώστε να προστατεύονται από εσκεμμένες και δόλιες επιθέσεις που μπορούν να πλήξουν την ακεραιότητα των περιουσιακών στοιχείων ΤΠ που διαθέτουν και να βλάψουν τα συμφέροντα της ΕΕ. Το πεδίο εφαρμογής των δραστηριοτήτων της CERT-ΕΕ καλύπτει την πρόληψη, τον εντοπισμό, την αντιμετώπιση και την αποκατάσταση·

3) «τμήμα της Επιτροπής»: κάθε Γενική Διεύθυνση ή υπηρεσία της Επιτροπής ή ιδιαίτερο γραφείο μέλους της Επιτροπής·

4) «Αρχή Ασφαλείας της Επιτροπής»: η αρχή που συγκροτείται δυνάμει της απόφασης (ΕΕ, Ευρατόμ) 2015/444·

5) «σύστημα επικοινωνίας και πληροφοριών» ή «CIS»: οποιοδήποτε σύστημα επιτρέπει τον χειρισμό πληροφοριών σε ηλεκτρονική μορφή, περιλαμβανομένων όλων των στοιχείων που απαιτούνται για τη λειτουργία του, καθώς και της υποδομής, της οργάνωσης, του προσωπικού και των πληροφοριών. Ο ορισμός καλύπτει επιχειρησιακές εφαρμογές, κοινές υπηρεσίες ΤΠ, συστήματα που αποτελούν αντικείμενο εξωτερικής ανάθεσης και συσκευές τελικού χρήστη·

6) «συμβούλιο εσωτερικής διοίκησης» (ΣΕΔ) (CMB): ασκεί το υψηλότερο επίπεδο εσωτερικής διοικητικής εποπτείας επί επιχειρησιακών και διοικητικών θεμάτων στην Επιτροπή·

7) «ιδιοκτήτης των δεδομένων»: το πρόσωπο που είναι υπεύθυνο να μεριμνά για την προστασία και τη χρήση ενός συγκεκριμένου συνόλου δεδομένων ο χειρισμός του οποίου γίνεται από ένα CIS·

8) «σύνολο δεδομένων»: σύνολο πληροφοριών που επιτελεί συγκεκριμένη επιχειρησιακή διεργασία ή δραστηριότητα της Επιτροπής·

9) «διαδικασία έκτακτης ανάγκης»: προκαθορισμένο σύνολο μεθόδων και αρμοδιοτήτων για την αντιμετώπιση επειγουσών καταστάσεων ώστε να μην υπάρξουν σοβαρές επιπτώσεις για την Επιτροπή·

10) «πολιτική ασφάλειας πληροφοριών»: σύνολο στόχων που άπτονται της ασφάλειας των πληροφοριών, οι οποίοι έχουν τεθεί, υλοποιούνται και ελέγχονται ή πρέπει να τεθούν, να υλοποιηθούν και να ελεγχθούν. Περιλαμβάνει, ενδεικτικά, τις αποφάσεις (ΕΕ, Ευρατόμ) 2015/444 και (ΕΕ, Ευρατόμ) 2015/443·

11) «διοικούσα επιτροπή ασφάλειας πληροφοριών» (ΔΕΑΠ): το όργανο διοίκησης που συνεπικουρεί το συμβούλιο εσωτερικής διοίκησης στα καθήκοντά του που σχετίζονται με την ασφάλεια ΤΠ·

12) «εσωτερικός πάροχος υπηρεσιών ΤΠ»: τμήμα της Επιτροπής που παρέχει κοινές υπηρεσίες ΤΠ·

13) «ασφάλεια ΤΠ» ή «ασφάλεια CIS»: η διαφύλαξη της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των CIS και των συνόλων δεδομένων που αυτά υποβάλλουν σε επεξεργασία·

14) «κατευθυντήριες οδηγίες ασφάλειας ΤΠ»: περιλαμβάνουν συνιστώμενα αλλά μη υποχρεωτικά μέτρα, τα οποία βοηθούν στην εφαρμογή προτύπων ασφάλειας ΤΠ ή λειτουργούν ως σημείο αναφοράς όταν δεν προβλέπεται σχετικό πρότυπο·

15) «συμβάν ασφάλειας ΤΠ»: γεγονός που μπορεί να επηρεάσει δυσμενώς την εμπιστευτικότητα, ακεραιότητα ή διαθεσιμότητα ενός CIS·

16) «μέτρο ασφάλειας ΤΠ»: τεχνικό ή οργανωτικό μέτρο που αποσκοπεί στην άμβλυνση των κινδύνων ασφάλειας ΤΠ·

17) «ανάγκη ασφάλειας ΤΠ»: ακριβής και σαφής ορισμός των επιπέδων εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας που σχετίζονται με μια πληροφορία ή ένα σύστημα ΤΠ με στόχο τον καθορισμό του επιπέδου ασφαλείας που απαιτείται·

18) «στόχος ασφάλειας ΤΠ»: δήλωση πρόθεσης για αντιμετώπιση συγκεκριμένων απειλών και/ή εκπλήρωση συγκεκριμένων οργανωτικών απαιτήσεων ή παραδοχών ασφαλείας·

19) «σχέδιο ασφάλειας ΤΠ»: τεκμηρίωση των μέτρων ασφάλειας ΤΠ που απαιτούνται για την εκπλήρωση των αναγκών ασφάλειας ΤΠ ενός CIS·

20) «πολιτική ασφάλειας ΤΠ»: σύνολο στόχων που άπτονται της ασφάλειας ΤΠ, οι οποίοι έχουν τεθεί, υλοποιούνται και ελέγχονται ή πρέπει να τεθούν, να υλοποιηθούν και να ελεγχθούν. Περιλαμβάνει την παρούσα απόφαση και τους κανόνες εφαρμογής της·

21) «απαίτηση ασφάλειας ΤΠ»: τυποποιημένη ανάγκη ασφάλειας ΤΠ μέσω προκαθορισμένης διεργασίας·

22) «κίνδυνος ασφάλειας ΤΠ»: η επίδραση που μπορεί να επιφέρει μια απειλή κατά της ασφάλειας ΤΠ σε ένα CIS εκμεταλλευόμενη ένα τρωτό σημείο. Στο πλαίσιο αυτό, ένας κίνδυνος για την ασφάλεια ΤΠ χαρακτηρίζεται από δύο παράγοντες: 1) την αβεβαιότητα, ήτοι την πιθανότητα κάποια απειλή για την ασφάλεια ΤΠ να προκαλέσει ανεπιθύμητο γεγονός, και 2) τον αντίκτυπο, ήτοι τις επιπτώσεις που το εν λόγω ανεπιθύμητο γεγονός μπορεί να έχει σε ένα CIS·

23) «πρότυπα ασφάλειας ΤΠ»: συγκεκριμένα υποχρεωτικά μέτρα ασφάλειας ΤΠ που βοηθούν στην επιβολή και την υποστήριξη της πολιτικής ασφάλειας ΤΠ·

24) «στρατηγική ασφάλειας ΤΠ»: σύνολο προγραμμάτων και δραστηριοτήτων που σχεδιάζονται με γνώμονα την επίτευξη των στόχων της Επιτροπής και τα οποία πρέπει να καταρτίζονται, να εφαρμόζονται και να ελέγχονται·

25) «απειλή κατά της ασφάλειας ΤΠ»: παράγοντας που είναι πιθανό να προκαλέσει την επέλευση ανεπιθύμητου γεγονότος το οποίο μπορεί να έχει ζημιογόνο αποτέλεσμα για ένα CIS. Οι απειλές αυτές μπορεί να είναι τυχαίες ή εσκεμμένες και χαρακτηρίζονται από απειλητικά στοιχεία, πιθανούς στόχους και μεθόδους επίθεσης·

26) «τοπικός υπεύθυνος ασφάλειας πληροφορικής» ή «ΤΥΑΠ»: ο υπάλληλος της Επιτροπής που είναι επιφορτισμένος με καθήκοντα συνδέσμου σε θέματα ασφάλειας ΤΠ σε ένα τμήμα της Επιτροπής·

27) «δεδομένα προσωπικού χαρακτήρα», «επεξεργασία δεδομένων προσωπικού χαρακτήρα», «υπεύθυνος της επεξεργασίας» και «αρχείο δεδομένων προσωπικού χαρακτήρα»: έχουν την έννοια που τους αποδίδεται στον κανονισμό (ΕΚ) αριθ. 45/2001 και ειδικότερα στο άρθρο 2 του εν λόγω κανονισμού·

28) «επεξεργασία πληροφοριών»: όλες οι λειτουργίες ενός CIS που αφορούν σύνολα δεδομένων, συμπεριλαμβανομένης της δημιουργίας, τροποποίησης, προβολής, αποθήκευσης, μετάδοσης, διαγραφής και αρχειοθέτησης πληροφοριών. Τα CIS μπορούν να παρέχουν επεξεργασία πληροφοριών ως σύνολο λειτουργικών δυνατοτήτων προς χρήστες και ως υπηρεσίες ΤΠ προς άλλα CIS·

29) «επαγγελματικό απόρρητο»: η προστασία πληροφοριών για επιχειρηματικά δεδομένα που αποτελούν εκ φύσεως επαγγελματικά απόρρητα, ιδίως πληροφοριών σχετικών με επιχειρήσεις που αφορούν τις εμπορικές τους σχέσεις και τα κοστολογικά τους στοιχεία, όπως ορίζεται στο άρθρο 339 της ΣΛΕΕ·

30) «αρμόδιος»: πρόσωπο που έχει την υποχρέωση να ενεργεί και να λαμβάνει αποφάσεις για την επίτευξη ζητούμενων αποτελεσμάτων·

31) «ασφάλεια στην Επιτροπή»: η ασφάλεια των προσώπων, των περιουσιακών στοιχείων και των πληροφοριών στην Επιτροπή, και ειδικότερα η σωματική ακεραιότητα των προσώπων και η φυσική ακεραιότητα των περιουσιακών στοιχείων, η ακεραιότητα, η εμπιστευτικότητα και η διαθεσιμότητα των πληροφοριών και των συστημάτων επικοινωνίας και πληροφοριών, καθώς και η απρόσκοπτη λειτουργία των δραστηριοτήτων της Επιτροπής·

32) «κοινή υπηρεσία ΤΠ»: η υπηρεσία που παρέχει ένα CIS σε άλλα CIS στο πλαίσιο της επεξεργασίας πληροφοριών·

33) «ιδιοκτήτης του συστήματος»: το πρόσωπο που είναι αρμόδιο γενικά για την προμήθεια, ανάπτυξη, ενοποίηση, τροποποίηση, λειτουργία, συντήρηση και απόσυρση ενός CIS·

34) «χρήστης»: κάθε πρόσωπο που χρησιμοποιεί λειτουργική δυνατότητα παρεχόμενη από CIS είτε εντός είτε εκτός της Επιτροπής.

Άρθρο 3

Αρχές που διέπουν την ασφάλεια ΤΠ στην Επιτροπή

1. Η ασφάλεια ΤΠ στην Επιτροπή βασίζεται στις αρχές της νομιμότητας, της διαφάνειας, της αναλογικότητας και της λογοδοσίας.

2. Οι πτυχές της ασφάλειας ΤΠ συνεκτιμώνται ήδη από την αρχή της ανάπτυξης και υλοποίησης των CIS της Επιτροπής. Για την επίτευξη του σκοπού αυτού η Γενική Διεύθυνση Πληροφορικής και η Γενική Διεύθυνση Ανθρωπίνων Πόρων και Ασφάλειας συμμετέχουν στο πλαίσιο των αντίστοιχων τομέων αρμοδιότητάς τους.

3. Η αποτελεσματική ασφάλεια ΤΠ εξασφαλίζει κατάλληλα επίπεδα όσον αφορά την τήρηση των ακόλουθων αρχών:

α) γνησιότητα: η εγγύηση ότι οι πληροφορίες είναι γνήσιες και από καλόπιστες πηγές·

β) διαθεσιμότητα: η ιδιότητα του συστήματος να είναι προσβάσιμο και έτοιμο προς χρήση κατόπιν αιτήματος εξουσιοδοτημένου φορέα·

γ) εμπιστευτικότητα: η ιδιότητα της μη κοινολόγησης πληροφοριών σε μη εξουσιοδοτημένα πρόσωπα, φορείς ή διαδικασίες·

δ) ακεραιότητα: η ιδιότητα της διαφύλαξης της ακρίβειας και της πληρότητας των πληροφοριών και των στοιχείων·

ε) μη άρνηση αναγνώρισης: η ικανότητα απόδειξης της διεξαγωγής ενέργειας ή γεγονότος, ούτως ώστε να μην είναι δυνατή η άρνηση της εν λόγω ενέργειας ή του γεγονότος·

στ) προστασία δεδομένων προσωπικού χαρακτήρα: η πρόβλεψη κατάλληλων εγγυήσεων για τα δεδομένα προσωπικού χαρακτήρα σε πλήρη συμμόρφωση με τον κανονισμό (ΕΚ) αριθ. 45/2001·

ζ) επαγγελματικό απόρρητο: η προστασία πληροφοριών που αποτελούν εκ φύσεως επαγγελματικά απόρρητα, ιδίως πληροφοριών σχετικών με επιχειρήσεις που αφορούν τις εμπορικές τους σχέσεις και τα κοστολογικά τους στοιχεία, όπως ορίζεται στο άρθρο 339 της ΣΛΕΕ.

4. Η ασφάλεια ΤΠ βασίζεται σε διαδικασία διαχείρισης κινδύνων. Η διαδικασία αυτή αποσκοπεί στον προσδιορισμό του επιπέδου των κινδύνων ασφάλειας ΤΠ και τον καθορισμό μέτρων ασφαλείας για τον περιορισμό των κινδύνων αυτών σε αποδεκτό επίπεδο και με αναλογικό κόστος.

5. Όλα τα CIS προσδιορίζονται, ανατίθενται σε ιδιοκτήτη συστήματος και καταγράφονται σε κατάλογο.

6. Οι απαιτήσεις ασφαλείας κάθε CIS καθορίζονται βάσει των αναγκών ασφαλείας του, καθώς και των αναγκών ασφαλείας των πληροφοριών που επεξεργάζεται. Με γνώμονα την κάλυψη συγκεκριμένων επιπέδων αναγκών ασφαλείας μπορεί να σχεδιάζονται CIS που παρέχουν υπηρεσίες σε άλλα CIS.

7. Τα σχέδια ασφάλειας ΤΠ και τα μέτρα ασφάλειας ΤΠ είναι ανάλογα με τις ανάγκες ασφαλείας του CIS.

Οι διεργασίες που σχετίζονται με τις εν λόγω αρχές και δραστηριότητες εξειδικεύονται στους κανόνες εφαρμογής.

ΚΕΦΑΛΑΙΟ 2

ΟΡΓΑΝΩΣΗ ΚΑΙ ΑΡΜΟΔΙΟΤΗΤΕΣ

Άρθρο 4

Συμβούλιο εσωτερικής διοίκησης

Το συμβούλιο εσωτερικής διοίκησης αναλαμβάνει τη γενική ευθύνη για τη διακυβέρνηση της ασφάλειας ΤΠ στο σύνολό της εντός της Επιτροπής.

Άρθρο 5

Διοικούσα επιτροπή ασφάλειας πληροφοριών (ΔΕΑΠ)

1. Της ΔΕΑΠ προεδρεύει ο αναπληρωτής γενικός γραμματέας που είναι αρμόδιος για τη διακυβέρνηση της ασφάλειας ΤΠ στην Επιτροπή. Τα μέλη της εκπροσωπούν τα συμφέροντα των τμημάτων της Επιτροπής σε θέματα επιχειρήσεων, τεχνολογίας και ασφάλειας, και περιλαμβάνουν εκπροσώπους της Γενικής Διεύθυνσης Πληροφορικής, της Γενικής Διεύθυνσης Ανθρωπίνων Πόρων και Ασφάλειας, της Γενικής Διεύθυνσης Προϋπολογισμού και, εκ περιτροπής ανά διετία, εκπροσώπους τεσσάρων άλλων τμημάτων της Επιτροπής, οι οποίοι συμμετέχουν στις εργασίες της όταν η ασφάλεια ΤΠ αποτελεί σημαντική παράμετρο για τις δραστηριότητές τους. Στη σύνθεσή της συμμετέχουν μόνο ανώτερα διοικητικά στελέχη.

2. Η ΔΕΑΠ συνεπικουρεί το συμβούλιο εσωτερικής διοίκησης στα καθήκοντά του που σχετίζονται με την ασφάλεια ΤΠ. Η ΔΕΑΠ αναλαμβάνει την επιχειρησιακή ευθύνη για τη διακυβέρνηση της ασφάλειας ΤΠ στο σύνολό της εντός της Επιτροπής.

3. Η ΔΕΑΠ εισηγείται την πολιτική ασφάλειας ΤΠ της Επιτροπής προς έγκριση από την Επιτροπή.

4. Η ΔΕΑΠ προβαίνει σε επανεξέταση και υποβολή αναφοράς σε εξαμηνιαία βάση στο συμβούλιο εσωτερικής διοίκησης σχετικά με θέματα διακυβέρνησης καθώς και με ζητήματα που σχετίζονται με την ασφάλεια ΤΠ, όπως σοβαρά συμβάντα ασφάλειας ΤΠ.

5. Η ΔΕΑΠ παρακολουθεί και επανεξετάζει τη συνολικότερη εφαρμογή της παρούσας απόφασης και υποβάλλει σχετική αναφορά στο συμβούλιο εσωτερικής διοίκησης.

6. Κατόπιν πρότασης της Γενικής Διεύθυνσης Πληροφορικής, η ΔΕΑΠ εξετάζει, εγκρίνει και παρακολουθεί την εφαρμογή της κυλιόμενης στρατηγικής ασφάλειας ΤΠ. Η ΔΕΑΠ υποβάλλει σχετική αναφορά στο συμβούλιο εσωτερικής διοίκησης.

7. Η ΔΕΑΠ παρακολουθεί, αξιολογεί και ελέγχει το περιβάλλον διαχείρισης κινδύνου για τις εσωτερικές πληροφορίες και έχει την εξουσία να εκδίδει τυπικές προδιαγραφές για βελτιώσεις όποτε κρίνεται αναγκαίο.

Οι διεργασίες που σχετίζονται με τις εν λόγω αρμοδιότητες και δραστηριότητες εξειδικεύονται στους κανόνες εφαρμογής.

Άρθρο 6

Γενική Διεύθυνση Ανθρώπινων Πόρων και Ασφάλειας

Σε σχέση με την ασφάλεια ΤΠ, η Γενική Διεύθυνση Ανθρώπινων Πόρων και Ασφάλειας έχει τις ακόλουθες αρμοδιότητες. Συγκεκριμένα:

1) διασφαλίζει την ευθυγράμμιση της πολιτικής ασφάλειας ΤΠ με την πολιτική ασφάλειας πληροφοριών της Επιτροπής·

2) θεσπίζει πλαίσιο για την εξουσιοδότηση της χρήσης τεχνολογιών κρυπτογράφησης για την αποθήκευση και μετάδοση πληροφοριών από τα CIS·

3) ενημερώνει τη Γενική Διεύθυνση Πληροφορικής σχετικά με συγκεκριμένες απειλές που θα μπορούσαν να έχουν σημαντικό αντίκτυπο στην ασφάλεια των CIS και των συνόλων δεδομένων που αυτά υποβάλλουν σε επεξεργασία·

4) διενεργεί επιθεωρήσεις ασφάλειας ΤΠ προκειμένου να αξιολογεί τη συμμόρφωση των CIS της Επιτροπής με την πολιτική ασφαλείας και αναφέρει τα αποτελέσματα στη ΔΕΑΠ·

5) θεσπίζει πλαίσιο για την εξουσιοδότηση πρόσβασης στα CIS της Επιτροπής από εξωτερικά δίκτυα και για τους σχετικούς κανόνες δέουσας ασφάλειας, και καταρτίζει τα σχετικά πρότυπα και κατευθυντήριες οδηγίες σε θέματα ασφάλειας ΤΠ σε στενή συνεργασία με τη Γενική Διεύθυνση Πληροφορικής·

6) προτείνει αρχές και κανόνες για την εξωτερική ανάθεση CIS ώστε να διατηρείται ο δέων έλεγχος της ασφάλειας των πληροφοριών·

7) καταρτίζει τα σχετικά πρότυπα και κατευθυντήριες οδηγίες σε θέματα ασφάλειας ΤΠ που προβλέπονται στο άρθρο 6, σε στενή συνεργασία με τη Γενική Διεύθυνση Πληροφορικής.

Οι διεργασίες που σχετίζονται με τις εν λόγω αρμοδιότητες και δραστηριότητες εξειδικεύονται στους κανόνες εφαρμογής.

Άρθρο 7

Γενική Διεύθυνση Πληροφορικής

Σε σχέση με τη συνολική ασφάλεια ΤΠ της Επιτροπής, η Γενική Διεύθυνση Πληροφορικής έχει τις ακόλουθες αρμοδιότητες. Συγκεκριμένα:

1) καταρτίζει πρότυπα και κατευθυντήριες οδηγίες σε θέματα ασφάλειας ΤΠ, με εξαίρεση τα προβλεπόμενα στο άρθρο 6, σε στενή συνεργασία με τη Γενική Διεύθυνση Ανθρώπινων Πόρων και Ασφάλειας, ώστε να διασφαλίζεται η συνεκτικότητα της πολιτικής ασφάλειας ΤΠ με την πολιτική ασφάλειας πληροφοριών της Επιτροπής, τα οποία και προτείνει στη ΔΕΑΠ·

2) αξιολογεί τις μεθόδους, τις διαδικασίες και τα αποτελέσματα σε θέματα διαχείρισης των κινδύνων ασφάλειας ΤΠ όλων των τμημάτων της Επιτροπής και υποβάλλει τακτικά σχετική αναφορά στη ΔΕΑΠ·

3) εισηγείται προς αναθεώρηση και έγκριση από τη ΔΕΑΠ και επικύρωση από το συμβούλιο εσωτερικής διοίκησης κυλιόμενη στρατηγική ασφάλειας ΤΠ, και προτείνει πρόγραμμα που περιλαμβάνει, μεταξύ άλλων, τον σχεδιασμό προγραμμάτων και δραστηριοτήτων για την υλοποίηση της στρατηγικής ασφάλειας ΤΠ·

4) παρακολουθεί την εκτέλεση της στρατηγικής ασφάλειας ΤΠ της Επιτροπής και υποβάλλει τακτικά σχετική αναφορά στη ΔΕΑΠ·

5) παρακολουθεί τους κινδύνους ασφάλειας ΤΠ και τα μέτρα ασφάλειας ΤΠ που εφαρμόζονται σε σχέση με τα CIS και υποβάλλει τακτικά σχετική αναφορά στη ΔΕΑΠ·

6) υποβάλλει τακτικά αναφορά στη ΔΕΑΠ σχετικά με τη συνολικότερη εφαρμογή και συμμόρφωση με την παρούσα απόφαση·

7) κατόπιν διαβούλευσης με τη Γενική Διεύθυνση Ανθρώπινων Πόρων και Ασφάλειας, ζητά από τους ιδιοκτήτες των συστημάτων να λαμβάνουν συγκεκριμένα μέτρα ασφάλειας ΤΠ για την άμβλυνση των κινδύνων ασφάλειας ΤΠ που αντιμετωπίζουν τα CIS της Επιτροπής·

8) μεριμνά ώστε οι ιδιοκτήτες των συστημάτων και οι ιδιοκτήτες των δεδομένων να έχουν στη διάθεσή τους επαρκή κατάλογο υπηρεσιών ασφάλειας ΤΠ της Γενικής Διεύθυνσης Πληροφορικής για να είναι σε θέση να εκπληρώνουν τις υποχρεώσεις τους σε θέματα ασφάλειας ΤΠ και να συμμορφώνονται με την πολιτική και τα πρότυπα ασφάλειας ΤΠ·

9) παρέχει επαρκή τεκμηρίωση στους ιδιοκτήτες των συστημάτων και τους ιδιοκτήτες των δεδομένων και προβαίνει σε διαβουλεύσεις μαζί τους, όταν κρίνεται σκόπιμο, σχετικά με τα μέτρα ασφάλειας ΤΠ που εφαρμόζονται για τις οικείες υπηρεσίες ΤΠ, ώστε να διευκολύνεται η συμμόρφωση με την πολιτική ασφάλειας ΤΠ και να παρέχεται υποστήριξη στους ιδιοκτήτες των συστημάτων κατά τη διαχείριση των κινδύνων ασφάλειας ΤΠ·

10) διοργανώνει τακτικές συνεδριάσεις του δικτύου των ΤΥΑΠ και παρέχει υποστήριξη στους ΤΥΑΠ κατά την άσκηση των καθηκόντων τους·

11) προσδιορίζει τις ανάγκες κατάρτισης και συντονίζει τα προγράμματα κατάρτισης σε θέματα ασφάλειας ΤΠ σε συνεργασία με τα τμήματα της Επιτροπής, και οργανώνει, υλοποιεί και συντονίζει εκστρατείες ευαισθητοποίησης για την ασφάλεια ΤΠ σε στενή συνεργασία με τη Γενική Διεύθυνση Ανθρώπινων Πόρων και Ασφάλειας·

12) μεριμνά για την ενημέρωση των ιδιοκτητών των συστημάτων και των δεδομένων, αλλά και άλλων υπαλλήλων επιφορτισμένων με αρμοδιότητες ασφάλειας ΤΠ τμημάτων της Επιτροπής, σχετικά με την πολιτική ασφάλειας ΤΠ·

13) ενημερώνει τη Γενική Διεύθυνση Ανθρώπινων Πόρων και Ασφάλειας για συγκεκριμένες απειλές και συμβάντα ασφάλειας ΤΠ καθώς και για εξαιρέσεις στην πολιτική ασφάλειας ΤΠ της Επιτροπής που κοινοποιούνται από τους ιδιοκτήτες των συστημάτων και θα μπορούσαν να έχουν σημαντικό αντίκτυπο στην ασφάλεια της Επιτροπής·

14) στο πλαίσιο του ρόλου της ως εσωτερικού παρόχου υπηρεσιών ΤΠ, υποβάλλει στην Επιτροπή κατάλογο των κοινών υπηρεσιών ΤΠ που παρέχουν καθορισμένα επίπεδα ασφαλείας. Προς τούτο προβαίνει σε συστηματική αξιολόγηση, διαχείριση και παρακολούθηση των κινδύνων ασφάλειας ΤΠ, με στόχο την εφαρμογή των μέτρων ασφαλείας που καθιστούν δυνατή την επίτευξη του καθορισμένου επιπέδου ασφαλείας.

Οι σχετικές διεργασίες και αναλυτικότερες αρμοδιότητες καθορίζονται περαιτέρω στους κανόνες εφαρμογής.

Άρθρο 8

Τμήματα της Επιτροπής

Σε σχέση με την ασφάλεια ΤΠ στο τμήμα του, κάθε προϊστάμενος τμήματος της Επιτροπής:

1) αναθέτει επισήμως καθήκοντα ιδιοκτήτη συστήματος για κάθε CIS σε μόνιμο ή έκτακτο υπάλληλο, ο οποίος καθίσταται αρμόδιος για την ασφάλεια ΤΠ του εν λόγω CIS, και αναθέτει επισήμως καθήκοντα ιδιοκτήτη δεδομένων για κάθε σύνολο δεδομένων που αποτελεί αντικείμενο χειρισμού στο πλαίσιο ενός CIS σε πρόσωπο το οποίο πρέπει να ανήκει στη διοικητική οντότητα του υπεύθυνου της επεξεργασίας για τα σύνολα δεδομένων που υπόκεινται στον κανονισμό (ΕΚ) αριθ. 45/2001·

2) ορίζει επισήμως τοπικό υπεύθυνο ασφάλειας πληροφορικής (ΤΥΑΠ) ο οποίος μπορεί να εκτελεί τα καθήκοντά του ανεξάρτητα από τους ιδιοκτήτες των συστημάτων και τους ιδιοκτήτες των πληροφοριών. Κάθε ΤΥΑΠ μπορεί να ορίζεται αρμόδιος για ένα ή περισσότερα τμήματα της Επιτροπής·

3) διασφαλίζει ότι έχουν εκπονηθεί και εφαρμόζονται κατάλληλες αξιολογήσεις κινδύνων ασφάλειας ΤΠ και σχέδια ασφάλειας ΤΠ·

4) μεριμνά για την υποβολή σύνοψης των κινδύνων και των μέτρων ασφάλειας ΤΠ σε τακτική βάση στη Γενική Διεύθυνση Πληροφορικής·

5) διασφαλίζει, με τη συνδρομή της Γενικής Διεύθυνσης Πληροφορικής, ότι έχουν θεσπιστεί όλες οι κατάλληλες διεργασίες, διαδικασίες και λύσεις που εξασφαλίζουν τον αποτελεσματικό εντοπισμό, την αναφορά και την επίλυση συμβάντων ασφάλειας ΤΠ σε σχέση με τα CIS της αρμοδιότητάς τους·

6) κινεί διαδικασία έκτακτης ανάγκης σε καταστάσεις έκτακτης ανάγκης που αφορούν την ασφάλεια ΤΠ·

7) υπέχει την τελική ευθύνη λογοδοσίας για την ασφάλεια ΤΠ, μεταξύ άλλων, και σε σχέση με τις αρμοδιότητες των ιδιοκτητών των συστημάτων και των ιδιοκτητών των δεδομένων·

8) αναλαμβάνει τους κινδύνους σε σχέση με τα CIS και τα σύνολα δεδομένων της αρμοδιότητάς του·

9) επιλύει οποιεσδήποτε διαφωνίες μεταξύ ιδιοκτητών των δεδομένων και ιδιοκτητών των συστημάτων και, σε περίπτωση που εξακολουθεί να υπάρχει διαφωνία, θέτει το θέμα προς επίλυση ενώπιον της ΔΕΑΠ·

10) διασφαλίζει ότι τα σχέδια ασφάλειας ΤΠ και τα μέτρα ασφάλειας ΤΠ εφαρμόζονται και ότι οι κίνδυνοι καλύπτονται επαρκώς.

Οι διεργασίες που σχετίζονται με τις εν λόγω αρμοδιότητες και δραστηριότητες εξειδικεύονται στους κανόνες εφαρμογής.

Άρθρο 9

Ιδιοκτήτες των συστημάτων

1. Ο ιδιοκτήτης του συστήματος είναι αρμόδιος για την ασφάλεια ΤΠ του CIS και λογοδοτεί στον προϊστάμενο του τμήματος της Επιτροπής.

2. Σε σχέση με την ασφάλεια ΤΠ, ο ιδιοκτήτης του συστήματος:

α) μεριμνά για τη συμμόρφωση του CIS με την πολιτική ασφάλειας ΤΠ·

β) μεριμνά για την ακριβή καταγραφή του CIS στον σχετικό κατάλογο·

γ) αξιολογεί τους κινδύνους ασφάλειας ΤΠ και προσδιορίζει τις ανάγκες ασφάλειας ΤΠ για κάθε CIS, σε συνεργασία με τους ιδιοκτήτες των δεδομένων και σε διαβούλευση με τη Γενική Διεύθυνση Πληροφορικής·

δ) εκπονεί σχέδιο ασφαλείας, το οποίο περιλαμβάνει, κατά περίπτωση, λεπτομερή στοιχεία σχετικά με τους αξιολογηθέντες κινδύνους και τα πρόσθετα μέτρα ασφαλείας που τυχόν απαιτούνται·

ε) εφαρμόζει κατάλληλα μέτρα ασφάλειας ΤΠ, τα οποία είναι ανάλογα με τους προσδιορισθέντες κινδύνους ασφάλειας ΤΠ, και εφαρμόζει τις συστάσεις που έχουν επικυρωθεί από τη ΔΕΑΠ·

στ) εντοπίζει οποιεσδήποτε εξαρτήσεις από άλλα CIS ή κοινές υπηρεσίες ΤΠ και εφαρμόζει μέτρα ασφαλείας, εφόσον απαιτούνται, με βάση τα επίπεδα ασφαλείας που προτείνονται από τα εν λόγω CIS ή τις κοινές υπηρεσίες ΤΠ·

ζ) διαχειρίζεται και παρακολουθεί τους κινδύνους ασφάλειας ΤΠ·

η) υποβάλλει τακτικά αναφορά στον προϊστάμενο του τμήματος της Επιτροπής σχετικά με το προφίλ κινδύνου του CIS της αρμοδιότητάς του και υποβάλλει αναφορά στη Γενική Διεύθυνση Πληροφορικής σχετικά με τους συναφείς κινδύνους, τις δραστηριότητες διαχείρισης κινδύνου και τα μέτρα ασφαλείας που λαμβάνει·

θ) προβαίνει σε διαβούλευση με τον ΤΥΑΠ του οικείου τμήματος ή τμημάτων της Επιτροπής σχετικά με πτυχές της ασφάλειας ΤΠ·

ι) παρέχει οδηγίες στους χρήστες σχετικά με τη χρήση του CIS και των σχετικών δεδομένων, καθώς και σχετικά με τις αρμοδιότητες των χρηστών σε σχέση με το CIS·

ια) ζητά την έγκριση της Γενικής Διεύθυνσης Ανθρώπινων Πόρων και Ασφάλειας, η οποία ενεργεί ως αρχή πιστοποίησης της ασφάλειας, για κάθε CIS που χρησιμοποιεί τεχνολογία κρυπτογράφησης·

ιβ) προβαίνει εκ των προτέρων σε διαβούλευση με την Αρχή Ασφαλείας της Επιτροπής σχετικά με κάθε σύστημα που επεξεργάζεται διαβαθμισμένες πληροφορίες της ΕΕ·

ιγ) μεριμνά για την αποθήκευση αντιγράφων ασφαλείας των κλειδιών αποκρυπτογράφησης σε λογαριασμό μεσεγγύησης. Η ανάκτηση των κρυπτογραφημένων δεδομένων εκτελείται μόνο εφόσον δοθεί σχετική έγκριση σύμφωνα με το πλαίσιο που ορίζεται από τη Γενική Διεύθυνση Ανθρώπινων Πόρων και Ασφάλειας·

ιδ) εφαρμόζει τις οδηγίες που τυχόν παρέχονται από τον αρμόδιο ή τους αρμόδιους υπεύθυνους της επεξεργασίας σχετικά με την προστασία δεδομένων προσωπικού χαρακτήρα και την εφαρμογή των κανόνων προστασίας δεδομένων που αφορούν την ασφάλεια της επεξεργασίας·

ιε) κοινοποιεί στη Γενική Διεύθυνση Πληροφορικής τυχόν εξαιρέσεις στην πολιτική ασφάλειας ΤΠ της Επιτροπής, συμπεριλαμβανομένων των σχετικών λόγων·

ιστ) αναφέρει οποιεσδήποτε μη επιλυθείσες διαφωνίες μεταξύ του ιδιοκτήτη των δεδομένων και του ιδιοκτήτη του συστήματος στον προϊστάμενο του τμήματος της Επιτροπής, και ενημερώνει εγκαίρως τα εμπλεκόμενα ενδιαφερόμενα μέρη για συμβάντα ασφάλειας ΤΠ, όπως απαιτείται αναλόγως της σοβαρότητάς τους κατά τα οριζόμενα στο άρθρο 15·

ιζ) σε περιπτώσεις συστημάτων που αποτελούν αντικείμενο εξωτερικής ανάθεσης, μεριμνά για τη συμπερίληψη κατάλληλων διατάξεων για την ασφάλεια ΤΠ στη σύμβαση εξωτερικής ανάθεσης, καθώς και για την αναφορά κατά τα οριζόμενα στο άρθρο 15 κάθε συμβάντος ασφάλειας ΤΠ που αφορά CIS το οποίο αποτελεί αντικείμενο εξωτερικής ανάθεσης·

ιη) στην περίπτωση CIS που παρέχει κοινές υπηρεσίες ΤΠ, μεριμνά για την παροχή και τη σαφή τεκμηρίωση καθορισμένου επιπέδου ασφαλείας, καθώς και για την εφαρμογή μέτρων ασφαλείας για το εν λόγω CIS προκειμένου να επιτευχθεί το καθορισμένο επίπεδο ασφαλείας.

3. Οι ιδιοκτήτες των συστημάτων μπορούν να αναθέτουν επισήμως μέρος ή το σύνολο των καθηκόντων τους που σχετίζονται με την ασφάλεια πληροφοριών, διατηρώντας ωστόσο την ευθύνη για την ασφάλεια ΤΠ των CIS της αρμοδιότητάς τους.

Οι διεργασίες που σχετίζονται με τις εν λόγω αρμοδιότητες και δραστηριότητες εξειδικεύονται στους κανόνες εφαρμογής.

Άρθρο 10

Ιδιοκτήτες των δεδομένων

1. Ο ιδιοκτήτης των δεδομένων είναι αρμόδιος για την ασφάλεια ΤΠ ενός συγκεκριμένου συνόλου δεδομένων και λογοδοτεί στον προϊστάμενο του τμήματος της Επιτροπής και είναι υπόλογος για την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα του συνόλου δεδομένων.

2. Σε σχέση με αυτό το σύνολο δεδομένων, ο ιδιοκτήτης των δεδομένων:

α) διασφαλίζει την ορθή διαβάθμιση όλων των συνόλων δεδομένων που βρίσκονται υπ' ευθύνη του, σύμφωνα με τις αποφάσεις (ΕΕ, Ευρατόμ) 2015/443 και (ΕΕ, Ευρατόμ) 2015/444·

β) προσδιορίζει τις ανάγκες ασφάλειας πληροφοριών και ενημερώνει τους οικείους ιδιοκτήτες των συστημάτων για τις εν λόγω ανάγκες·

γ) συμμετέχει στην αξιολόγηση κινδύνων του CIS·

δ) αναφέρει οποιεσδήποτε μη επιλυθείσες διαφωνίες μεταξύ του ιδιοκτήτη των δεδομένων και του ιδιοκτήτη του συστήματος στον προϊστάμενο του τμήματος της Επιτροπής·

ε) ενημερώνει εγκαίρως για συμβάντα ασφάλειας ΤΠ κατά τα οριζόμενα στο άρθρο 15.

3. Οι ιδιοκτήτες των δεδομένων μπορούν να αναθέτουν επισήμως μέρος ή το σύνολο των καθηκόντων τους που σχετίζονται με την ασφάλεια πληροφοριών, διατηρώντας ωστόσο τις υποχρεώσεις τους κατά τα οριζόμενα στο παρόν άρθρο.

Οι διεργασίες που σχετίζονται με τις εν λόγω αρμοδιότητες και δραστηριότητες εξειδικεύονται στους κανόνες εφαρμογής.

Άρθρο 11

Τοπικοί υπεύθυνοι ασφάλειας πληροφορικής (ΤΥΑΠ)

Σε σχέση με την ασφάλεια ΤΠ, ο ΤΥΑΠ:

α) εντοπίζει εκ των προτέρων και ενημερώνει τους ιδιοκτήτες των συστημάτων και των δεδομένων αλλά και άλλους υπαλλήλους επιφορτισμένους με αρμοδιότητες ασφάλειας ΤΠ τμημάτων της Επιτροπής σχετικά με την πολιτική ασφάλειας ΤΠ·

β) ασκεί καθήκοντα συνδέσμου ως μέρος του δικτύου των ΤΥΑΠ με τη Γενική Διεύθυνση Πληροφορικής όσον αφορά ζητήματα που σχετίζονται με την ασφάλεια ΤΠ στο τμήμα ή τα τμήματα της Επιτροπής·

γ) παρίσταται στις τακτικές συνεδριάσεις των ΤΥΑΠ·

δ) διατηρεί την εποπτεία της διαδικασίας διαχείρισης κινδύνων ασφάλειας πληροφοριών και της ανάπτυξης και εφαρμογής σχεδίων ασφαλείας συστημάτων επικοινωνίας·

ε) συμβουλεύει τους ιδιοκτήτες των δεδομένων, τους ιδιοκτήτες των συστημάτων και τους προϊστάμενους τμημάτων της Επιτροπής όσον αφορά ζητήματα που σχετίζονται με την ασφάλεια ΤΠ·

στ) συνεργάζεται με τη Γενική Διεύθυνση Πληροφορικής για τη διάδοση ορθών πρακτικών ασφάλειας ΤΠ και προτείνει εξειδικευμένα προγράμματα ευαισθητοποίησης και κατάρτισης·

ζ) υποβάλλει αναφορές στον προϊστάμενο του τμήματος ή των τμημάτων της Επιτροπής σχετικά με την ασφάλεια ΤΠ, τις εντοπισθείσες ελλείψεις και βελτιώσεις.

Οι διεργασίες που σχετίζονται με τις εν λόγω αρμοδιότητες και δραστηριότητες εξειδικεύονται στους κανόνες εφαρμογής.

Άρθρο 12

Χρήστες

1. Σε σχέση με την ασφάλεια ΤΠ, οι χρήστες:

α) συμμορφώνονται με την πολιτική ασφάλειας ΤΠ και με τις οδηγίες του ιδιοκτήτη του συστήματος σχετικά με τη χρήση κάθε CIS·

β) ενημερώνουν εγκαίρως για συμβάντα ασφάλειας ΤΠ κατά τα οριζόμενα στο άρθρο 15.

2. Η χρήση του CIS της Επιτροπής κατά παράβαση της πολιτικής ασφάλειας ΤΠ ή των οδηγιών του ιδιοκτήτη του συστήματος μπορεί να οδηγήσει στην κίνηση πειθαρχικής διαδικασίας.

Οι διεργασίες που σχετίζονται με τις εν λόγω αρμοδιότητες και δραστηριότητες εξειδικεύονται στους κανόνες εφαρμογής.

ΚΕΦΑΛΑΙΟ 3

ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΥΠΟΧΡΕΩΣΕΙΣ ΣΧΕΤΙΚΑ ΜΕ ΤΗΝ ΑΣΦΑΛΕΙΑ

Άρθρο 13

Εφαρμογή της παρούσας απόφασης

1. Η έγκριση των κανόνων εφαρμογής για το άρθρο 6, καθώς και των σχετικών προτύπων και κατευθυντήριων οδηγιών, θα αποτελέσει αντικείμενο απόφασης εξουσιοδότησης της Επιτροπής υπέρ του μέλους της Επιτροπής που είναι αρμόδιο για θέματα ασφαλείας.

2. Η έγκριση όλων των άλλων κανόνων εφαρμογής σε σχέση με την παρούσα απόφαση, καθώς και των σχετικών προτύπων και κατευθυντήριων οδηγιών σε θέματα ΤΠ, θα αποτελέσει αντικείμενο απόφασης εξουσιοδότησης της Επιτροπής υπέρ του μέλους της Επιτροπής που είναι αρμόδιο για την πληροφορική.

3. Πριν από την έγκριση των κανόνων εφαρμογής, των προτύπων και των κατευθυντήριων οδηγιών που αναφέρονται στις παραγράφους 1 και 2 ανωτέρω λαμβάνεται η σύμφωνη γνώμη της ΔΕΑΠ.

Άρθρο 14

Υποχρέωση συμμόρφωσης

1. Η συμμόρφωση με τις διατάξεις που παρατίθενται στην πολιτική και στα πρότυπα ασφάλειας ΤΠ είναι υποχρεωτική.

2. Μη συμμόρφωση με την πολιτική και τα πρότυπα ΤΠ μπορεί να έχει ως αποτέλεσμα κίνηση πειθαρχικής διαδικασίας σύμφωνα με τις Συνθήκες, τον κανονισμό υπηρεσιακής κατάστασης και το καθεστώς που εφαρμόζεται στο λοιπό προσωπικό της Ένωσης, καθώς και συμβατικές κυρώσεις και/ή νομικές διαδικασίες δυνάμει εθνικών νομοθετικών και κανονιστικών διατάξεων.

3. Η Γενική Διεύθυνση Πληροφορικής ενημερώνεται για οποιεσδήποτε εξαιρέσεις στην πολιτική ασφάλειας ΤΠ.

4. Σε περίπτωση που η ΔΕΑΠ κρίνει ότι ένα CIS της Επιτροπής διατρέχει διαρκή, μη αποδεκτό κίνδυνο, η Γενική Διεύθυνση Πληροφορικής σε συνεργασία με τον ιδιοκτήτη του συστήματος προτείνει μέτρα άμβλυνσης προς έγκριση από τη ΔΕΑΠ. Τα μέτρα αυτά μπορεί να περιλαμβάνουν, μεταξύ άλλων, μέτρα ενισχυμένης παρακολούθησης και αναφοράς, περιορισμού και αποσύνδεσης υπηρεσίας.

5. Η ΔΕΑΠ επιβάλλει την εφαρμογή εγκεκριμένων μέτρων άμβλυνσης όποτε κρίνεται αναγκαίο. Η ΔΕΑΠ δύναται επίσης να εισηγείται στον Γενικό Διευθυντή της Γενικής Διεύθυνσης Ανθρώπινων Πόρων και Ασφάλειας την κίνηση διοικητικής έρευνας. Η Γενική Διεύθυνση Πληροφορικής υποβάλλει αναφορά στη ΔΕΑΠ σχετικά με την εξέλιξη της κατάστασης σε περίπτωση επιβολής μέτρων άμβλυνσης.

Οι διεργασίες που σχετίζονται με τις εν λόγω αρμοδιότητες και δραστηριότητες εξειδικεύονται στους κανόνες εφαρμογής.

Άρθρο 15

Χειρισμός συμβάντων ασφάλειας ΤΠ

1. Η Γενική Διεύθυνση Πληροφορικής είναι αρμόδια για την εξασφάλιση της κύριας επιχειρησιακής ικανότητας αντιμετώπισης συμβάντων ασφάλειας ΤΠ στην Ευρωπαϊκή Επιτροπή.

2. Ως εμπλεκόμενος φορέας που συνεισφέρει στην αντιμετώπιση των συμβάντων ασφάλειας ΤΠ, η Γενική Διεύθυνση Ανθρώπινων Πόρων και Ασφάλειας:

α) έχει δικαίωμα πρόσβασης σε συνοπτικά πληροφοριακά στοιχεία για όλα τα αρχεία συμβάντων και στα πλήρη αρχεία κατόπιν σχετικού αιτήματος·

β) συμμετέχει στις ομάδες διαχείρισης κρίσεων συμβάντων ασφάλειας ΤΠ και στις διαδικασίες έκτακτης ανάγκης ασφάλειας ΤΠ·

γ) είναι αρμόδια για τις σχέσεις με τις υπηρεσίες επιβολής του νόμου και τις υπηρεσίες πληροφοριών·

δ) διενεργεί εγκληματολογική ανάλυση για την ασφάλεια στον κυβερνοχώρο σύμφωνα με το άρθρο 11 της απόφασης (ΕΕ, Ευρατόμ) 2015/443·

ε) κρίνει εάν συντρέχει ανάγκη να κινηθεί επίσημη έρευνα·

στ) ενημερώνει τη Γενική Διεύθυνση Πληροφορικής για οποιαδήποτε συμβάντα ασφάλειας ΤΠ που ενδέχεται να συνιστούν κίνδυνο για άλλα CIS.

3. Μεταξύ της Γενικής Διεύθυνσης Πληροφορικής και της Γενικής Διεύθυνσης Ανθρώπινων Πόρων και Ασφάλειας υπάρχει τακτική επικοινωνία για την ανταλλαγή πληροφοριών και τον συντονισμό του χειρισμού συμβάντων ασφαλείας, ιδίως δε συμβάντων ασφάλειας ΤΠ για τα οποία ενδεχομένως απαιτείται επίσημη έρευνα.

4. Οι υπηρεσίες συντονισμού συμβάντων της ομάδας αντιμετώπισης έκτακτων αναγκών στην πληροφορική για τα θεσμικά και λοιπά όργανα και τους οργανισμούς της ΕΕ («CERT-ΕΕ») μπορούν να χρησιμοποιούνται προς υποστήριξη της διαδικασίας χειρισμού συμβάντων όταν κρίνεται σκόπιμο, καθώς και για την ανταλλαγή γνώσεων με άλλα θεσμικά όργανα και οργανισμούς της ΕΕ που ενδέχεται να επηρεάζονται.

5. Οι ιδιοκτήτες των συστημάτων που εμπλέκονται σε ένα συμβάν ασφάλειας ΤΠ:

α) ενημερώνουν αμέσως τον προϊστάμενο του οικείου τμήματος της Επιτροπής, τη Γενική Διεύθυνση Πληροφορικής, τη Γενική Διεύθυνση Ανθρώπινων Πόρων και Ασφάλειας, τον ΤΥΑΠ και, κατά περίπτωση, τον ιδιοκτήτη των δεδομένων όταν πρόκειται για σοβαρά συμβάντα ασφάλειας ΤΠ, ιδίως εφόσον αφορούν παραβίαση της εμπιστευτικότητας των δεδομένων·

β) συνεργάζονται με τις αρμόδιες αρχές της Επιτροπής και τηρούν τις οδηγίες τους σε θέματα επικοινωνίας, αντιμετώπισης και αποκατάστασης των συμβάντων.

6. Οι χρήστες αναφέρουν εγκαίρως κάθε συμβάν ή υπόνοια συμβάντος ασφάλειας ΤΠ στην αρμόδια υπηρεσία υποστήριξης ΤΠ.

7. Οι ιδιοκτήτες των δεδομένων αναφέρουν εγκαίρως κάθε συμβάν ή υποψία συμβάντος ασφάλειας ΤΠ στην αρμόδια ομάδα αντιμετώπισης συμβάντων ασφαλείας ΤΠ.

8. Η Γενική Διεύθυνση Πληροφορικής, με την υποστήριξη των λοιπών συνεισφερόντων εμπλεκόμενων φορέων, είναι αρμόδια για τον χειρισμό οποιουδήποτε συμβάντος ασφάλειας ΤΠ που εντοπίζεται σε σχέση με CIS της Επιτροπής, εφόσον δεν πρόκειται για συστήματα που αποτελούν αντικείμενο εξωτερικής ανάθεσης.

9. Η Γενική Διεύθυνση Πληροφορικής ενημερώνει σχετικά με τα συμβάντα ασφάλειας ΤΠ τα τμήματα της Επιτροπής που επηρεάζονται, τους αρμόδιους ΤΥΑΠ και, κατά περίπτωση, την CERT-ΕΕ βάσει της «ανάγκης γνώσης».

10. Η Γενική Διεύθυνση Πληροφορικής υποβάλλει τακτικά αναφορά στη ΔΕΑΠ σχετικά με σοβαρά συμβάντα ασφάλειας ΤΠ που επηρεάζουν τα CIS της Επιτροπής.

11. Ο αρμόδιος ΤΥΑΠ έχει πρόσβαση, κατόπιν σχετικού αιτήματος, σε αρχεία συμβάντων ασφάλειας ΤΠ που αφορούν το CIS του τμήματος της Επιτροπής.

12. Σε περίπτωση σοβαρού συμβάντος ασφάλειας ΤΠ η Γενική Διεύθυνση Πληροφορικής αποτελεί το σημείο επαφής για τη διαχείριση της κατάστασης κρίσης συντονίζοντας τις ομάδες διαχείρισης κρίσεων συμβάντων ασφάλειας ΤΠ.

13. Σε περίπτωση κατάστασης έκτακτης ανάγκης ο Γενικός Διευθυντής της Γενικής Διεύθυνσης Πληροφορικής δύναται να αποφασίσει να κινήσει διαδικασία έκτακτης ανάγκης ΤΠ. Η Γενική Διεύθυνση Πληροφορικής εκπονεί διαδικασίες έκτακτης ανάγκης προς έγκριση από τη ΔΕΑΠ.

14. Η Γενική Διεύθυνση Πληροφορικής υποβάλλει έκθεση σχετικά με την εκτέλεση των διαδικασιών έκτακτης ανάγκης στη ΔΕΑΠ και στους προϊστάμενους των τμημάτων της Επιτροπής που επηρεάζονται.

Οι διεργασίες που σχετίζονται με τις εν λόγω αρμοδιότητες και δραστηριότητες εξειδικεύονται στους κανόνες εφαρμογής.

ΚΕΦΑΛΑΙΟ 4

ΤΕΛΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Άρθρο 16

Διαφάνεια

Η παρούσα απόφαση κοινοποιείται στο προσωπικό της Επιτροπής και σε όλα τα πρόσωπα τα οποία αφορά και δημοσιεύεται στην *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης*.

Άρθρο 17

Σχέση με άλλες πράξεις

Οι διατάξεις της παρούσας απόφασης εφαρμόζονται με την επιφύλαξη της απόφασης (ΕΕ, Ευρατόμ) 2015/443, της απόφασης (ΕΕ, Ευρατόμ) 2015/444, του κανονισμού (ΕΚ) αριθ. 45/2001, του κανονισμού (ΕΚ) αριθ. 1049/2001 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([1]), της απόφασης 2002/47/ΕΚ, ΕΚΑΧ, Ευρατόμ της Επιτροπής ([2]), του κανονισμού (ΕΕ, Ευρατόμ) αριθ. 883/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([3]), και της απόφασης 1999/352/ΕΚ, ΕΚΑΧ, Ευρατόμ.

Άρθρο 18

Κατάργηση και μεταβατικά μέτρα

Η απόφαση C(2006) 3602, της 16ης Αυγούστου 2006, καταργείται.

Οι κανόνες εφαρμογής και τα πρότυπα ασφάλειας ΤΠ που θεσπίστηκαν δυνάμει του άρθρου 10 της απόφασης C(2006) 3602 παραμένουν σε ισχύ στον βαθμό που δεν αντίκεινται στην παρούσα απόφαση, έως ότου αντικατασταθούν από τους κανόνες εφαρμογής και τα πρότυπα που πρόκειται να θεσπιστούν βάσει του άρθρου 13 της παρούσας απόφασης. Κάθε αναφορά στο άρθρο 10 της απόφασης C(2006) 3602 νοείται ως αναφορά στο άρθρο 13 της παρούσας απόφασης.

Άρθρο 19

Έναρξη ισχύος

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

Βρυξέλλες, 10 Ιανουαρίου 2017.

Για την Επιτροπή
Ο Πρόεδρος
Jean-Claude JUNCKER

([1]) Κανονισμός (ΕΚ) αριθ. 1049/2001 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 30ής Μαΐου 2001, για την πρόσβαση του κοινού στα έγγραφα του Ευρωπαϊκού Κοινοβουλίου, του Συμβουλίου και της Επιτροπής (ΕΕ L 145 της 31.5.2001, σ. 43).

([2]) Απόφαση 2002/47/ΕΚ, ΕΚΑΧ, Ευρατόμ της Επιτροπής, της 23ης Ιανουαρίου 2002, για την τροποποίηση του εσωτερικού της κανονισμού (ΕΕ L 21 της 24.1.2002, σ. 23).

([3]) Κανονισμός (ΕΕ, Ευρατόμ) αριθ. 883/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Σεπτεμβρίου 2013, σχετικά με τις έρευνες που πραγματοποιούνται από την Ευρωπαϊκή Υπηρεσία Καταπολέμησης της Απάτης (OLAF) και την κατάργηση του κανονισμού (ΕΚ) αριθ. 1073/1999 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου και του κανονισμού (Ευρατόμ) αριθ. 1074/1999 του Συμβουλίου (ΕΕ L 248 της 18.9.2013, σ. 1).