ΑΠΟΦΑΣΗ (ΕΕ, Ευρατόμ) 2018/559 ΤΗΣ ΕΠΙΤΡΟΠΗΣ

της 6ης Απριλίου 2018

για τη θέσπιση εκτελεστικών κανόνων για το άρθρο 6 της απόφασης (ΕΕ, Ευρατόμ) 2017/46 της 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,

Έχοντας υπόψη την απόφαση (ΕΕ, Ευρατόμ) 2017/46 της Επιτροπής, της 10ης Ιανουαρίου 2017, σχετικά με την ασφάλεια των συστημάτων επικοινωνίας και πληροφοριών στην Ευρωπαϊκή Επιτροπή ([1]), και ιδίως το άρθρο 6,

Εκτιμώντας τα ακόλουθα:

(1) Με την έκδοση της απόφασης (ΕΕ, Ευρατόμ) 2017/46, η Επιτροπή πρέπει να αναθεωρήσει, να επικαιροποιήσει και να ενοποιήσει τους κανόνες εφαρμογής που συνδέονται με την καταργηθείσα απόφαση C(2006) 3602 της Επιτροπής σχετικά με την ασφάλεια των συστημάτων επικοινωνίας και πληροφοριών που χρησιμοποιεί η Επιτροπή.

(2) Το μέλος της Επιτροπής που είναι αρμόδιο για θέματα ασφάλειας, σε πλήρη συμμόρφωση με τον εσωτερικό κανονισμό, έχει εξουσιοδοτηθεί να θεσπίσει εκτελεστικούς κανόνες σύμφωνα με το άρθρο 13 της απόφασης (ΕΕ, Ευρατόμ) 2017/46 ([2]).

(3) Συνεπώς, οι κανόνες εφαρμογής της απόφασης C(2006) 3602 θα πρέπει να καταργηθούν,

ΕΞΕΔΩΣΕ ΤΗΝ ΠΑΡΟΥΣΑ ΑΠΟΦΑΣΗ:

ΚΕΦΑΛΑΙΟ 1

ΓΕΝΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Άρθρο 1

Αντικείμενο και πεδίο εφαρμογής

1. Το αντικείμενο και το πεδίο εφαρμογής της παρούσας απόφασης παρατίθενται στο άρθρο 1 της απόφασης (ΕΕ, Ευρατόμ) 2017/46.

2. Οι διατάξεις της παρούσας απόφασης εφαρμόζονται σε όλα τα συστήματα επικοινωνίας και πληροφοριών (CIS). Ωστόσο, οι αρμοδιότητες που ορίζονται στην παρούσα απόφαση δεν εφαρμόζονται στα CIS που επεξεργάζονται διαβαθμισμένες πληροφορίες της ΕΕ. Οι αντίστοιχες αρμοδιότητες για τα συστήματα αυτά καθορίζονται από τον ιδιοκτήτη του συστήματος και την Αρχή Ασφάλειας της Επιτροπής σύμφωνα με την απόφαση (ΕΕ, Ευρατόμ) 2015/444 της Επιτροπής ([3]).

3. Το κεφάλαιο 2 της παρούσας απόφασης προβαίνει σε επισκόπηση της πρακτικής εφαρμογής της οργάνωσης και των αρμοδιοτήτων σχετικά με την ασφάλεια ΤΠ. Το κεφάλαιο 3 της παρούσας απόφασης προβαίνει σε επισκόπηση των διαδικασιών σχετικά με το άρθρο 6 της απόφασης (ΕΕ, Ευρατόμ) 2017/46.

Άρθρο 2

Ορισμοί

Στην παρούσα απόφαση ισχύουν οι ορισμοί του άρθρου 2 της απόφασης (ΕΕ, Ευρατόμ) 2017/46. Για τους σκοπούς της παρούσας απόφασης ισχύουν επίσης οι ακόλουθοι ορισμοί:

1. «Αρχή Έγκρισης Κρυπτογραφικών Μεθόδων» (CAA): λειτουργία που αναλαμβάνει η Αρχή Ασφάλειας της Επιτροπής, η οποία υπάγεται στην εποπτεία του Γενικού Διευθυντή Ανθρώπινων Πόρων και Ασφάλειας·

([1]) ΕΕ L 6 της 11.1.2017, σ. 40.
([2]) Απόφαση C(2017) 7428 της Επιτροπής, της 8ης Νοεμβρίου 2017, για τη χορήγηση εξουσιοδότησης για την έγκριση εκτελεστικών κανόνων, προτύπων και κατευθυντήριων γραμμών σχετικά με την ασφάλεια των συστημάτων επικοινωνίας και πληροφοριών στην Ευρωπαϊκή Επιτροπή.
([3]) Απόφαση (ΕΕ, 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).

2. «Σύνδεση εξωτερικού δικτύου»: οποιαδήποτε σύνδεση ηλεκτρονικής επικοινωνίας μεταξύ του εσωτερικού δικτύου της Επιτροπής και οποιουδήποτε άλλου δικτύου, συμπεριλαμβανομένου του διαδικτύου. Από τον ορισμό αυτό εξαιρούνται τα τρίτα δίκτυα που, βάσει σύμβασης, προβλέπεται ότι αποτελούν μέρος του εσωτερικού δικτύου της Επιτροπής.

3. «Μεσεγγύηση κλειδιού»: διαδικασία για την αποθήκευση αντιγράφων των κρυπτογραφικών κλειδιών από ένα ή περισσότερα χωριστά μέρη, που διασφαλίζει τον διαχωρισμό καθηκόντων, ώστε να υπάρχει η δυνατότητα ανάκτησης των εν λόγω κλειδιών σε περίπτωση απώλειας του επιχειρησιακού αντιγράφου. Τα κλειδιά μπορεί να χωρίζονται σε δύο ή περισσότερα τμήματα, καθένα από τα οποία φυλάσσεται από διαφορετικό μέρος, ώστε να εξασφαλίζεται ότι κανένα μεμονωμένο μέρος δεν έχει στη διάθεσή του ολόκληρο το κλειδί.

4. «RASCI»: συντομογραφία για την ανάθεση αρμοδιοτήτων με βάση τους ακόλουθους δείκτες ανάθεσης:

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

β) «υπόλογος» (A): πρόσωπο που λογοδοτεί για ενέργειες, αποφάσεις και επιδόσεις·

γ) «πάροχος υποστήριξης» (S): πρόσωπο που έχει την υποχρέωση να συνεργάζεται με τον αρμόδιο για την εκτέλεση καθήκοντος·

δ) «πάροχος συμβουλών/γνωμοδότησης» (C): πρόσωπο από το οποίο ζητείται η παροχή συμβουλών ή γνωμοδότησης·

ε) «ενημερωμένος» (I): που έχει επικαιροποιηθεί με βάση τις σχετικές πληροφορίες.

ΚΕΦΑΛΑΙΟ 2

ΟΡΓΑΝΩΣΗ ΚΑΙ ΑΡΜΟΔΙΟΤΗΤΕΣ

Άρθρο 3

Ρόλοι και αρμοδιότητες

Οι ρόλοι και οι αρμοδιότητες που σχετίζονται με τα άρθρα 4 έως 8 της παρούσας απόφασης ορίζονται στο Παράρτημα σύμφωνα με το υπόδειγμα RASCI.

Άρθρο 4

Ευθυγράμμιση με την πολιτική ασφάλειας πληροφοριών της Επιτροπής

1. Η Γενική Διεύθυνση Ανθρώπινων Πόρων και Ασφάλειας αναθεωρεί την πολιτική ασφάλειας ΤΠ της Επιτροπής και τα σχετικά πρότυπα και κατευθυντήριες γραμμές, ώστε να εξασφαλιστεί ότι ευθυγραμμίζονται προς τις γενικές πολιτικές ασφάλειας, ιδίως με την απόφαση (ΕΕ, Ευρατόμ) 2015/443 της Επιτροπής ([1]) και την απόφαση (ΕΕ, Ευρατόμ) 2015/444.

2. Κατόπιν αιτήματος άλλων υπηρεσιών της Επιτροπής, η Γενική Διεύθυνση Ανθρώπινων Πόρων και Ασφάλειας μπορεί να αναθεωρήσει τις πολιτικές ασφάλειας ΤΠ ή άλλα έγγραφα ασφάλειας ΤΠ των εν λόγω υπηρεσιών, ώστε να εξασφαλιστεί η συνέπειά τους προς την πολιτική ασφάλειας πληροφοριών της Επιτροπής. Ο προϊστάμενος της οικείας υπηρεσίας της Επιτροπής διασφαλίζει την αποκατάσταση τυχόν ανακολουθιών.

3. Στο πλαίσιο των αρμοδιοτήτων της για την ασφάλεια πληροφοριών, η Γενική Διεύθυνση Ανθρώπινων Πόρων και Ασφάλειας, συνεργάζεται με τη Γενική Διεύθυνση Πληροφορικής για να εξασφαλιστεί ότι οι διαδικασίες ασφάλειας ΤΠ λαμβάνουν πλήρως υπόψη τη διαβάθμιση και τις αρχές ασφάλειας που ορίζονται στην απόφαση (ΕΕ, Ευρατόμ) 2015/443, και ιδίως στα άρθρα 3 και 9.

ΚΕΦΑΛΑΙΟ 3

ΔΙΑΔΙΚΑΣΙΕΣ ΑΣΦΑΛΕΙΑΣ ΤΠ

Άρθρο 5

Τεχνολογίες κρυπτογράφησης

1. Η χρήση τεχνολογιών κρυπτογράφησης για την προστασία των διαβαθμισμένων πληροφοριών της ΕΕ (ΔΠΕΕ) πρέπει να συμμορφώνεται με την απόφαση (ΕΕ, Ευρατόμ) 2015/444.

2. Οι αποφάσεις σχετικά με τη χρήση τεχνολογιών κρυπτογράφησης για την προστασία δεδομένων που δεν είναι ΔΠΕΕ λαμβάνονται από τον ιδιοκτήτη του συστήματος για κάθε CIS, λαμβάνοντας υπόψη τόσο τους κινδύνους που επιδιώκεται να μετριαστούν μέσω της κρυπτογράφησης όσο και τους κινδύνους που ενέχει η ίδια η κρυπτογράφηση.

3. Για όλες τις χρήσεις των τεχνολογιών κρυπτογράφησης απαιτείται προηγούμενη έγκριση από την CAA, εκτός αν η κρυπτογράφηση χρησιμοποιείται μόνο για την προστασία της εμπιστευτικότητας δεδομένων που δεν είναι ΔΠΕΕ υπό διαμετακόμιση και χρησιμοποιεί τυποποιημένα πρωτόκολλα επικοινωνίας δικτύου.

([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).

4. Με την εξαίρεση της παραγράφου 3 του παρόντος άρθρου, οι υπηρεσίες της Επιτροπής μεριμνούν ώστε τα αντίγραφα ασφαλείας των κλειδιών αποκρυπτογράφησης να αποθηκεύονται με μεσεγγύηση κλειδιού, με σκοπό την ανάκτηση των αποθηκευμένων δεδομένων σε περίπτωση που το κλειδί αποκρυπτογράφησης δεν είναι διαθέσιμο. Η ανάκτηση των κρυπτογραφημένων δεδομένων με τη χρήση των αντιγράφων ασφαλείας των κλειδιών αποκρυπτογράφησης εκτελείται μόνο εφόσον δοθεί σχετική έγκριση σύμφωνα με το πρότυπο που ορίζεται από την CAA.

5. Οι αιτήσεις έγκρισης για τη χρήση τεχνολογιών κρυπτογράφησης είναι τυπικά τεκμηριωμένες και περιλαμβάνουν λεπτομερή στοιχεία σχετικά με το CIS και τα προς προστασία δεδομένα, τις τεχνολογίες που πρόκειται να χρησιμοποιηθούν και τις σχετικές ασφαλείς λειτουργικές διαδικασίες. Οι εν λόγω αιτήσεις έγκρισης υπογράφονται από τον ιδιοκτήτη του συστήματος.

6. Οι αιτήσεις έγκρισης για τη χρήση τεχνολογιών κρυπτογράφησης αξιολογούνται από την CAA σύμφωνα με τα δημοσιευμένα πρότυπα και απαιτήσεις.

Άρθρο 6

Επιθεωρήσεις ασφάλειας ΤΠ

1. Η Γενική Διεύθυνση Ανθρώπινων Πόρων και Ασφάλειας διενεργεί επιθεωρήσεις ασφάλειας ΤΠ, ώστε να εξακριβώσει αν τα μέτρα ασφάλειας ΤΠ συμμορφώνονται προς την πολιτική ασφάλειας ΤΠ της Επιτροπής και να ελέγξει την ακεραιότητα των εν λόγω μέτρων ελέγχου.

2. Η Γενική Διεύθυνση Ανθρώπινων Πόρων και Ασφάλειας μπορεί να διενεργήσει επιθεώρηση ασφάλειας ΤΠ:

α) με δική της πρωτοβουλία·

β) κατόπιν αιτήματος της διοικούσας επιτροπής ασφάλειας πληροφοριών (ΔΕΑΠ)·

γ) κατόπιν αιτήματος που λαμβάνει από ιδιοκτήτη συστήματος·

δ) κατόπιν συμβάντος που θέτει σε κίνδυνο την ασφάλεια· ή

ε) κατόπιν διαπίστωσης υψηλού κινδύνου σε ένα συγκεκριμένο σύστημα.

3. Οι ιδιοκτήτες των δεδομένων μπορούν να ζητήσουν επιθεώρηση ασφάλειας ΤΠ πριν από την αποθήκευση πληροφοριών τους σε ένα CIS.

4. Τα αποτελέσματα της επιθεώρησης τεκμηριώνονται με επίσημη έκθεση προς τον ιδιοκτήτη του συστήματος, που κοινοποιείται και στους τοπικούς υπευθύνους ασφάλειας πληροφορικής (ΤΥΑΠ), και η οποία περιλαμβάνει πορίσματα και συστάσεις για τη βελτίωση της συμμόρφωσης του CIS με την πολιτική ασφάλειας ΤΠ. Η Γενική Διεύθυνση Ανθρώπινων Πόρων και Ασφάλειας υποβάλλει στη ΔΕΑΠ έκθεση σχετικά με σημαντικά ζητήματα και συστάσεις.

5. Η Γενική Διεύθυνση Ανθρώπινων Πόρων και Ασφάλειας παρακολουθεί την εφαρμογή των συστάσεων.

6. Κατά περίπτωση, οι επιθεωρήσεις ασφάλειας ΤΠ περιλαμβάνουν τον έλεγχο των υπηρεσιών, εγκαταστάσεων και εξοπλισμού που παρέχονται στον ιδιοκτήτη του συστήματος, συμπεριλαμβανομένων τόσο των εσωτερικών όσο και των εξωτερικών παρόχων υπηρεσιών.

Άρθρο 7

Πρόσβαση από εξωτερικά δίκτυα

1. Η Γενική Διεύθυνση Ανθρώπινων Πόρων και Ασφάλειας θεσπίζει τους κανόνες σε ένα πρότυπο που επιτρέπει την πρόσβαση μεταξύ CIS της Επιτροπής και εξωτερικών δικτύων.

2. Οι κανόνες αυτοί διακρίνουν διάφορα είδη εξωτερικών δικτυακών συνδέσεων και προβλέπουν κατάλληλους κανόνες ασφάλειας για κάθε είδος σύνδεσης, μεταξύ άλλων ως προς το αν απαιτείται προηγούμενη έγκριση της σύνδεσης από τη σχετική αρχή, όπως αναφέρεται στην παράγραφο 4 του παρόντος άρθρου.

3. Αν απαιτείται, η έγκριση χορηγείται βάσει επίσημης αίτησης και διαδικασίας έγκρισης. Η έγκριση ισχύει επί ορισμένο χρονικό διάστημα και λαμβάνεται πριν από την ενεργοποίηση της σύνδεσης.

4. Η Γενική Διεύθυνση Ανθρώπινων Πόρων και Ασφάλειας έχει τη συνολική ευθύνη για την έγκριση των αιτήσεων, αλλά είναι στη διακριτική της ευχέρεια να αναθέσει την αρμοδιότητα της έγκρισης για ορισμένους τύπους σύνδεσης σύμφωνα με το άρθρο 17 παράγραφος 3 της απόφασης (ΕΕ, Ευρατόμ) 2015/443 και σύμφωνα με τις προϋποθέσεις που καθορίζονται στην παράγραφο 8.

5. Η εγκρίνουσα αρχή μπορεί να επιβάλει πρόσθετες απαιτήσεις ασφάλειας ως προϋπόθεση για την έγκριση, με σκοπό την προστασία των CIS και των δικτύων της Επιτροπής από τους κινδύνους τυχόν μη εγκεκριμένης πρόσβασης ή άλλων παραβιάσεων της ασφάλειας.

6. Η Γενική Διεύθυνση Πληροφορικής είναι ο βασικός πάροχος υπηρεσιών δικτύου για την Επιτροπή. Κάθε άλλη υπηρεσία της Επιτροπής που λειτουργεί σε δίκτυο που δεν παρέχεται από τη Γενική Διεύθυνση Πληροφορικής λαμβάνει προηγουμένως τη σύμφωνη γνώμη της ΔΕΑΠ. Η υπηρεσία της Επιτροπής τεκμηριώνει την επιχειρησιακή αιτιολόγηση για το αίτημα και αποδεικνύει ότι οι έλεγχοι του δικτύου είναι επαρκείς ώστε να ικανοποιούνται οι απαιτήσεις για τον έλεγχο των εισερχόμενων και εξερχόμενων ροών πληροφοριών.

7. Ο ιδιοκτήτης ενός CIS καθορίζει τις απαιτήσεις ασφάλειας για εξωτερική πρόσβαση στο εν λόγω CIS και διασφαλίζει την εφαρμογή κατάλληλων μέτρων για την προστασία της ασφάλειάς του, με την υποστήριξη των ΤΥΑΠ.

8. Τα μέτρα ασφάλειας που εφαρμόζονται για τις εξωτερικές συνδέσεις δικτύου βασίζονται στις αρχές της «ανάγκης γνώσης» και του «ελάχιστου προνομίου», γεγονός που εξασφαλίζει ότι τα μεμονωμένα άτομα λαμβάνουν μόνο τις πληροφορίες και τα δικαιώματα πρόσβασης που χρειάζονται για να εκτελέσουν τα επίσημα καθήκοντά τους για την Επιτροπή.

9. Όλες οι εξωτερικές συνδέσεις δικτύου φιλτράρονται και ελέγχονται, ώστε να εντοπίζονται πιθανές παραβιάσεις της ασφάλειας.

10. Όταν πραγματοποιούνται συνδέσεις που επιτρέπουν την εξωτερική ανάθεση ενός CIS, η έγκριση εξαρτάται από την επιτυχή ολοκλήρωση της διαδικασίας που περιγράφεται στο άρθρο 8.

Άρθρο 8

Εξωτερική ανάθεση CIS

1. Για τους σκοπούς της παρούσας απόφασης, θεωρείται ότι γίνεται εξωτερική ανάθεση ενός CIS, όταν αυτό προβλέπεται βάσει σύμβασης με τρίτο μέρος, σύμφωνα με την οποία το CIS στεγάζεται σε εγκαταστάσεις εκτός Επιτροπής. Περιλαμβάνει την εξωτερική ανάθεση μεμονωμένων ή πολλαπλών CIS ή άλλες υπηρεσίες ΤΠ, κέντρα δεδομένων σε εγκαταστάσεις εκτός Επιτροπής, καθώς και τη διαχείριση συνόλων δεδομένων της Επιτροπής από εξωτερικές υπηρεσίες.

2. Η εξωτερική ανάθεση CIS λαμβάνει υπόψη τον ευαίσθητο χαρακτήρα ή τη διαβάθμιση των διαχειριζόμενων πληροφοριών, ως εξής:

α) Τα CIS που διαχειρίζονται ΔΠΕΕ είναι διαπιστευμένα σύμφωνα με την απόφαση (ΕΕ, Ευρατόμ) 2015/444, απαιτείται δε να προηγηθεί διαβούλευση με την Αρχή διαπίστευσης της ασφάλειας (ΑΔΑ) της Επιτροπής. Τα συστήματα που διαχειρίζονται ΔΠΕΕ δεν επιδέχονται εξωτερική ανάθεση.

β) Ο ιδιοκτήτης ενός CIS που διαχειρίζεται πληροφορίες που δεν είναι ΔΠΕΕ εφαρμόζει αναλογικά μέτρα για την κάλυψη των αναγκών ασφάλειας σύμφωνα με τις σχετικές νομικές υποχρεώσεις ή τον ευαίσθητο χαρακτήρα των πληροφοριών, λαμβάνοντας υπόψη τους κινδύνους της εξωτερικής ανάθεσης. Η Γενική Διεύθυνση Ανθρώπινων Πόρων και Ασφάλειας μπορεί να επιβάλει πρόσθετες απαιτήσεις.

γ) Τα έργα ανάπτυξης που αποτελούν αντικείμενο εξωτερικής ανάθεσης λαμβάνουν υπόψη τον ευαίσθητο χαρακτήρα του ανεπτυγμένου κώδικα και των τυχόν δεδομένων που χρησιμοποιούνται στις δοκιμές κατά τη διάρκεια της ανάπτυξης.

3. Πέραν των αρχών που προβλέπονται στο άρθρο 3 της απόφασης (ΕΕ, Ευρατόμ) 2017/46, στην εξωτερική ανάθεση CIS εφαρμόζονται οι ακόλουθες αρχές:

α) οι ρυθμίσεις εξωτερικής ανάθεσης σχεδιάζονται έτσι ώστε να αποφευχθεί η εξάρτηση από συγκεκριμένους προμηθευτές·

β) οι ρυθμίσεις ασφάλειας για την εξωτερική ανάθεση ελαχιστοποιούν τις δυνατότητες του προσωπικού τρίτων μερών να έχει πρόσβαση ή να τροποποιήσει τις πληροφορίες της Επιτροπής·

γ) το προσωπικό τρίτων μερών που έχει πρόσβαση σε CIS το οποίο αποτελεί αντικείμενο εξωτερικής ανάθεσης παρέχει συμφωνίες εμπιστευτικότητας·

δ) η εξωτερική ανάθεση ενός CIS αναφέρεται στον κατάλογο των CIS.

4. Ο ιδιοκτήτης του συστήματος με τη συμμετοχή του ιδιοκτήτη των δεδομένων:

α) αξιολογεί και τεκμηριώνει τους κινδύνους που σχετίζονται με την εξωτερική ανάθεση·

β) θεσπίζει σχετικές απαιτήσεις ασφάλειας·

γ) διαβουλεύεται με τους ιδιοκτήτες των συστημάτων και όλων των άλλων συνδεδεμένων CIS για να εξασφαλιστεί η συμπερίληψη των απαιτήσεών τους όσον αφορά την ασφάλεια·

δ) εξασφαλίζει τη συμπερίληψη των κατάλληλων απαιτήσεων και δικαιωμάτων ασφάλειας στη σύμβαση εξωτερικής ανάθεσης·

ε) εκπληρώνει τυχόν άλλες απαιτήσεις που καθορίζονται στη λεπτομερή διαδικασία, όπως αναφέρεται στην παράγραφο 8 του παρόντος άρθρου.

Οι εν λόγω δράσεις ολοκληρώνονται πριν από την υπογραφή της σύμβασης ή άλλης συμφωνίας για την εξωτερική ανάθεση ενός ή περισσότερων CIS.

5. Οι ιδιοκτήτες των συστημάτων διαχειρίζονται τους κινδύνους που σχετίζονται με την εξωτερική ανάθεση κατά τη διάρκεια ζωής του CIS, ώστε να πληρούνται οι καθορισμένες απαιτήσεις ασφάλειας.

6. Οι ιδιοκτήτες των συστημάτων εξασφαλίζουν ότι τα συμβαλλόμενα τρίτα μέρη υποχρεούνται να κοινοποιούν αμέσως στην Επιτροπή όλα τα συμβάντα ασφάλειας ΤΠ που επηρεάζουν ένα CIS της Επιτροπής που αποτελεί αντικείμενο εξωτερικής ανάθεσης.

7. Ο ιδιοκτήτης του συστήματος είναι υπεύθυνος για την εξασφάλιση της συμμόρφωσης του CIS, της σύμβασης εξωτερικής ανάθεσης και των ρυθμίσεων ασφάλειας προς τους κανόνες της Επιτροπής σχετικά με την ασφάλεια πληροφοριών και την ασφάλεια ΤΠ.

8. Η Γενική Διεύθυνση Ανθρώπινων Πόρων και Ασφάλειας θεσπίζουν το λεπτομερές πρότυπο που σχετίζεται με τις αρμοδιότητες και τις δραστηριότητες που προβλέπονται στις παραγράφους 1 έως 7 σύμφωνα με το άρθρο 10.

ΚΕΦΑΛΑΙΟ 4

ΔΙΑΦΟΡΕΣ ΚΑΙ ΤΕΛΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Άρθρο 9

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 10

Πρότυπα

1. Οι διατάξεις της παρούσας απόφασης εμπλουτίζονται, εφόσον απαιτείται, με περαιτέρω λεπτομέρειες για τα πρότυπα και/ή τις κατευθυντήριες γραμμές που πρέπει να θεσπιστούν σύμφωνα με την απόφαση (ΕΕ, Ευρατόμ) 2017/46 και με την απόφαση C(2017) 7428. Τα πρότυπα και οι κατευθυντήριες γραμμές ασφάλειας ΤΠ παρέχουν περαιτέρω λεπτομέρειες σχετικά με τους εν λόγω κανόνες εφαρμογής και την απόφαση (ΕΕ, Ευρατόμ) 2017/46 για ειδικούς τομείς ασφάλειας σύμφωνα με το πρότυπο ISO 27001:2013 παράρτημα Α. Τα εν λόγω πρότυπα και κατευθυντήριες γραμμές βασίζονται στις βέλτιστες βιομηχανικές πρακτικές και επιλέγονται ώστε να είναι κατάλληλα για το περιβάλλον ΤΠ της Επιτροπής.

2. Τα πρότυπα, εφόσον απαιτείται, αναπτύσσονται σύμφωνα με το πρότυπο ISO 27001:2013 παράρτημα Α στους ακόλουθους τομείς:

1) Οργάνωση της ασφάλειας πληροφοριών·

2) Ασφάλεια ανθρώπινων πόρων·

3) Διαχείριση στοιχείων ενεργητικού·

4) Έλεγχος πρόσβασης·

5) Κρυπτογραφία·

6) Υλική και περιβαλλοντική ασφάλεια·

7) Επιχειρησιακή ασφάλεια·

8) Ασφάλεια επικοινωνιών·

9) Απόκτηση, ανάπτυξη και συντήρηση συστημάτων·

10) Σχέσεις με τον πάροχο·

11) Διαχείριση περιστατικών ασφάλειας πληροφοριών·

12) Πτυχές ασφάλειας πληροφοριών της διαχείρισης της επιχειρησιακής συνέχειας·

13) Συμμόρφωση.

3. Η ΔΕΑΠ εγκρίνει τα πρότυπα που αναφέρονται στις παραγράφους 1 και 2 του παρόντος άρθρου πριν από τη θέσπισή τους.

4. Οι κανόνες εφαρμογής της απόφασης C(2006) 3602 που σχετίζονται με το πεδίο εφαρμογής της παρούσας απόφασης καταργούνται.

5. Τα πρότυπα και οι κατευθυντήριες γραμμές που θεσπίστηκαν με την απόφαση C(2006) 3602, της 16ης Αυγούστου 2006, παραμένουν σε ισχύ, στον βαθμό που δεν έρχονται σε αντίθεση με τους παρόντες κανόνες εφαρμογής, έως ότου καταργηθούν ή αντικατασταθούν από πρότυπα ή κατευθυντήριες γραμμές που θα θεσπιστούν δυνάμει του άρθρου 13 της απόφασης (ΕΕ, Ευρατόμ) 2017/46.

Άρθρο 11

Έναρξη ισχύος

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

Βρυξέλλες, 6 Απριλίου 2018.

Για την Επιτροπή,
εξ ονόματος του Προέδρου,
Günther OETTINGER
Μέλος της Επιτροπής

ΠΑΡΑΡΤΗΜΑ

ΡΟΛΟΙ ΚΑΙ ΑΡΜΟΔΙΟΤΗΤΕΣ (RASCI)

Το μοντέλο RASCI αναθέτει ρόλους σε οντότητες, χρησιμοποιώντας τις ακόλουθες συντομογραφίες:

α) R — Αρμόδιος

β) A — Υπόλογος

γ) S — Πάροχος υποστήριξης

δ) C — Πάροχος συμβουλών/γνωμοδότησης

ε) I — Ενημερωμένος

Ρόλος / Διαδικασία	ΔΕΑΠ	ΑΠ (ΑΔ)	Υπηρεσίες της Επιτροπής	Ιδιοκτήτης του συστήματος	Ιδιοκτήτης των δεδομένων	ΤΥΑΠ	DIGIT	Ανάδοχοι
Ευθυγράμμιση με την πολιτική ασφάλειας πληροφοριών της Επιτροπής		**R/A**	**S**				**S**	
Τεχνολογίες κρυπτογράφησης		**C**	**A**	**R**	**I**	**C**		
Επιθεωρήσεις ασφάλειας ΤΠ	**I**	**A/R**		**S**	**I**	**I**	**S**	
Πρόσβαση από εξωτερικά δίκτυα	**C** [1]	**C**	**A**	**R**	**I**	**S**	**S**	
Εξωτερική ανάθεση CIS		**S/C**	**A**	**R/C** [2]	**S**	**C**		**S**

[1] Η ΔΕΑΠ γνωμοδοτεί και/ή παρέχει συμβουλές σχετικά με τη λειτουργία των εσωτερικών δικτύων σε κάθε υπηρεσία της Επιτροπής εκτός της Γενικής Διεύθυνσης Πληροφορικής.

[2] Ο ιδιοκτήτης ενός CIS που αποτελεί αντικείμενο εξωτερικής ανάθεσης είναι υπεύθυνος και ο ιδιοκτήτης οποιουδήποτε άλλου CIS με το οποίο διασυνδέεται ένα CIS που αποτελεί αντικείμενο εξωτερικής ανάθεσης γνωμοδοτεί και/ή παρέχει συμβουλές.