Συμβούλιο
της Ευρωπαϊκής Ένωσης

Βρυξέλλες, 18 Ιουλίου 2022
(OR. en)

11468/22
ADD 1

AVIATION 171
DELACT 120

ΔΙΑΒΙΒΑΣΤΙΚΟ ΣΗΜΕΙΩΜΑ

Αποστολέας:	Για τη Γενική Γραμματέα της Ευρωπαϊκής Επιτροπής, η κα Martine DEPREZ, Διευθύντρια
Ημερομηνία Παραλαβής:	14 Ιουλίου 2022
Αποδέκτης:	Γενική Γραμματεία του Συμβουλίου
Αριθ. εγγρ. Επιτρ.:	C(2022) 4882 final - ANNEX
Θέμα:	ΠΑΡΑΡΤΗΜΑ του ΚΑΤ' ΕΞΟΥΣΙΟΔΟΤΗΣΗ ΚΑΝΟΝΙΣΜΟΥ ΤΗΣ ΕΠΙΤΡΟΠΗΣ για τη θέσπιση κανόνων εφαρμογής του κανονισμού (ΕΕ) 2018/1139 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου όσον αφορά τις απαιτήσεις για τη διαχείριση κινδύνων για την ασφάλεια των πληροφοριών με ενδεχόμενο αντίκτυπο στην ασφάλεια της αεροπορίας για τους φορείς που καλύπτονται από τους κανονισμούς (ΕΕ) αριθ. 748/2012 και (ΕΕ) αριθ. 139/2014 της Επιτροπής, και για την τροποποίηση των κανονισμών (ΕΕ) αριθ. 748/2012 και (ΕΕ) αριθ. 139/2014 της Επιτροπής

Διαβιβάζεται συνημμένως στις αντιπροσωπίες το έγγραφο - C(2022) 4882 final - ANNEX.

συνημμ.: C(2022) 4882 final - ANNEX

ΕΥΡΩΠΑΪΚΗ
ΕΠΙΤΡΟΠΗ

Βρυξέλλες, 14.7.2022
C(2022) 4882 final

ANNEX

ΠΑΡΑΡΤΗΜΑ

του

ΚΑΤ' ΕΞΟΥΣΙΟΔΟΤΗΣΗ ΚΑΝΟΝΙΣΜΟΥ ΤΗΣ ΕΠΙΤΡΟΠΗΣ

για τη θέσπιση κανόνων εφαρμογής του κανονισμού (ΕΕ) 2018/1139 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου όσον αφορά τις απαιτήσεις για τη διαχείριση κινδύνων για την ασφάλεια των πληροφοριών με ενδεχόμενο αντίκτυπο στην ασφάλεια της αεροπορίας για τους φορείς που καλύπτονται από τους κανονισμούς (ΕΕ) αριθ. 748/2012 και (ΕΕ) αριθ. 139/2014 της Επιτροπής, και για την τροποποίηση των κανονισμών (ΕΕ) αριθ. 748/2012 και (ΕΕ) αριθ. 139/2014 της Επιτροπής

ΠΑΡΑΡΤΗΜΑ

ΑΣΦΑΛΕΙΑ ΤΩΝ ΠΛΗΡΟΦΟΡΙΩΝ — ΑΠΑΙΤΗΣΕΙΣ ΠΟΥ ΑΦΟΡΟΥΝ ΤΟΥΣ ΦΟΡΕΙΣ

[ΜΕΡΟΣ-IS.D.OR]

IS.D.OR.100 Πεδίο εφαρμογής

Το παρόν μέρος καθορίζει τις απαιτήσεις τις οποίες πρέπει να πληρούν οι φορείς που αναφέρονται στο άρθρο 2 του παρόντος κανονισμού.

IS.D.OR.200 Σύστημα διαχείρισης της ασφάλειας των πληροφοριών (ISMS)

α) Για την επίτευξη των στόχων που ορίζονται στο άρθρο 1, ο φορέας δημιουργεί, εφαρμόζει και διατηρεί σύστημα διαχείρισης της ασφάλειας των πληροφοριών (ISMS), το οποίο διασφαλίζει ότι ο φορέας:

1) θεσπίζει πολιτική για την ασφάλεια των πληροφοριών, η οποία καθορίζει τις γενικές αρχές του φορέα όσον αφορά τον ενδεχόμενο αντίκτυπο των κινδύνων για την ασφάλεια των πληροφοριών στην ασφάλεια της αεροπορίας·

2) προσδιορίζει και επανεξετάζει τους κινδύνους για την ασφάλεια των πληροφοριών σύμφωνα με την IS.D.OR.205·

3) καθορίζει και εφαρμόζει μέτρα αντιμετώπισης των κινδύνων για την ασφάλεια των πληροφοριών σύμφωνα με την IS.D.OR.210·

4) εφαρμόζει εσωτερικό σύστημα αναφοράς για την ασφάλεια των πληροφοριών σύμφωνα με την IS.D.OR.215·

5) καθορίζει και εφαρμόζει, σύμφωνα με την IS.D.OR.220, τα μέτρα που απαιτούνται για την ανίχνευση γεγονότων που αφορούν την ασφάλεια των πληροφοριών, προσδιορίζει τα γεγονότα που θεωρούνται συμβάντα με ενδεχόμενο αντίκτυπο στην ασφάλεια της αεροπορίας, εκτός από όσα επιτρέπονται από την IS.D.OR.205 στοιχείο ε), αντιδρά στα εν λόγω συμβάντα ασφάλειας πληροφοριών και διασφαλίζει την αποκατάσταση έπειτα από αυτά·

6) εφαρμόζει τα μέτρα που έχουν κοινοποιηθεί από την αρμόδια αρχή ως άμεση αντίδραση σε συμβάν ασφάλειας πληροφοριών ή τρωτό σημείο με αντίκτυπο στην ασφάλεια της αεροπορίας·

7) λαμβάνει τα κατάλληλα μέτρα, σύμφωνα με την IS.D.OR.225, για την αντιμετώπιση των ευρημάτων που κοινοποιούνται από την αρμόδια αρχή·

8) εφαρμόζει εξωτερικό σύστημα αναφοράς σύμφωνα με την IS.D.OR.230, ώστε να μπορεί η αρμόδια αρχή να λαμβάνει τα κατάλληλα μέτρα·

9) συμμορφώνεται με τις απαιτήσεις της IS.D.OR.235 όταν αναθέτει με σύμβαση σε άλλους φορείς οποιοδήποτε μέρος των δραστηριοτήτων που αναφέρονται στην IS.D.OR.200·

10) συμμορφώνεται με τις απαιτήσεις που αφορούν το προσωπικό οι οποίες καθορίζονται στην IS.D.OR.240·

11) συμμορφώνεται με τις απαιτήσεις τήρησης αρχείων που καθορίζονται στην IS.D.OR.245·

12) παρακολουθεί τη συμμόρφωση του φορέα με τις απαιτήσεις του παρόντος κανονισμού και παρέχει ανατροφοδότηση σχετικά με τα ευρήματα στον υπόλογο διευθυντή ή, στην περίπτωση των φορέων σχεδιασμού, στον επικεφαλής του φορέα σχεδιασμού, προκειμένου να διασφαλίζεται η αποτελεσματική εφαρμογή διορθωτικών μέτρων·

13) προστατεύει, με την επιφύλαξη των εφαρμοστέων απαιτήσεων αναφοράς συμβάντων, την εμπιστευτικότητα κάθε πληροφορίας που ενδέχεται να έχει λάβει ο φορέας από άλλους φορείς, ανάλογα με το επίπεδο ευαισθησίας της.

β) Προκειμένου να πληροί συνεχώς τις απαιτήσεις που αναφέρονται στο άρθρο 1, ο φορέας εφαρμόζει διαδικασία συνεχούς βελτίωσης σύμφωνα με την IS.D.OR.260.

γ) Ο φορέας τεκμηριώνει, σύμφωνα με την IS.D.OR.250, όλες τις βασικές διεργασίες,

διαδικασίες, ρόλους και αρμοδιότητες που απαιτούνται για τη συμμόρφωση με την IS.D.OR.200 στοιχείο α) και θεσπίζει διαδικασία τροποποίησης της εν λόγω τεκμηρίωσης. Η διαχείριση των αλλαγών των εν λόγω διεργασιών, διαδικασιών, ρόλων και αρμοδιοτήτων πραγματοποιείται σύμφωνα με την IS.D.OR.255.

δ) Οι διεργασίες, οι διαδικασίες, οι ρόλοι και οι αρμοδιότητες που καθορίζονται από τον φορέα για τη συμμόρφωση με την IS.D.OR.200 στοιχείο α) αντιστοιχούν στη φύση και την πολυπλοκότητα των δραστηριοτήτων του, βάσει εκτίμησης των κινδύνων για την ασφάλεια των πληροφοριών που είναι εγγενείς στις εν λόγω δραστηριότητες, και μπορούν να ενσωματωθούν σε άλλα υφιστάμενα συστήματα διαχείρισης που εφαρμόζονται ήδη από τον φορέα.

ε) Με την επιφύλαξη της υποχρέωσης συμμόρφωσης με τις απαιτήσεις υποβολής αναφορών που περιέχονται στον κανονισμό (ΕΕ) αριθ. 376/2014([1]) και τις απαιτήσεις της IS.D.OR.200 στοιχείο α) σημείο 13), ο φορέας μπορεί να λάβει έγκριση από την αρμόδια αρχή για τη μη εφαρμογή των απαιτήσεων που αναφέρονται στα στοιχεία α) έως δ) και των σχετικών απαιτήσεων που περιέχονται στις IS.D.OR.205 έως IS.D.OR.260, εάν αποδείξει στην εν λόγω αρχή ότι οι δραστηριότητες, οι εγκαταστάσεις και οι πόροι του, καθώς και οι υπηρεσίες τις οποίες εκτελεί, παρέχει, λαμβάνει και συντηρεί, δεν ενέχουν κινδύνους για την ασφάλεια των πληροφοριών με ενδεχόμενο αντίκτυπο στην ασφάλεια της αεροπορίας ούτε για τον ίδιο ούτε για άλλους φορείς. Η έγκριση βασίζεται σε τεκμηριωμένη εκτίμηση κινδύνων για την ασφάλεια των πληροφοριών, η οποία διενεργείται από τον φορέα ή τρίτο μέρος σύμφωνα με την IS.D.OR.205 και εξετάζεται και εγκρίνεται από την αρμόδια αρχή του.

Η συνεχιζόμενη ισχύς της εν λόγω έγκρισης θα επανεξετάζεται από την αρμόδια αρχή σύμφωνα με τον εφαρμοστέο κύκλο ελέγχου εποπτείας και όποτε εφαρμόζονται αλλαγές στο πεδίο εργασιών του φορέα.

IS.D.OR.205 Εκτίμηση κινδύνων για την ασφάλεια των πληροφοριών

α) Ο φορέας προσδιορίζει όλα τα στοιχεία του τα οποία θα μπορούσαν να εκτεθούν σε κινδύνους για την ασφάλεια των πληροφοριών. Αυτά περιλαμβάνουν:

1) τις δραστηριότητες, τις εγκαταστάσεις και τους πόρους του φορέα, καθώς και τις υπηρεσίες τις οποίες εκτελεί, παρέχει, λαμβάνει ή συντηρεί ο φορέας·

2) τον εξοπλισμό, τα συστήματα, τα δεδομένα και τις πληροφορίες που συμβάλλουν στη λειτουργία των στοιχείων που απαριθμούνται στο σημείο 1).

β) Ο φορέας προσδιορίζει τις διεπαφές που έχει με άλλους φορείς και οι οποίες θα μπορούσαν να οδηγήσουν σε αμοιβαία έκθεση σε κινδύνους για την ασφάλεια των πληροφοριών.

([1]) Κανονισμός (ΕΕ) αριθ. 376/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 3ης Απριλίου 2014, για την αναφορά, ανάλυση και παρακολούθηση περιστατικών στην πολιτική αεροπορία, την τροποποίηση του κανονισμού (ΕΕ) αριθ. 996/2010 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου και την κατάργηση της οδηγίας 2003/42/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου και των κανονισμών της Επιτροπής (ΕΚ) αριθ. 1321/2007 και (ΕΚ) αριθ. 1330/2007 (ΕΕ L 122 της 24.4.2014, σ. 18).

γ) Όσον αφορά τα στοιχεία και τις διεπαφές που αναφέρονται στα στοιχεία α) και β), ο φορέας προσδιορίζει τους κινδύνους για την ασφάλεια των πληροφοριών που μπορεί να έχουν ενδεχόμενο αντίκτυπο στην ασφάλεια της αεροπορίας. Για κάθε κίνδυνο που προσδιορίζεται, ο φορέας:

1) καθορίζει το επίπεδο κινδύνου σύμφωνα με προκαθορισμένη ταξινόμηση που καταρτίζεται από τον φορέα·

2) συσχετίζει κάθε κίνδυνο και το επίπεδό του με το αντίστοιχο στοιχείο ή διεπαφή που προσδιορίζεται σύμφωνα με τα στοιχεία α) και β).

Στην προκαθορισμένη ταξινόμηση που αναφέρεται στο σημείο 1) λαμβάνεται υπόψη το ενδεχόμενο επέλευσης του σεναρίου απειλής και η σοβαρότητα των συνεπειών του για την ασφάλεια. Με βάση την εν λόγω ταξινόμηση, και λαμβανομένου υπόψη του αν ο φορέας διαθέτει δομημένη και επαναλαμβανόμενη διαδικασία διαχείρισης κινδύνων για πτητικές λειτουργίες, ο φορέας είναι σε θέση να διαπιστώσει αν ο κίνδυνος είναι αποδεκτός ή πρέπει να αντιμετωπιστεί σύμφωνα με την IS.D.OR.210.

Προκειμένου να διευκολύνεται η αμοιβαία συγκρισιμότητα των εκτιμήσεων κινδύνων, στον καθορισμό του επιπέδου κινδύνου σύμφωνα με το σημείο 1) λαμβάνονται υπόψη συναφείς πληροφορίες που αποκτώνται σε συντονισμό με τους φορείς που αναφέρονται στο στοιχείο β).

δ) Ο φορέας επανεξετάζει και επικαιροποιεί την εκτίμηση κινδύνων που διενεργείται σύμφωνα με τα στοιχεία α), β) και γ) σε οποιαδήποτε από τις ακόλουθες περιπτώσεις:

1) όταν υπάρχει αλλαγή στα στοιχεία που υπόκεινται σε κινδύνους για την ασφάλεια των πληροφοριών·

2) όταν υπάρχει αλλαγή στις διεπαφές μεταξύ του φορέα και άλλων φορέων ή στους κινδύνους που κοινοποιούνται από τους άλλους φορείς·

3) όταν υπάρχει αλλαγή στις πληροφορίες ή τις γνώσεις που χρησιμοποιούνται για τον προσδιορισμό, την ανάλυση και την ταξινόμηση των κινδύνων·

4) όταν υπάρχουν διδάγματα που αντλήθηκαν από την ανάλυση συμβάντων ασφάλειας πληροφοριών.

IS.D.OR.210 Αντιμετώπιση κινδύνων για την ασφάλεια των πληροφοριών

α) Ο φορέας αναπτύσσει μέτρα για την αντιμετώπιση των μη αποδεκτών κινδύνων που προσδιορίζονται σύμφωνα με την IS.D.OR.205, τα εφαρμόζει εγκαίρως και ελέγχει τη συνεχή αποτελεσματικότητά τους. Τα μέτρα αυτά επιτρέπουν στον φορέα:

1) να ελέγχει τις περιστάσεις που συμβάλλουν στην πραγματική επέλευση του σεναρίου απειλής·

2) να μειώνει τις συνέπειες στην ασφάλεια της αεροπορίας που συνδέονται με την υλοποίηση του σεναρίου απειλής·

3) να αποφεύγει τους κινδύνους.

Τα μέτρα αυτά δεν επιφέρουν νέους ενδεχόμενους μη αποδεκτούς κινδύνους για την ασφάλεια της αεροπορίας.

β) Το πρόσωπο που αναφέρεται στην IS.D.OR.240 στοιχεία α) και β) και το λοιπό επηρεαζόμενο προσωπικό του φορέα ενημερώνονται για το αποτέλεσμα της εκτίμησης κινδύνων που διενεργείται σύμφωνα με την IS.D.OR.205, τα αντίστοιχα σενάρια απειλής και τα μέτρα που πρέπει να εφαρμοστούν.

Ο φορέας ενημερώνει επίσης τους φορείς με τους οποίους έχει διεπαφή σύμφωνα με την IS.D.OR.205 στοιχείο β) για κάθε κίνδυνο που είναι κοινός μεταξύ των δύο φορέων.

IS.D.OR.215 Εσωτερικό σύστημα αναφοράς για την ασφάλεια των πληροφοριών

α) Ο φορέας θεσπίζει εσωτερικό σύστημα αναφοράς για τη συλλογή και αξιολόγηση γεγονότων που αφορούν την ασφάλεια των πληροφοριών, συμπεριλαμβανομένων εκείνων που πρέπει να αναφέρονται σύμφωνα με την IS.D.OR.230.

β) Το εν λόγω σύστημα και η διαδικασία που αναφέρεται στην IS.D.OR.220 επιτρέπουν στον φορέα:

1) να προσδιορίζει ποια από τα γεγονότα που αναφέρονται σύμφωνα με το στοιχείο α) θεωρούνται συμβάντα ασφάλειας πληροφοριών ή τρωτά σημεία με ενδεχόμενο αντίκτυπο στην ασφάλεια της αεροπορίας·

2) να προσδιορίζει τις αιτίες και τους παράγοντες που συμβάλλουν στα συμβάντα ασφάλειας πληροφοριών και τα τρωτά σημεία που προσδιορίζονται σύμφωνα με το σημείο 1) και να τα αντιμετωπίζει στο πλαίσιο της διαδικασίας διαχείρισης κινδύνων για την ασφάλεια των πληροφοριών σύμφωνα με τις IS.D.OR.205 και IS.D.OR.220·

3) να διασφαλίζει την αξιολόγηση όλων των γνωστών συναφών πληροφοριών που σχετίζονται με τα συμβάντα ασφάλειας πληροφοριών και τα τρωτά σημεία που προσδιορίζονται σύμφωνα με το σημείο 1)·

4) να διασφαλίζει την εφαρμογή μεθόδου εσωτερικής διανομής των πληροφοριών, ανάλογα με τις ανάγκες.

γ) Κάθε συμβεβλημένος φορέας που ενδέχεται να εκθέσει τον φορέα σε κινδύνους για την ασφάλεια των πληροφοριών με ενδεχόμενο αντίκτυπο στην ασφάλεια της αεροπορίας υποχρεούται να αναφέρει στον φορέα τα γεγονότα που αφορούν την ασφάλεια των πληροφοριών. Οι αναφορές αυτές υποβάλλονται σύμφωνα με τις διαδικασίες που καθορίζονται στις ειδικές συμβατικές ρυθμίσεις και αξιολογούνται σύμφωνα με το στοιχείο β).

δ) Ο φορέας συνεργάζεται σε έρευνες με κάθε άλλο φορέα που συμβάλλει σημαντικά

στην ασφάλεια των πληροφοριών των δραστηριοτήτων του.

ε) Ο φορέας μπορεί να ενσωματώσει το εν λόγω σύστημα αναφοράς σε άλλα συστήματα υποβολής αναφορών που έχει ήδη εφαρμόσει.

IS.D.OR.220 Συμβάντα ασφάλειας πληροφοριών — ανίχνευση, αντίδραση και αποκατάσταση

α) Με βάση το αποτέλεσμα της εκτίμησης κινδύνων που διενεργείται σύμφωνα με την IS.D.OR.205 και το αποτέλεσμα της αντιμετώπισης κινδύνων που διενεργείται σύμφωνα με την IS.D.OR.210, ο φορέας εφαρμόζει μέτρα για την ανίχνευση συμβάντων και τρωτών σημείων που υποδεικνύουν την πιθανή επέλευση μη αποδεκτών κινδύνων και τα οποία ενδέχεται να έχουν αντίκτυπο στην ασφάλεια της αεροπορίας. Τα εν λόγω μέτρα ανίχνευσης επιτρέπουν στον φορέα:

1) να εντοπίζει αποκλίσεις από τις προκαθορισμένες βασικές λειτουργικές επιδόσεις·

2) να ενεργοποιεί προειδοποιήσεις για την ενεργοποίηση κατάλληλων μέτρων απόκρισης, σε περίπτωση τυχόν απόκλισης.

β) Ο φορέας εφαρμόζει μέτρα για την αντιμετώπιση τυχόν συνθηκών γεγονότος που προσδιορίζεται σύμφωνα με το στοιχείο α) και ενδέχεται να εξελιχθεί ή να έχει εξελιχθεί σε συμβάν ασφάλειας πληροφοριών. Τα εν λόγω μέτρα αντίδρασης επιτρέπουν στον φορέα:

1) να εκκινεί την αντίδραση στις προειδοποιήσεις που αναφέρονται στο στοιχείο α) σημείο 2) ενεργοποιώντας προκαθορισμένους πόρους και πορεία ενεργειών·

2) να συγκρατεί την εξάπλωση μιας επίθεσης και να αποφεύγει την πλήρη υλοποίηση ενός σεναρίου απειλής·

3) να ελέγχει τον τρόπο αστοχίας των επηρεαζόμενων στοιχείων που ορίζονται στην IS.D.OR.205 στοιχείο α).

γ) Ο φορέας εφαρμόζει μέτρα που αποσκοπούν στην αποκατάσταση έπειτα από συμβάντα ασφάλειας πληροφοριών, συμπεριλαμβανομένων μέτρων έκτακτης ανάγκης, εάν απαιτείται. Τα εν λόγω μέτρα αποκατάστασης επιτρέπουν στον φορέα:

1) να άρει την κατάσταση που προκάλεσε το συμβάν ή να την περιορίσει σε ανεκτό επίπεδο·

2) να φθάσει σε ασφαλή κατάσταση των προσβεβλημένων στοιχείων που ορίζονται στην IS.D.OR.205 στοιχείο α) εντός χρόνου αποκατάστασης που έχει προηγουμένως καθορίσει ο φορέας.

IS.D.OR.225 Απάντηση σε ευρήματα που έχουν κοινοποιηθεί από την αρμόδια αρχή

α) Μετά την παραλαβή της κοινοποίησης των ευρημάτων που έχει υποβάλει η αρμόδια αρχή, ο φορέας:

1) προσδιορίζει τη βασική αιτία ή αιτίες και τους παράγοντες που συνέβαλαν στην περίπτωση μη συμμόρφωσης·

2) καταρτίζει σχέδιο διορθωτικών μέτρων·

3) αποδεικνύει τη διόρθωση της μη συμμόρφωσης κατά τρόπο ικανοποιητικό στην αρμόδια αρχή.

β) Τα μέτρα που αναφέρονται στο στοιχείο α) τίθενται σε εφαρμογή εντός της προθεσμίας που έχει συμφωνηθεί με την αρμόδια αρχή.

IS.D.OR.230 Εξωτερικό σύστημα αναφοράς για την ασφάλεια των πληροφοριών

α) Ο φορέας εφαρμόζει σύστημα αναφοράς για την ασφάλεια των πληροφοριών που συμμορφώνεται με τις απαιτήσεις που καθορίζονται στον κανονισμό (ΕΕ) αριθ. 376/2014 και στις κατ' εξουσιοδότηση και εκτελεστικές πράξεις του, εάν ο εν λόγω κανονισμός εφαρμόζεται στον φορέα.

β) Με την επιφύλαξη των υποχρεώσεων που απορρέουν από τον κανονισμό (ΕΕ) αριθ. 376/2014, ο φορέας διασφαλίζει ότι κάθε συμβάν ασφάλειας πληροφοριών ή τρωτό σημείο, που ενδέχεται να συνιστά σημαντικό κίνδυνο για την ασφάλεια της αεροπορίας, αναφέρεται στην οικεία αρμόδια αρχή. Επιπλέον:

1) όταν ένα τέτοιο συμβάν ή τρωτό σημείο επηρεάζει αεροσκάφος ή σχετικό σύστημα ή παρελκόμενο, ο φορέας το αναφέρει επίσης στον κάτοχο της έγκρισης σχεδιασμού·

2) όταν ένα τέτοιο συμβάν ή τρωτό σημείο επηρεάζει σύστημα ή συστατικό στοιχείο που χρησιμοποιείται από τον φορέα, ο φορέας το αναφέρει στον φορέα που είναι υπεύθυνος για τον σχεδιασμό του συστήματος ή του συστατικού στοιχείου.

γ) Ο φορέας αναφέρει τις καταστάσεις που αναφέρονται στο στοιχείο β) ως εξής:

1) υποβάλλεται κοινοποίηση στην αρμόδια αρχή και, κατά περίπτωση, στον κάτοχο της έγκρισης σχεδιασμού ή στον φορέα που είναι υπεύθυνος για τον σχεδιασμό του συστήματος ή του συστατικού στοιχείου, μόλις η κατάσταση περιέλθει σε γνώση του φορέα·

2) υποβάλλεται αναφορά στην αρμόδια αρχή και, κατά περίπτωση, στον κάτοχο της έγκρισης σχεδιασμού ή στον φορέα που είναι υπεύθυνος για τον σχεδιασμό του συστήματος ή του συστατικού στοιχείου, το συντομότερο δυνατόν, αλλά όχι αργότερα από 72 ώρες από τη στιγμή που η κατάσταση έχει περιέλθει σε γνώση του φορέα, εκτός εάν αυτό δεν είναι δυνατό λόγω εξαιρετικών περιστάσεων.

Η αναφορά συντάσσεται με τη μορφή που ορίζεται από την αρμόδια αρχή και περιέχει όλες τις σχετικές πληροφορίες σχετικά με την κατάσταση που έχει περιέλθει σε γνώση του φορέα·

3) υποβάλλεται έκθεση παρακολούθησης στην αρμόδια αρχή και, κατά περίπτωση, στον κάτοχο της έγκρισης σχεδιασμού ή στον φορέα που είναι υπεύθυνος για τον

σχεδιασμό του συστήματος ή του συστατικού στοιχείου, στην οποία παρέχονται λεπτομερή στοιχεία σχετικά με τα μέτρα που έχει λάβει ή προτίθεται να λάβει ο φορέας για την αποκατάσταση από το συμβάν και τα μέτρα που προτίθεται να λάβει για την πρόληψη παρόμοιων συμβάντων ασφάλειας πληροφοριών στο μέλλον.

Η έκθεση παρακολούθησης υποβάλλεται μόλις προσδιοριστούν τα εν λόγω μέτρα και συντάσσεται με τη μορφή που ορίζεται από την αρμόδια αρχή.

IS.D.OR.235 Ανάθεση δραστηριοτήτων διαχείρισης της ασφάλειας των πληροφοριών βάσει σύμβασης

α) Ο φορέας διασφαλίζει ότι, όταν αναθέτει με σύμβαση σε άλλους φορείς οποιοδήποτε μέρος των δραστηριοτήτων που αναφέρονται στην IS.D.OR.200, οι δραστηριότητες που ανατίθενται με σύμβαση συμμορφώνονται με τις απαιτήσεις του παρόντος κανονισμού και ο συμβεβλημένος φορέας εργάζεται υπό την εποπτεία του. Ο φορέας διασφαλίζει την κατάλληλη διαχείριση των κινδύνων που συνδέονται με τις δραστηριότητες που ανατίθενται με σύμβαση.

β) Ο φορέας διασφαλίζει ότι η αρμόδια αρχή μπορεί να έχει πρόσβαση, κατόπιν αιτήματος, στον συμβεβλημένο φορέα για να διαπιστώσει τη συνεχή συμμόρφωση με τις εφαρμοστέες απαιτήσεις που καθορίζονται στον παρόντα κανονισμό.

IS.D.OR.240 Απαιτήσεις που αφορούν το προσωπικό

α) Ο υπόλογος διευθυντής του οργανισμού ή, στην περίπτωση των φορέων σχεδιασμού, ο επικεφαλής του φορέα σχεδιασμού, ο οποίος έχει οριστεί σύμφωνα με τον κανονισμό (ΕΕ) αριθ. 748/2012 και τον κανονισμό (ΕΕ) αριθ. 139/2014, όπως αναφέρεται στο άρθρο 2 παράγραφος 1) στοιχεία α) και β) του παρόντος κανονισμού, έχει την εξουσία νομικού προσώπου να διασφαλίζει τη χρηματοδότηση και την εκτέλεση όλων των δραστηριοτήτων που απαιτούνται από τον παρόντα κανονισμό. Το πρόσωπο αυτό:

1) διασφαλίζει ότι είναι διαθέσιμοι όλοι οι αναγκαίοι πόροι για τη συμμόρφωση με τις απαιτήσεις του παρόντος κανονισμού·

2) καταρτίζει και προωθεί την πολιτική ασφάλειας των πληροφοριών που καθορίζεται στην IS.D.OR.200 στοιχείο α) σημείο 1)·

3) αποδεικνύει στοιχειώδη κατανόηση του παρόντος κανονισμού.

β) Ο υπόλογος διευθυντής ή, στην περίπτωση των φορέων σχεδιασμού, ο επικεφαλής του φορέα σχεδιασμού, διορίζει ένα πρόσωπο ή ομάδα προσώπων για να διασφαλίζει ότι ο φορέας συμμορφώνεται με τις απαιτήσεις του παρόντος κανονισμού και καθορίζει την έκταση της εξουσίας του/της. Το εν λόγω πρόσωπο ή ομάδα προσώπων λογοδοτεί απευθείας στον υπόλογο διευθυντή ή, στην περίπτωση των φορέων σχεδιασμού, στον επικεφαλής του φορέα σχεδιασμού, και διαθέτει τις κατάλληλες γνώσεις, το υπόβαθρο και την πείρα για την εκτέλεση των καθηκόντων του/της. Στις διαδικασίες καθορίζεται ποιος αντικαθιστά οποιοδήποτε πρόσωπο απουσιάζει για μεγάλο χρονικό διάστημα από τη δουλειά του.

γ) Ο υπόλογος διευθυντής ή, στην περίπτωση των φορέων σχεδιασμού, ο επικεφαλής του φορέα σχεδιασμού, διορίζει ένα πρόσωπο ή ομάδα προσώπων που είναι αρμόδιο/-α για τη διαχείριση της λειτουργίας παρακολούθησης της συμμόρφωσης που αναφέρεται στην IS.D.OR.200 στοιχείο α) σημείο 12).

δ) Όταν ο φορέας ανταλλάσσει οργανωτικές δομές, πολιτικές, διεργασίες και διαδικασίες για την ασφάλεια των πληροφοριών, με άλλους φορείς ή με τομείς του ίδιου του φορέα που δεν αποτελούν μέρος της έγκρισης ή της δήλωσης, ο υπόλογος διευθυντής ή, στην περίπτωση των φορέων σχεδιασμού, ο επικεφαλής του φορέα σχεδιασμού, μπορεί να αναθέτει τις δραστηριότητές του σε κοινό αρμόδιο πρόσωπο.

Στην περίπτωση αυτή, θεσπίζονται μέτρα συντονισμού μεταξύ του υπόλογου διευθυντή του φορέα ή, στην περίπτωση των φορέων σχεδιασμού, του επικεφαλής του φορέα σχεδιασμού, και του κοινού αρμόδιου προσώπου, ώστε να διασφαλίζεται επαρκής ενσωμάτωση της διαχείρισης της ασφάλειας των πληροφοριών εντός του φορέα.

ε) Ο υπόλογος διευθυντής ή ο επικεφαλής του φορέα σχεδιασμού ή το κοινό αρμόδιο πρόσωπο που αναφέρεται στο στοιχείο δ) έχει την εξουσία νομικού προσώπου να θεσπίζει και να διατηρεί τις οργανωτικές δομές, τις πολιτικές, τις διεργασίες και τις διαδικασίες που απαιτούνται για την εφαρμογή της IS.D.OR.200.

στ) Ο φορέας εφαρμόζει διαδικασία που διασφαλίζει ότι διαθέτει επαρκές προσωπικό σε υπηρεσία για την εκτέλεση των δραστηριοτήτων που καλύπτονται από το παρόν παράρτημα.

ζ) Ο φορέας εφαρμόζει διαδικασία που διασφαλίζει ότι το προσωπικό που αναφέρεται στο στοιχείο στ) διαθέτει την αναγκαία επάρκεια για την εκτέλεση των καθηκόντων του.

η) Ο φορέας εφαρμόζει διαδικασία που διασφαλίζει ότι το προσωπικό αναγνωρίζει τις αρμοδιότητες που συνδέονται με τους ανατιθέμενους ρόλους και καθήκοντα.

θ) Ο φορέας διασφαλίζει ότι η ταυτότητα και η αξιοπιστία του προσωπικού που έχει πρόσβαση σε συστήματα πληροφοριών και δεδομένα που υπόκεινται στις απαιτήσεις του παρόντος κανονισμού είναι δεόντως εξακριβωμένες.

IS.D.OR.245 Τήρηση αρχείων

α) Ο φορέας τηρεί αρχεία των δραστηριοτήτων του όσον αφορά τη διαχείριση της ασφάλειας των πληροφοριών

1) Ο φορέας διασφαλίζει ότι αρχειοθετούνται και είναι ανιχνεύσιμα τα ακόλουθα αρχεία:

i) κάθε έγκριση που λαμβάνεται και κάθε σχετική εκτίμηση κινδύνων για την ασφάλεια των πληροφοριών σύμφωνα με την IS.D.OR.200 στοιχείο ε)·

ii) συμβάσεις για την ανάθεση δραστηριοτήτων που αναφέρονται στην IS.D.OR.200 στοιχείο α) σημείο 9)·

iii) αρχεία των κύριων διαδικασιών, όπως αναφέρονται στην IS.D.OR.200 στοιχείο δ)·

iv) αρχεία των κινδύνων που εντοπίστηκαν στην εκτίμηση κινδύνων που αναφέρεται στην IS.D.OR.205 μαζί με τα σχετικά μέτρα αντιμετώπισης κινδύνων που αναφέρονται στην IS.D.OR.210·

v) αρχεία των συμβάντων ασφάλειας πληροφοριών και των τρωτών σημείων που αναφέρονται σύμφωνα με τα συστήματα αναφοράς που προβλέπονται στις IS.D.OR.215 και IS.D.OR.230·

vi) αρχεία των συμβάντων ασφάλειας πληροφοριών τα οποία ενδέχεται να χρειαστεί να επαναξιολογηθούν για να αποκαλυφθούν μη ανιχνευμένα συμβάντα ασφάλειας πληροφοριών ή τρωτά σημεία.

2) Τα αρχεία που αναφέρονται στο σημείο 1) σημείο i) διατηρούνται τουλάχιστον έως 5 έτη μετά τη λήξη ισχύος της έγκρισης.

3) Τα αρχεία που αναφέρονται στο σημείο 1) σημείο ii) διατηρούνται τουλάχιστον έως 5 έτη μετά την τροποποίηση ή τη λύση της σύμβασης.

4) Τα αρχεία που αναφέρονται στο σημείο 1) σημεία iii), iv) και v) διατηρούνται τουλάχιστον για περίοδο 5 ετών.

5) Τα αρχεία που αναφέρονται στο σημείο 1) σημείο vi) διατηρούνται έως ότου τα εν λόγω γεγονότα που αφορούν την ασφάλεια των πληροφοριών επαναξιολογηθούν σύμφωνα με περιοδικότητα που καθορίζεται σε διαδικασία την οποία θεσπίζει ο φορέας.

β) Ο φορέας τηρεί αρχεία των προσόντων και της πείρας του προσωπικού του που συμμετέχει σε δραστηριότητες διαχείρισης της ασφάλειας των πληροφοριών.

1) Τα αρχεία των προσόντων και της πείρας του προσωπικού διατηρούνται για όσο διάστημα το πρόσωπο εργάζεται για τον φορέα και για τουλάχιστον 3 έτη μετά την αποχώρησή του από τον φορέα.

2) Τα μέλη του προσωπικού έχουν, κατόπιν αίτησής τους, πρόσβαση στα ατομικά τους αρχεία. Επιπλέον, ο φορέας, κατόπιν αίτησής τους, τους χορηγεί αντίγραφο του ατομικού τους αρχείου κατά την αποχώρησή τους από τον φορέα.

γ) Η μορφή των αρχείων καθορίζεται στις διαδικασίες του φορέα.

δ) Τα αρχεία αποθηκεύονται κατά τρόπο που εξασφαλίζει προστασία έναντι φθοράς, παραποίησης και κλοπής, ενώ οι πληροφορίες προσδιορίζονται, όταν απαιτείται, ανάλογα με την αντίστοιχη διαβάθμιση ασφάλειας. Ο φορέας μεριμνά ώστε τα αρχεία να αποθηκεύονται με τη χρήση μέσων που διασφαλίζουν την ακεραιότητα, τη γνησιότητα και την εξουσιοδοτημένη πρόσβαση.

IS.D.OR.250 Εγχειρίδιο διαχείρισης της ασφάλειας των πληροφοριών (ISMM)

α) Ο φορέας θέτει στη διάθεση της αρμόδιας αρχής εγχειρίδιο διαχείρισης της ασφάλειας των πληροφοριών (ISMM) και, κατά περίπτωση, τυχόν αναφερόμενα σχετικά εγχειρίδια και διαδικασίες, το οποίο περιέχει:

1) δήλωση υπογεγραμμένη από τον υπόλογο διευθυντή ή, στην περίπτωση των φορέων σχεδιασμού, από τον επικεφαλής του φορέα σχεδιασμού, με την οποία βεβαιώνεται ότι ο φορέας θα εργάζεται ανά πάσα στιγμή σύμφωνα με το παρόν παράρτημα και με το εγχειρίδιο διαχείρισης της ασφάλειας των πληροφοριών. Εάν ο υπόλογος διευθυντής ή, στην περίπτωση των φορέων σχεδιασμού, ο επικεφαλής του φορέα σχεδιασμού, δεν είναι ο γενικός διευθυντής (CEO) του φορέα, τότε η δήλωση υπογράφεται από τον εν λόγω γενικό διευθυντή·

2) τον/τους τίτλο/-ους, το/τα ονοματεπώνυμο/-α, τα καθήκοντα, τις δομές λογοδοσίας, τις αρμοδιότητες και τις εξουσίες του προσώπου ή των προσώπων που αναφέρονται στην IS.D.OR.240 στοιχεία β) και γ)·

3) τον τίτλο, το ονοματεπώνυμο, τα καθήκοντα, τις δομές λογοδοσίας, τις αρμοδιότητες και τις εξουσίες του κοινού αρμόδιου προσώπου που αναφέρεται στην IS.D.OR.240 στοιχείο δ), κατά περίπτωση·

4) την πολιτική ασφάλειας των πληροφοριών του φορέα, όπως αναφέρεται στην IS.D.OR.200 στοιχείο α) σημείο 1)·

5) γενική περιγραφή του αριθμού και των κατηγοριών προσωπικού και του εφαρμοζόμενου συστήματος για τον προγραμματισμό της διαθεσιμότητας προσωπικού, όπως απαιτείται από την IS.D.OR.240·

6) τον/τους τίτλο/-ους, το/τα ονοματεπώνυμο/-α, τα καθήκοντα, τις δομές λογοδοσίας, τις αρμοδιότητες και τις εξουσίες των βασικών προσώπων που είναι υπεύθυνα για την εφαρμογή της IS.D.OR.200, συμπεριλαμβανομένου του προσώπου ή των προσώπων που είναι υπεύθυνα για τη λειτουργία παρακολούθησης της συμμόρφωσης που αναφέρεται στην IS.D.OR.200 στοιχείο α) σημείο 12)·

7) οργανόγραμμα που δείχνει τις σχετικές αλυσίδες λογοδοσίας και ευθύνης για τα πρόσωπα που αναφέρονται στα σημεία 2) και 6)·

8) περιγραφή του εσωτερικού συστήματος αναφοράς, όπως απαιτείται από την IS.D.OR.215·

9) τις διαδικασίες που καθορίζουν τον τρόπο με τον οποίο ο φορέας διασφαλίζει τη συμμόρφωση με το παρόν μέρος, και ιδίως:

i) την τεκμηρίωση που αναφέρεται στην IS.D.OR.200 στοιχείο γ)·

ii) τις διαδικασίες που καθορίζουν τον τρόπο με τον οποίο ο φορέας ελέγχει τυχόν δραστηριότητες που ανατίθενται με σύμβαση και αναφέρονται στην IS.D.OR.200 στοιχείο α) σημείο 9)·

iii) τη διαδικασία τροποποίησης του εγχειριδίου διαχείρισης της ασφάλειας των πληροφοριών που καθορίζεται στο στοιχείο γ)·

10) τις λεπτομέρειες των επί του παρόντος εγκεκριμένων εναλλακτικών μέσων συμμόρφωσης.

β) Η αρχική έκδοση του εγχειριδίου διαχείρισης της ασφάλειας των πληροφοριών εγκρίνεται και αντίγραφο φυλάσσεται από την αρμόδια αρχή. Το εγχειρίδιο διαχείρισης της ασφάλειας των πληροφοριών τροποποιείται ανάλογα με τις ανάγκες, ώστε να

παραμένει επικαιροποιημένη η περιγραφή του συστήματος διαχείρισης της ασφάλειας των πληροφοριών του φορέα. Αντίγραφο τυχόν τροποποιήσεων του εγχειριδίου διαχείρισης της ασφάλειας των πληροφοριών παρέχεται στην αρμόδια αρχή.

γ) Η διαχείριση των τροποποιήσεων του εγχειριδίου διαχείρισης της ασφάλειας των πληροφοριών πραγματοποιείται σύμφωνα με διαδικασία την οποία θεσπίζει ο φορέας. Τυχόν τροποποιήσεις που δεν περιλαμβάνονται στο πεδίο εφαρμογής της διαδικασίας αυτής, καθώς και τυχόν τροποποιήσεις που αφορούν τις αλλαγές που απαριθμούνται στην IS.D.OR.255 στοιχείο β), εγκρίνονται από την αρμόδια αρχή.

δ) Ο φορέας μπορεί να ενσωματώσει το εγχειρίδιο διαχείρισης της ασφάλειας των πληροφοριών σε άλλα εγχειρίδια διαχείρισης που έχει στην κατοχή του, υπό την προϋπόθεση ότι υπάρχει σαφής παραπομπή που υποδεικνύει ποια τμήματα του εγχειριδίου διαχείρισης αντιστοιχούν στις διάφορες απαιτήσεις του παρόντος παραρτήματος.

IS.D.OR.255 Αλλαγές του συστήματος διαχείρισης της ασφάλειας των πληροφοριών

α) Η διαχείριση των αλλαγών του συστήματος διαχείρισης της ασφάλειας των πληροφοριών και η κοινοποίησή τους στην αρμόδια αρχή μπορούν να πραγματοποιούνται στο πλαίσιο διαδικασίας που καταρτίζεται από τον φορέα. Η διαδικασία αυτή εγκρίνεται από την αρμόδια αρχή.

β) Όσον αφορά τις αλλαγές του συστήματος διαχείρισης της ασφάλειας των πληροφοριών που δεν καλύπτονται από τη διαδικασία που αναφέρεται στο στοιχείο α), ο φορέας υποβάλλει αίτηση και λαμβάνει έγκριση που εκδίδεται από την αρμόδια αρχή.

Όσον αφορά τις αλλαγές αυτές:

1) η αίτηση υποβάλλεται πριν από την υλοποίηση της εν λόγω αλλαγής, ώστε να μπορεί η αρμόδια αρχή να διαπιστώσει τη συνεχή συμμόρφωση προς τον παρόντα κανονισμό και να τροποποιήσει, αν είναι αναγκαίο, το πιστοποιητικό του φορέα και τους συνημμένους σε αυτό σχετικούς όρους έγκρισης·

2) ο φορέας θέτει στη διάθεση της αρμόδιας αρχής κάθε πληροφορία που ζητεί για την αξιολόγηση της αλλαγής·

3) η αλλαγή εφαρμόζεται μόνο μετά την παραλαβή επίσημης έγκρισης από την αρμόδια αρχή·

4) κατά την εφαρμογή των εν λόγω αλλαγών ο φορέας λειτουργεί υπό τους όρους που καθορίζει η αρμόδια αρχή.

IS.D.OR.260 Συνεχής βελτίωση

α) Ο φορέας αξιολογεί, χρησιμοποιώντας επαρκείς δείκτες επιδόσεων, την αποτελεσματικότητα και την ωριμότητα του συστήματος διαχείρισης της ασφάλειας των πληροφοριών. Η εν λόγω αξιολόγηση διενεργείται σε ημερολογιακή βάση που προκαθορίζεται από τον φορέα ή έπειτα από συμβάν ασφάλειας πληροφοριών.

β) Εάν διαπιστωθούν ελλείψεις μετά την αξιολόγηση που διενεργείται σύμφωνα με το στοιχείο α), ο φορέας λαμβάνει τα αναγκαία μέτρα βελτίωσης για να διασφαλίσει ότι το σύστημα διαχείρισης της ασφάλειας των πληροφοριών εξακολουθεί να συμμορφώνεται με τις εφαρμοστέες απαιτήσεις και διατηρεί τους κινδύνους για την ασφάλεια των πληροφοριών σε αποδεκτό επίπεδο. Επιπλέον, ο φορέας επαναξιολογεί τα στοιχεία του συστήματος διαχείρισης της ασφάλειας των πληροφοριών που επηρεάζονται από τα θεσπισθέντα μέτρα.