Ε.Ε. Παρ. III(I) **Κ.Δ.Π. 389/2020**
Αρ. 5342, 21.8.2020
Αριθμός 389

Ο ΠΕΡΙ ΑΣΦΑΛΕΙΑΣ ΔΙΚΤΥΩΝ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΩΝ ΝΟΜΟΣ ΤΟΥ 2020

Απόφαση δυνάμει των άρθρων 17(ιζ), 17(ιη), 17(ιθ), 17(κβ), 17(κγ), 19(1)(β), 19(1)(γ), 20(1)(α), 20(1)(β), 20(1)(γ), 46(1), 46(4) και 46(5)

Η Αρχή Ψηφιακής Ασφάλειας (στο εξής «η Αρχή»),

(α) ασκώντας τις εξουσίες που της παρέχουν τα άρθρα 17(ιζ), 17(ιη), 17(ιθ), 17(κβ), 17(κγ), 19(1)(β), 19(1)(γ), 20(1)(α), 20(1)(β), 20(1)(γ), 46(1), 46(4)και 46(5) του περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών Νόμου του 2020, και

89(I)/2020.

(β) λαμβάνοντας υπόψη την Οδηγία (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 6ης Ιουλίου 2016,

εκδίδει την παρούσα Απόφαση με την οποία καθορίζεται το πλαίσιο των ελάχιστων μέτρων ασφάλειας δικτύων και συστημάτων πληροφοριών και το οποίο έχει ως στόχο να βοηθήσει τους Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών και τους Φορείς Κρίσιμων Υπηρεσιών Πληροφοριών στην Κύπρο, να συμμορφωθούν με τις απαιτήσεις και τις υποχρεώσεις του Νόμου και της Οδηγίας (ΕΕ) 2016/1148.

Συνοπτικός τίτλος.

1. Η παρούσα Απόφαση θα αναφέρεται ως η περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών (Μέτρα Ασφάλειας Φορέων Εκμετάλλευσης Βασικών Υπηρεσιών και Φορέων Κρίσιμων Υποδομών Πληροφοριών) Απόφαση του 2020.

ΜΕΡΟΣ Ι
Εισαγωγικές Διατάξεις

Ερμηνεία.

2. (1) Στη παρούσα Απόφαση εκτός εάν από το κείμενο προκύπτει διαφορετική έννοια:

«Αρχή» σημαίνει την Αρχή Ψηφιακής Ασφάλειας·

«Μικρός Οργανισμός» σημαίνει τον οργανισμό ή επιχείρηση με τα χαρακτηριστικά μικρής επιχείρησης όπως ορίστηκε στη σύσταση της Επιτροπής, της 6ης Μαΐου 2003, σχετικά με τον ορισμό των πολύ μικρών, των μικρών και των μεσαίων επιχειρήσεων (Σύσταση 2003/361/ΕΚ)·

Σύσταση 2003/361/ΕΚ.

«Νόμος» σημαίνει τον περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών Νόμο του 2020 και περιλαμβάνει κάθε Νόμο που τον τροποποιεί ή τον αντικαθιστά·

89(I) ΤΟΥ 2020.

«ουσιώδης υπηρεσία» σημαίνει κάθε υπηρεσία που είναι ουσιαστική για τη διασφάλιση της λειτουργίας κρίσιμων τομέων της κοινωνικής και οικονομικής δράσης, συμπεριλαμβανομένου των βασικών υπηρεσιών και των υπηρεσιών που παρέχουν οι φορείς κρίσιμων υποδομών πληροφοριών·

«φορέας» σημαίνει φορέας εκμετάλλευσης βασικών υπηρεσιών ή φορέας κρίσιμων υποδομών πληροφοριών, όπως ορίζονται στο Νόμο.

(2) Εκτός εάν από το κείμενο προκύπτει διαφορετική έννοια οι όροι που χρησιμοποιούνται στο παρόν Διάταγμα έχουν την έννοια που αποδίδει σ' αυτούς ο Νόμος.

Πεδίο Εφαρμογής.

3. Η παρούσα Απόφαση πραγματεύεται τον καθορισμό των ελάχιστων απαιτήσεων και υποχρεώσεων σχετικά με την ασφάλεια δικτύων και συστημάτων πληροφοριών τις οποίες πρέπει να τηρούν οι φορείς.

Σκοπός.

4. Σκοπός των ρυθμιστικών υποχρεώσεων που επιβάλλονται στους φορείς είναι η ενίσχυση της ασφάλειας και της ανθεκτικότητας των υποδομών και των υπηρεσιών τους, η αντιμετώπιση περιστατικών παραβίασης ασφάλειας και η διασφάλιση της επιχειρησιακής συνέχειας των δικτύων, των συστημάτων πληροφοριών και των υπηρεσιών τους σε περίπτωση καταστρεπτικής βλάβης ή σε περίπτωση ανωτέρας βίας.

ΜΕΡΟΣ ΙΙ

Γενικοί όροι και υποχρεώσεις φορέων εκμετάλλευσης βασικών υπηρεσιών και φορέων κρίσιμων υποδομών πληροφοριών

Γενικός όρος.

5. Όλοι οι αδειοδοτημένοι φορείς οφείλουν να λαμβάνουν τα απαραίτητα μέτρα έτσι ώστε να διασφαλίζεται η ορθή και αποτελεσματική λειτουργία του δικτύου τους σε περίπτωση βλαβών ή/και αλλαγών στα κανονικά επίπεδα λειτουργίας, από φυσικά αίτια ή κακόβουλες ενέργειες.

Υποχρεώσεις φορέων.

6. Κάθε φορέας οφείλει να συμμορφώνεται με τις ακόλουθες υποχρεώσεις:

(1) Να προβαίνει, σε ετήσια βάση, σε αξιολόγηση κινδύνων (risk assessment) των δικτύων, συστημάτων πληροφοριών και ουσιωδών υπηρεσιών του προκειμένου να εντοπίζει σημαντικές αδυναμίες και ευάλωτα σημεία στις δικτυακές του υποδομές, σύμφωνα με τις πρόνοιες του Μέρος ΙΙΙ της παρούσας Απόφασης. Ο φορέας υποχρεούται να υποβάλλει στην Αρχή πληροφορίες για την αξιολόγηση κινδύνων που διενεργεί, ως αναφέρονται στο άρθρο 13, με στόχο την ενημέρωση της Αρχής.

(2)(α) Να προετοιμάζει σχέδια επιχειρησιακής συνέχειας (business continuity plans) σύμφωνα με τις πρόνοιες του Μέρους IV της παρούσας Απόφασης, τα οποία πρέπει να βασίζονται στα αποτελέσματα της αξιολόγησης κινδύνων, την οποία έχει πραγματοποιήσει για το δίκτυο και τις υπηρεσίες του.

(β) Ειδικότερα, οφείλει όπως, για ενδεχόμενα εκτάκτων συνθηκών, καταστροφικής βλάβης και ανωτέρας βίας, καταρτίζει και κοινοποιεί στην Αρχή σχέδιο αποκατάστασης από καταστροφή (disaster recovery plan) το οποίο να καταγράφει με λεπτομέρεια τη λήψη μέτρων αποκατάστασης.

(3) Να εφαρμόζει Σύστημα/Πλαίσιο Διαχείρισης Ασφάλειας και να λαμβάνει κατάλληλα και αναλογικά τεχνικά και οργανωτικά μέτρα, σύμφωνα με τις πρόνοιες του Μέρους V της παρούσας Απόφασης, για τη διαχείριση των κινδύνων, για την αποτροπή και την ελαχιστοποίηση του αντίκτυπου συμβάντων, και για τη διασφάλιση της συνέχειας των υπηρεσιών του, όσον αφορά την ασφάλεια των δικτύων και συστημάτων πληροφοριών που χρησιμοποιεί στις δραστηριότητές του.

(4) Να παρακολουθεί συνεχώς και σε πραγματικό χρόνο την κατάσταση των στοιχείων/εξοπλισμού των δικτύων, συστημάτων πληροφοριών και ουσιωδών υπηρεσιών του ως προς τη λειτουργική τους δυνατότητα και τις πιθανές βλάβες οι οποίες μπορούν να προκύψουν κατά τη λειτουργία του εξοπλισμού.

Οι φορείς οφείλουν επίσης να διατηρούν προσωπικό το οποίο να εργάζεται με ωράριο βάρδιας και/ή να τελεί σε κατάσταση επιφυλακής-ετοιμότητας (standby) ώστε να μπορεί να ανταποκριθεί άμεσα σε βλάβες που πιθανόν να επηρεάσουν τις παρεχόμενες υπηρεσίες, εκτός του καθιερωμένου ωραρίου.

(5) Να διασφαλίζει την επιχειρησιακή ακεραιότητα του δικτύου του, διασφαλίζοντας ότι ο εξοπλισμός είναι αξιόπιστος, ασφαλής έναντι εξωτερικών απειλών (π.χ. κακόβουλων επιθέσεων) και διαθέτει δυνατότητα υποβαθμισμένης λειτουργίας ακόμα και στην περίπτωση που υποστεί μερική βλάβη, υπό την επιφύλαξη ανωτέρας βίας. Κατά το σχεδιασμό και την επιλογή της αρχιτεκτονικής του δικτύου τους, οι φορείς θα πρέπει να λαμβάνουν υπόψη θέματα εφεδρείας (redundancy) και φυσικής ασφάλειας (physical security) του εξοπλισμού τους.

(6) Να διαθέτει ή και να εξασφαλίζει τη διαθεσιμότητα κατάλληλων και επαρκών αποθεμάτων (ανταλλακτικών) εξοπλισμού και να διατηρεί κατάλληλα καταρτισμένο προσωπικό έτσι ώστε σε περιπτώσεις βλαβών που επηρεάζουν την λειτουργικότητα του δικτύου να μπορεί να αποκαταστήσει τη λειτουργία του δικτύου και των παρεχόμενων υπηρεσιών καθ' όλη τη διάρκεια του εικοσιτετραώρου.

(7) Να συμμορφώνεται, με πρότυπα ή προδιαγραφές που θεσπίζονται σε κοινοτικό επίπεδο, χαρακτηρίζονται ως υποχρεωτικά και έχουν δημοσιευθεί σε κατάλογο προτύπων ή και

προδιαγραφών στην Επίσημη Εφημερίδα των Ευρωπαϊκών Κοινοτήτων, ή/και εθνικά πρότυπα, όπου εφαρμόζεται.

ΜΕΡΟΣ ΙΙΙ
Αξιολόγηση Κινδύνων

Αξιολόγηση κινδύνων.

7. (1) Λαμβάνοντας υπόψη την εξέλιξη της τεχνολογίας, το κόστος εφαρμογής και τις μεταβαλλόμενες επιπτώσεις και πιθανότητες εκδήλωσης κινδύνων που αφορούν την εμπιστευτικότητα, την ακεραιότητα, τη διαθεσιμότητα και την αυθεντικότητα πληροφοριών, ο φορέας καταρτίζει, εφαρμόζει και διατηρεί κατάλληλα τεχνικά και οργανωτικά μέτρα ώστε να διασφαλίζεται ένα επίπεδο ασφάλειας ανάλογο προς τον κίνδυνο. Ο φορέας εφαρμόζει τα μέτρα ασφάλειας πληροφοριών με σκοπό τη μείωση του κινδύνου σε αποδεκτό επίπεδο και τη διασφάλιση της κατάλληλης αντιμετώπισης των κινδύνων, εκτός εάν τα μέτρα ασφάλειας είναι ανεπαρκή όσον αφορά τη συγκεκριμένη κατάσταση του οργανισμού με βάση, μεταξύ άλλων, τις διαδικασίες διαχείρισης κινδύνου που εφαρμόζει. Εάν ο οργανισμός θεωρεί ότι τα μέτρα ασφάλειας είναι ανεπαρκή, ή αν πρέπει να λαμβάνει υπόψη επιπρόσθετες υποχρεώσεις (π.χ. από άλλο νομικό πλαίσιο), τότε ο οργανισμός πρέπει να αποφασίσει πώς θα αντιμετωπίσει κατάλληλα τους κινδύνους που έχει επισημάνει. Το πλαίσιο αξιολόγησης κινδύνων αναφέρεται στο Παράρτημα Ι.

(2) Οι φορείς, στο πλαίσιο των λαμβανόμενων μέτρων για προστασία του δικτύου τους, υποχρεούνται να διενεργούν σε τακτά χρονικά διαστήματα και τουλάχιστο σε ετήσια βάση αξιολόγηση κινδύνων.

(3) Προκειμένου να αξιολογείται το κατάλληλο επίπεδο ασφάλειας, ο οργανισμός πρέπει να καθιερώνει, να εφαρμόζει και να διατηρεί διαδικασία για τη διαχείριση κινδύνων ασφάλειας πληροφοριών, συμπεριλαμβανομένων, κατά περίπτωση:

(α) Τον προσδιορισμό του οργανωτικού πλαισίου, συμπεριλαμβανομένων των κριτηρίων για την αξιολόγηση και τον μετριασμό των κινδύνων ασφάλειας πληροφοριών, των ρόλων και αρμοδιοτήτων, των ιδιοκτητών κινδύνου, των κριτηρίων ανάλυσης του κινδύνου για τις επιπτώσεις και την πιθανότητα, τις κλίμακες βαθμολογιών κινδύνου, τα κριτήρια αξιολόγησης κινδύνων, και τις πολιτικές ανάληψης κινδύνων και ανοχής στους κινδύνους,

(β) τον εντοπισμό των κινδύνων για την ασφάλεια πληροφοριών, λαμβάνοντας υπόψη τις διάφορες απειλές, σενάρια απειλών και ευπάθειες που αφορούν την εμπιστευτικότητα, την ακεραιότητα, τη διαθεσιμότητα και την αυθεντικότητα των πληροφοριών,

(γ) την ανάλυση κινδύνων για την ασφάλεια πληροφοριών, λαμβάνοντας υπόψη τα κριτήρια εκτίμησης των κινδύνων σε σχέση με τις επιπτώσεις και την πιθανότητα, καθώς και άλλων σχετικών κριτηρίων για τον προσδιορισμό της βαθμολογίας κινδύνου,

(δ) την αξιολόγηση των κινδύνων για την ασφάλεια πληροφοριών, λαμβάνοντας υπόψη τα κριτήρια αξιολόγησης των κινδύνων και την πολιτική ανάληψης κινδύνων, προκειμένου να καθοριστούν οι κατάλληλες στρατηγικές αντιμετώπισης των κινδύνων,

(ε) την αντιμετώπιση των κινδύνων ασφάλειας πληροφοριών, λαμβάνοντας υπόψη, μεταξύ άλλων, τη διατήρηση / αποδοχή του κινδύνου, τη μεταφορά κινδύνου, την αποφυγή κινδύνου ή τη μείωση του κινδύνου.

(4) Κατά την αξιολόγηση του κατάλληλου επιπέδου ασφάλειας, πρέπει να λαμβάνονται ειδικότερα υπόψη οι κίνδυνοι που προκύπτουν από τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, μη εγκεκριμένη κοινοποίηση ή πρόσβαση σε πληροφορίες που μεταδίδονται, αποθηκεύονται ή υποβάλλονται, κατ' άλλο, τρόπο σε επεξεργασία.

(5) Κατά την αξιολόγηση του κατάλληλου επιπέδου ασφάλειας, πρέπει να λαμβάνονται ειδικότερα υπόψη οι κίνδυνοι οι οποίοι θα μπορούσαν να επιδράσουν δυνητικά σε ουσιώδεις οικονομικές και κοινωνικές λειτουργίες και υπηρεσίες που παρέχονται από τον φορέα.

(6) Το αποτέλεσμα της αξιολόγησης κινδύνων, κοινοποιείται στην Αρχή, κατά τα διαλαμβανόμενα στο Άρθρο 6(1). Η Αρχή έχει το δικαίωμα πρόσβασης στη διαδικασία διαχείρισης κινδύνων και στο σχέδιο αντιμετώπισης κινδύνων που καταρτίζει ο φορέας. Εάν η Αρχή κρίνει ότι η διαδικασία διαχείρισης κινδύνων και το σχέδιο αντιμετώπισης κινδύνων δεν αντιμετωπίζουν επαρκώς τους κινδύνους που έχουν εντοπιστεί από τον φορέα, η Αρχή έχει την εξουσία να επιβάλει ή να συμφωνήσει διορθωτικά μέτρα/δράσεις στον φορέα.

ΜΕΡΟΣ IV
Επιχειρησιακή Συνέχεια και Αντιμετώπιση Εκτάκτων Συνθηκών

Καταρτισμός Σχεδίου Επιχειρησιακής Συνέχειας.

8. Οι φορείς πρέπει να καταρτίζουν σχέδιο επιχειρησιακής συνέχειας (Business Continuity Plan), το οποίο αποσκοπεί στη διασφάλιση της αδιάλειπτης/απρόσκοπτης λειτουργίας των δικτύων, των συστημάτων πληροφοριών και των παρεχόμενων υπηρεσιών τους.

Το σχέδιο καταρτίζεται αφού προηγηθεί η αξιολόγηση κινδύνου και στη βάση των ευρημάτων/αποτελεσμάτων αυτής. Περιέχει περιγραφή των μέτρων που λαμβάνει ο φορέας για την αποκατάσταση της λειτουργίας των στοιχείων του δικτύου του και την αποκατάσταση των υπηρεσιών και των πληροφοριών του. Το ελάχιστο περιεχόμενο του σχεδίου επιχειρησιακής συνέχειας περιγράφεται στο Παράρτημα ΙΙ.

Καταρτισμός Σχεδίου Αποκατάστασης από Καταστροφές.

9. Οι φορείς υποχρεούνται να καταρτίζουν Σχέδιο Αποκατάστασης από Καταστροφές (Disaster Recovery Plan), στο πλαίσιο του οποίου καταγράφονται οι απαραίτητες δράσεις που αποσκοπούν στη διατήρηση της διαθεσιμότητας των υπηρεσιών που παρέχονται και στη διατήρηση του υψηλότερου δυνατού επιπέδου υπηρεσιών για την ανταπόκριση στις απαιτήσεις οποιασδήποτε δημόσιας αρχής, σε περίπτωση καταστρεπτικής βλάβης ή ανωτέρας βίας.

Το Σχέδιο Αποκατάστασης από Καταστροφές θα πρέπει να αναθεωρείται στη βάση καθορισμένων διαδικασιών από προσωπικό του παροχέα το οποίο είναι υπεύθυνο για τον καταρτισμό και την αναγκαία αναθεώρηση του Σχεδίου. Το ελάχιστο περιεχόμενο του σχεδίου αποκατάστασης από καταστροφές περιγράφεται στο Παράρτημα ΙΙ.

Έλεγχοι.

10. Οι φορείς οφείλουν να ελέγχουν την αποτελεσματικότητα του Σχεδίου Επιχειρησιακής Συνέχειας και του Σχεδίου Αποκατάστασης από Καταστροφές συστηματικά και τουλάχιστον σε ετήσια βάση.

Οι φορείς υποχρεούνται να διαθέτουν καταγεγραμμένες διαδικασίες βάσει των οποίων πραγματοποιούνται οι συγκεκριμένοι έλεγχοι. Η συχνότητα και το εύρος των ελέγχων καθορίζεται από τους κινδύνους που έχουν αναγνωριστεί και τα εφαρμοζόμενα μέτρα ασφάλειας.

ΜΕΡΟΣ V
Εφαρμογή Συστήματος/Πλαισίου Διαχείρισης Ασφάλειας - Εφαρμογή Τεχνικών και Οργανωτικών Μέτρων

Εφαρμογή Πλαισίου Μέτρων Ασφάλειας.

11. (1) Οι φορείς υποχρεούνται να εφαρμόζουν κατ' ελάχιστον το Πλαίσιο Μέτρων Ασφάλειας που δημοσιεύεται από την Αρχή και το οποίο θεσπίζει μέτρα, προετοιμασίας (prepare), προστασίας και εντοπισμού (protect and detect) και ανταπόκρισης (respond), με στόχο τη θέσπιση, εφαρμογή και διατήρηση μιας πολυεπίπεδης προσέγγισης άμυνας για τη διατήρηση της εμπιστευτικότητας, ακεραιότητας, διαθεσιμότητας, αυθεντικότητας και ανθεκτικότητας των συστημάτων δικτύων και πληροφοριών και των παρεχομένων υπηρεσιών. Το πλαίσιο των ελάχιστων τεχνικών και οργανωτικών μέτρων περιγράφεται στο Παράρτημα ΙΙΙ.

(2) Οι φορείς πρέπει να εφαρμόζουν κατάλληλα μέτρα προετοιμασίας διασφαλίζοντας ότι λαμβάνουν υπόψη τον κίνδυνο για την ασφάλεια πληροφοριών στην καθημερινή λειτουργία τους και εξασφαλίζουν τη δέσμευση της διοίκησης στο ανώτατο επίπεδο για την αντιμετώπιση απειλών, ευπαθειών και κινδύνων ασφάλειας σύμφωνα με το Μέρος 1.1 του Παραρτήματος ΙΙΙ.

(3) Οι φορείς πρέπει να εφαρμόζουν κατάλληλα μέτρα προστασίας και εντοπισμού διασφαλίζοντας ότι θεσπίζουν, εφαρμόζουν και διατηρούν επαρκή μέτρα ασφάλειας πληροφοριών κατάλληλα για την έκθεση τους σε κίνδυνο. Κατ' ελάχιστον πρέπει να λαμβάνονται μέτρα πρόληψης, εντοπισμού και αντίδρασης από τεχνολογική, διοικητική και φυσική άποψη σύμφωνα με το Μέρος 1.2 του Παραρτήματος ΙΙΙ.

(4) Οι φορείς πρέπει να εφαρμόζουν κατάλληλα μέτρα ανταπόκρισης διασφαλίζοντας ότι είναι σε θέση να ανταποκρίνονται σε συμβάντα και περιστατικά που ενδέχεται να επηρεάσουν την εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα ή αυθεντικότητα των πληροφοριών. Κατ' ελάχιστον πρέπει να λαμβάνονται μέτρα για τη διασφάλιση της επιχειρησιακής ανθεκτικότητας και επιχειρησιακής συνέχειας και αποκατάστασης από καταστροφές, καθώς και την επαναφορά στις κανονικές τους δραστηριότητες σύμφωνα με το Μέρος 1.3 του Παραρτήματος ΙΙΙ.

Υπεύθυνος για την ασφάλεια δικτύων και συστημάτων πληροφοριών.

12. (1) Για την εφαρμογή του Πλαισίου απαιτείται η κατανομή ρόλων και αρμοδιοτήτων για την ασφάλεια των δικτύων και συστημάτων πληροφοριών εντός του οργανισμού.

(2) Ο φορέας οφείλει να ορίζει έναν υπεύθυνο για την ασφάλεια δικτύων και συστημάτων πληροφοριών, όπου:

(α) Ο υπεύθυνος ασφάλειας δικτύων και πληροφοριών διορίζεται βάσει επαγγελματικών προσόντων και κυρίως βάσει ειδικών γνώσεων στον τομέα της ασφάλειας δικτύων και πληροφοριών και της ικανότητας εκπλήρωσης των καθηκόντων που αναφέρονται στο εδάφιο (3),

(β) ο υπεύθυνος ασφάλειας δικτύων και πληροφοριών πρέπει να εκτελεί αποκλειστικά αυτά τα καθήκοντα. Για μικρούς οργανισμούς, ο υπεύθυνος ασφάλειας δικτύων και πληροφοριών δύναται να εκτελεί και άλλα καθήκοντα μόνο όταν δεν οδηγούν σε σύγκρουση συμφερόντων και λαμβάνοντας υπόψη το επίπεδο κρισιμότητας του φορέα, με την έγκριση της Αρχής,

(γ) ο φορέας κοινοποιεί στην Αρχή τα στοιχεία επικοινωνίας του υπευθύνου ασφάλειας δικτύων και πληροφοριών,

(δ) ο φορέας διασφαλίζει ότι οι υποψήφιοι για τη θέση του υπεύθυνου ασφάλειας δικτύων και πληροφοριών ελέγχονται επαρκώς, ώστε να εξασφαλίζεται ότι το εν λόγω πρόσωπο θα διεκπεραιώνει τα καθήκοντά του δεόντως.

Ελάχιστες αρμοδιότητες.

(3) Ο υπεύθυνος ασφάλειας δικτύων και πληροφοριών που ορίζεται από τον φορέα έχει τουλάχιστον τα ακόλουθα καθήκοντα:

(α) Να ενημερώνει και να συμβουλεύει τον φορέα και τους υπαλλήλους που έχουν πρόσβαση στα συστήματα δικτύων και πληροφοριών τους σχετικά με τις υποχρεώσεις τους σύμφωνα με το παρόν πλαίσιο,

(β) να παρακολουθεί τη συμμόρφωση με το παρόν πλαίσιο, με άλλες εθνικές ή ευρωπαϊκές πρόνοιες για την ασφάλεια πληροφοριών, και με τις πολιτικές του φορέα σε σχέση με την ασφάλεια δικτύων και συστημάτων πληροφοριών,

(γ) να παρέχει συμβουλές όσον αφορά τη διαχείριση της ασφάλειας πληροφοριών και να παρακολουθεί τις επιδόσεις της σύμφωνα με το Μέρος ΙΙΙ για τη διαχείριση κινδύνου.

(δ) να συνεργάζεται και να ενεργεί ως ενιαίο σημείο επαφής με την Αρχή για θέματα που σχετίζονται με τις δραστηριότητες της Αρχής στο πλαίσιο των αρμοδιοτήτων της, μεταξύ άλλων με την παροχή υποστήριξης σε δραστηριότητες εξωτερικού ελέγχου, με την εκ των προτέρων παροχή εγγράφων και πληροφοριών στην Αρχή, όπως αναφέρονται στο άρθρο 13.

(ε) να παρέχει αναφορές σχετικά με απειλές για την ασφάλεια πληροφοριών, ευπάθειες και κινδύνους προς τη διοίκηση ανώτατου επιπέδου μέσω επίσημων και τακτικών εκθέσεων.

Θέση του Υπευθύνου ασφάλειας δικτύων και συστημάτων πληροφοριών.

(4) Ο κάθε φορέας διασφαλίζει ότι ο υπεύθυνος ασφάλειας δικτύων και πληροφοριών συμμετέχει δεόντως και εγκαίρως σε όλα τα ζητήματα που σχετίζονται με την ασφάλεια δικτύων και συστημάτων πληροφοριών-

(α) Ο φορέας υποστηρίζει τον υπεύθυνο ασφάλειας δικτύων και πληροφοριών στην εκτέλεση των καθηκόντων του, όπως αυτά αναφέρονται στο εδάφιο 3.

(β) Ο φορέας μεριμνά ώστε ο υπεύθυνος ασφάλειας δικτύων και πληροφοριών να μην λαμβάνει οδηγίες που έρχονται σε σύγκρουση με την άσκηση των καθηκόντων του. Δεν απολύεται ούτε τιμωρείται από τον φορέα για τη δέουσα εκτέλεση των καθηκόντων του.

(γ) Ο υπεύθυνος ασφάλειας δικτύων και πληροφοριών αναφέρεται απευθείας στο ανώτατο διοικητικό επίπεδο του φορέα όσον αφορά τα καθήκοντά του που καθορίζονται στην παρούσα Απόφαση.

(δ) Ο υπεύθυνος ασφάλειας δικτύων και πληροφοριών δεσμεύεται από κανόνες εμπιστευτικότητας και επαγγελματικού απορρήτου όσον αφορά την εκτέλεση των καθηκόντων του.

(ε) Ο φορέας διασφαλίζει ότι ο υπεύθυνος ασφάλειας έχει πρόσβαση στους απαραίτητους οικονομικούς και ανθρώπινους πόρους, διαδικασίες και τεχνικά και οργανωτικά μέτρα, για να είναι σε θέση να εκτελεί τα καθήκοντά του και να υποστηρίζει κατάλληλα τον φορέα σε θέματα ασφάλειας δικτύων και συστημάτων πληροφοριών για συμμόρφωση με τις υποχρεώσεις που θέτει η Αρχή.

(στ) Ο φορέας διασφαλίζει ότι ο υπεύθυνος ασφάλειας έχει τις κατάλληλες γνώσεις, εκπαίδευση και εμπειρία που να συνάδουν με τα καθήκοντα του και ότι ο υπεύθυνος ασφάλειας αναβαθμίζει σε τακτά χρονικά διαστήματα τις γνώσεις του. Η Αρχή δύναται να παρέχει κατευθυντήριες οδηγίες για θέματα σχετικά με την κατάλληλη εκπαίδευση και εμπειρία του υπεύθυνου ασφαλείας.

Καταγραφή και παροχή Πληροφοριών.

13.(1) Για την εφαρμογή της παρούσας απόφασης οι φορείς έχουν υποχρέωση να καταγράφουν όλες τις σχετικές πληροφορίες σε σχέση με τη διαχείριση των κινδύνων ασφάλειας πληροφοριών και να παρέχουν την εν λόγω πληροφόρηση στην Αρχή ετήσια ή και κατόπιν αιτήματος, προκειμένου να επιτευχθούν οι στόχοι ασφάλειας πληροφοριών που απαιτούνται από το παρόν Πλαίσιο.

(2) Ο κάθε φορέας πρέπει να είναι σε θέση και υποχρεούται να παρέχει την ακόλουθη πληροφόρηση στην Αρχή, προκειμένου να αποδείξει τη συμμόρφωσή του προς τις υποχρεώσεις που υπέχει βάσει του παρόντος Πλαισίου:

(α) Τη μεθοδολογία διαχείρισης κινδύνου, συμπεριλαμβανομένων των κριτηρίων αξιολόγησης κινδύνου για τις επιπτώσεις και την πιθανότητα, τις κλίμακες βαθμολόγησης κινδύνου, τα κριτήρια εκτίμησης κινδύνων και την πολιτική ανάληψης κινδύνων / την ανοχή κινδύνου, σύμφωνα με Μέρος ΙΙΙ της παρούσας Απόφασης,

(β) την αξιολόγηση κινδύνου, συμπεριλαμβανομένου του εντοπισμού, της ανάλυσης και της αξιολόγησης όλων των κινδύνων για την ασφάλεια πληροφοριών εντός του οργανισμού, σύμφωνα με το Μέρος ΙΙΙ της παρούσας Απόφασης,

(γ) το μητρώο κινδύνων, το οποίο παρέχει επισκόπηση της ανάλυσης κινδύνου και της εκτίμησης κινδύνου όλων των κινδύνων για την ασφάλεια πληροφοριών που έχουν εντοπιστεί εντός του οργανισμού,

(δ) το σχέδιο αντιμετώπισης κινδύνων, το οποίο προσδιορίζει τα μέτρα εξυγίανσης για όλους τους κινδύνους που έχουν εντοπιστεί εντός του οργανισμού για την ασφάλεια

πληροφοριών, δηλαδή τη διατήρηση / αποδοχή του κινδύνου, τη μεταφορά κινδύνου, την αποφυγή κινδύνου ή τη μείωση του κινδύνου, σύμφωνα με το Μέρος ΙΙΙ της παρούσας Απόφασης,

(ε) τη δομή διακυβέρνησης, συμπεριλαμβανομένων των εσωτερικών ρόλων και αρμοδιοτήτων όσον αφορά στην ασφάλεια δικτύων και πληροφοριών, σύμφωνα με το άρθρο 12 σχετικά με τον υπεύθυνο ασφάλειας πληροφοριών,

(στ) την πολιτική ασφάλειας και τη στρατηγική για την ασφάλεια πληροφοριών,

(ζ) το σχέδιο εφαρμογής για τα μέτρα ασφάλειας δικτύων και πληροφοριών, το οποίο προβλέπει έναν μηχανισμό παρακολούθησης της εφαρμογής σε επιχειρησιακό επίπεδο,

(η) το σχέδιο επιχειρησιακής συνέχειας (business continuity plan),

(θ) το σχέδιο αποκατάστασης μετά από καταστροφή (disaster recovery plan).

ΜΕΡΟΣ VI
Ενημέρωση και εφαρμογή της παρούσας Απόφασης

Ενημέρωση επηρεαζόμενων και καταναλωτών.

14.(1) Οι φορείς οφείλουν να ενημερώνουν όλους τους επηρεαζόμενους, συμπεριλαμβανομένων και των καταναλωτών όπου εφαρμόζεται, σχετικά με γεγονότα τα οποία απειλούν ή και επηρεάζουν τη λειτουργία του δικτύου, των συστημάτων πληροφοριών ή και την παροχή των υπηρεσιών τους στη βάση σαφών διαδικασιών που έχουν καταγράψει. Νοείται ότι στους επηρεαζόμενους είναι δυνατόν να συμπεριλαμβάνονται και επηρεαζόμενοι φορείς εκμετάλλευσης βασικών υπηρεσιών ή και φορείς κρίσιμων υποδομών πληροφοριών κατόπιν υπόδειξης ή σύμφωνης γνώμης της Αρχής.

(2) Η σχετική ανακοίνωση για καταστροφικά συμβάντα ή απειλές ή γεγονότα που αναμένεται να επηρεάσουν δυσμενώς δικτύων, συστημάτων πληροφοριών και ουσιωδών υπηρεσιών και τις παρεχόμενες υπηρεσίες θα πρέπει να κοινοποιείται σε μέσα ευρείας κάλυψης. Ενδεικτικοί τρόποι ενημέρωσης των καταναλωτών είναι η ανάρτηση σχετικής ανακοίνωσης στην ιστοσελίδα του φορέων και η αποστολή μηνυμάτων ηλεκτρονικής αλληλογραφίας.

(3) Στο πλαίσιο της ανακοίνωσης, οι φορείς οφείλουν να ενημερώνουν όλους τους επηρεαζόμενους, συμπεριλαμβανομένων και των καταναλωτών όπου εφαρμόζεται, τουλάχιστον για την έκταση του γεγονότος, τις ενδεχόμενες επιπτώσεις, τα μέτρα που λαμβάνει ο φορέας για την αντιμετώπισή του, τον εκτιμώμενο χρόνο αποκατάστασης της υπηρεσίας και να απευθύνουν συμβουλές στους καταναλωτές, όπου αυτό εφαρμόζεται.

Ενημέρωση Αρχής.

Κ.Δ.Π. 218/2019.

15.(1) Οι φορείς οφείλουν να ενημερώνουν την Αρχή σχετικά με γεγονότα τα οποία απειλούν ή και επηρεάζουν τη λειτουργία του δικτύου, την ακεραιότητα, εμπιστευτικότητα, την αυθεντικότητα και τη διαθεσιμότητα της πληροφορίας στο δίκτυό τους και την παροχή των υπηρεσιών, σύμφωνα με τη διαδικασία και τον τύπο που ορίζεται στην Απόφαση αναφορικά με την υποχρέωση των φορέων εκμετάλλευσης βασικών υπηρεσιών ή και φορέων κρίσιμων υποδομών πληροφοριών ή και παροχέων ψηφιακών υπηρεσιών, για κοινοποίηση κάθε συμβάντος το οποίο έχει σοβαρό αντίκτυπο στη συνέχιση των υπηρεσιών που παρέχουν.

(2) Οι φορείς θα πρέπει να κοινοποιούν τα στοιχεία επικοινωνίας εξουσιοδοτημένου αντιπροσώπου με τον οποίο η Αρχή θα επικοινωνεί για θέματα που αφορούν τη συμμόρφωση των φορέων με τις πρόνοιες της παρούσας απόφασης. Οι φορείς υποχρεούνται να κοινοποιούν στην Αρχή, κάθε τροποποίηση των στοιχείων επικοινωνίας του εξουσιοδοτημένου προσώπου.

ΜΕΡΟΣ VIII
Έλεγχος και διαβουλεύσεις

Έλεγχος και αξιολόγηση πληροφοριών.

16.(1) Με την επιφύλαξη των γενικών εξουσιών και καθηκόντων ελέγχου/έρευνας που έχει σύμφωνα με την ισχύουσα νομοθεσία και ιδιαίτερα τα άρθρα 17(ιζ)(ιη)(ιθ) και 20(1)(α) του Νόμου και τις δυνάμει του Νόμου εκδοθείσες Αποφάσεις, η Αρχή δύναται κατά την κρίση της να ελέγχει την ορθή εκτέλεση των υποχρεώσεων που απορρέουν από τη παρούσα Απόφαση και τα σχετικά παραρτήματα, καθώς επίσης και την ακρίβεια των πληροφοριών που του παρέχονται σύμφωνα με τη παρούσα Απόφαση.

(2) Σε περίπτωση κατά την οποία ο προβλεπόμενος στο εδάφιο (1) έλεγχος από την Αρχή απαιτεί σύμβαση παροχής υπηρεσιών από τεχνικούς συμβούλους ή άλλα πρόσωπα, η Αρχή λαμβάνει εύλογα μέτρα για την εξασφάλιση της ανεξαρτησίας τους καθώς και για την τήρηση εκ μέρους τους εμπιστευτικότητας και αμεροληψίας.

(3) Για την άσκηση των αρμοδιοτήτων της η Αρχή δύναται να διεξάγει έρευνα σύμφωνα με το άρθρο 23 του Νόμου και να επιβάλλει διορθωτικά μέτρα έχοντας την εξουσία να:

(α) Δίνει εντολή σε φορέα να της παρέχει όλα τα σχετικά έγγραφα σύμφωνα με το άρθρο 13.

(β) Εκδίδει κατευθυντήριες γραμμές και δεσμευτικές οδηγίες προς τους φορείς όσον αφορά την παροχή εγγράφων και πληροφοριών στην Αρχή και τη μορφή τους.

(γ) Διενεργεί ελέγχους ασφάλειας πληροφοριών προκειμένου να αξιολογήσει κατά πόσον ο φορέας συμμορφώνεται με τις υποχρεώσεις του, όπως αυτές περιγράφονται στο παρόν Πλαίσιο.

(δ) Εκδίδει κατευθυντήριες γραμμές και δεσμευτικές οδηγίες όσον αφορά τους φορείς που δεν εκπληρώνουν τις υποχρεώσεις τους σύμφωνα με αυτό το Πλαίσιο.

Επιπλέον, η Αρχή έχει την εξουσία να εκδίδει επίσημες γνωμοδοτήσεις και κατευθυντήριες γραμμές για να βοηθά τους φορείς στην εφαρμογή συγκεκριμένων μέτρων που καθορίζονται στα Παραρτήματα της παρούσας Απόφασης.

Δημόσιες διαβουλεύσεις.

17.(1) Με την επιφύλαξη των γενικών καθηκόντων και εξουσιών της Αρχής και των διαδικασιών που ορίζει η ίδια σε σχέση με δημόσιες διαβουλεύσεις και των δυνάμει του Νόμου εκδοθέντων Αποφάσεων, η Αρχή, εάν το θεωρεί αναγκαίο, δύναται να έχει διαβουλεύσεις με τα κατά περίπτωση ενδιαφερόμενα μέρη σε σχέση με θέματα ασφάλειας δικτύων και συστημάτων πληροφοριών.

(2) Το αντικείμενο των διαβουλεύσεων που αναφέρονται στο εδάφιο (1) καθορίζεται από την Αρχή και μπορεί να αφορά, μεταξύ άλλων:

(α) Την ανταλλαγή απόψεων για την ανάγκη διατήρησης ή προσαρμογής της παρούσας Απόφασης και των παραρτημάτων αυτής, εν όψει της εμπειρίας στην πρακτική εφαρμογή τους και των σχετικών εξελίξεων στις προσφερόμενες υπηρεσίες, στις σχετικές προδιαγραφές και στις ανάγκες της αγοράς,

(β) τον καθορισμό εθελοντικών διαδικασιών, ορισμών και μεθόδων σε περίπτωση κατά την οποία τα στοιχεία αυτά δεν προσδιορίζονται στις διατάξεις της παρούσας Απόφασης ή των Παραρτημάτων αυτής,

(γ) οποιοδήποτε διαδικαστικό ή άλλο θέμα ήθελε προκύψει κατά την πρακτική εφαρμογή της παρούσας Απόφασης.

Προσθήκη και τροποποίηση Παραρτημάτων.

18.(1) Η Αρχή δύναται με απόφαση του Επιτρόπου να προσθέτει παραρτήματα στην παρούσα Απόφαση ή να τροποποιεί το περιεχόμενο των παραρτημάτων μέσω τροποποιητικών αποφάσεων.

(2) Πριν την έκδοση Απόφασης δυνάμει του εδαφίου (1) του παρόντος άρθρου, η Αρχή ακολουθεί την διαδικασία διενέργειας Δημόσιας Διαβούλευσης, με βάση τις σχετικές νομοθετικές πρόνοιες.

ΜΕΡΟΣ IX
Συμμόρφωση – κυρώσεις

Παραβίαση υποχρέωσης.

19.(1) Σε περίπτωση που φορέας παραβιάζει υποχρέωση που απορρέει από τη παρούσα Απόφαση, ο Επίτροπος του κοινοποιεί Απόφαση που περιέχει τουλάχιστον :

(α) Περιγραφή της διαπιστωμένης παραβίασης,

(β) προθεσμία για συμμόρφωση ή/και για καθορισμό σχετικού πλάνου ενεργειών, που καθορίζεται κατά την κρίση της Αρχής και δεν μπορεί να είναι μεγαλύτερη από έξι (6) μήνες και

(γ) προθεσμίες για την εθελοντική υποβολή παρατηρήσεων, αίτηση ακρόασης ή/και αίτηση παράτασης της προθεσμίας από τον ενδιαφερόμενο παροχέα, κατ' εφαρμογή των εκάστοτε Κανονισμών/Διατάγματος/Απόφασης περί συλλογής πληροφοριών και επιβολής διοικητικού προστίμου.

(2) Σε εξαιρετικές περιπτώσεις, μετά από αιτιολογημένη αίτηση του ενδιαφερομένου φορέα και εφόσον αυτό δικαιολογείται αντικειμενικά, η Αρχή μπορεί να χορηγήσει παράταση της προθεσμίας συμμόρφωσης.

Διοικητικό πρόστιμο.

20. Δυνάμει του εδαφίου (κστ) του άρθρου 17 του Νόμου και χωρίς περιορισμό των άλλων κυρώσεων που μπορεί να προβλέπει αυτός, και οι δυνάμει αυτού εκδοθείσες Αποφάσεις, η Αρχή μπορεί να επιβάλει διοικητικό πρόστιμο κατ' εφαρμογή του άρθρου 43 του Νόμου ή οποιουδήποτε άλλου Νόμου τον τροποποιεί ή τον αντικαθιστά σε κάθε φορέα που παραβιάζει οποιαδήποτε από τις υποχρεώσεις του, όπως ορίζονται στη παρούσα Απόφαση.

ΜΕΡΟΣ X
Τελικές Διατάξεις

Έναρξη Ισχύος.

21. (1) Η παρούσα Απόφαση τίθεται σε ισχύ από την ημερομηνία δημοσίευσής της στην Επίσημη Εφημερίδα της Δημοκρατίας.

Οι φορείς οφείλουν να συμμορφωθούν με το ακόλουθο πρόγραμμα ενεργειών:

(α) Μέχρι 31 Δεκεμβρίου 2020
- Αποστολή έκθεσης στην Αρχή στην οποία θα καταγράφεται η παρούσα κατάσταση ασφάλειας δικτυών και συστημάτων πληροφοριών στον φορέα
  - Ο φορέας οφείλει να ενημερώσει την Αρχή, περιληπτικά, για το πρόγραμμα ασφάλειας που ακολουθεί κατά την εν λόγω ημερομηνία, με αναφορά στις πρόνοιες της παρούσας Απόφασης, τα οποία ο φορέας πληροί ήδη. Επίσης, ο φορέας λαμβάνοντας υπόψη και το Άρθρο 13 της παρούσας Απόφασης, θα ενημερώσει την Αρχή σχετικά με τα έγγραφα και τις πληροφορίες που είναι ήδη διαθέσιμα, όπου αυτό εφαρμόζεται.
  - Για την ομοιόμορφη αποτύπωση της υφιστάμενης κατάστασης η Αρχή είναι δυνατόν να παρέχει πρότυπο έγγραφο, με συγκεκριμένα πεδία.

(β) Μέχρι 31 Δεκεμβρίου 2021
- Υποβολή των εγγράφων και πληροφοριών σύμφωνα με τις απαιτήσεις του άρθρου 13 της παρούσας Απόφασης
  - Ο φορέας θα πρέπει να υποβάλει όλα τα προβλεπόμενα έγγραφα λαμβάνοντας υπόψη τις απαιτήσεις του άρθρου 13 της παρούσας Απόφασης, στην Αρχή για

αξιολόγηση. Η Αρχή δύναται να ζητήσει πρόσθετες πληροφορίες και εάν το κρίνει απαραίτητο, δύναται να ζητήσει τροποποιήσεις και βελτιώσεις. Όπως αναφέρεται στις παραγράφους 13(2)(δ) και 13(2)(ζ), τα έγγραφα θα πρέπει συνοδεύονται από λεπτομερές πρόγραμμα υλοποίησης των απαραίτητων μέτρων ασφάλειας για μείωση των κινδύνων που έχουν εντοπισθεί, σε αποδεκτά επίπεδα.

- Τα έγγραφα θα υποβάλλονται ηλεκτρονικά σε συγκεκριμένη πλατφόρμα που είναι δυνατόν να θέσει σε λειτουργία προς αυτό το σκοπό, η Αρχή.

(γ) Μέχρι 31 Δεκεμβρίου 2022

- Ολοκλήρωση της υλοποίησης και εφαρμογής των μέτρων ασφάλειας που αντιμετωπίζουν τους υψηλότερους σε κρισιμότητα, κινδύνους που έχουν εντοπιστεί
  - Ο φορέας θα πρέπει να μεριμνήσει ώστε να υλοποιηθούν και να εφαρμοστούν όσα μέτρα χρειάζονται ή/και περισσότερα (από τον κατάλογο μέτρων που περιλαμβάνονται στο Πλαίσιο Κυβερνοασφάλειας) για μείωση των υψηλότερων σε κρισιμότητα, κινδύνων που έχουν εντοπιστεί, σε αποδεκτά επίπεδα.
- Πρόγραμμα υλοποίησης του συνόλου του Πλαισίου
  - Ο φορέας θα πρέπει να υποβάλει επικαιροποιημένη κατάσταση κινδύνων, όπου θα πρέπει να φαίνεται η υλοποίηση των μέτρων για τους υψηλότερους κινδύνους, και να καθορίζεται το πρόγραμμα υλοποίησης του συνόλου του Πλαισίου, για μείωση και των υπολοίπων κινδύνων σε αποδεκτά επίπεδα.

(δ) Μέχρι 31 Δεκεμβρίου 2023 και μετέπειτα, σε ετήσια βάση

- Ολοκλήρωση της υλοποίησης του υπόλοιπου Πλαισίου
  - Ο φορέας θα πρέπει να μεριμνήσει ώστε να υλοποιηθεί το σύνολο του Πλαισίου, και να υποβάλει επικαιροποιημένη κατάσταση κινδύνων, όπου θα φαίνεται η υλοποίηση τους και η συνεπαγόμενη μείωση των κινδύνων, που έχουν εντοπισθεί, σε αποδεκτά επίπεδα.
- Υποβολή των εγγράφων και πληροφοριών σύμφωνα με τις απαιτήσεις του άρθρου 13 της παρούσας Απόφασης
  - Ο φορέας θα πρέπει να υποβάλει όλα τα προβλεπόμενα έγγραφα λαμβάνοντας υπόψη τις απαιτήσεις του άρθρου 13 της παρούσας Απόφασης, στην Αρχή για αξιολόγηση, επικαιροποιημένα για το νέο έτος, και συνέχιση του κύκλου εφαρμογής του Πλαισίου.
  - Τα έγγραφα θα υποβάλλονται ηλεκτρονικά σε συγκεκριμένη πλατφόρμα που θα θέσει σε λειτουργία προς αυτό το σκοπό, η Αρχή.

Σημειώνεται ότι η Αρχή θα διενεργεί εποπτικούς ελέγχους και ελέγχους συμμόρφωσης για την επιβεβαίωση εφαρμογής του Πλαισίου και των λοιπών υποχρεώσεων που προκύπτουν από τη Νομοθεσία, με βάση προτεραιοποίηση η οποία θα απορρέει από τον βαθμό κρισιμότητας του κάθε φορέα, του επιπέδου των κινδύνων που έχουν εντοπιστεί, και σε περιπτώσεις σημαντικών αλλαγών στο περιβάλλον των φορέων ή του κυβερνοχώρου ευρύτερα.

Σε εξαιρετικές περιπτώσεις, μετά από αιτιολογημένη αίτηση του ενδιαφερομένου φορέα και εφόσον αυτό δικαιολογείται αντικειμενικά, η Αρχή μπορεί να αποδεχτεί κατάλληλη προσαρμογή των προθεσμιών συμμόρφωσης για κάθε περίπτωση ξεχωριστά.

ΠΑΡΑΡΤΗΜΑ Ι : ΠΛΑΙΣΙΟ ΑΞΙΟΛΟΓΗΣΗΣ ΚΙΝΔΥΝΩΝ

(1) Οι φορείς θα πρέπει να λαμβάνουν υπόψη και να αξιολογούν όλους τους παράγοντες (ενδεικτικά, στοιχεία δικτύου, εγκαταστάσεις, προσωπικό) οι οποίοι σχετίζονται και μπορούν να επηρεάσουν την ακεραιότητα του δικτύου και τη διαθεσιμότητα των υπηρεσιών, σύμφωνα με όλα τα μέτρα ασφάλειας της κατηγορίας «Διαχείριση Κινδύνων» που αναφέρονται στο Παράρτημα ΙΙΙ.

(2) Ως βέλτιστη πρακτική, οι φορείς προτρέπονται όπως καθορίζουν κριτήρια/παραμέτρους βάσει των οποίων ιεραρχούνται τα στοιχεία του δικτύου τους ως προς την κρισιμότητά/σημασία τους αναφορικά με το ρόλο τους στην υποστήριξη των ουσιωδών υπηρεσιών τους. Η ιεράρχηση της σημασίας των μερών του δικτύου επηρεάζει σημαντικά τη λήψη διορθωτικών μέτρων.

(3) Οι φορείς, στη βάση των προαναφερθέντων κριτηρίων, καθορίζουν τα κρίσιμα μέρη/στοιχεία του δικτύου, βλάβη στα οποία δύναται να έχει σημαντική επίπτωση στην εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα και αυθεντικότητα των δικτύων, συστημάτων πληροφοριών και ουσιωδών υπηρεσιών.

(4) Οι φορείς θα πρέπει να εξετάζουν τόσο ενδογενείς κινδύνους, οι οποίοι εξαρτώνται από το επίπεδο της εσωτερικής αξιοπιστίας και ανθεκτικότητας του δικτύου, όσο και εξωγενείς απειλές, όπως καιρικές συνθήκες, φυσικές καταστροφές, ατυχήματα και πράξεις δολιοφθοράς. Επίσης, θα πρέπει να εξετάζουν κινδύνους οι οποίοι ενδεχομένως να προέρχονται από άλλα διασυνδεόμενα δίκτυα.

(5) Οι φορείς θα πρέπει να αξιολογούν την πιθανότητα πραγματοποίησης των κινδύνων, να εκτιμούν την επίδρασή τους στην εύρυθμη λειτουργία του δικτύου και των παρεχόμενων υπηρεσιών, λαμβάνοντας σοβαρά υπόψη τις εγγενείς αδυναμίες του δικτύου. Οι φορείς οφείλουν να εφαρμόζουν τα απαραίτητα μέτρα και ελέγχους για την αντιμετώπιση των κινδύνων που έχουν προσδιορίσει στο πλαίσιο της άσκησης αξιολόγησης κινδύνων.

(6) Οι φορείς προσδιορίζουν τρόπους αξιολόγησης της αποτελεσματικότητας των μέτρων που τηρούν και εφαρμόζουν διαδικασίες για την αξιολόγηση της αποτελεσματικότητας των εφαρμοζόμενων μέτρων.

(7) Οι φορείς αναθεωρούν την αξιολόγηση κινδύνων σε τακτά χρονικά διαστήματα λαμβάνοντας υπόψη α) την αποτελεσματικότητα των εφαρμοζόμενων μέτρων, β) την αναγνώριση νέων απειλών, γ) οργανωτικές ή τεχνολογικές αλλαγές και δ) άλλα γεγονότα που θα έθεταν καινούρια δεδομένα τα οποία οφείλουν να λάβουν υπόψη τους.

(8) Η Αρχή δύναται να ορίσει πρόσθετες πληροφορίες που θα πρέπει να περιλαμβάνονται στην αξιολόγηση κινδύνων, για εξυπηρέτηση της διενέργειας εθνικών αξιολογήσεων κινδύνων και για σκοπούς αυτοματοποιημένης επεξεργασίας πληροφοριών.

ΠΑΡΑΡΤΗΜΑ ΙΙ: ΣΧΕΔΙΟ ΕΠΙΧΕΙΡΗΣΙΑΚΗΣ ΣΥΝΕΧΕΙΑΣ ΚΑΙ ΣΧΕΔΙΟ ΑΠΟΚΑΤΑΣΤΑΣΗΣ ΑΠΟ ΚΑΤΑΣΤΡΟΦΕΣ

Το σχέδιο επιχειρησιακής συνέχειας και το σχέδιο αποκατάστασης από καταστροφές κάθε φορέα θα πρέπει να περιλαμβάνει τα ακόλουθα (σύμφωνα με όλα τα μέτρα ασφάλειας της κατηγορίας «Επιχειρησιακή συνέχεια και ανθεκτικότητα» που αναφέρονται στο Παράρτημα ΙΙΙ):

(1) Προσδιορισμό του προσωπικού που εμπλέκεται στην περίπτωση όπου απειλείται η επιχειρησιακή συνέχεια των δικτύων, συστημάτων πληροφοριών και ουσιωδών υπηρεσιών, του ρόλου του και των αρμοδιοτήτων του.

(2) Προσδιορισμό των περιστατικών/συνθηκών κατά τις οποίες ενεργοποιείται το σχέδιο επιχειρησιακής συνέχειας ή/και το σχέδιο αποκατάστασης από καταστροφές.

(3) Διαδικασίες διάχυσης πληροφορίας στο αρμόδιο προσωπικό σχετικά με το εκάστοτε πρόβλημα.

(4) Λειτουργικές διαδικασίες για την ανάλυση αναφορών περιστατικών, την εκτίμηση του προβλήματος και την αποκατάσταση των δικτύων, συστημάτων πληροφοριών και ουσιωδών υπηρεσιών.

(5) Χρόνους αποκατάστασης σε διαφορετικές συνθήκες βλάβης.

(6) Στοιχεία επικοινωνίας του προσωπικού του φορέα με τεχνικούς, προμηθευτές, εργολάβους του φορέα, με άλλους φορείς κατά περίπτωση, καθώς και διαδικασίες συνεργασίας μεταξύ τους, που αφορούν στην υλοποίηση διαδικασιών, οι οποίες ορίζονται στο σχέδιο επιχειρησιακής συνέχειας.

(7) Πληροφορίες σχετικά με τη διαθεσιμότητα εξοπλισμού αντικατάστασης.

(8) Αξιολόγηση των μέτρων που λήφθηκαν για την επίλυση συγκεκριμένου προβλήματος και διαδικασίες αναθεώρησης του σχεδίου επιχειρησιακής συνέχειας και του σχεδίου αποκατάστασης από καταστροφές.

ΠΑΡΑΡΤΗΜΑ III: ΠΛΑΙΣΙΟ ΜΕΤΡΩΝ ΑΣΦΑΛΕΙΑΣ

1.ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ

Τα μέτρα ασφάλειας σχετικά με την ασφάλεια δικτύων και πληροφοριών περιγράφονται λεπτομερώς πιο κάτω, ανά κατηγορία, συμπεριλαμβανομένου του στόχου και της περιγραφής των μέτρων.

1.1 ΠΡΟΕΤΟΙΜΑΣΙΑ (PREPARE)

Στόχος του πυλώνα ΠΡΟΕΤΟΙΜΑΣΙΑ (PREPARE) είναι να διασφαλίζει ότι οι φορείς λαμβάνουν υπόψη τον κίνδυνο για την ασφάλεια πληροφοριών στην καθημερινή τους λειτουργία και ότι εξασφαλίζουν δέσμευση της διοίκησης στο ανώτατο επίπεδο για την αντιμετώπιση απειλών, ευπαθειών και κινδύνων ασφάλειας.

Κατηγορία	#	Μέτρο	Στόχος Μέτρου	Περιγραφή Μέτρου
Στρατηγική	STR1	Στρατηγική για την ασφάλεια πληροφοριών	Να θεσπιστεί στρατηγική ασφάλειας πληροφοριών στην οποία να αναλύονται οι στόχοι και η προσέγγιση υψηλού επιπέδου με σκοπό τον μετριασμό των κινδύνων για την ασφάλεια πληροφοριών.	Καθορισμός του οράματος και της δέσμευσης για την ασφάλεια πληροφοριών σε μια στρατηγική που θα περιγράφει λεπτομερώς συγκεκριμένους στόχους αναφορικά με την ασφάλεια, καθώς και την προσέγγιση για την ασφάλεια και τη διαχείριση του κινδύνου, και τα μέσα για την επικύρωση της αποτελεσματικότητας της στρατηγικής με την υποστήριξη από βασικούς δείκτες επιδόσεων. Η στρατηγική ασφάλειας πληροφοριών αντικατοπτρίζεται στην πολιτική ασφάλειας πληροφοριών, όπως περιγράφεται στο μέτρο [GOV3]. Τα στελέχη γνωρίζουν τη στρατηγική και την πολιτική ασφάλειας πληροφοριών, όπως περιγράφεται στο μέτρο [TA1].
Διακυβέρνηση	GOV1	Ρόλοι και αρμοδιότητες σχετικά με την ασφάλεια πληροφοριών	Να καθοριστούν οι ρόλοι και οι αρμοδιότητες σχετικά με την ασφάλεια πληροφοριών εντός του οργανισμού.	Καθορισμός των ρόλων και των αρμοδιοτήτων όσον αφορά την ασφάλεια δικτύων και πληροφοριών για όλα τα στελέχη που ασχολούνται με την επεξεργασία πληροφοριών ή έχουν πρόσβαση σε συστήματα επεξεργασίας πληροφοριών. Οι καθορισμένοι ρόλοι και αρμοδιότητες αντικατοπτρίζονται στην πολιτική ασφάλειας των πληροφοριών [GOV3]. Τα στελέχη πρέπει να είναι επαρκώς ενημερωμένα και να έχουν επίγνωση των ρόλων και των ευθυνών τους όσον αφορά την ασφάλεια δικτύων και πληροφοριών, όπως ορίζεται στα μέτρα [TA1, TA2]. Οι ρόλοι και οι αρμοδιότητες που σχετίζονται με την ασφάλεια των πληροφοριών θα πρέπει να καθορίζονται από τη διοίκηση, ώστε να εξασφαλίζεται η υπευθυνότητα για τις αποφάσεις της διοίκησης που σχετίζονται με την ασφάλεια δικτύων και συστημάτων πληροφοριών.
Διακυβέρνηση	GOV2	Συμμόρφωση με νομικές και κανονιστικές υποχρεώσεις	Να εξασφαλιστεί η συμμόρφωση με όλες τις εφαρμοστέες νομικές και κανονιστικές υποχρεώσεις όσον αφορά την ασφάλεια δικτύων και πληροφοριών.	Δημιουργία και διατήρηση κεντρικού αποθετηρίου, και συμμόρφωση με όλες τις σχετικές νομοθετικές, κανονιστικές και ρυθμιστικές απαιτήσεις, και συμβατικές απαιτήσεις όσον αφορά την ασφάλεια δικτύων και πληροφοριών.
Διακυβέρνηση	GOV3	Πολιτικές, πρότυπα, κατευθυντήριες γραμμές και διαδικασίες ασφάλειας πληροφοριών.	Να θεσπιστούν πολιτικές, πρότυπα, κατευθυντήριες γραμμές και διαδικασίες για την ασφάλεια πληροφοριών που να αντικατοπτρίζουν	Καθορισμός των μέτρων ασφάλειας πληροφοριών και λεπτομερής περιγραφή της εφαρμογής τους στα πλαίσια μιας πολιτικής ασφάλειας πληροφοριών που θα αντικατοπτρίζει τους στόχους που περιγράφονται στη στρατηγική ασφάλειας πληροφοριών [STR1]. Η πολιτική ασφάλειας των πληροφοριών θα πρέπει να περιλαμβάνει τους ρόλους και τις αρμοδιότητες σε επίπεδο οργάνωσης, όπως ορίζεται στο [GOV1]. Εφαρμογή

Κατηγορία	#	Μέτρο	Στόχος Μέτρου	Περιγραφή Μέτρου
			τη στρατηγική ασφάλειας πληροφοριών.	συγκεκριμένων πολιτικών και διαδικασιών για την ασφάλεια πληροφοριών σε σχέση με συγκεκριμένες επεξεργασίες, συστήματα ή δραστηριότητες, ανάλογα με τις ανάγκες. Καθορισμός επιχειρησιακών κατευθυντήριων γραμμών για την ασφάλεια πληροφοριών και τυποποιημένες διαδικασίες λειτουργίας για συγκεκριμένες δραστηριότητες που σχετίζονται με πληροφορίες ή συστήματα επεξεργασίας πληροφοριών σε επιχειρησιακό επίπεδο.
Διαχείριση κινδύνων	RM1	Μεθοδολογία	Να θεσπιστεί μεθοδολογία διαχείρισης κινδύνων, η οποία αντικατοπτρίζει τη διαδικασία εκτίμησης κινδύνου του οργανισμού, τα κριτήρια ανάλυσης κινδύνου, τα κριτήρια αποδοχής κινδύνων και την πολιτική ανάληψης κινδύνων.	Θέσπιση μεθοδολογίας για τη διαχείριση κινδύνων μέσω του καθορισμού της διαδικασίας εκτίμησης κινδύνων, των κριτηρίων ανάλυσης κινδύνου (δηλαδή των κριτηρίων επιπτώσεων, των κριτηρίων πιθανότητας, της βαθμολογίας κινδύνου), των κριτηρίων αποδοχής κινδύνων και της πολιτικής ανάληψης κινδύνων από τον οργανισμό. Η μεθοδολογία διαχείρισης κινδύνου θα επιτρέψει στον οργανισμό να αξιολογήσει τους κινδύνους για την ασφάλεια πληροφοριών που αντιμετωπίζει, και να εφαρμόσει τα κατάλληλα μέτρα για την αντιμετώπιση ή τον μετριασμό τους. Ο οργανισμός θα πρέπει να θέσει σε εφαρμογή διαδικασίες και εργαλεία, ανάλογα με την περίπτωση, προκειμένου να στηρίξει τις διαδικασίες διαχείρισης κινδύνων, έχοντας κατ' ελάχιστον ένα μητρώο κινδύνων, ένα σχέδιο αντιμετώπισης κινδύνων και μια δομή διακυβέρνησης της ασφάλειας πληροφοριών στην οποία θα περιγράφονται λεπτομερώς οι ρόλοι και οι αρμοδιότητες. Η οριζόμενη μεθοδολογία διαχείρισης κινδύνων θα πρέπει να επικυρώνεται, να συμφωνείται και να υποστηρίζεται από τη διοίκηση ανώτατου επιπέδου και άλλους σχετικούς φορείς εντός του οργανισμού.
Διαχείριση κινδύνων	RM2	Πλαίσιο	Να καταρτιστεί κατάλογος στοιχείων ενεργητικού, συστημάτων και διαδικασιών εντός του οργανισμού.	Κατάρτιση καταλόγου στοιχείων ενεργητικού, συστημάτων και διαδικασιών εντός του οργανισμού και καταγραφή των εξαρτήσεων και αλληλεξαρτήσεων μεταξύ αυτών των στοιχείων ενεργητικού, των συστημάτων και των διαδικασιών με σκοπό τη σαφή αποτύπωση του πλαισίου / περιβάλλοντος στο οποίο θα πραγματοποιηθεί η εκτίμηση κινδύνου. Μια σαφής εικόνα του πλαισίου του οργανισμού θα επιτρέψει τον εντοπισμό των κινδύνων εντός του οργανισμού.
Διαχείριση κινδύνων	RM3	Εντοπισμός κινδύνων	Να εντοπιστούν οι απειλές, ευπάθειες και κίνδυνοι στους οποίους εκτίθενται τα στοιχεία ενεργητικού, τα συστήματα και οι διαδικασίες του οργανισμού.	Προσδιορισμός και κατάρτιση καταλόγου απειλών, ευπαθειών και κινδύνων στους οποίους είναι εκτεθειμένος ο οργανισμός όσον αφορά τα στοιχεία ενεργητικού, τα συστήματα και τις διαδικασίες που προσδιορίζονται στο μέτρο [RM2]. Οι κίνδυνοι που θα εντοπιστούν στα πλαίσια αυτής της διαδικασίας πρέπει να αποτυπώνονται σε μητρώο κινδύνων ώστε να μπορεί ο οργανισμός να παρακολουθεί τις απειλές, τις ευπάθειες και τους κινδύνους στους οποίους είναι εκτεθειμένος.

Κατηγορία	#	Μέτρο	Στόχος Μέτρου	Περιγραφή Μέτρου
Διαχείριση κινδύνων	RM4	Ανάλυση κινδύνου	Να αναλυθούν οι κίνδυνοι για την ασφάλεια πληροφοριών στο πλαίσιο των στοιχείων ενεργητικού ανάλογα με τις διάφορες πιθανότητες και επιπτώσεις.	Ανάλυση των κινδύνων για την ασφάλεια πληροφοριών όσον αφορά τα στοιχεία ενεργητικού, όπως προσδιορίζονται στο [RM2], λαμβάνοντας υπόψη τις διαφορετικές πιθανότητες και τις βαθμολογίες των επιπτώσεων, όπως ορίζονται στο [RM1]. Ο οργανισμός προσδιορίζει τη βαθμολογία κινδύνου προκειμένου να αξιολογήσει την κατάλληλη στρατηγική μετριασμού της [RM5]. Κατά την αξιολόγηση του κατάλληλου επιπέδου ασφάλειας, λαμβάνονται ιδίως υπόψη οι κίνδυνοι που προκύπτουν από τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, άνευ αδείας κοινοποίηση ή πρόσβαση σε πληροφορίες που διαβιβάζονται, αποθηκεύονται ή υποβάλλονται κατ' άλλο τρόπο σε επεξεργασία. Επίσης, λαμβάνονται υπόψη οι κίνδυνοι που παρουσιάζονται οι οποίοι θα μπορούσαν να έχουν επιδράσουν δυνητικά σε ουσιώδεις οικονομικές και κοινωνικές λειτουργίες και υπηρεσίες που παρέχονται από τον ΦΕΒΥ ή ΦΚΥΠ. Τα αποτελέσματα της ανάλυσης κινδύνου θα πρέπει να καταγράφονται στο μητρώο κινδύνων του οργανισμού.
Διαχείριση κινδύνων	RM5	Αξιολόγηση κινδύνων	Να αξιολογηθούν οι κίνδυνοι για την ασφάλεια πληροφοριών με βάση την πολιτική ανάληψης κινδύνων του οργανισμού και να καθοριστούν οι κατάλληλες στρατηγικές αντιμετώπισης.	Καθορισμός κατάλληλων και επαρκών στρατηγικών για την αντιμετώπιση των κινδύνων που αναλύονται σύμφωνα με το [RM4]. Ο οργανισμός λαμβάνει υπόψη τη μείωση του κινδύνου, τη μεταφορά κινδύνου, την αποφυγή του κινδύνου και την αποδοχή (ή τη διατήρηση) κινδύνου ως κατάλληλες στρατηγικές αντιμετώπισης κινδύνων. Κατά την αξιολόγηση των στρατηγικών αντιμετώπισης κινδύνων, ο οργανισμός λαμβάνει υπόψη την πολιτική ανάληψης κινδύνων όπως ορίζεται στο [RM1]. Το αποτέλεσμα της αξιολόγησης κινδύνων θα πρέπει να καταγράφεται στο μητρώο κινδύνων του οργανισμού.
Διαχείριση κινδύνων	RM6	Αντιμετώπιση κινδύνων	Να καθοριστούν οι δράσεις για την αντιμετώπιση των κινδύνων για την ασφάλεια πληροφοριών.	Καθορισμός κατάλληλων και επαρκών μέτρων αντιμετώπισης του κινδύνου στα πλαίσια της εφαρμογής της στρατηγικής αντιμετώπισης κινδύνων που καθορίζεται στη διαδικασία αξιολόγησης των κινδύνων, όπως αυτή περιγράφεται στην [RM5]. Κατά τον καθορισμό των μέτρων, ο οργανισμός λαμβάνει υπόψη προληπτικά μέτρα, μέτρα εντοπισμού και μέτρα αντίδρασης από διοικητική, τεχνολογική και φυσική άποψη, προκειμένου να διασφαλίσει, κατά περίπτωση, μια πολυεπίπεδη άμυνα. Κατά τον καθορισμό των δράσεων αντιμετώπισης κινδύνων, ο φορέας εξετάζει τα μέτρα ασφάλειας που περιγράφονται στο Πλαίσιο μέτρων ασφάλειας (το παρόν έγγραφο). Το αποτέλεσμα της αντιμετώπισης κινδύνων θα πρέπει να καταγράφεται στο σχέδιο αντιμετώπισης κινδύνων του οργανισμού.
Ευαισθητοποίηση και εκπαίδευση	TA1	Ευαισθητοποίηση σχετικά με την ασφάλεια πληροφοριών	Να θεσπιστεί πρόγραμμα ενημέρωσης σχετικά με την ασφάλεια πληροφοριών για όλα τα στελέχη εντός	Καθορισμός προγράμματος ευαισθητοποίησης όσον αφορά την ασφάλεια των πληροφοριών, ώστε να υπάρχει επαρκής ευαισθητοποίηση των στελεχών σχετικά με τους ρόλους και τις ευθύνες όσον αφορά την ασφάλεια δικτύων και πληροφοριών, όπως ορίζεται στο [GOV1].

Κατηγορία	#	Μέτρο	Στόχος Μέτρου	Περιγραφή Μέτρου
			του οργανισμού, λαμβάνοντας υπόψη τα στοιχεία που περιγράφονται στις πολιτικές, τα πρότυπα, τις κατευθυντήριες γραμμές και τις διαδικασίες ασφάλειας πληροφοριών.	
Ευαισθητοποίηση και εκπαίδευση	TA2	Ευαισθητοποίηση και εκπαίδευση σε θέματα ασφάλειας πληροφοριών	Να παρέχει εκπαίδευση προς όλα τα στελέχη του οργανισμού, όπως ορίζεται στο πρόγραμμα ασφάλειας πληροφοριών.	Επαρκής ενημέρωση των στελεχών σχετικά με τους ρόλους και τις αρμοδιότητες τους όσον αφορά την ασφάλεια δικτύων και πληροφοριών, όπως ορίζεται στο [GOV1] μέσω κατάλληλης εκπαίδευσης και κατάρτισης που προσφέρεται με την υποστήριξη της διοίκησης ανώτατου επιπέδου. Οι εκπαιδεύσεις σχετικά με την ασφάλεια πληροφοριών περιλαμβάνουν συγκεκριμένες πληροφορίες σχετικά με τις επιχειρησιακές δραστηριότητες των στελεχών για λογαριασμό του οργανισμού στο πλαίσιο της επεξεργασίας πληροφοριών ή της πρόσβασης σε συστήματα επεξεργασίας πληροφοριών.
Διαχείριση τρίτων μερών και προμηθευτών	TPS1	Δέουσα επιμέλεια για τρίτα μέρη και προμηθευτές	Να επιδεικνύει τη δέουσα επιμέλεια σχετικά με τρίτα μέρη και προμηθευτές	Επίδειξη δέουσας επιμέλειας κατά τον εντοπισμό και τη σύναψη συμβατικών σχέσεων με τρίτα μέρη και προμηθευτές, λαμβανομένων υπόψη των κινδύνων τρίτων μερών, μεταξύ άλλων, της εξάρτησης από τον εκάστοτε προμηθευτή, της διαχείρισης περιστατικών και της ευθύνης σε σχέση με την ασφάλεια δικτύων και πληροφοριών. Ο οργανισμός επιδεικνύει τη δέουσα επιμέλεια ως προς την ασφάλεια πληροφοριών όταν αναλαμβάνει τη συνεργασία με τρίτα μέρη ιδίως στο πλαίσιο της απόκτησης ή της παράδοσης λογισμικού.
Διαχείριση τρίτων μερών και προμηθευτών	TPS2	Σχέσεις με τρίτα μέρη και προμηθευτές	Να διασφαλιστεί η ενσωμάτωση συμβατικών ρητρών ασφάλειας πληροφοριών στις σχέσεις με τρίτα μέρη και προμηθευτές.	Διατήρηση κεντρικού αποθετηρίου προμηθευτών, πωλητών και άλλων τρίτων μερών. Ο οργανισμός θα πρέπει να διασφαλίζει ότι όλες οι σχέσεις με τρίτα μέρη υποστηρίζονται από κατάλληλες συμβατικές ρήτρες, προκειμένου να διασφαλίζεται ότι, μεταξύ άλλων, οι ρόλοι, οι αρμοδιότητες και η ευθύνη σε περίπτωση συμβάντων όσον αφορά την ασφάλεια δικτύων και πληροφοριών είναι δεόντως καταγραμμένα.

1.2 ΠΡΟΣΤΑΣΙΑ ΚΑΙ ΕΝΤΟΠΙΣΜΟΣ (PROTECT AND DETECT)

Στόχος του πυλώνα ΠΡΟΣΤΑΣΙΑ ΚΑΙ ΕΝΤΟΠΙΣΜΟΣ (PROTECT AND DETECT) είναι να διασφαλίζει ότι οι φορείς θεσπίζουν, εφαρμόζουν και διατηρούν επαρκή μέτρα ασφάλειας πληροφοριών κατάλληλα για την έκθεση τους σε κίνδυνο. Ο εν λόγω πυλώνας συνεπάγεται τη λήψη μέτρων πρόληψης, εντοπισμού και αντίδρασης από τεχνολογική, διοικητική και φυσική άποψη.

Κατηγορία	#	Μέτρο	Στόχος Μέτρου	Περιγραφή Μέτρου
Ασφάλεια δεδομένων	DS1	Διαχείριση του κύκλου ζωής των πληροφοριών	Να εξασφαλιστεί η προστασία δεδομένων καθ' όλο τον κύκλο ζωής των πληροφοριών, συμπεριλαμβανομένης της συλλογής, καταχώρησης, οργάνωσης, δομής, αποθήκευσης, προσαρμογής ή μεταβολής, ανάκτησης, αναζήτησης, χρήσης, κοινοποίησης με διαβίβαση, διάδοσης ή κάθε άλλη μορφή διάθεσης, συσχέτισης ή συνδυασμού, περιορισμού, διαγραφής ή καταστροφής.	Θέσπιση, εφαρμογή και διατήρηση μέτρων ασφάλειας πληροφοριών για την προστασία πληροφοριών καθ' όλη τη διάρκεια του κύκλου ζωής των πληροφοριών. Κύκλος ζωής των πληροφοριών θεωρούνται ως όλα τα στάδια που σχετίζονται με την επεξεργασία των πληροφοριών, ενώ η επεξεργασία αφορά κάθε πράξη, ή σειρά πράξεων, που πραγματοποιείται σε δεδομένα προσωπικού χαρακτήρα, ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, είτε με αυτοματοποιημένα μέσα είτε όχι, όπως η συλλογή, καταχώριση, οργάνωση, δομή, αποθήκευση, προσαρμογή ή μεταβολή, ανάκτηση, αναζήτηση, χρήση, κοινοποίηση με διαβίβαση, διάδοση ή κάθε άλλη μορφή διάθεσης, συσχέτιση ή συνδυασμός, περιορισμός, διαγραφή ή καταστροφή.
Ασφάλεια δεδομένων	DS2	Ταξινόμηση και επισήμανση πληροφοριών	Να εξασφαλιστεί ότι τα δεδομένα ταξινομούνται και επισημαίνονται κατά τρόπο ώστε να αντικατοπτρίζεται η ευαισθησία τους ώστε να εξασφαλίζεται η κατάλληλη επεξεργασία τους.	Θέσπιση, εφαρμογή και διατήρηση μιας πολιτικής ταξινόμησης και επισήμανσης που διασφαλίζει την ταξινόμηση και επισήμανση των πληροφοριών, σύμφωνα με την εμπιστευτικότητα και την ευαισθησία τους. Εξέταση ενδεχομένου εφαρμογής συστημάτων ταξινόμησης και επισήμανσης με βάση τις διεθνείς και βιομηχανικές βέλτιστες πρακτικές, όπως το πρωτόκολλο «Traffic Light Protocol». Τουλάχιστον, ο οργανισμός θα πρέπει να γίνεται διάκριση μεταξύ των δημόσιων, ιδιωτικών και διαβαθμισμένων πληροφοριών.
Ασφάλεια δεδομένων	DS3	Εφεδρικά αντίγραφα και ανάκτηση δεδομένων	Να καταστεί δυνατή η αποκατάσταση των πληροφοριών στο πλαίσιο συμβάντων και περιστατικών ασφάλειας.	Θέσπιση, εφαρμογή και διατήρηση διαδικασίας εφεδρικών αντιγράφων και ανάκτησης δεδομένων, προκειμένου να διασφαλίζεται η έγκαιρη και αποτελεσματική αποκατάσταση δεδομένων μετά την ύπαρξη ενός συμβάντος ή περιστατικού, ή κατόπιν αιτήματος. Οι διαδικασίες εφεδρικών αντιγράφων και ανάκτησης δεδομένων θα πρέπει να δοκιμάζονται επαρκώς και συχνά, προκειμένου να διασφαλίζεται η ορθή και αξιόπιστη λειτουργία όλων των υποστηρικτικών διαδικασιών και συστημάτων. Τα συστήματα και οι υποδομές υποστήριξης, που επιτρέπουν την εφεδρεία και την αποκατάσταση δεδομένων, θα πρέπει να είναι γεωγραφικά διεσπαρμένες (αποθήκευση σε άλλη τοποθεσία) προκειμένου να προστατεύονται από φυσικούς κινδύνους ασφάλειας.

Κατηγορία	#	Μέτρο	Στόχος Μέτρου	Περιγραφή Μέτρου
Ασφάλεια δεδομένων	DS4	Μεταφορές και ανταλλαγή πληροφοριών	Να εφαρμοστούν επαρκή μέτρα στο πλαίσιο της διαβίβασης και ανταλλαγής πληροφοριών εσωτερικά ή με τρίτα μέρη, προκειμένου να διασφαλιστεί η ασφαλής μεταφορά δεδομένων.	Θέσπιση, εφαρμογή και διατήρηση διαδικασιών μεταφοράς και ανταλλαγής πληροφοριών προκειμένου να διασφαλίζεται η προστασία των πληροφοριών κατά τη μεταφορά ή την ανταλλαγή τους εσωτερικά ή με τρίτα μέρη. Η μεταφορά και ανταλλαγή πληροφοριών θα πρέπει να λαμβάνει υπόψη τις κανονιστικές και νομοθετικές απαιτήσεις, όπως ορίζονται στο [GOV2], για παράδειγμα κατά την επεξεργασία πληροφοριών στο πλαίσιο διεθνών διαβιβάσεων δεδομένων.
Ασφάλεια δεδομένων	DS5	Πρόληψη απώλειας δεδομένων και διαρροής δεδομένων	Να εξασφαλιστεί η προστασία των δεδομένων από εκούσια ή ακούσια απώλεια και διαρροή δεδομένων.	Θέσπιση, εφαρμογή και διατήρηση εύλογων μέτρων για τη μείωση του κινδύνου απώλειας δεδομένων και διαρροής δεδομένων, λαμβάνοντας τα κατάλληλα τεχνικά και οργανωτικά μέτρα για πρόληψη. Τα μέτρα πρόληψης, απώλειας ή διαρροής δεδομένων θα πρέπει να λαμβάνουν υπόψη εξωτερικούς και εσωτερικούς φορείς απειλής που θα μπορούσαν δυνητικά να αποκαλύψουν διαβαθμισμένες ή ευαίσθητες πληροφορίες. Θα πρέπει να εφαρμόζονται επαρκή μέτρα ελέγχου πρόσβασης για διεπαφή με τα μέτρα πρόληψης για την απώλεια δεδομένων και διαρροή δεδομένων. Οι πολιτικές για την ανταλλαγή και κοινοποίηση δεδομένων θα πρέπει να είναι βάσει του ρόλου του χρήστη, όπως ορίζεται στο [IAM1]. Κατά τον καθορισμό των μέτρων πρόληψης για την απώλεια και τη διαρροή δεδομένων, ο οργανισμός θα πρέπει να εξετάζει την ταξινόμηση, την προστασία και την παρακολούθηση των πληροφοριών.
Διαχείριση αλλαγών	CM1	Διαχείριση αλλαγών	Να διασφαλιστεί ότι οι αλλαγές στις διαδικασίες και τα συστήματα πληροφοριών εφαρμόζονται με ασφάλεια, χωρίς να θίγεται το απόρρητο, η ακεραιότητα, η διαθεσιμότητα ή η αυθεντικότητα των πληροφοριών.	Θέσπιση, εφαρμογή και διατήρηση διαδικασιών διαχείρισης αλλαγών για τον έλεγχο και τη διαχείριση αλλαγών σε συστήματα, εφαρμογές και άλλα υποστηρικτικά στοιχεία ενεργητικού στο πλαίσιο της επεξεργασίας πληροφοριών. Κατά τον καθορισμό της διαδικασίας διαχείρισης αλλαγών, ο οργανισμός πρέπει να προνοεί αιτήσεις αλλαγής, προκειμένου να λαμβάνονται υπόψη οι αλλαγές που ζητούνται από τους συμμετέχοντες. Η διαδικασία διαχείρισης αλλαγών θα πρέπει να επιτρέπει στον οργανισμό να αξιολογεί τους κινδύνους στο πλαίσιο αιτημάτων αλλαγών και να σχεδιάζει αλλαγές λαμβάνοντας υπόψη κατάλληλα μέτρα ασφάλειας. Η διαδικασία διαχείρισης αλλαγών θα πρέπει να περιλαμβάνει την προετοιμασία και την επαλήθευση των αλλαγών.

Κατηγορία	#	Μέτρο	Στόχος Μέτρου	Περιγραφή Μέτρου
Διαχείριση αλλαγών	CM2	Διαχείριση διαμόρφωσης (configuration)	Να εντοπίζονται, να διατηρούνται και να επαληθεύονται οι πληροφορίες για τα στοιχεία ενεργητικού και τις διαμορφώσεις του οργανισμού.	Θέσπιση, εφαρμογή και διατήρηση διαδικασιών διαχείρισης διαμόρφωσης για τον έλεγχο και τη διαχείριση των διαμορφώσεων των στοιχείων ενεργητικού που υποστηρίζουν δίκτυα και συστήματα πληροφοριών. Ο οργανισμός τηρεί μητρώο των διαμορφώσεων που ισχύουν για τα εν λόγω στοιχεία ενεργητικού. Οι οργανισμοί καθορίζουν και καταγράφουν τις σχέσεις ανάμεσα στις διαμορφώσεις των στοιχείων ενεργητικού με σκοπό τον προσδιορισμό των αλληλεξαρτήσεων και τη διασφάλιση της κατάλληλης διαχείρισης της αλλαγής όσον αφορά την τροποποίηση των διαμορφώσεων.
Διαχείριση στοιχείων ενεργητικού	AM1	Διαχείριση του κύκλου ζωής στοιχείων ενεργητικού	Να διασφαλιστεί ότι τα στοιχεία ενεργητικού είναι ασφαλή καθ' όλη τη διάρκεια του κύκλου ζωής τους, συμπεριλαμβανομένης της προμήθειας, της ανάπτυξης, της συντήρησης και της διάθεσης τους.	Θέσπιση, εφαρμογή και διατήρηση μέτρων ασφάλειας πληροφοριών στο πλαίσιο του σχεδίου διαχείρισης του κύκλου ζωής των στοιχείων ενεργητικού, προκειμένου να διασφαλίζεται ότι η ασφάλεια των πληροφοριών είναι αναπόσπαστο κομμάτι αυτού του κύκλου ζωής, δηλαδή την προμήθεια, την εγκατάσταση, τη συντήρηση και τη διάθεση. Η διαχείριση του κύκλου ζωής των πληροφοριών, όπως περιγράφεται στο μέτρο [DS1], θα πρέπει να αποτελεί μέρος του σχεδίου διαχείρισης του κύκλου ζωής των στοιχείων ενεργητικού. Το σχέδιο διαχείρισης του κύκλου ζωής των στοιχείων ενεργητικού πρέπει να περιγράφει όλες τις διαδικασίες για τον χειρισμό των πληροφοριών σύμφωνα με την πολιτική ταξινόμησης και επισήμανσης των δεδομένων, όπως περιγράφεται στο μέτρο [DS2].
Διαχείριση στοιχείων ενεργητικού	AM2	Καταγραφή των στοιχείων ενεργειακού και ιδιοκτησία	Να διασφαλιστεί ότι τα στοιχεία ενεργητικού καταγράφονται σε κατάλογο και ότι η ιδιοκτησία καθορίζεται με σκοπό την επίτευξη της ιχνηλασιμότητας και της ευθύνης για τα στοιχεία.	Θέσπιση, εφαρμογή και διατήρηση καταλόγου καταγραφής των στοιχείων ενεργητικού, προκειμένου να διασφαλίσει ότι ο οργανισμός έχει σαφή, ακριβή και ενημερωμένη κατάσταση των στοιχείων (π.χ. υλισμικό, λογισμικό, πληροφορίες) που διατηρεί. Ο κατάλογος θα πρέπει να προσδιορίζει τον ιδιοκτήτη των στοιχείων αυτών. Ο κατάλογος θα πρέπει επίσης να επιτρέπει στον οργανισμό να παρακολουθεί όλα τα στοιχεία ενεργητικού για τα οποία θα πρέπει να εφαρμόζει και να διατηρεί μέτρα ασφάλειας πληροφοριών.
Διαχείριση στοιχείων ενεργητικού	AM3	Παρακολούθηση στοιχείων ενεργητικού	Να διασφαλιστεί ότι τα στοιχεία ενεργητικού είναι υπό παρακολούθηση για επιθέσεις, ανωμαλίες και απειλές κατά της ασφάλειας, προκειμένου να ενεργοποιηθούν οι διαδικασίες για την αντιμετώπιση συμβάντων και περιστατικών.	Θέσπιση, εφαρμογή και διατήρηση δυνατοτήτων παρακολούθησης των στοιχείων ενεργητικού, ώστε ο οργανισμός να είναι σε θέση να εντοπίζει ανωμαλίες σε σχέση με κανονικές συνθήκες (π.χ. τοποθεσία, χρήση) και/ή τη λειτουργία των στοιχείων αυτών. Ο οργανισμός θα πρέπει να αναφέρει στην πολιτική αποδεκτής χρήσης, όπως περιγράφεται στο [HRS6], τι συνιστά αποδεκτή χρήση και/ή λειτουργία των στοιχείων ενεργητικού. Ο οργανισμός θα μπορούσε επίσης να εξετάσει την συμπερίληψη της περιγραφής της αποδεκτής χρήσης, της λειτουργίας και της τοποθεσίας των στοιχείων στον κατάλογο των στοιχείων ενεργητικού, όπως περιγράφεται στο [AM2], προκειμένου να υπάρχει πλήρης απογραφή των στοιχείων αυτών. Όταν εντοπίζονται ανωμαλίες, θα

Κατηγορία	#	Μέτρο	Στόχος Μέτρου	Περιγραφή Μέτρου
				πρέπει να ενεργοποιούνται διαδικασίες διαχείρισης συμβάντων και περιστατικών προκειμένου ο οργανισμός να είναι ανθεκτικός στην παρουσία ανωμαλιών.
Διαχείριση στοιχείων ενεργητικού	AM4	Διαχείριση διαθεσιμότητας	Να διασφαλιστεί η διαθεσιμότητα δικτύων και συστημάτων πληροφοριών με την επίτευξη επαρκούς διαθεσιμότητας πόρων, εφεδρείας και συστημάτων / διαδικασιών υψηλής διαθεσιμότητας.	Θέσπιση, εφαρμογή και διατήρηση διαδικασιών διαχείρισης της διαθεσιμότητας προκειμένου να διασφαλίζεται ότι παρέχεται το επιθυμητό επίπεδο των επιχειρησιακών υπηρεσιών από τον οργανισμό. Ο οργανισμός θα πρέπει να διασφαλίζει ανά πάσα στιγμή τη διαθεσιμότητα των πόρων (π.χ. χώροι, προσωπικό, συστήματα πληροφορικής, κ.λπ.). Όπως περιγράφεται στο μέτρο [NS6], ο οργανισμός θα πρέπει να εγγυάται την εφεδρεία και την υψηλή διαθεσιμότητα όλων των συστημάτων πληροφορικής, προκειμένου να διασφαλίζεται η έγκαιρη και αποτελεσματική ανάκτηση των δεδομένων μετά την ύπαρξη ενός συμβάντος ή περιστατικού, ή κατόπιν αιτήματος. Ο οργανισμός θα πρέπει να δημιουργήσει εφεδρικά αντίγραφα των πληροφοριών που περιγράφονται στο [DS3].
Διαχείριση στοιχείων ενεργητικού	AM5	Κρυπτογραφία	Να διασφαλιστεί η εμπιστευτικότητα, ακεραιότητα και αυθεντικότητα των πληροφοριών με την υιοθέτηση κατάλληλων κρυπτογραφικών λύσεων.	Θέσπιση, εφαρμογή και διατήρηση πολιτικής σχετικά με τη χρήση κρυπτογραφικών μέτρων, προκειμένου να διασφαλίζονται η εμπιστευτικότητα, η ακεραιότητα και η αυθεντικότητα των δεδομένων κατά την αποθήκευση, τη χρήση και τη μεταφορά. Η πολιτική κρυπτογράφησης θα πρέπει να λαμβάνει υπόψη την εφαρμογή κρυπτογραφικών μέτρων σε όλα τα στάδια του κύκλου ζωής των πληροφοριών και να εξετάζει εφαρμογές, συστήματα, εξοπλισμό δικτύου και διαύλους επικοινωνίας.
Διαχείριση στοιχείων ενεργητικού	AM6	Διαχείριση χωρητικότητας	Να εξασφαλιστεί η κατάλληλη χωρητικότητα και επίδοση των υπηρεσιών των συστημάτων και διαδικασιών πληροφοριών.	Θέσπιση, εφαρμογή και διατήρηση διαδικασίας διαχείρισης της χωρητικότητας προκειμένου να διασφαλιστεί ότι η χωρητικότητα και οι επιδόσεις των συστημάτων πληροφορικής του οργανισμού δεν επηρεάζονται αρνητικά από αυξημένα επίπεδα ζήτησης υπηρεσιών. Η διαδικασία διαχείρισης χωρητικότητας θα πρέπει να περιλαμβάνει τη διαχείριση της επιχειρησιακής ικανότητας, προκειμένου να διασφαλίζεται ότι οι επιχειρησιακές ανάγκες μετατρέπονται σε απαιτήσεις χωρητικότητας, διαχείριση της χωρητικότητας υπηρεσιών ώστε να γίνεται σωστή διαχείριση της χωρητικότητας των υποσυστημάτων πληροφορικής και ένα μηχανισμό υποβολής εκθέσεων διαχείρισης χωρητικότητας.

Κατηγορία	#	Μέτρο	Στόχος Μέτρου	Περιγραφή Μέτρου
Διαχείριση ταυτότητας και πρόσβασης	IAM1	Έλεγχος πρόσβασης βάσει ρόλου	Να επαληθευτεί της η αυθεντικότητα και εξουσιοδότηση χρηστών, με βάση το ελάχιστο προνόμιο και τους οργανωτικούς ρόλους και αρμοδιότητες.	Θέσπιση, εφαρμογή και διατήρηση μέτρων διαχείρισης ταυτότητας και πρόσβασης τα οποία εξετάζουν μέτρα πρόσβασης με βάση το ρόλο, με σκοπό να παρέχουν τεχνικά και οργανωτικά μέσα για την επιβολή της αρχής του ελάχιστου προνομίου και να διαχειρίζονται αντίστοιχα τους προνομιούχους χρήστες. Ο έλεγχος πρόσβασης βάσει ρόλου θα πρέπει να διασφαλίζει ότι χορηγούνται επαρκείς άδειες σε χρήστες με βάση τις αρμοδιότητες τους που συνδέονται με αντίστοιχους ρόλους. Ο έλεγχος πρόσβασης βάσει ρόλου θα πρέπει να γίνεται σύμφωνα με τις διαδικασίες ασφάλειας των ανθρώπινων πόρων, όπως ορίζεται στο [HRS1], προκειμένου να διασφαλιστεί ότι οι ρόλοι πρόσβασης είναι ευθυγραμμισμένοι με τους ρόλους και αρμοδιότητες των στελεχών στο πλαίσιο του οργανισμού.
Διαχείριση ταυτότητας και πρόσβασης	IAM2	Έλεγχος εξωτερικής πρόσβασης	Να εξασφαλιστούν επαρκή μέτρα στο πλαίσιο της εξωτερικής πρόσβασης σε οργανωτικούς πόρους.	Θέσπιση, εφαρμογή και διατήρηση μέτρων ελέγχου πρόσβασης για εξωτερική και εξ αποστάσεως πρόσβαση σε οργανωτικούς πόρους. Ο οργανισμός θα πρέπει να διασφαλίζει τη δυνατότητα απομακρυσμένης πρόσβασης στο δίκτυο με τη χρήση εικονικών ιδιωτικών δικτύων (VPN) και την πρόσβαση σε εξ αποστάσεως εφαρμογές μέσω της χρήσης εξωτερικών εφαρμογών διεπαφών. Ο οργανισμός εφαρμόζει επαρκή μέτρα διαχείρισης ταυτότητας και πρόσβασης, ώστε να αντικατοπτρίζει την πολιτική ασφάλειας πληροφοριών, όπως ορίζεται στο [GOV3], και τον ειδικό έλεγχο πρόσβασης βάσει ρόλου, όπως ορίζεται στο μέτρο [IAM1].
Διαχείριση ταυτότητας και πρόσβασης	IAM3	Διαχείριση προνομιούχων χρηστών	Να εξασφαλιστούν επαρκή μέτρα για τους χρήστες που έχουν προνομιακή πρόσβαση σε οργανωτικούς πόρους, συστήματα και δίκτυα.	Θέσπιση, εφαρμογή και διατήρηση μέτρων για τη διασφάλιση της ορθής διαχείρισης των προνομιούχων χρηστών, και ενεργοποίηση τους μόνο όταν χρειάζεται. Ο οργανισμός διασφαλίζει ότι στους χρήστες δεν χορηγούνται προνομιακά δικαιώματα εξ ορισμού και ότι εφαρμόζονται κατάλληλα τεχνικά και οργανωτικά μέτρα για τη διασφάλιση της προστασίας των προνομιακών δικαιωμάτων των χρηστών από κακόβουλες πράξεις ή από άλλες αρνητικές συμπεριφορές ή προθέσεις. Ο οργανισμός διασφαλίζει ότι τα συστήματα και οι εφαρμογές δεν λειτουργούν εξ ορισμού με προνομιακά δικαιώματα χρήστη, προκειμένου να μετριάζεται ο κίνδυνος της κλιμάκωσης προνομίων.

Κατηγορία	#	Μέτρο	Στόχος Μέτρου	Περιγραφή Μέτρου
Διαχείριση ταυτότητας και πρόσβασης	IAM4	Ισχυρά μέτρα για επαλήθευση ταυτότητας	Να εξασφαλιστεί ότι γίνεται επαλήθευση της ταυτότητας των εξουσιοδοτημένων ατόμων με ασφάλεια και με τη χρήση μέτρων ισχυρής επαλήθευσης ταυτότητας.	Θέσπιση, εφαρμογή και διατήρηση ισχυρών μέτρων ελέγχου πρόσβασης και επαλήθευσης της ταυτότητας, προκειμένου να διασφαλίζεται ότι τα εξουσιοδοτημένα άτομα αναγνωρίζονται δεόντως και γίνεται επαλήθευση της ταυτότητας τους κατά την επεξεργασία οργανωτικών πόρων. Ο οργανισμός πρέπει να εξετάσει την επαλήθευση μέσω πολλών παραγόντων προκειμένου να αποδείξει την ταυτότητά ενός ατόμου. Η διαδικασία αυτή πρέπει να περιλαμβάνει τουλάχιστον δύο από τις ακόλουθες αρχές: παροχή ταυτότητας με την κατοχή συγκεκριμένου στοιχείου (π.χ. κλειδί ή άλλο μέσο εξακρίβωσης της ταυτότητας), με τη γνώση ενός στοιχείου (π.χ. κωδικός ή φράση πρόσβασης, ή άλλο μυστικό), με βιομετρικά ή μορφολογικά χαρακτηριστικά (π.χ. σάρωση ίριδας, αποτύπωμα δακτύλου ή οπτική επαλήθευση ταυτότητας από ένα αξιόπιστο μέρος, όπως έναν φρουρό ασφαλείας).
Διαχείριση ταυτότητας και πρόσβασης	IAM5	Διαχείριση διαπιστευτηρίων	Να διασφαλιστεί ασφαλής διαχείριση διαπιστευτηρίων για πρόσβαση σε εταιρικούς πόρους, και ότι επαληθεύεται η ταυτότητα των χρηστών με ασφάλεια για χρήση υπηρεσιών του οργανισμού.	Θέσπιση, εφαρμογή και διατήρηση διαδικασιών διαχείρισης διαπιστευτηρίων για να εξασφαλίζεται η κατάλληλη διαχείριση των μέσων ταυτοποίησης και επαλήθευσης με τα οποία οι χρήστες μπορούν να έχουν πρόσβαση σε οργανωτικούς πόρους. Ο οργανισμός θα πρέπει να εξετάσει τη χρήση ομαδοποιημένων διαπιστευτηρίων (π.χ. single sign-on) προκειμένου να βελτιώσει την εμπειρία του χρήστη σε θέματα ταυτοποίησης και πρόσβασης. Ο οργανισμός πρέπει να εξετάσει τη διαχείριση διαπιστευτηρίων για τους χρήστες, τα συστήματα και τα δίκτυα προκειμένου να διασφαλίσει τον έλεγχο της πρόσβασης καθ' όλη τη διάρκεια του κύκλου ζωής πληροφοριών, όπως ορίζεται στο μέτρο [DS1].
Διαχείριση ταυτότητας και πρόσβασης	IAM6	Ιχνηλασιμότητα και έλεγχος	Να διασφαλιστεί η μη-άρνηση ανιχνευσιμότητας των ενεργειών των χρηστών που εκτελούνται στο πλαίσιο των οργανωτικών πόρων, ώστε να είναι δυνατή η ανίχνευση και η διερεύνηση εκούσιων ή ακούσιων δραστηριοτήτων που έχουν αρνητικό αντίκτυπο.	Θέσπιση, εφαρμογή και διατήρηση μέτρων διαχείρισης ταυτότητας και πρόσβασης για τη διασφάλιση της χρονολογικής ιχνηλασιμότητας και της ικανότητας ελέγχου, ώστε να ανατίθεται ευθύνη στους χρήστες που εκτελούν εντολές σε συστήματα επεξεργασίας πληροφοριών. Ο φορέας εξετάζει μέτρα που διασφαλίζουν τη μη-άρνηση από χρήστες. Ο οργανισμός πρέπει να εξετάζει τη δυνατότητα ιχνηλασιμότητας και ελέγχου στο πλαίσιο της διαχείρισης ταυτότητας και πρόσβασης που ισχύει για τα συστήματα, τις εφαρμογές και τα δίκτυα.

Κατηγορία	#	Μέτρο	Στόχος Μέτρου	Περιγραφή Μέτρου
Διαχείριση ταυτότητας και πρόσβασης	IAM7	Διαχείριση του κύκλου ζωής της ταυτότητας	Να διασφαλιστεί ότι οι ρόλοι και η έγκριση της ταυτότητας αντικατοπτρίζουν τον κύκλο ζωής της ταυτότητας του χρήστη.	Θέσπιση, εφαρμογή και διατήρηση επαρκών μέτρων διαχείρισης ταυτότητας και πρόσβασης καθ' όλη τη διάρκεια του κύκλου ζωής της ταυτότητας, που περιλαμβάνει μεταξύ άλλων, παροχή, επαλήθευση της ταυτότητας, έγκριση και αφαίρεση ταυτοτήτων. Οι έλεγχοι για τη διαχείριση του κύκλου ζωής της ταυτότητας θα πρέπει να ενσωματωθούν στις διαδικασίες ασφάλειας περί ανθρώπινων πόρων, όπως ορίζεται στο μέτρο [HRS1], προκειμένου να διασφαλιστεί ότι οι ρόλοι πρόσβασης ευθυγραμμίζονται με τον κύκλο ζωής της εργοδότησης των στελεχών μέσα στον οργανισμό.
Διαχείριση ευπαθειών και ενημερώσεων ασφάλειας	VM1	Ανίχνευση και εντοπισμός ευπαθειών	Να διασφαλιστεί ότι οι ευπάθειες συστημάτων είναι γνωστές στον οργανισμό, προκειμένου να τύχουν κατάλληλου χειρισμού.	Κατάρτιση, εφαρμογή και διατήρηση σχεδίου και προσέγγισης βάσει του κινδύνου για τη δοκιμή εφαρμογών, συστημάτων και δικτύων για ευπάθειες και αδυναμίες, οι οποίες θα μπορούσαν να τύχουν εκμετάλλευσης από απειλές. Ο οργανισμός θα πρέπει να εξετάζει την ανίχνευση για τον εντοπισμό ευπαθειών που προκύπτουν από νέες ή τροποποιημένες διαδικασίες ή συστήματα στα πλαίσια επεξεργασίας πληροφοριών. Οι ευπάθειες πρέπει να ανιχνεύονται και να εντοπίζονται στο πλαίσιο των απειλών κατά της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών. Ο οργανισμός θα πρέπει να εξετάζει το ενδεχόμενο διενέργειας δοκιμών διείσδυσης, ως μέσο για την ανίχνευση και τον εντοπισμό ευπαθειών. Τα αποτελέσματα των προσπαθειών ανίχνευσης και εντοπισμού ευπαθειών θα πρέπει να καταγράφονται όπως περιγράφεται στο μέτρο [VM2].
Διαχείριση ευπαθειών και ενημερώσεων ασφάλειας	VM2	Καταγραφή και αναφορά ευπαθειών	Να διασφαλιστεί ότι οι ευπάθειες καταγράφονται και υποβάλλονται σε σχετικές εκθέσεις, ώστε να είναι δυνατή η λήψη τεκμηριωμένων αποφάσεων από τη διοίκηση όσον αφορά τον χειρισμό τους.	Θέσπιση, εφαρμογή και διατήρηση διαδικασιών για την καταγραφή και την αναφορά των ευπαθειών που έχουν εντοπιστεί, ώστε να είναι δυνατή η αποκατάσταση και η ενημέρωση συστημάτων και διαδικασιών για τη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών. Η καταγραφή ευπαθειών και η υποβολή σχετικών εκθέσεων θα πρέπει να είναι το αποτέλεσμα των προσπαθειών ανίχνευσης και εντοπισμού ευπαθειών, όπως περιγράφεται στο μέτρο [VM1]. Ο οργανισμός πρέπει να εξετάζει το ενδεχόμενο συμπερίληψης στοιχείων για ευπάθειες υψηλού κινδύνου σε γενικές εκθέσεις προς τη διοίκηση, ώστε να εξασφαλίζεται η εκ των άνω προς τα κάτω επίγνωση των ευπαθειών με δυνητικές επιπτώσεις και να προσδιορίζονται τα κατάλληλα μέτρα για την αποκατάσταση και την εφαρμογή διορθωτικών συστημάτων και διαδικασιών, όπως περιγράφεται στο μέτρο [VM3].
Διαχείριση ευπαθειών και ενημερώσεων ασφάλειας	VM3	Αποκατάσταση ευπαθειών και ενημερώσεις ασφάλειας	Να εξασφαλιστεί η αποκατάσταση των ευπαθειών συστημάτων και η	Θέσπιση, εφαρμογή και διατήρηση διαδικασιών για την αποκατάσταση ευπαθειών και την εισαγωγή ενημερώσεων ασφάλειας για

Κατηγορία	#	Μέτρο	Στόχος Μέτρου	Περιγραφή Μέτρου
			εφαρμογή ενημερώσεων ασφάλειας, κατόπιν απόφασης της διοίκησης.	ευπάθειες που εντοπίζονται σε συστήματα, εφαρμογές και στοιχεία δικτύου, και τα οποία απαιτούν μετριασμό ως αποτέλεσμα της αξιολόγησης της διοίκησης. Η αποκατάσταση ευπαθειών και οι ενημερώσεις ασφάλειας πρέπει να είναι το αποτέλεσμα απόφασης της διοίκησης με βάση την καταγραφή ευπαθειών και την υποβολή σχετικών εκθέσεων, όπως περιγράφεται στο μέτρο [VM2].
Ασφάλεια δικτύου	NS1	Ασφάλεια περιμέτρου	Να διασφαλιστεί ότι η διεπαφή του τοπικού δικτύου με το εξωτερικό δίκτυο προστατεύεται από επιθέσεις, απειλές και άλλες εκούσιες ή ακούσιες ενέργειες με δυνητικά αρνητικές επιπτώσεις.	Θέσπιση, εφαρμογή και διατήρηση κατάλληλων μέτρων ασφάλειας δικτύου με σκοπό την προστασία της περιμέτρου του δικτύου από εξωτερικές απειλές και τη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών που βρίσκονται στο εσωτερικό δίκτυο. Ο οργανισμός θα πρέπει να λαμβάνει υπόψη ότι η ασφάλεια περιμέτρου αποτελεί ένα μόνο συγκεκριμένο επίπεδο σε μια πολυεπίπεδη αρχιτεκτονική άμυνας. Για την προστασία από επιθέσεις στο δίκτυο, ο οργανισμός λαμβάνει υπόψη τις ειδικές για τον οργανισμό, απειλές και τις ειδικές για τον τομέα, απειλές και κινδύνους για το δίκτυο. Ο οργανισμός λαμβάνει υπόψη τα τείχη προστασίας και τα συστήματα ανίχνευσης και πρόληψης εισβολής, όπως περιγράφονται στο μέτρο [NS7]. Ο οργανισμός λαμβάνει εύλογα μέτρα για να διασφαλίσει ότι η κίνηση δεδομένων φιλτράρεται με βάση τις πολιτικές ασφάλειας του οργανισμού.
Ασφάλεια δικτύου	NS2	Διαχωρισμός και τμηματοποίηση του δικτύου	Να εξασφαλιστεί ο διαχωρισμός του λογικού δικτύου, σύμφωνα με τις επιχειρηματικές λειτουργίες, και να αποφευχθεί η εξάπλωση κακόβουλων στοιχείων.	Θέσπιση, εφαρμογή και διατήρηση κατάλληλου διαχωρισμού και τμηματοποίησης του δικτύου, προκειμένου να διασφαλιστεί - λογικός ή/και φυσικός - διαχωρισμός των δικτύων πληροφοριών. Κατά τον σχεδιασμό, την εφαρμογή και τη διατήρηση των μέτρων διαχωρισμού και τμηματοποίησης του δικτύου, ο οργανισμός λαμβάνει υπόψη τους διάφορους τομείς λειτουργικής δραστηριότητας του οργανισμού. Ο οργανισμός λαμβάνει υπόψη τη φύση και την έκταση των δεδομένων που υποβάλλονται σε επεξεργασία στο πλαίσιο συγκεκριμένων επιχειρηματικών δραστηριοτήτων, προκειμένου να διασφαλίζεται επαρκής διαχωρισμός. Ο οργανισμός θα πρέπει να εξετάσει το ενδεχόμενο να υιοθετήσει εικονική τοπική δικτύωση (VLAN) κατά το σχεδιασμό του διαχωρισμού και της αρχιτεκτονικής του δικτύου σε τμήματα. Ο οργανισμός θα πρέπει να εξετάζει τουλάχιστον τον διαχωρισμό των τομέων έρευνας και ανάπτυξης, της διοίκησης, της κεντρικής υποδομής πληροφοριών και των δημόσια διαθέσιμων (στο διαδίκτυο) εφαρμογών και συστημάτων.

Κατηγορία	#	Μέτρο	Στόχος Μέτρου	Περιγραφή Μέτρου
Ασφάλεια δικτύου	NS3	Προστασία από άρνηση παροχής υπηρεσιών	Να διασφαλιστεί η προστασία των οργανωτικών πόρων από επιθέσεις άρνησης παροχής υπηρεσιών, και ότι δεν επηρεάζονται οι νόμιμες δραστηριότητες παροχής υπηρεσιών.	Θέσπιση, εφαρμογή και διατήρηση επαρκούς προστασίας από άρνηση παροχής υπηρεσιών και διανεμημένη άρνηση παροχής υπηρεσιών, προκειμένου να διασφαλίζεται η έγκαιρη και ποιοτική παροχή της υπηρεσίας σε εξουσιοδοτημένους και επικυρωμένους χρήστες και να διατηρείται σταθερό επίπεδο παραγωγικότητας. Κατά τον σχεδιασμό των σχετικών μέτρων προστασίας, ο οργανισμός θα πρέπει να εξετάσει την ενσωμάτωση ικανοτήτων για τον εντοπισμό νόμιμων χρηστών και εφαρμογών έναντι κακόβουλων προσπαθειών πρόσβασης σε πόρους. Ο οργανισμός θα πρέπει να λαμβάνει υπόψη μέτρα εφεδρείας και υψηλής διαθεσιμότητας, όπως περιγράφονται στο μέτρο [NS6], προκειμένου να εξασφαλίζεται η απρόσκοπτη λειτουργία σε περίπτωση απειλής κατά της διαθεσιμότητας πληροφοριών και υπηρεσιών.
Ασφάλεια δικτύου	NS4	Ασφαλή πρωτόκολλα επικοινωνίας	Να διασφαλιστούν κατάλληλα πρωτοκόλλα επικοινωνίας προκειμένου να επιτευχθεί ασφαλής επικοινωνία μεταξύ των πόρων του δικτύου.	Θέσπιση, εφαρμογή και διατήρηση ασφαλών πρωτοκόλλων για τη διευκόλυνση της διακίνησης πληροφοριών μεταξύ σημείων δικτύου, εφαρμογών και συστημάτων, προκειμένου να διασφαλίζεται η εμπιστευτικότητα και η ακεραιότητα των πληροφοριών κατά τη μεταφορά τους, και να αποτρέπονται επιθέσεις και απειλές στο δίκτυο, όπως για παράδειγμα υποκλοπές επικοινωνιών. Ο οργανισμός εξετάζει τα πλέον σύγχρονα πρωτόκολλα επικοινωνίας κατά τη διασφάλιση της μεταφοράς και ανταλλαγής πληροφοριών μέσω δικτύων επικοινωνίας. Ο οργανισμός πρέπει να λαμβάνει υπόψη μέτρα ασφάλειας που υποστηρίζονται από κρυπτογραφικά μέσα, όπως αυτά ορίζονται στο μέτρο [AM5] για την ασφάλεια των επικοινωνιών, χρησιμοποιώντας τεχνολογίες όπως το Hypertext Transfer Protocol Secure (HTTPS), το Internet Protocol security (IPsec), το Transport Layer Security (TLS) / Secure Sockets Layer (SSL), ανάλογα με το επιδιωκόμενο επίπεδο τεχνολογίας.
Ασφάλεια δικτύου	NS5	Έλεγχος πρόσβασης στο δίκτυο	Να εξασφαλιστεί ότι η πρόσβαση στο λογικό δίκτυο από εξωτερικά και εσωτερικά συστήματα ασφαλίζεται κατάλληλα, ώστε μόνο τα εξουσιοδοτημένα πρόσωπα να μπορούν να έχουν πρόσβαση σε οργανωτικούς πόρους.	Θέσπιση, εφαρμογή και διατήρηση μέτρων ελέγχου πρόσβασης στο δίκτυο, ώστε να διασφαλίζεται η λογική πρόσβαση στο δίκτυο του οργανισμού και στους πόρους πληροφοριών, και να αποτρέπεται η μη εξουσιοδοτημένη πρόσβαση. Ο οργανισμός θα πρέπει να εξετάζει συγκεκριμένα τεχνικά και οργανωτικά μέτρα, όπως τους μηχανισμούς επαλήθευσης ταυτότητας για πρόσβαση στο δίκτυο, προκειμένου να διευκολύνει τη λειτουργία του εν λόγω μέτρου. Ο οργανισμός θα πρέπει να εξετάζει το ενδεχόμενο ελέγχου πρόσβασης στο δίκτυο για ενσύρματη, ασύρματη και άλλου είδους σύνδεση με το δίκτυο. Ο οργανισμός θα πρέπει να εξετάσει το ενδεχόμενο ενσωμάτωσης του ελέγχου της πρόσβασης στο δίκτυο με κεντρικά διαπιστευτήρια και με διαδικασίες διαχείρισης της ταυτότητας και της πρόσβασης, όπως ορίζεται στο μέτρο [IAM5].

Κατηγορία	#	Μέτρο	Στόχος Μέτρου	Περιγραφή Μέτρου
Ασφάλεια δικτύου	NS6	Εφεδρεία και υψηλή διαθεσιμότητα	Να εξασφαλιστεί της η διαθεσιμότητα πληροφοριών και δικτύων πληροφοριών με την επίτευξη επαρκούς διαθεσιμότητας πόρων, εφεδρικού εξοπλισμού, συστημάτων και συνδέσεων υψηλής διαθεσιμότητας.	Θέσπιση, εφαρμογή και διατήρηση επαρκών μέτρων για να διασφαλίζεται ένα εύλογο επίπεδο εφεδρείας και υψηλής διαθεσιμότητας, ιδίως για τα συστήματα, τις υπηρεσίες και τις εφαρμογές ζωτικής σημασίας που επεξεργάζονται διαβαθμισμένες ή/και επιχειρησιακές πληροφορίες. Ο οργανισμός πρέπει να εξετάζει το ενδεχόμενο εφεδρείας και υψηλής διαθεσιμότητας σε όλα τα επίπεδα τεχνολογίας, μεταξύ άλλων, αποθήκευσης, επικοινωνίας και επεξεργασίας. Ο οργανισμός λαμβάνει υπόψη τεχνολογίες εφεδρείας και υψηλής διαθεσιμότητας όπως είναι τα συστήματα εναλλακτικής σύνδεσης ή εφεδρείας, Redundant Arrays of Independent Disks (RAID), και εγκαταστάσεις αποθήκευσης δεδομένων σε cold, warm και hot.
Ασφάλεια δικτύου	NS7	Ανίχνευση και πρόληψη εισβολών	Να διασφαλιστεί η ανίχνευση και η πρόληψη από εξωτερικές απόπειρες εισβολής και επιθέσεις ασφάλειας.	Θέσπιση, εφαρμογή και διατήρηση επαρκών μέτρων για τον εντοπισμό και την πρόληψη εισβολών στο δίκτυο και τους πόρους του οργανισμού. Ο οργανισμός θα πρέπει να λαμβάνει υπόψη τα συστήματα ανίχνευσης εισβολών (IDS) και τα συστήματα πρόληψης εισβολών (IPS) για τον μετριασμό του κινδύνου απόπειρας εξωτερικής εισβολής. Ο οργανισμός εξετάζει το ενδεχόμενο δημιουργίας κονσόλας διαχείρισης για την παρακολούθηση του δικτύου με στόχο την καταχώρηση όλων των αποπειρών εισβολής για περαιτέρω ανάλυση. Στα πλαίσια σχεδιασμού των διαδικασιών ανίχνευσης και πρόληψης εισβολών, ο οργανισμός πρέπει να εξετάσει το ενδεχόμενο αυτόματης ενεργοποίησης μοχλών για την αντιμετώπιση συμβάντων, όπως ορίζεται στο [EIM2],. Ο οργανισμός πρέπει να λαμβάνει υπόψη τις λύσεις για τη διαχείριση συμβάντων και περιστατικών ασφάλειας (SIEM) για την υποστήριξη των διαδικασιών πρόληψης και ανίχνευσης εισβολών.
Ασφάλεια συστημάτων	SS1	Καταπολέμηση κακόβουλου λογισμικού	Να διασφαλιστεί ότι δεν θα επηρεαστούν οργανωτικοί πόροι από κακόβουλο λογισμικό και κώδικα.	Θέσπιση, εφαρμογή και διατήρηση επαρκών μέτρων για την προστασία των συστημάτων από μολύνσεις από κακόβουλο λογισμικό και κώδικα, προκειμένου να διασφαλίζεται η εμπιστευτικότητα, η ακεραιότητα, η διαθεσιμότητα και η αυθεντικότητα των πληροφοριών. Ο οργανισμός εξετάζει σειρά μέτρων για την καταπολέμηση κακόβουλου λογισμικού, μεταξύ άλλων, λειτουργικά συστήματα, συστήματα και υπηρεσίες δικτύου, λειτουργικά συστήματα εξοπλισμού δικτύου, τερματικά σημεία χρηστών και κινητές συσκευές, καθώς και φορητές συσκευές περιεχομένου. Ο οργανισμός πρέπει να διασφαλίζει ότι τα μέτρα καταπολέμησης του κακόβουλου λογισμικού βασίζονται σε ενημερωμένα δεδομένα με σκοπό τον εντοπισμό και την επίλυση απειλών από κακόβουλο λογισμικό.

Κατηγορία	#	Μέτρο	Στόχος Μέτρου	Περιγραφή Μέτρου
Ασφάλεια συστημάτων	SS2	Θωράκιση συστημάτων και συσκευών και βασικές απαιτήσεις ασφάλειας	Να ελαχιστοποιηθεί, στο μέτρο του δυνατού, η επιφάνεια επίθεσης των συστημάτων πληροφοριών, μέσω της μείωσης της λειτουργικότητας και των χαρακτηριστικών τους.	Θέσπιση, εφαρμογή και διατήρηση διαδικασίας για τη θωράκιση συστημάτων και συσκευών με βάση καθορισμένες βασικές απαιτήσεις ασφάλειας, ώστε να αποτρέπεται η μη εξουσιοδοτημένη πρόσβαση και χρήση των πόρων και των υπηρεσιών του συστήματος. Ο οργανισμός εξετάζει τα λειτουργικά συστήματα, τις εφαρμογές και κάθε άλλο λογισμικό που είναι εγκατεστημένο σε συσκευές που εμπίπτουν στο πεδίο εφαρμογής της διαδικασίας θωράκισης. Ο οργανισμός πρέπει να εξετάζει τις κατευθυντήριες γραμμές και τα έγγραφα για τη θωράκιση συστημάτων που παρέχονται από τους προμηθευτές λογισμικού και υλισμικού, καθώς και τις κατευθυντήριες γραμμές και τις βέλτιστες πρακτικές που δημοσιεύονται από ομάδες συστημάτων τεχνολογίας, ρυθμιστικές αρχές και άλλες διεθνείς βέλτιστες πρακτικές ή πλαίσια. Ο οργανισμός πρέπει να λαμβάνει υπόψη, τουλάχιστον, τα default configurations και την κατάργηση των μη αναγκαίων προκαθορισμένων λογαριασμών, την εξασφάλιση ενιαίων πρωτογενών λειτουργιών ανά διακομιστή για την αποφυγή λειτουργιών με διαφορετικά επίπεδα ασφάλειας στον ίδιο εξυπηρετητή, παρέχοντας μόνο τις απαραίτητες υπηρεσίες, τα πρωτόκολλα και τους daemons, χρησιμοποιώντας παραμέτρους για την ασφάλεια του συστήματος με στόχο την πρόληψη της κατάχρησης, και την αφαίρεση κάθε περιττής λειτουργίας, όπως των scripts, των drivers, των χαρακτηριστικών και των υποσυστημάτων, προκειμένου να ελαχιστοποιηθεί η επιφάνεια επίθεσης του συστήματος. Ο οργανισμός θα πρέπει να εξετάσει το ενδεχόμενο εφαρμογής τείχων προστασίας στο επίπεδο συστημάτων (firewalls), προκειμένου να αποτρέπονται οι επιπτώσεις από κακόβουλο κώδικα στην ασφάλεια των πληροφοριών που αποθηκεύονται στο τελικό σημείο.
Ασφάλεια συστημάτων	SS3	Ασφάλεια κινητών συσκευών	Να εξασφαλιστεί η κατάλληλη ασφάλεια των κινητών συσκευών που έχουν πρόσβαση σε οργανωτικούς πόρους.	Θέσπιση, εφαρμογή και διατήρηση μέτρων ασφάλειας κινητών συσκευών προκειμένου να διασφαλίζεται η εμπιστευτικότητα, η ακεραιότητα, η διαθεσιμότητα και η αυθεντικότητα των κινητών συστημάτων που χρησιμοποιούνται από τα στελέχη για να συνδέονται, αλληλοεπιδρούν ή επεξεργάζονται οργανωτικά στοιχεία υποδομής και πόρους. Ο οργανισμός πρέπει να εξετάζει τη διαχείριση κινητών συσκευών, μέτρα ασφαλούς αποθήκευσης και κρυπτογράφησης, όπως ορίζονται στο μέτρο [DS5], ισχυρή επαλήθευση ταυτότητας, όπως ορίζεται στο μέτρο [IAM4], και μέτρα ασφαλούς επικοινωνίας και δικτύωσης, όπως ορίζονται στο μέτρο [NS4]. Ο φορέας διασφαλίζει την επαρκή προστασία των κινητών συσκευών και των πληροφοριών που διατηρούνται σε κινητές συσκευές έναντι κλοπής και απώλειας. Ο οργανισμός πρέπει να εξετάζει τη δυνατότητα εξ αποστάσεως καθαρισμού και του εντοπισμού της γεωγραφικής θέσης.

Κατηγορία	#	Μέτρο	Στόχος Μέτρου	Περιγραφή Μέτρου
Ασφάλεια συστημάτων	SS4	Διαχείριση διαμόρφωσης εφαρμογών	Να διασφαλιστεί η κατάλληλη διαχείρισης των εφαρμογών που χρησιμοποιούνται για την πρόσβαση ή επεξεργασία οργανωτικών πόρων.	Θέσπιση, εφαρμογή και διατήρηση μέτρων διαχείρισης της διαμόρφωσης εφαρμογών με σκοπό την πρόληψη της μη επιτρεπόμενης και κακόβουλης εγκατάστασης, της διαμόρφωσης ή της τροποποίησης εφαρμογών και του λογισμικού σε οργανωτικά στοιχεία και συσκευές. Ο οργανισμός πρέπει να εξετάσει το ενδεχόμενο δημιουργίας κεντρικής διεπαφής για τη διαχείριση και διαμόρφωση εφαρμογών ώστε να εξασφαλίζεται ότι όλες οι οργανωτικές συσκευές υπόκεινται σε κεντρική διαχείριση, ενώ η διαμόρφωση και οι ενημερώσεις λογισμικού μπορούν να προωθηθούν στις τελικές συσκευές. Αυτή η κεντρική διεπαφή διαχείρισης πρέπει να επιτρέπει στον οργανισμό να θεσπίζει κατάλογο ορισμένων επιτρεπόμενων ή μη επιτρεπόμενων τύπων εφαρμογών.
Ασφάλεια εφαρμογών	AS1	Ασφαλής κύκλος ζωής ανάπτυξης λογισμικού	Να διασφαλιστούν επαρκή μέτρα ασφάλειας στο πλαίσιο των δραστηριοτήτων ανάπτυξης λογισμικού που αναπτύσσει ο οργανισμός.	Θέσπιση, εφαρμογή και διατήρηση ασφαλών πρακτικών ανάπτυξης λογισμικού σε παραδοσιακές διαδικασίες κύκλου ζωής ανάπτυξης λογισμικού, ώστε να διασφαλίζεται ότι η ασφάλεια είναι ενσωματωμένη στο σχεδιασμό στο πλαίσιο των δραστηριοτήτων ανάπτυξης εφαρμογών και λογισμικού. Ο οργανισμός πρέπει να εξετάσει το ενδεχόμενο εφαρμογής, τουλάχιστον, μιας αξιολόγησης κινδύνου στο αρχικό στάδιο του έργου, διενέργειας δοκιμών ασφάλειας και εξέτασης κώδικα στα στάδια ανάπτυξης του έργου, και διενέργεια αξιολόγησης ασφάλειας και ασφαλούς διαμόρφωσης στην παράδοση του έργου. Ο οργανισμός πρέπει να διασφαλίζει ότι εφαρμόζονται κατάλληλα μέτρα για τον διαχωρισμό των περιβαλλόντων ανάπτυξης λογισμικού από το επιχειρησιακό περιβάλλον παραγωγής. Ο οργανισμός διασφαλίζει ότι τα δεδομένα που χρησιμοποιούνται για τη διενέργεια δοκιμών είναι ανώνυμα και δεν συνδέονται με εμπιστευτικές και ευαίσθητες πληροφορίες στο πλαίσιο αναπτυξιακών δραστηριοτήτων.
Ασφάλεια ανθρώπινων πόρων	HRS1	Κύκλος ζωής της εργοδότησης	Να υλοποιούνται επαρκή μέτρα για την εξασφάλιση ότι τα στελέχη που εργάζονται για λογαριασμό του οργανισμού, τα οποία έχουν πρόσβαση σε οργανωτικούς πόρους, υποστηρίζουν την πολιτική ασφάλειας πληροφοριών και τους στόχους του οργανισμού.	Κατάρτιση, εφαρμογή και διατήρηση σχεδίου για να διασφαλιστεί ότι η ασφάλεια πληροφοριών είναι ενσωματωμένη καθ' όλη τη διάρκεια του κύκλου ζωής της εργοδότησης (δηλαδή πριν, κατά τη διάρκεια και μετά την εργοδότηση των εργαζομένων) και να καταβάλει κάθε εύλογη προσπάθεια προκειμένου να διασφαλίσει ότι οι εργαζόμενοι κατανοούν τις ευθύνες τους σε σχέση με την ασφάλεια πληροφοριών. Το σχέδιο περιλαμβάνει κατάλληλα μέτρα ασφάλειας πληροφοριών σε κάθε φάση της εργοδότησης, π.χ. έλεγχοι ιστορικού πριν την πρόσληψη, κατάρτιση και ευαισθητοποίηση των εργαζομένων, ενσωμάτωση επαρκών προνοιών στις συμβάσεις εργασίας, κατάρτιση πολιτικής αποδεκτής χρήσης, επιστροφή των συσκευών των εργαζομένων που περιέχουν κρίσιμες πληροφορίες, και αφαίρεση της πρόσβασης σε συστήματα και εφαρμογές σύμφωνα με τον κύκλο ζωής της διαχείρισης ταυτότητας, όπως

Κατηγορία	#	Μέτρο	Στόχος Μέτρου	Περιγραφή Μέτρου
				ορίζεται στο μέτρο [IAM7].
Ασφάλεια ανθρώπινων πόρων	HRS2	Παρακολούθηση εργαζομένων	Να εξασφαλιστεί ότι τα στελέχη που εργάζονται για λογαριασμό του οργανισμού συμμορφώνονται με την πολιτική ασφάλειας πληροφοριών και τηρούν τις ευθύνες ασφάλειας τους καθ' όλη τη διάρκεια του κύκλου ζωής της απασχόλησης.	Θέσπιση, εφαρμογή και διατήρηση σχεδίου για την παρακολούθηση της συμμόρφωσης των εργαζομένων με τις υποχρεώσεις και τις ευθύνες τους όσον αφορά την ασφάλεια πληροφοριών, καθ' όλη τη διάρκεια του κύκλου ζωής της απασχόλησης.
Ασφάλεια ανθρώπινων πόρων	HRS3	Πειθαρχικά μέτρα και επιβολή	Να εξασφαλιστεί ότι τα στελέχη που εργάζονται για λογαριασμό του οργανισμού, είναι υπεύθυνα για τις εκούσιες ή ακούσιες δραστηριότητες που επηρεάζουν τους στόχους ασφάλειας πληροφοριών του οργανισμού.	Θέσπιση, εφαρμογή και διατήρηση σειράς πειθαρχικών μέτρων προκειμένου να διασφαλιστεί η συμμόρφωση των στελεχών με τις υποχρεώσεις και τις ευθύνες τους όσον αφορά την ασφάλεια πληροφοριών και την ανάληψη δράσης σε περίπτωση παραβίασης των υποχρεώσεων και των ευθυνών αυτών. Ο οργανισμός πρέπει να εξετάσει το ενδεχόμενο θέσπισης επίσημης διαδικασίας επιβολής κυρώσεων για στελέχη που δεν συμμορφώνονται με τις υποχρεώσεις και τις ευθύνες τους στον τομέα της ασφάλειας πληροφοριών. Η μη συμμόρφωση με τις υποχρεώσεις και τις ευθύνες όσον αφορά την ασφάλεια πληροφοριών εντοπίζεται μέσω των διαδικασιών παρακολούθησης των εργαζομένων [HRS2].
Ασφάλεια ανθρώπινων πόρων	HRS4	Εξωτερικοί συνεργάτες	Να εξασφαλιστεί ότι οι εξωτερικοί συνεργάτες που εργάζονται για λογαριασμό του οργανισμού τηρούν την πολιτική ασφάλειας πληροφοριών και τους στόχους ασφάλειας του οργανισμού.	Θέσπιση, εφαρμογή και διατήρηση μέτρων για την ασφάλεια πληροφοριών σε σχέση με το εξωτερικό εργατικό δυναμικό, π.χ. με τους αναδόχους συμβάσεων, προκειμένου να διασφαλίζεται η δέουσα προστασία των πληροφοριών που ανταλλάσσονται με εξωτερικούς συνεργάτες.
Ασφάλεια ανθρώπινων πόρων	HRS5	Προστασία από απειλές που προέρχονται από εσωτερικά πρόσωπα	Να εξασφαλιστεί η προστασία από απειλές κατά της ασφάλειας δικτύων και πληροφοριών από το εσωτερικό του οργανισμού.	Θέσπιση, εφαρμογή και διατήρηση κατάλληλων μέτρων για την πρόληψη, τον εντοπισμό και την παρακολούθηση των επιθέσεων από εσωτερικά πρόσωπα, από άγνοια, αμέλεια, ή κακόβουλες ή επαγγελματικές προθέσεις. Ο οργανισμός πρέπει να εκπαιδεύει και να ευαισθητοποιεί τους εργαζόμενους σχετικά με τις πρακτικές ασφάλειας των πληροφοριών εντός του οργανισμού, σύμφωνα με το μέτρο [TA2], να διενεργεί επαρκή έλεγχο των υποψηφίων σύμφωνα με το μέτρο [HRS1], και να

Κατηγορία	#	Μέτρο	Στόχος Μέτρου	Περιγραφή Μέτρου
				παρακολουθεί τους εργαζόμενους [HRS2], ώστε να μειώνεται η πιθανότητα να υπάρξουν εσωτερικές επιθέσεις.
Ασφάλεια ανθρώπινων πόρων	HRS6	Συμφωνίες εργοδότησης και αποδεκτή χρήση	Να διασφαλιστεί ότι οι ευθύνες που αφορούν την ασφάλεια πληροφοριών και την αποδεκτή χρήση των στοιχείων ενεργητικού, ενσωματώνονται στις συμφωνίες εργοδότησης και στις διαδικασίες έναρξης απασχόλησης, για την επίτευξη υπευθυνότητας και ευαισθητοποίησης.	Θέσπιση, εφαρμογή και διατήρηση μιας αποδεκτής πολιτικής χρήσης, η οποία προσδιορίζει τις χρήσεις που ο οργανισμός θεωρεί αποδεκτές χρήσεις των συστημάτων πληροφοριών που τίθενται στη διάθεση των στελεχών, ώστε να εξασφαλίζεται ότι τα στελέχη γνωρίζουν τι αναμένεται από αυτούς όσον αφορά τη χρήση, π.χ., ηλεκτρονικών υπολογιστών και κινητών συσκευών. Ο οργανισμός θα πρέπει να εξετάζει το ενδεχόμενο να ελέγχει την επίγνωση σχετικά με την πολιτική αποδεκτής χρήσης. Ο οργανισμός θα πρέπει επίσης να συνάπτει επαρκείς συμφωνίες εργοδότησης, στις οποίες να αναφέρονται με σαφήνεια οι υποχρεώσεις και οι ευθύνες του εργαζομένου όσον αφορά την ασφάλεια πληροφοριών.
Φυσική ασφάλεια	PS1	Περιβαλλοντικά μέτρα	Να εξασφαλιστούν επαρκή μέτρα για την προστασία του οργανισμού από τις επιπτώσεις φυσικών καταστροφών, όπως οι πλημμύρες, οι σεισμοί και οι πυρκαγιές.	Θέσπιση, εφαρμογή και διατήρηση κατάλληλων μέτρων για την προστασία του οργανισμού από τις επιπτώσεις φυσικών καταστροφών, όπως οι πλημμύρες, οι σεισμοί και οι πυρκαγιές. Ο οργανισμός πρέπει να λαμβάνει υπόψη τη γεωγραφική θέση κατά τη δημιουργία της υποδομής δικτύου και να εξασφαλίζει ότι τα κρίσιμα στοιχεία υποδομής και συστήματα είναι γεωγραφικά διάσπαρτα.
Φυσική ασφάλεια	PS2	Έλεγχος περιμετρικής πρόσβασης	Να διασφαλιστεί η φυσική περίμετρος του οργανισμού, με την εξασφάλιση και αποτροπή της μη εξουσιοδοτημένης πρόσβασης.	Θέσπιση, εφαρμογή και διατήρηση φυσικής περιμέτρου ασφάλειας με σκοπό την προστασία των εγκαταστάσεων επεξεργασίας πληροφοριών. Ο οργανισμός πρέπει να καθιερώσει κατάλληλα μέτρα ελέγχου της περιμετρικής πρόσβασης με την εφαρμογή φυσικών συνόρων, όπως φράχτες, πόρτες και τοίχοι. Ο οργανισμός απαιτεί επίσης από τους υπαλλήλους και τους επισκέπτες να αποδεικνύουν την ταυτότητά τους στους φρουρούς ασφαλείας προκειμένου να εισέλθουν (σε κάποιο μέρος) του οργανισμού. Ο οργανισμός θα πρέπει να εξετάσει την εγκατάσταση καμερών κλειστού κυκλώματος με σκοπό τον εντοπισμό εισβολέων στα όρια του οργανισμού.
Φυσική ασφάλεια	PS3	Έλεγχος εσωτερικής πρόσβασης	Να εξασφαλιστεί ο έλεγχος της πρόσβασης σε εσωτερικούς χώρους εργασίας και τις εγκαταστάσεις, ώστε να διασφαλίζεται ότι η φυσική	Θέσπιση, εφαρμογή και διατήρηση εσωτερικών μέτρων πρόσβασης, ευθυγραμμισμένων με τους ρόλους που περιγράφονται στο [IAM1], προκειμένου να διασφαλιστεί ότι μόνο τα στελέχη με έννομο συμφέρον έχουν πρόσβαση σε (συγκεκριμένα μέρη) του οργανισμού, π.χ. με τη δημιουργία ειδικών σαρωτών ταυτότητας για την πρόσβαση σε ένα μέρος του οργανισμού.

Κατηγορία	#	Μέτρο	Στόχος Μέτρου	Περιγραφή Μέτρου
			πρόσβαση περιορίζεται κατόπιν ανάγκης.	
Φυσική ασφάλεια	PS4	Ασφάλεια καλωδίωσης, εξοπλισμού και εγκαταστάσεων	Να εξασφαλιστεί ότι για την καλωδίωση και τον εξοπλισμό που υποστηρίζουν την επεξεργασία των πληροφοριών, εξασφαλίζεται η φυσική προστασία από παρεμβολές, υποκλοπή ή ζημιά.	Θέσπιση, εφαρμογή και διατήρηση κατάλληλων μέτρων προκειμένου να προστατεύει την καλωδίωση και τον λοιπό εξοπλισμό από παρεμβολές, υποκλοπή ή ζημιά, οι οποίες θα προκαλούσαν διακοπή στις υπηρεσίες του οργανισμού. Ο οργανισμός πρέπει να εξασφαλίζει ότι τα καλώδια που παρέχουν ηλεκτρική ενέργεια σε κρίσιμες υποδομές προστατεύονται δεόντως και να εκπαιδεύει τους υπαλλήλους σύμφωνα με το μέτρο [TA2], ώστε να γνωρίζουν τη σημασία του εξοπλισμού που υποστηρίζει τις δραστηριότητες επεξεργασίας πληροφοριών. Η φυσική πρόσβαση στα λογικά δίκτυα θα πρέπει επίσης να προστατεύεται με κατάλληλα μέτρα ώστε να αποτρέπεται η μη εξουσιοδοτημένη φυσική πρόσβαση στο λογικό εξοπλισμό και το δίκτυο του οργανισμού. Ο φορέας εξετάζει κατάλληλα μέτρα πρόσβασης στο δίκτυο, όπως ορίζονται στο [NS5]. Ο οργανισμός διασφαλίζει τη φυσική ακεραιότητα και την τακτική συντήρηση των εγκαταστάσεων στις οποίες είναι εγκατεστημένος ο εξοπλισμός δικτύου, καθώς και την ορθή λειτουργία των μέτρων ασφάλειας.
Φυσική ασφάλεια	PS5	Εσωτερικά περιβαλλοντικά μέτρα	Να εξασφαλιστεί ότι οι εσωτερικοί χώροι και οι εγκαταστάσεις του οργανισμού προστατεύονται από φυσικές ζημιές.	Θέσπιση, εφαρμογή και διατήρηση μέτρων φυσικής ασφάλειας και προστασίας, ώστε να αποφεύγεται η φυσική ζημία στους εσωτερικούς χώρους και τις εγκαταστάσεις του οργανισμού. Κατά την εφαρμογή εσωτερικών περιβαλλοντικών μέτρων, ο οργανισμός θα πρέπει να εξετάζει τους κινδύνους που σχετίζονται με τη φωτιά και τη θερμοκρασία, την υγρασία, την ηλεκτρική ενέργεια, τη χρήση του νερού και άλλα στοιχεία που θα μπορούσαν να επηρεάσουν αρνητικά τη φυσική ασφάλεια των στοιχείων ενεργητικού. Ο οργανισμός πρέπει να εξετάζει την πυρόσβεση, τον έλεγχο της υγρασίας και άλλα μέτρα ανάλογα με τα χαρακτηριστικά των εσωτερικών φυσικών χώρων, όπως είναι τα κέντρα δεδομένων ή άλλους χώρους όπου βρίσκεται εξοπλισμός επεξεργασίας πληροφοριών.

1.3 ΑΝΤΑΠΟΚΡΙΣΗ (RESPOND)

Στόχος του πυλώνα ΑΝΤΑΠΟΚΡΙΣΗ (RESPOND) είναι να διασφαλίζει ότι οι φορείς είναι σε θέση να ανταποκρίνονται σε συμβάντα και περιστατικά που ενδέχεται να επηρεάσουν την εμπιστευτικότητα, την ακεραιότητα, τη διαθεσιμότητα ή την αυθεντικότητα πληροφοριών. Ο εν λόγω πυλώνας συνεπάγεται την υιοθέτηση της επιχειρησιακής ανθεκτικότητας και μέτρων επιχειρησιακής συνέχειας και αποκατάστασης των καταστροφών, καθώς και την αποκατάσταση των κανονικών δραστηριοτήτων.

Κατηγορία	#	Μέτρο	Στόχος Μέτρου	Περιγραφή Μέτρου
Διαχείριση συμβάντων και περιστατικών	EIM1	Ετοιμότητα και εντοπισμός συμβάντων και περιστατικών	Να διασφαλίζει ότι ο οργανισμός είναι σε θέση να εντοπίζει συμβάντα και περιστατικά που ενδέχεται να συνιστούν απειλή για τους στόχους της ασφάλειας πληροφοριών του οργανισμού και να ενεργοποιεί τις αντίστοιχες διαδικασίες αντιμετώπισης περιστατικών.	Θέσπιση, εφαρμογή και διατήρηση σχεδίου διαχείρισης και αντιμετώπισης συμβάντων και περιστατικών προκειμένου να διασφαλιστεί ότι ο οργανισμός είναι έτοιμος να αντιδράσει σε περίπτωση σοβαρού συμβάντος ή περιστατικού που αφορά την ασφάλεια πληροφοριών. Ο οργανισμός εξετάζει το ενδεχόμενο ευθυγράμμισης των διαδικασιών του για την αντιμετώπιση συμβάντων και περιστατικών με γενικές δυνατότητες παρακολούθησης και ειδικές λειτουργίες παρακολούθησης της ασφάλειας, όπως τις υπηρεσίες ανίχνευσης και πρόληψης εισβολών που περιγράφονται στο μέτρο [NS7].
Διαχείριση συμβάντων και περιστατικών	EIM2	Ανάλυση και αξιολόγηση συμβάντων και περιστατικών	Να διασφαλιστεί ότι ο οργανισμός είναι σε θέση να αναλύει και να αξιολογεί συμβάντα και περιστατικά που αφορούν την ασφάλεια πληροφοριών, ούτως ώστε να ενεργοποιεί κατάλληλες διαδικασίες περιορισμού και ανάκτησης.	Θέσπιση, εφαρμογή και διατήρηση διαδικασιών που επιτρέπουν την ανάλυση και την αξιολόγηση συμβάντων και περιστατικών, ώστε να είναι σε θέση ο οργανισμός να λαμβάνει αιτιολογημένες αποφάσεις σχετικά με τις δράσεις και τα μέτρα που πρέπει να ληφθούν για την αντιμετώπιση ή την αποκατάσταση από συμβάντα και περιστατικά που αφορούν την ασφάλεια. Ο οργανισμός εξετάζει τον αντίκτυπο στα υποκείμενα δεδομένων, στις επιχειρηματικές δραστηριότητες, στα εξωτερικά μέρη και στο οικοσύστημα των φορέων. Ο οργανισμός διασφαλίζει ότι η ανάλυση και αξιολόγηση συμβάντων και περιστατικών διεκπεραιώνεται σε συνεννόηση με την ανώτατη διοίκηση για τη σύνδεση συμβάντων και περιστατικών με σενάρια υψηλού κινδύνου.
Διαχείριση συμβάντων και περιστατικών	EIM3	Περιορισμός και ανάκτηση από συμβάντα και περιστατικά	Να εξασφαλιστεί επαρκής περιορισμός και αποκατάσταση από συμβάντα και περιστατικά ασφάλειας που επηρεάζουν αρνητικά τους στόχους ασφάλειας πληροφοριών του οργανισμού.	Θέσπιση, εφαρμογή και διατήρηση διαδικασιών για τον περιορισμό και την ανάκτηση από συμβάντα και περιστατικά, ώστε να περιορίζονται στο ελάχιστο οι επιπτώσεις στα συστήματα, τις εφαρμογές, τα δίκτυα και τα δεδομένα, καθώς και να διασφαλίζονται, στο μέτρο του δυνατού, οι κρίσιμες λειτουργίες του οργανισμού. Ο οργανισμός εξετάζει τους στόχους αποκατάστασης από συμβάντα και περιστατικά, λαμβάνοντας υπόψη τον στόχο του σημείου ανάκτησης (RPO) και τον χρόνο αποκατάστασης (RTO), προκειμένου να προσδιορίσει τη στοχοθετημένη διάρκεια και το επίπεδο των υπηρεσιών εντός των οποίων πρέπει να αποκατασταθεί μια επιχειρηματική διαδικασία μετά από κάποιο περιστατικό.
Διαχείριση συμβάντων και περιστατικών	EIM4	Δραστηριότητες μετά το συμβάν και το περιστατικό	Να διασφαλιστεί ότι ο οργανισμός μαθαίνει από συμβάντα και περιστατικά ασφάλειας, προκειμένου να αποτρέπονται παρόμοια συμβάντα και περιστατικά στο μέλλον.	Θέσπιση, εφαρμογή και διατήρηση διαδικασιών μετά την εκδήλωση συμβάντων και περιστατικών, προκειμένου να αποτυπωθούν τα διδάγματα που έχουν αντληθεί από τα συμβάντα και περιστατικά ασφάλειας πληροφοριών και να προσδιορίζουν κατά πόσον πρέπει να θεσπιστούν πρόσθετα μέτρα ασφάλειας για την πρόληψη παρόμοιων συμβάντων και περιστατικών. Ο οργανισμός εξετάζει το ενδεχόμενο θέσπισης εκ των υστέρων διαδικασίας, η οποία περιλαμβάνει συνάντηση για την αξιολόγηση του συμβάντος ή περιστατικού με τους επηρεαζόμενους ιδιοκτήτες του συστήματος, τους διαχειριστές δεδομένων και άλλα ενδιαφερόμενα μέρη που συμμετείχαν στην

Κατηγορία	#	Μέτρο	Στόχος Μέτρου	Περιγραφή Μέτρου
				αντιμετώπιση του περιστατικού, με σκοπό την ανταλλαγή διδαγμάτων και τον προσδιορισμό προληπτικών μέτρων.
Διαχείριση συμβάντων και περιστατικών	EIM5	Ρυθμιστικές υποχρεώσεις κοινοποίησης συμβάντος και συνεργασίας	Να διασφαλίσει ότι ο οργανισμός ενημερώνει τα σχετικά ενδιαφερόμενα μέρη στην περίπτωση συμβάντων ή περιστατικών ασφάλειας, όπως περιγράφεται σε νομικές και ρυθμιστικές υποχρεώσεις.	Θέσπιση, εφαρμογή και διατήρηση διαδικασιών για τη διασφάλιση της συμμόρφωσης με ρυθμιστικές και νομοθετικές απαιτήσεις όσον αφορά την κοινοποίηση περιστατικών. Ο οργανισμός διασφαλίζει ότι υπάρχουν επαρκείς διαδικασίες κοινοποίησης και υποβολής εκθέσεων για συμβάντα και περιστατικά ασφάλειας πληροφοριών σε αρμόδιες ρυθμιστικές αρχές, όπως την ΑΨΑ. Στο πλαίσιο των δεδομένων προσωπικού χαρακτήρα, ο οργανισμός διασφαλίζει τη συμμόρφωση με τις σχετικές νομοθετικές και ρυθμιστικές διατάξεις που αφορούν την προστασία των δεδομένων προσωπικού χαρακτήρα και επικοινωνεί, όπου είναι απαραίτητο, με την αρμόδια αρχή προστασίας δεδομένων.
Διαχείριση συμβάντων και περιστατικών	EIM6	Επικοινωνία με ενδιαφερόμενους φορείς για συμβάντα και περιστατικά	Να εξασφαλίζει ότι ο οργανισμός κοινοποιεί πληροφορίες σχετικά με συμβάντα και περιστατικά ασφάλειας δικτύων και πληροφοριών σε εσωτερικούς και εξωτερικούς ενδιαφερόμενους φορείς.	Θέσπιση, εφαρμογή και διατήρηση διαδικασιών για τη διασφάλιση σχετικής επικοινωνίας όσον αφορά συμβάντα και περιστατικά ασφάλειας πληροφοριών προς εξωτερικούς και εσωτερικούς αποδέκτες, προκειμένου να εξασφαλίζεται η επίγνωση του συμβάντος ή περιστατικού και να παρέχεται στους εξωτερικούς και εσωτερικούς ενδιαφερόμενους φορείς η δυνατότητα να καθορίζουν κατάλληλα μέτρα αντίδρασης, εάν αυτό είναι απαραίτητο. Ο οργανισμός πρέπει να εξετάζει το ενδεχόμενο συνεργασίας με εξωτερικούς και εσωτερικούς ενδιαφερόμενους φορείς όσον αφορά τον περιορισμό συμβάντων και περιστατικών, προκειμένου να ελαχιστοποιούνται οι σχετικές επιπτώσεις και οι εκ των υστέρων δραστηριότητες προκειμένου να καθορίζονται προληπτικά μέτρα, όπως με την ΑΨΑ και τις υπηρεσίες έκτακτης ανάγκης.
Επιχειρησιακή συνέχεια και ανθεκτικότητα	BCR1	Ανάλυση επιχειρησιακών επιπτώσεων	Να εξασφαλιστεί ότι ο οργανισμός έχει αναλύσει και αξιολογήσει τις κρίσιμες επιχειρηματικές διαδικασίες που πρέπει να ληφθούν υπόψη στο σχέδιο επιχειρησιακής συνέχειας, ώστε να μπορέσει ο οργανισμός να αποκαταστήσει τις επιχειρηματικές διαδικασίες σε αποδεκτό επίπεδο, το συντομότερο δυνατόν, σε περίπτωση συμβάντος ή περιστατικού.	Θέσπιση, εφαρμογή και διατήρηση διαδικασίας ανάλυσης επιχειρησιακών επιπτώσεων προκειμένου να προσδιορίσει όλα τα κρίσιμα περιουσιακά στοιχεία εντός του οργανισμού. Η ανάλυση των επιχειρησιακών επιπτώσεων θα επιτρέψει στον οργανισμό να ιεραρχήσει τις λειτουργίες και τα συστήματα με βάση την αναγκαιότητα παροχής επιχειρησιακών υπηρεσιών. Η ανάλυση των επιχειρησιακών επιπτώσεων διενεργείται βάσει συστήματος ταξινόμησης που λαμβάνει υπόψη καθορισμένα επίπεδα κρισιμότητας και εξετάζει εάν κρίσιμες λειτουργίες ή συστήματα λειτουργούν αυτόνομα ή συνδέονται με άλλη λειτουργία ή σύστημα του οργανισμού.

Κατηγορία	#	Μέτρο	Στόχος Μέτρου	Περιγραφή Μέτρου
Επιχειρησιακή συνέχεια και ανθεκτικότητα	BCR2	Σχέδιο επιχειρησιακής συνέχειας	Να εξασφαλιστεί ότι ο οργανισμός διαθέτει σχέδιο για τη διατήρηση της συνέχειας των κρίσιμων επιχειρηματικών διαδικασιών και την αποκατάσταση κατά τη διάρκεια συμβάντος ή περιστατικού και μετά από αυτό.	Θέσπιση, εφαρμογή και διατήρηση σχεδίου επιχειρησιακής συνέχειας προκειμένου να διασφαλιστεί ότι ο οργανισμός μπορεί να ανταποκρίνεται σε καταστάσεις έκτακτης ανάγκης με άμεσο και κατάλληλο τρόπο, και είναι σε θέση να διατηρεί επιχειρηματικές λειτουργίες ελαχιστοποιώντας τις συνέπειες και τις ζημίες που προκύπτουν από ένα περιστατικό. Το σχέδιο επιχειρησιακής συνέχειας περιλαμβάνει το σχέδιο αποκατάστασης από καταστροφή, όπως περιγράφεται στο μέτρο [BCR4] και λαμβάνει υπόψη την ανάλυση των επιχειρησιακών επιπτώσεων.
Επιχειρησιακή συνέχεια και ανθεκτικότητα	BCR3	Ασκήσεις και προσομοιώσεις επιχειρησιακής συνέχειας	Να διασφαλιστεί ότι ο οργανισμός και τα στελέχη του γνωρίζουν τις ευθύνες τους κατά τη διάρκεια ενός συμβάντος ή περιστατικού που ενεργοποιεί το σχέδιο επιχειρησιακής συνέχειας.	Θέσπιση, εφαρμογή και διατήρηση μέτρων για τον έλεγχο, την αναθεώρηση και τη βελτίωση του σχεδίου επιχειρησιακής συνέχειας μέσω ασκήσεων όπου προσομοιώνονται συμβάντα και περιστατικά στον οργανισμό, με σκοπό τον έλεγχο της ανταπόκρισης του οργανισμού σε παρόμοια συμβάντα και περιστατικά, και τη βελτίωση των διαδικασιών επιχειρησιακής συνέχειας. Οι ασκήσεις και οι προσομοιώσεις επιχειρησιακής συνέχειας θα πρέπει να παρέχουν στον οργανισμό τη δυνατότητα να εντοπίζει ευκαιρίες βελτίωσης και να επιτυγχάνει καλύτερα αποτελέσματα με την πάροδο του χρόνου. Ο οργανισμός θα πρέπει να εξετάσει το ενδεχόμενο να συνδέσει το σχέδιο επιχειρησιακής συνέχειας με τις διαδικασίες διαχείρισης αλλαγών, όπως περιγράφονται στο [CM1], προκειμένου να λαμβάνονται υπόψη στο σχέδιο επιχειρησιακής συνέχειας οι συνέπειες από όποιες αλλαγές εντός του οργανισμού. Ο οργανισμός θα πρέπει να διενεργεί ασκήσεις και προσομοιώσεις επιχειρησιακής συνέχειας σε τακτά χρονικά διαστήματα, προκειμένου οι εργαζόμενοι να είσαι σε επαγρύπνηση για συμβάντα και περιστατικά που θα μπορούσαν να βλάψουν τον οργανισμό. Κατά την κατάρτιση του σχεδίου επιχειρησιακής συνέχειας, ο οργανισμός εξετάζει και την αποκατάσταση από καταστροφή, όπως ορίζεται στο μέτρο [BCR4].
Επιχειρησιακή συνέχεια και ανθεκτικότητα	BCR4	Σχέδιο αποκατάστασης από καταστροφή	Να εξασφαλιστεί ότι ο οργανισμός διαθέτει σχέδιο για την αποκατάσταση των συστημάτων κρίσιμων πληροφοριών σε αποδεκτό επίπεδο κατά τη διάρκεια ή μετά από περιστατικό.	Θέσπιση, εφαρμογή και διατήρηση σχεδίου αποκατάστασης από καταστροφή, προκειμένου να διασφαλίζεται η αποκατάσταση και η ανάκτηση όλων των κρίσιμων διαδικασιών των συστημάτων πληροφορικής και των υποστηρικτικών στοιχείων ενεργητικού, όπως η παροχή ηλεκτρικής ενέργειας, μετά την ύπαρξη ενός περιστατικού. Το σχέδιο αποκατάστασης από καταστροφή θα πρέπει να περιλαμβάνει σαφείς οδηγίες για το προσωπικό πληροφορικής, ώστε να εξασφαλίζεται έγκαιρη και αποτελεσματική αντίδραση σε όλα τα περιστατικά που επηρεάζουν το περιβάλλον πληροφορικής του οργανισμού. Στο σχέδιο αποκατάστασης από καταστροφή θα πρέπει να καθορίζεται ο στόχος του σημείου ανάκτησης (RPO) και ο στόχος για τον χρόνο αποκατάστασης (RTO), ώστε να αποφεύγονται μη αποδεκτές συνέπειες για τον οργανισμό.

2.ΠΡΟΣΑΡΤΗΜΑ Α: ΠΗΓΕΣ ΓΙΑ ΠΕΡΑΙΤΕΡΩ ΠΛΗΡΟΦΟΡΗΣΗ ΣΧΕΤΙΚΑ ΜΕ ΤΑ ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ

Το παρόν παράρτημα παρέχει ενημερωτικές αναφορές στις κατευθυντήριες γραμμές που δημοσιεύονται από δημόσιους οργανισμούς όπως ο ENISA και οι αρμόδιες εθνικές αρχές, οι οποίες μπορούν να βοηθήσουν τους φορείς να εφαρμόσουν τα μέτρα ασφάλειας πληροφοριών που περιέχονται στο Πλαίσιο.

Πυλώνας	Ενημερωτικές Αναφορές			
	Τίτλος	Συγγραφέας	Ημερ.δημοσίευσης	URL
PREPARE	Governance framework for European standardisation	ENISA	July 01, 2016	https://www.enisa.europa.eu/publications/policy-industry-research
	NCSS Good Practice Guide	ENISA	November 14, 2016	https://www.enisa.europa.eu/publications/ncss-good-practice-guide
	National Cyber Security Strategies: An Implementation Guide	ENISA	December 19, 2012	https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide
	Secure ICT Procurement in Electronic Communications	ENISA	December 11, 2014	https://www.enisa.europa.eu/publications/secure-ict-procurement-in-electronic-communications
	Supply Chain Integrity: An overview of the ICT supply chain risks and challenges, and vision for the way forward	ENISA	September 11, 2015	https://www.enisa.europa.eu/publications/sci-2015
	Good Practice Guide on Training Methodologies	ENISA	November 12, 2014	https://www.enisa.europa.eu/publications/good-practice-guide-on-training-methodologies
	Cyber Security Culture in organisations	ENISA	February 06, 2018	https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations
	Incident notification for DSPs in the context of the NIS Directive	ENISA	February 27, 2017	https://www.enisa.europa.eu/publications/incident-notification-for-dsps-in-the-context-of-the-nis-directive
	The cost of incidents affecting CIIs	ENISA	August 05, 2016	https://www.enisa.europa.eu/publications/the-cost-of-incidents-affecting-ciis
	Communication network dependencies for ICS/SCADA Systems	ENISA	February 01, 2017	https://www.enisa.europa.eu/publications/ics-scada-dependencies
	Stocktaking, Analysis and Recommendations on the protection of CIIs	ENISA	January 21, 2016	https://www.enisa.europa.eu/publications/stocktaking-analysis-and-recommendations-on-the-protection-of-ciis
PROTECT AND DETECT	Defining and Understanding Security in the Software Development Life Cycle	SANS	/	https://software-security.sans.org/resources/paper/cissp/defining-understanding-security-software-development-life-cycle
	Secure Software Engineering Initiatives	ENISA	May 01, 2011	https://www.enisa.europa.eu/publications/secure-software-engineering-initiatives
	Asset protection	CPNI	/	https://www.cpni.gov.uk/protecting-my-asset

Πυλώνας	Ενημερωτικές Αναφορές			
	Τίτλος	Συγγραφέας	Ημερ.δημοσίευσης	URL
	Physical Security	CPNI	/	https://www.cpni.gov.uk/physical-security
	Good Practice Guide on Vulnerability Disclosure. From challenges to recommendations	ENISA	January 18, 2016	https://www.enisa.europa.eu/publications/vulnerability-disclosure
	Effective Patch Management	ENISA	August 28, 2018	https://www.enisa.europa.eu/publications/info-notes/effective-patch-management
RESPOND	Business and IT Continuity: Overview and Implementation Principles	ENISA	February 01, 2008	https://www.enisa.europa.eu/publications/business-and-it-continuity-overview-and-implementation-principles
	Business Continuity for SMEs	ENISA	March 24, 2010	https://www.enisa.europa.eu/publications/business-continuity-for-smes
	Enabling and managing end-to-end resilience	ENISA	January 24, 2011	https://www.enisa.europa.eu/publications/end-to-end-resilience
	Strategies for incident response and cyber crisis cooperation	ENISA	August 25, 2016	https://www.enisa.europa.eu/publications/strategies-for-incident-response-and-cyber-crisis-cooperation
	Actionable information for security incident response	ENISA	January 19, 2015	https://www.enisa.europa.eu/publications/actionable-information-for-security
	Good Practice Guide for Incident Management	ENISA	December 20, 2010	https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management
	NCSS Good Practice Guide	ENISA	November 14, 2016	https://www.enisa.europa.eu/publications/ncss-good-practice-guide

3.ΠΡΟΣΑΡΤΗΜΑ Β: ΟΔΗΓΙΕΣ ΕΦΑΡΜΟΓΗΣ: ISO/IEC 27001 AND NIST SP800-53

Το παρόν παράρτημα περιλαμβάνει αναφορές στις οδηγίες εφαρμογής ανά μέτρο ασφάλειας. Οι οδηγίες εφαρμογής στον παρακάτω πίνακα αναφέρονται σε δύο διεθνή πρότυπα: ISO / IEC 27001 και NIST SP800-53 Rev. 4, και παρέχονται για υποβοήθεια στην κατανόηση του περιεχόμενου των μέτρων ασφάλειας από τους φορείς.

Ref.	Control	ISO/IEC 27001	NIST SP800-53 Rev. 4
AM1	Asset lifecycle management	A.8	CM-8, PL-4, PS-4, PS-5, RA-2, MP-2, MP-3, MP-4, MP-5, MP-6, MP7, PE-16, PE-18, PE-20, SC-8, SC-28
AM2	Inventory of assets and ownership	A.8.1.1, A.8.1.2	CM-8
AM3	Asset monitoring	A.12.4	PE-20
AM4	Availability management	A.11.2.4, A.17.2	SC-5, SC-36
AM5	Cryptographic controls	§10, A.18.1.5	SC-12, SC-13
AM6	Capacity management	A.12.1.3	AU-4, CP-2, SC-5
AS1	Secure software development lifecycle	A.14.2	SA-8, SA-10, SA-11
BCR 1	Business impact analysis	A.16.1.1, A.17.1.1, A.17.1.2	RA-2, RA-3, PM-9
BCR 2	Business continuity plan	A.16.1.1, A.17.1.1, A.17.1.2	CP-2, CP-6, CP-7, CP-8, CP-9, CP-10, CP-11, CP-13, IR-8
BCR 3	Business continuity exercises and simulations	A.17.1.3	CP-4, IR-2, IR-3, PM-14
BCR 4	Disaster recovery plan	A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3	CP-2, IR-8, CP-4, IR-3, PM-14
CM1	Change management	A.12.1.2	CM-3, CM-5, SA-10
CM2	Configuration management	A.5.1.1, A.5.1.2, A.6.1.1, A.8.1.1, A.8.1.2, A.9.2.3, A.9.4.5, A.12.1.1, A.12.1.2, A.12.1.4, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4, A.18.1.1, A.18.1.2; A.18.2.2	CM-1, CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-8, CM-9, CM-10, CM-11
DS1	Information lifecycle management	§8.1, A.8.1, A.8.2, A.8.3	SA-1, SA-3, SA-4, SA-5, SA-8, SA-9, SA-11, SA-12, MP-1, MP-2, MP-3, MP-4, MP-5, MP-6, MP-7, MP-8
DS2	Classification and labelling of information	A.8.2	SC-28, SE-1, AC-16
DS3	Backup and data recovery	A.12.1, A.12.3	CP-1, CP-2, CP-3, CP-4, CP-5, CP-6, CP-7, CP-9, CP-10, CP-11
DS4	Information transfers and exchange	A.13.2	AC-4, AC-17, AC-18, AC-19, AC-20, CA-3, PE-17, SC-7, SC-8, SC-15, CA-3, PS-6, SA-9, SC-8, PS-6
DS5	Data loss and data leakage prevention	A.8.3.1	MP-1, MP-2, MP-3, MP-4, MP-5, MP-6, MP-7, MP-8
EIM1	Event and incident readiness and detection	A.12.4.1, A.16.1.1, A.16.1.3., A.16.1.4	IR-1, IR-3, IR-4, IR-8, AC-2, AU-12, CA-7, CM-3, SC-7, AU-3, AU-6, AU-11, AU-12, AU-14
EIM2	Event and incident analysis and evaluation	A.16.1.4	AU-6, IR-4
EIM3	Event and incident containment and recovery	A.16.1.5	IR-4, IR-9
EIM4	Post-event and post-incident activities	A.16.1.6, A.16.1.7	IR-4, AU-4, AU-9, AU-10(3), AU-11
EIM5	Regulatory incident notification and collaboration requirements	A.18.1.1, A.18.1.4	IR-1
EIM6	Event and incident stakeholder communication	A.16.1.2, A.16.1.3	AU-6, IR-6, IR-7
GOV 1	Information security roles and responsibilities	§5.3, A.6.1	PL-1, PL-4
GOV 2	Compliance with legal and regulatory requirements	§4.2, A.6.1.3, A.18.1	AR-2, AU-6, AU-11
GOV 3	Information security policies, standards, guidelines and procedures	§5.2, A.5.1	

Ref.	Control	ISO/IEC 27001	NIST SP800-53 Rev. 4
HRS 1	Employment lifecycle	A.7	PS-1, PS-2, PS-5
HRS 2	Employee monitoring	A.12.4	PS-8
HRS 3	Disciplinary measures and enforcement	A.12.4	PS-8
HRS 4	External human resources	A.15.2	PS-7
HRS 5	Insider threat protection	A.7, A.12.4	PS-1, PS-2, PS-5, PS-8
HRS 6	Employment agreements and acceptable use	A.8.1.3	PS-6
IAM1	Role based access control	A.9.1.1	AT-3, AC-2, AC-3, AT-3
IAM2	External access controls	A.9.1.2, A.13.2.	SA-9, AC-20, CA-2, CA-3, CP-2
IAM3	Privileged users management	A.9.1.1, A.9.2.3.	AT-3, AC-2, AC-3, AT-3
IAM4	Strong authentication	A.9.1.2	AC-3, AC-5, AC-6
IAM5	Credential management		IA-5, IA-6, IA-9, IA-10, IA-11
IAM6	Traceability and auditing	A.12.7	AU-1, AU-2, AU-3, AU-4, AU-5, AU-6, AU-7, AU-8, AU-9, AU-10, AU-11, AU-12, AU-13, AU-14, AU-15, AU-16
IAM7	Identity lifecycle management	A.9.1, A.9.3	AC-6, AC-13, AC-24
NS1	Perimeter security	A.13.1.1, A.13.1.2	SC-5, SC-7, SC-30, SI-8, AC-4, CA-3
NS2	Network segregation and segmentation	A.13.1.3	SC-3, SC-44, SC-37, PM-7
NS3	Denial of service protection	A.13.1.1, A.13.1.2	SC-5, SC-30, SI-8, AC-4, CA-3
NS4	Secure communication protocols	A.13	SC-8, SC-9, SC-10, SC-11, SC-12, SC-13
NS5	Network access control	A.13.1.1, A.13.1.2	SC-14, AC-1, AC-18, AC-24
NS6	Redundancy and high availability	A.11.2.4, A.17.2	SC-5, SC-36
NS7	Intrusion detection and prevention	A.13.1.2	IR-4, IR-10, SC-28, SI-4, SI-5
PS1	Environmental controls	A.11.1.4, A.11.2.1, A.11.2.2	PE-1, PE-13, PE-14, PE-15, PE-18
PS2	Perimeter access controls	A.11.1.1, A.11.1.2, A.11.1.3	PE-3, PE-6
PS3	Internal access controls	A.11.1.1, A.11.1.2, A.11.1.3	PE-2, PE-3, PE-6
PS4	Cabling, equipment and facilities security	A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3, A.11.2.4, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8	PE-9, PE-10, PE-11, PE-12
PS5	Internal environmental controls	A.11.1.3, A.11.1.5	PE-3, PE-5
RM1	Methodology	ISO 27005	PM-8, PM-9, PM-11, SA-14
RM2	Context	§4, ISO 27005	CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5, PM-15, PM-16
RM3	Risk Identification	ISO 27005	RA-3, SI-5, PM-12, PM-16
RM4	Risk Analysis	§6.1, §6.2, ISO 27005	RA-1, RA-2, RA-3, RA-4, RA-5, RA-6
RM5	Risk Evaluation	§6.1, §6.2, ISO 27005	RA-1, RA-2, RA-3, RA-4, RA-5, RA-6
RM6	RiskTreatment	§6.1, §6.2, ISO 27005	RA-1, RA-2, RA-3, RA-4, RA-5, RA-6
SS1	Anti-malware	A.12.2.1	SI-3
SS2	System and device hardening, and baseline security requirements	A.12.1, A.12.5, A.12.6	CM-1, CM-2, CM-3, CM-4, CM-6
SS3	Mobile device security	A.6.2.1, A.11.2.6, A.13.2.1	SC-8, SC-42, SC-43, SI-3, AC-17, AC-18, AC-19
SS4	Application configuration management	A.12.1, A.12..4.1	CM-3, CM-5, SA-10, SI-2
STR1	Information security strategy		PL-1, PL-2, PL-8, PL-9
TA1	Information security awareness program	§7.3, A.7.2.2	AT-1, AT-2, AT-3, AT-4, AT-5
TA2	Information security awareness,	§7.3, A.7.2.2	AT-1, AT-2, AT-3, AT-4, AT-5

Ref.	Control	ISO/IEC 27001	NIST SP800-53 Rev. 4
	education and training		
TPS1	Third party and suppliers due diligence	A.15	PS-7, SA-9, SA-12, AU-16, AC-17, IA-8
TPS2	Third party and supplier relationships	A.15	PS-7, SA-9, SA-12, AU-16, AC-17, IA-8
VM1	Vulnerability scanning and identification	A.12.6	RA-5, SA-22, SI-2
VM2	Documentation and reporting of vulnerabilities	A.12.6	
VM3	Vulnerability remediation and patching		RA-5, SA-22, SI-2

4.ΠΡΟΣΑΡΤΗΜΑ Γ: ΓΛΩΣΣΑΡΙΟ

Το παρόν παράρτημα παρέχει ορισμούς των βασικών όρων που χρησιμοποιούνται στο πλαίσιο μέτρων ασφαλείας. Οι ορισμοί μπορούν να χρησιμοποιηθούν ως ερμηνευτική βάση για τους ορισμούς που περιλαμβάνονται στις γενικές διατάξεις της νομοθεσίας.

Όρος	Αγγλικός Όρος	Περιγραφή
Στοιχείο ενεργητικού	Asset	An asset constitutes any resource that can be valuable for an organisation.
Επιφάνεια επίθεσης	Attack Surface	The collection of different points such as components, software or vulnerabilities (in a computing device or network) where an unauthorised or unauthenticated user can enter or extract data from an environment.
Επαλήθευση ταυτότητας	Authentication	The process of confirming a claimed characteristic of a user, device or other entity.
Διαθεσιμότητα	Availability	Ensuring that information or services are accessible when an authorized entity requires access.
Εμπιστευτικότητα	Confidentiality	Ensuring that information is not accessible to unauthorised users, processes or other entities.
Διαπιστευτήριο	Credential	Evidence used for validating or authenticating an identity.
Κρυπτογράφηση	Cryptography	Set of techniques for transforming data in order to hide its contents and prevent unauthorised modification or use.
Διαρροή δεδομένων	Data leakage	The (un)intentional exposure of secured information to an untrusted destination or recipient.
Απώλεια δεδομένων	Data loss	Event that leads to data being compromised, destroyed or stolen.
Άρνηση υπηρεσίας	Denial of Service	The intentional obstruction of access to services or resources.
Δέουσα επιμέλεια	Due diligence	The investigation of a process, person or business.
Συμβάν	Event	Manifestation or shift of a certain set of circumstances.
Τείχος προστασίας (firewall)	Firewall	A system that creates a barrier between different networks, which restricts and monitors traffic coming in from an untrusted network to a trusted network in order to protect the trusted network against various threats.
Θωράκιση / Σκλήρυνση	Hardening	Reducing the vulnerability surface of a system to improve security.
Περιστατικό	Incident	An event that has a potential or actual negative impact on the confidentiality, integrity or availability of a system.
Ακεραιότητα	Integrity	Integrity ensures the consistency, accuracy, and trustworthiness of data.
Κακόβουλο λογισμικό	Malware	Software that can perform an unauthorized process that has a negative impact on the integrity, availability or confidentiality of a resource. Examples include, but are not limited to, ransomware, virus, worm and spyware.
Ενημερώσεις Ασφάλειας	Patching	A set of changes made to software in order to fix bugs, weaknesses or vulnerabilities and enhance the performance of that software.
Περίμετρος δικτύου	Network perimeter	Boundary between the private/local part of a network and the public/provider part of a network or the internet.
Κίνδυνος	Risk	A risk is the likelihood of a threat exploiting a vulnerability resulting in an impact.
Απειλή	Threat	An event which could negatively impact an asset.
Πρωτόκολλο για τη σήμανση πληροφοριών	Traffic Light Protocol	Classification scheme defined by the FIRST.Org as a standard for information classification.
Ευπάθεια	Vulnerability	Weakness or error in an information system that could be exploited by a threat in order to compromise the security of the information system.
Εντοπισμός κινδύνων	Risk identification	Procedure of finding, listing and describing risks.
Ανάλυση κινδύνων	Risk analysis	Process of understanding the risk and determining the corresponding risk level.
Αξιολόγηση κινδύνων	Risk evaluation	Process of comparing the outcome of the risk analysis to defined risk criteria in order to assess which risks are tolerable.
Αντιμετώπιση κινδύνων	Risk treatment	Process of modifying the risk by lowering the likelihood or impact of the risk.

5.ΠΡΟΣΑΡΤΗΜΑ Δ: ΕΓΓΡΑΦΟ ΑΝΑΦΟΡΑΣ της ΟΜΑΔΑΣ ΣΥΝΕΡΓΑΣΙΑΣ NIS

Ο πιο κάτω πίνακας αποδεικνύει ότι οι έλεγχοι ασφάλειας, όπως περιγράφονται στο έγγραφο αναφοράς της Ομάδας Συνεργασίας NIS καλύπτονται από αυτό το Πλαίσιο Μέτρων Ασφάλειας.

NIS Cooperation Group Reference Document	Πλαίσιο Μέτρων Ασφάλειας ΑΨΑ
1. Governance and ecosystem	
1.1. Information System Security Governance & Risk Management	
Information system security risk analysis	RM4
Information system security policy	GOV1; GOV3
Information system security accreditation	RM2, RM3, RM4
Information system security indicators	STR1
Information system security audit	GOV3
Human resource security	HRS1, HRS2, HRS3, HRS4, HRS5, HRS6
1.2. Ecosystem Management	
Ecosystem mapping	TPS2
Ecosystem relations	TPS1
2. Protection	
2.1. IT Security Architecture	
Systems configuration	SS2
System segregation	NS2, SS2
Traffic filtering	NS1
Cryptography	AM5
2.2. IT Security Administration	
Administration accounts	GOV1, IAM1, IAM3
Administration information systems	GOV1, IAM1
2.3. Identity and Access Management	
Authentication and identification	IAM1, IAM4, IAM5
Access rights	IAM2, IAM3
2.4. IT Security Maintenance	
IT security maintenance procedure	AM5, IAM2, SS1
Industrial control systems	STR1, GOV2
2.5. Physical and Environmental Security	PS1, PS2, PS3, PS4, PS5
3. Defence	
3.1. Detection	
Detection	EIM1
Logging	AM3
Logs correlation and analysis	AM3
3.2. Computer Security Incident Management	
Information system security incident response	EIM1, EIM2, EIM3
Incident report	EIM5
Communication with competent authorities	EIM6
4. Resilience	
4.1. Continuity of operations	
Business continuity management	BCR1, BCR2, BCR3
Disaster recovery management	BCR4
4.2. Crisis management	
Crisis management organization	GOV3, BCR2
Crisis management process	GOV3, BCR2