Όνομα Οργανισμού

Πολιτική Διακυβέρνησης Ασφάλειας Πληροφοριών

|  |  |
| --- | --- |
| **Περιεχόμενο:** | Πολιτική Διακυβέρνησης Ασφάλειας Πληροφοριών |
| **Δημιουργός:** |  |
| **Έκδοση:** | 1.0 |
| **Ημερομηνία Έκδοσης:** | ηη/μμ/χχχχ |
| **Εμπιστευτικότητα:** |  |
| **Ιδιοκτήτης:** |  |

Διανομή

| Ρόλος | Όνομα | Οργανισμός | Τοποθεσία | Αριθμός Αντιτύπων |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Καταγραφή Τροποποιήσεων

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Κατάσταση Έκδοσης | Έκδοση | Ημερομηνία | Ενέργειες από | Περιγραφή |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Αναφορές

|  |  |  |
| --- | --- | --- |
| **Αρ.** |  | **Αναφορά Εγγράφου** |
| 1 |  |  |
| 2 |  |  |
| 3 |  |  |

Υποστηρικτικό Υλικό

|  |  |
| --- | --- |
| **Αρ.** | **Αναφορά** |
| 1 |  |
| 2 |  |
| 3 |  |

Ειδικό Λεξιλόγιο

Οι όροι και συντμήσεις ορίζονται πιο κάτω:

| Όροι και συντμήσεις | Περιγραφή |
| --- | --- |
|  |  |
|  |  |
|  |  |

Πίνακας Περιεχόμενων

[1. Εισαγωγή 4](#_Toc188364064)

[1.1. Σκοπός 4](#_Toc188364065)

[1.2. Πεδίο Εφαρμογής 4](#_Toc188364066)

[2. Οργανόγραμμα (Παράδειγμα) 5](#_Toc188364067)

[3. Ρόλοι και Αρμοδιότητες Ασφάλειας Πληροφοριών 6](#_Toc188364068)

[3.1. Ρόλοι και Αρμοδιότητες/Υποχρεώσεις Ανώτατης Διοίκησης 6](#_Toc188364069)

[3.2. Υπεύθυνος για την Ασφάλεια Δικτύων και Συστημάτων Πληροφοριών (ΥΑΠ) 7](#_Toc188364070)

[3.2.1. Ελάχιστες Αρμοδιότητες ΥΑΠ 8](#_Toc188364071)

[3.2.2. Θέση του Υπεύθυνου Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών 8](#_Toc188364072)

[3.3. Υπεύθυνος Επιχειρησιακής Συνέχειας και Αποκατάστασης από Καταστροφές 9](#_Toc188364073)

[3.4. Υπεύθυνοι επεξεργασίας πληροφοριών ή κάτοχοι πρόσβασης σε συστήματα επεξεργασίας πληροφοριών 10](#_Toc188364074)

[3.5. Διευθυντής Ασφάλειας Πληροφοριών 11](#_Toc188364075)

[3.6. Αναλυτές ασφάλειας πληροφοριών - Information Security Analysts 11](#_Toc188364076)

[3.7. Εκπαιδευτής ευαισθητοποίησης ασφάλειας- Security Awareness Trainer 12](#_Toc188364077)

[3.8. Steering Committee (Διευθύνουσα Επιτροπή) 12](#_Toc188364078)

[4. Συμμόρφωση με Νομικές και Κανονιστικές Υποχρεώσεις 13](#_Toc188364079)

[5. Αναθεώρηση 14](#_Toc188364080)

[6. Αναφορές 15](#_Toc188364081)

# Εισαγωγή

# Σκοπός

Το έγγραφο αυτό καθορίζει την Διακυβέρνηση της Ασφάλειας Πληροφοριών του [Όνομα Οργανισμού].

Η Διακυβέρνηση της Ασφάλειας Πληροφοριών μεταξύ άλλων περιλαμβάνει την Δήλωση Εφαρμογής Πλαισίου Κ.Δ.Π. 389/2020, καθώς και το Οργανόγραμμα του [Όνομα Οργανισμού].

Ακολούθως, περιλαμβάνει τις Υποχρεώσεις του Οργανισμού όσον αφορά την Ασφάλεια Πληροφοριών καθώς και τους Ρόλους και Αρμοδιότητες του Υπεύθυνου Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών, του Υπεύθυνου Επιχειρησιακής Συνέχειας και Αποκατάστασης από Καταστροφές, και των Υπεύθυνων επεξεργασίας πληροφοριών ή κατόχων πρόσβασης σε συστήματα επεξεργασίας πληροφοριών του [Όνομα Οργανισμού] έτσι όπως αναφέρονται στην Απόφαση Κ.Δ.Π. 389/2020.

Στην συνέχεια, περιλαμβάνει το κεντρικό αποθετήριο με τις νομικές, κανονιστικές, ρυθμιστικές και συμβατικές υποχρεώσεις σχετικά με την ασφάλεια δικτύων και πληροφοριών που ο [Όνομα Οργανισμού] οφείλει να συμμορφώνεται.

Ο [Όνομα Οργανισμού] έχει ως στόχο τη διεξαγωγή δραστηριοτήτων με επαγγελματικότητα, εφαρμόζοντας υψηλές προδιαγραφές για την παροχή υπηρεσιών, τόσο εσωτερικά όσο και εξωτερικά.

# Πεδίο Εφαρμογής

Αυτή η πολιτική ισχύει για όλους τους υπαλλήλους του [Όνομα Οργανισμού] που έχουν πρόσβαση στις πληροφορίες του Οργανισμού και στα πληροφοριακά συστήματα του συμπεριλαμβανομένων και των σταδίων που βρίσκονται οι πληροφορίες αυτές(αποθηκευμένες, σε κατάσταση μεταφοράς ή/ και κατά την διάθεση/καταστροφή τους).

# Οργανόγραμμα (Παράδειγμα)

**Υποσημείωση:** Ο κάθε οργανισμός δύναται να καθορίσει μόνο τους ρόλους οι οποίοι ευθυγραμμίζονται με τις ανάγκες και την δομή του και να απαλείψει τους ρόλους οι οποίοι δεν εφαρμόζονται σε κάθε περίπτωση. Επιπρόσθετα, ανάλογα με το μέγεθος του κάθε οργανισμού, θα υπάρχουν περιπτώσεις κατά τις οποίες δεν θα είναι εφικτός ο διορισμός ξεχωριστών ατόμων για τον κάθε ρόλο. Σε μια τέτοια περίπτωση ο οργανισμός δύναται να καθορίσει πέραν του ενός ρόλου σε ένα άτομο, νοουμένου ότι δεν θα προκύπτει σύγκρουση συμφέροντος μεταξύ των ρόλων αυτών.

# Ρόλοι και Αρμοδιότητες Ασφάλειας Πληροφοριών

Ο [Όνομα Οργανισμού] διαθέτει διακριτή οργανωτική μονάδα αρμόδια για την ασφάλεια δικτύων, συστημάτων και πληροφοριών του οργανισμού, με σαφείς ρόλους και αρμοδιότητες ώστε να μην υφίστανται περιπτώσεις αντικρουόμενων καθηκόντων όπως παρουσιάζεται στο πιο πάνω Οργανόγραμμα. Ο [Όνομα Οργανισμού] έχει ορίσει σαφείς ρόλους, αρμοδιότητες και ευθύνες όσον αφορά στην κυβερνοασφάλεια για το σύνολο του προσωπικού. Οι ρόλοι και οι αρμοδιότητες αναθεωρούνται περιοδικά με σκοπό την διασφάλιση της καταλληλόλητας τους. Ο [Όνομα Οργανισμού] εντοπίζει, αξιολογεί και αντιμετωπίζει οποιαδήποτε εμφάνιση αντικρουόμενων καθηκόντων

# Ρόλοι και Αρμοδιότητες/Υποχρεώσεις Ανώτατης Διοίκησης

Οι ρόλοι και οι αρμοδιότητες στην Ανώτατη Διοίκηση, το Διοικητικό Συμβούλιο (BoD - Board of Directors), και τα steering committees διαφέρουν ανάλογα με τη φύση του οργανισμού, τον τομέα δραστηριότητάς του, και την Οργανική δομή. Παρακάτω παρουσιάζονται γενικοί ρόλοι και αρμοδιότητες για κάθε επίπεδο:

Ανώτατη Διοίκηση:

1. Διευθύνων Σύμβουλος (CEO):

• Καθορίζει τη στρατηγική και την κατεύθυνση του οργανισμού.

• Υπεύθυνος για την επίτευξη των επιχειρηματικών στόχων.

• Αντιπροσωπεύει τον οργανισμό εξωτερικά.

1. Πρόεδρος:

• Διευθύνει τις συνεδριάσεις του Διοικητικού Συμβουλίου.

• Συνεργάζεται στενά με τον CEO για την ανάπτυξη και εφαρμογή στρατηγικών.

1. Διευθυντική Ομάδα:

• Υλοποιεί τις αποφάσεις της Ανώτατης Διοίκησης.

• Διαχειρίζεται τις λειτουργικές πτυχές του οργανισμού.

Διοικητικό Συμβούλιο (BoD):

1. Μέλη του Διοικητικού Συμβουλίου:

• Αναλαμβάνουν την εποπτεία των δραστηριοτήτων της Ανώτατης Διοίκησης.

• Καθορίζουν πολιτικές, παρακολουθούν τη στρατηγική κατεύθυνση.

1. Πρόεδρος του Διοικητικού Συμβουλίου:

• Διευθύνει τις συνεδριάσεις του BoD.

• Εκπροσωπεί το BoD προς την Ανώτατη Διοίκηση.

Steering Committee (Διευθύνουσα Επιτροπή):

1. Πρόεδρος του Steering Committee:

• Διοικεί τις συνεδριάσεις και συντονίζει τις δραστηριότητες του steering committee.

• Συνεργάζεται με την Ανώτατη Διοίκηση για την υλοποίηση συγκεκριμένων στρατηγικών.

1. Μέλη του Steering Committee:

• Συμβουλεύουν για τα θέματα που σχετίζονται με τον τομέα τους.

• Συνεργάζονται με την Ανώτατη Διοίκηση για την εφαρμογή προγραμμάτων.

Κάθε επίπεδο στην ιεραρχία και η συνεργασία μεταξύ αυτών των επιπέδων θεωρείται ως κρίσιμος παράγοντας στη λήψη αποφάσεων, την εποπτεία, και την υλοποίηση των στόχων του Οργανισμού.

# Υπεύθυνος για την Ασφάλεια Δικτύων και Συστημάτων Πληροφοριών (ΥΑΠ)

Ο [Όνομα Οργανισμού], στα πλαίσια εφαρμογής της Απόφασης Κ.Δ.Π 389/2020, έχει ορίσει στέλεχος κατάλληλο και με επαρκή εμπειρία στην Ασφάλεια Δικτύων & Πληροφοριών ως Υπεύθυνο Ασφάλειας Δικτύων, Συστημάτων και Πληροφοριών (ΥΑΠ) και έχει κοινοποιήσει τα στοιχεία επικοινωνίας τους στις ανάλογες Αρχές.

* Ο ΥΑΠ έχει διοριστεί βάσει επαγγελματικών προσόντων και κυρίως βάσει ειδικών γνώσεων στον τομέα της ασφάλειας δικτύων και συστημάτων πληροφοριών και της ικανότητας εκπλήρωσης των καθηκόντων που αναφέρονται στο πιο κάτω (Ελάχιστες Αρμοδιότητες).
* Ο ΥΑΠ εκτελεί αποκλειστικά καθήκοντα σχετικά με την Ασφάλεια Δικτύων, Συστημάτων & Πληροφοριών και δεν μπορεί παράλληλα να απασχολείται για καθήκοντα εκτός αυτών . Στην περίπτωση όπου ο οργανισμός είναι μικρός, ο υπεύθυνος Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών δύναται να εκτελεί και άλλα καθήκοντα εφόσον δεν οδηγούν σε σύγκρουση συμφερόντων και λαμβάνοντας υπόψη το επίπεδο κρισιμότητας του οργανισμού, με την έγκριση της Αρχής Ψηφιακής Ασφάλειας.
* Ο [Όνομα Οργανισμού] έχει κοινοποιήσει στην Αρχή Ψηφιακής Ασφάλειας τα στοιχεία επικοινωνίας του υπεύθυνου ΥΑΠ.
* Ο [Όνομα Οργανισμού] έχει διασφαλίσει ότι οι υποψήφιοι για τη θέση του υπεύθυνου ΥΑΠ έχουν ελεγχθεί επαρκώς, ώστε να εξασφαλιστεί ότι το εν λόγω πρόσωπο θα διεκπεραιώνει τα καθήκοντά του δεόντως. Η καταλληλόλητα του ΥΑΠ αξιολογείται περιοδικά.

# Ελάχιστες Αρμοδιότητες ΥΑΠ

Ο ΥΑΠ που έχει οριστεί από τον [Όνομα Οργανισμού] έχει τουλάχιστον τις ακόλουθες αρμοδιότητες/καθήκοντα:

* Να ενημερώνει και να συμβουλεύει τον [Όνομα Οργανισμού] και τους υπαλλήλους που έχουν πρόσβαση στα συστήματα δικτύων και πληροφοριών τους σχετικά με τις υποχρεώσεις τους σύμφωνα με την Απόφαση Κ.Δ.Π. 389/2020 και άλλες σχετικές νομικές και κανονιστικές υποχρεώσεις
* Να παρακολουθεί τη συμμόρφωση με την Απόφαση Κ.Δ.Π. 389/2020, με άλλες εθνικές ή ευρωπαϊκές πρόνοιες για την ασφάλεια πληροφοριών, και με τις πολιτικές του [Όνομα Οργανισμού] σε σχέση με την ασφάλεια δικτύων και συστημάτων πληροφοριών.
* Να παρέχει συμβουλές όσον αφορά τη διαχείριση της ασφάλειας πληροφοριών και να παρακολουθεί τις επιδόσεις της σύμφωνα με την μεθοδολογία και διαδικασία διαχείρισης κινδύνου.
* Να συνεργάζεται και να ενεργεί ως ενιαίο σημείο επαφής με την Αρχή Ψηφιακής Ασφάλειας για θέματα που σχετίζονται με τις δραστηριότητες της Αρχής Ψηφιακής Ασφάλειας στο πλαίσιο αρμοδιοτήτων της, μεταξύ άλλων με την παροχή υποστήριξης σε δραστηριότητες εξωτερικού ελέγχου, με την εκ των προτέρων παροχή εγγράφων και πληροφοριών στην Αρχή Ψηφιακής Ασφάλειας, όπως αναφέρεται στο Άρθρο 13 της Απόφασης Κ.Δ.Π. 389/2020.
* Να παρέχει αναφορές σχετικά με απειλές για την ασφάλεια πληροφοριών, ευπάθειες και κινδύνους προς τη διοίκηση ανώτατου επιπέδου μέσω επίσημων και τακτικών εκθέσεων.
* 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 Απόφασης Κ.Δ.Π. 389/2020. Ο [Όνομα Οργανισμού] υποβάλλει στην Αρχή Ψηφιακής Ασφάλειας πληροφορίες για την αξιολόγηση κινδύνων που διενεργεί, ως αναφέρονται στο Άρθρο 13, με στόχο την ενημέρωση της Αρχής Ψηφιακής Ασφάλειας.

# Θέση του Υπεύθυνου Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών

Ο [Όνομα Οργανισμού] διασφαλίζει ότι ο υπεύθυνος Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών συμμετέχει δεόντως και εγκαίρως σε όλα τα ζητήματα που σχετίζονται με την ασφάλεια δικτύων και συστημάτων πληροφοριών:

1. Ο [Όνομα Οργανισμού] υποστηρίζει τον υπεύθυνο Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών στην εκτέλεση των καθηκόντων του, όπως αναφέρονται πιο πάνω (Ελάχιστες Αρμοδιότητες).
2. Ο [Όνομα Οργανισμού] μεριμνά ώστε ο υπεύθυνος Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών να μην λαμβάνει οδηγίες που έρχονται σε σύγκρουση με την άσκηση των καθηκόντων του. Δεν απολύεται ούτε τιμωρείται από τον [Όνομα Οργανισμού] για τη δέουσα εκτέλεση των καθηκόντων του.
3. Ο υπεύθυνος Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών αναφέρεται απευθείας στο ανώτατο διοικητικό επίπεδο του [Όνομα Οργανισμού] όσον αφορά τα καθήκοντα του που καθορίζονται στο Κ.Δ.Π. 389/2020.
4. Ο υπεύθυνος Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών δεσμεύεται από κανόνες εμπιστευτικότητας και επαγγελματικού απορρήτου όσον αφορά την εκτέλεση των καθηκόντων του.
5. Ο [Όνομα Οργανισμού] διασφαλίζει ότι ο υπεύθυνος Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών 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 Ψηφιακής Ασφάλειας.
6. Ο [Όνομα Οργανισμού] διασφαλίζει ότι ο υπεύθυνος Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών έχει τις κατάλληλες γνώσεις, εκπαίδευση και εμπειρία που να συνάδουν με τα καθήκοντα του και ότι ο υπεύθυνος Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών αναβαθμίζει σε τακτά χρονικά διαστήματα τις γνώσεις του. Η Αρχή Ψηφιακής Ασφάλειας δύναται να παρέχει κατευθυντήριες οδηγίες για θέματα σχετικά με την κατάλληλη εκπαίδευση και εμπειρία του υπεύθυνου Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών.

# Υπεύθυνος Επιχειρησιακής Συνέχειας και Αποκατάστασης από Καταστροφές

Ο Υπεύθυνος Επιχειρησιακής Συνέχειας και Αποκατάστασης από Καταστροφές είναι υπεύθυνος για το συντονισμό του Πλάνου Επιχειρησιακής Συνέχειας και του Πλάνου Αποκατάστασης από Καταστροφές, σε περίπτωση διακοπής της επιχειρησιακής λειτουργίας του [Όνομα Οργανισμού] και για το σχεδιασμό των δύο αυτών Πλάνων.

Επιπρόσθετα είναι υπεύθυνος για τη διανομή των Πλάνων στο προσωπικό που εμπλέκεται σε διαδικασίες αποκατάστασης κρίσιμων επιχειρησιακών λειτουργιών και αποκατάστασης επιχειρήσεων.

Συγκεκριμένα, ο Υπεύθυνος Επιχειρησιακής Συνέχειας και Αποκατάστασης από Καταστροφές είναι υπεύθυνος για:

* Τον προσδιορισμό και την αξιολόγηση κρίσιμων επιχειρηματικών διαδικασιών που θα συμπεριληφθούν στο Πλάνο Επιχειρησιακής Συνέχειας και στο Πλάνο Αποκατάστασης από Καταστροφές.
* Την εποπτεία και τον συντονισμό:
  + Της αξιολόγησης κινδύνων και των επιπτώσεών τους.
  + Της αξιολόγησης επάρκειας και συμβατότητας των Πλάνων με τα επιχειρηματικά σχέδια.
* Τη διατήρηση αρχείων σχετικά με τις αναθεωρήσεις και ενημερώσεις του Πλάνου Επιχειρησιακής Συνέχειας και του Πλάνου Αποκατάστασης από Καταστροφές και για την παρακολούθηση πιθανών αλλαγών στον [Όνομα Οργανισμού] , οι οποίες ενδέχεται να απαιτούν ανασκόπηση του Πλάνου Επιχειρησιακής Συνέχειας και του Πλάνου Αποκατάστασης από Καταστροφές.
* Την εποπτεία του επιπέδου ετοιμότητας των εναλλακτικών τοποθεσιών αποκατάστασης κρίσιμών επιχειρησιακών λειτουργιών (όπου ισχύει) σχετικά με τους πόρους και τις εφαρμογές.
* Τον εντοπισμό του συμβάντος που είναι υπεύθυνο για την διακοπή της επιχειρηματικής λειτουργίας και την επιβολή των σχετικών σχεδίων (π.χ. Πολιτική Διαχείρισης Συμβάντων και Περιστατικών, Σχέδιο Διαχείρισης Κρίσεων και Σχέδιο Αποκατάστασης από Καταστροφές)
* Την υπόδειξη ενός κατάλληλου χώρου ως εναλλακτική τοποθεσία αποκατάστασης κρίσιμων επιχειρησιακών λειτουργιών, στην περίπτωση που απαιτείται η μετάθεση σε έναν τέτοιο εναλλακτικό χώρο αποκατάστασης κρίσιμων επιχειρησιακών λειτουργιών μετά από διακοπή της επιχειρησιακής λειτουργίας.
* Το συντονισμό και την εποπτεία της αποκατάστασης των κρίσιμων επιχειρησιακών λειτουργιών και των επιχειρησιακών διαδικασιών που εξασφαλίζουν τη συνεχή λειτουργία του [Όνομα Οργανισμού].
* Το συντονισμό των διαδικασιών των σχεδίων ασφάλειας των υποδομών και των εγκαταστάσεων, σε περίπτωση μετεγκατάστασης σε εναλλακτική τοποθεσία.
* Την εποπτεία της μεταφοράς και της διαχείρισης των εργαζομένων καθώς και του απαραίτητου εξοπλισμού στον εναλλακτικό χώρο αποκατάστασης κρίσιμων επιχειρησιακών λειτουργιών (όπου εφαρμόζεται).
* Τη διαχείριση ζητημάτων σχετικά με το Ανθρώπινο Δυναμικό που προκύπτουν από την εφαρμογή ή τον έλεγχο του Πλάνου Επιχειρησιακής Συνέχειας και του Πλάνου Αποκατάστασης από Καταστροφές.
* Την ανασκόπηση, τον έλεγχο και των αναθεώρηση του Πλάνου Επιχειρησιακής Συνέχειας και του Πλάνου Αποκατάστασης από Καταστροφές.
* Τον προγραμματισμό και το συντονισμό στην εκτέλεση δράσεων για τη συνεχή ενημέρωση και εκπαίδευση των μελών που εμπλέκονται στο Πλάνο Επιχειρησιακής Συνέχειας και στο Πλάνο Αποκατάστασης από Καταστροφές.

# Υπεύθυνοι επεξεργασίας πληροφοριών ή κάτοχοι πρόσβασης σε συστήματα επεξεργασίας πληροφοριών

|  |  |  |  |
| --- | --- | --- | --- |
| Ονοματεπώνυμο | Τίτλος | Ρόλοι και αρμοδιότητες | Σχετικές Προσβάσεις |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Διευθυντής Ασφάλειας Πληροφοριών

Ο CISO, ή ο επικεφαλής υπεύθυνος ασφάλειας πληροφοριών, είναι ένα ανώτερο στέλεχος που επιβλέπει την ασφάλεια πληροφοριών, κυβερνοχώρου και τεχνολογίας ενός οργανισμού. Οι αρμοδιότητες του CISO περιλαμβάνουν την ανάπτυξη, την εφαρμογή και την επιβολή πολιτικών ασφαλείας για την προστασία κρίσιμων δεδομένων. Οι ακριβείς ευθύνες θα διαφέρουν ανάλογα με τον οργανισμό. Παραδοσιακά, ένας CISO εστιάζει στην ανάπτυξη και την καθοδήγηση του προγράμματος ασφάλειας πληροφοριών. Αυτό περιλαμβάνει την προστασία των περιουσιακών στοιχείων, των εφαρμογών, των συστημάτων και της τεχνολογίας του οργανισμού, ενώ παράλληλα επιτρέπει και προωθεί τα επιχειρηματικά αποτελέσματα.

# Αναλυτές ασφάλειας πληροφοριών - Information Security Analysts

Οι Αναλυτές Ασφάλειας Πληροφοριών (Information Security Analysts) αναλαμβάνουν τον ρόλο της παρακολούθησης και ανάλυσης των συστημάτων ασφαλείας. Είναι υπεύθυνοι για τον εντοπισμό και τον χειρισμό απειλών, την εφαρμογή ασφαλιστικών μέτρων, και τη διαχείριση περιστατικών ασφαλείας. Επίσης, συμμετέχουν στην ανάπτυξη και την εφαρμογή πολιτικών ασφαλείας και στην εκπαίδευση του προσωπικού.

Οι αναλυτές ασφάλειας πληροφοριών κάνουν συνήθως τα εξής:

* + - Παρακολουθούν τα δίκτυα του οργανισμού τους για παραβιάσεις ασφάλειας και διερευνούν πότε έχουν συμβεί.
    - Χρησιμοποιούν και διατηρούν λογισμικό, όπως τείχη προστασίας και προγράμματα κρυπτογράφησης δεδομένων, για την προστασία ευαίσθητων πληροφοριών.
    - Ελέγχουν για τρωτά σημεία σε συστήματα υπολογιστών και δικτύου.
    - Ερευνούν τις τελευταίες τάσεις ασφάλειας της τεχνολογίας πληροφοριών (IT).
    - Προετοιμάζουν αναφορές που τεκμηριώνουν γενικές μετρήσεις, απόπειρες επιθέσεων και παραβιάσεις ασφάλειας.
    - Να αναπτύξουν πρότυπα ασφαλείας και βέλτιστες πρακτικές για τον οργανισμό
    - Προτείνουν βελτιώσεις ασφαλείας στη διοίκηση ή στο ανώτερο προσωπικό πληροφορικής. Οι αναλυτές ασφάλειας πληροφοριών δύναται να σχεδιάζουν και εκτελούν μέτρα ασφαλείας για την προστασία των δικτύων και των συστημάτων υπολογιστών ενός οργανισμού.
    - Βοηθούν τους χρήστες υπολογιστών όταν πρέπει να εγκαταστήσουν ή να μάθουν για νέα προϊόντα και διαδικασίες ασφαλείας.
* Παραμένουν ενημερωμένοι για την ασφάλεια πληροφορικής και για τις πιο πρόσφατες μεθόδους που χρησιμοποιούν οι εισβολείς για να διεισδύσουν σε συστήματα υπολογιστών. Οι αναλυτές πρέπει να ερευνήσουν νέες τεχνολογίες ασφαλείας για να αποφασίσουν τι θα προστατεύσει αποτελεσματικότερα τον οργανισμό τους.

# Εκπαιδευτής ευαισθητοποίησης ασφάλειας- Security Awareness Trainer

Ο Εκπαιδευτής ευαισθητοποίησης για την ασφάλεια (Security Awareness Trainer) είναι υπεύθυνος για την εκπαίδευση και ευαισθητοποίηση του προσωπικού σχετικά με τις βέλτιστες πρακτικές ασφαλείας. Αναπτύσσει εκπαιδευτικά προγράμματα και υλικό, προωθεί τη συνείδηση των απειλών και την ανάγκη συμμόρφωσης με τις πολιτικές ασφαλείας. Επικεντρώνεται στην ανάπτυξη μιας ασφαλούς πολιτιστικής συμπεριφοράς στον οργανισμό, βελτιώνοντας την ευαισθητοποίηση των εργαζομένων σε θέματα ασφαλείας.

Άλλα καθήκοντα μπορεί να περιλαμβάνουν, αλλά δεν περιορίζονται σε:

* + - Εκπαίδευση και διαχείριση τεχνολογικού κινδύνου σε συνεργασία τη Διεύθυνση του Οργανισμού.
    - Ανάπτυξη και εφαρμογή συνεχούς εκπαίδευσης και εκπαίδευσης ευαισθητοποίησης για την ασφάλεια των χρηστών.
    - Η οικοδόμηση και η οδήγηση στρατηγικής και πλαισίου κυβερνοασφάλειας, με πρωτοβουλίες για τη διασφάλιση των περιουσιακών στοιχείων στον κυβερνοχώρο και της τεχνολογίας του οργανισμού.
    - Εφαρμογή και διαχείριση της διαδικασίας διακυβέρνησης, κινδύνου και συμμόρφωσης (GRC).
    - Δοκιμές phishing για να διδάξουν στους υπαλλήλους πώς να αναγνωρίζουν αυτές τις επιθέσεις.
    - Μια πρακτική ανάλυση των κοινών επιθέσεων στον κυβερνοχώρο.
    - Αναφορά στα υψηλότερα επίπεδα του οργανισμού (ο Διευθύνων Σύμβουλος και το διοικητικό συμβούλιο, ή ισοδύναμο).
    - Ανάπτυξη, αιτιολόγηση και αξιολόγηση επενδύσεων στον κυβερνοχώρο.

# Steering Committee (Διευθύνουσα Επιτροπή)

Η Διευθύνουσα Επιτροπή ή άλλη κατάλληλη επιτροπή εκτελεστικού επιπέδου, θα πρέπει να παρέχει στη διοίκηση προσδοκίες, μαζί με τη λογοδοσία, για την επίβλεψη, τον συντονισμό και την ανάθεση της ευθύνης για την αποτελεσματικότητα του προγράμματος κυβερνοασφάλειας. Η εμπειρογνωμοσύνη στον τομέα της κυβερνοασφάλειας θα πρέπει να διατηρείται από αυτή την Επιτροπή. Εάν χρειάζεται, η Επιτροπή θα πρέπει να προσλάβει εξωτερικούς εμπειρογνώμονες με την κατάλληλη πείρα για να βοηθήσουν στις αρμοδιότητες επίβλεψης.

Η Επιτροπή θα πρέπει να επανεξετάζει τις εκθέσεις αξιολόγησης που περιγράφουν την αποτελεσματικότητα του προγράμματος κυβερνοασφάλειας σε τακτική βάση (π.χ. τουλάχιστον ετησίως). Οι συστάσεις για διορθωτικές ενέργειες θα πρέπει να συζητούνται όποτε απαιτείται. Η Επιτροπή θα πρέπει να διασφαλίζει ότι οι ετήσιες αυτοαξιολογήσεις αξιολογούν την ικανότητα του οργανισμού να ανταποκρίνεται σε καθορισμένες απαιτήσεις ασφάλειας στον κυβερνοχώρο. Η Επιτροπή θα πρέπει να εγκρίνει την ιεράρχηση των δραστηριοτήτων αποκατάστασης, συμπεριλαμβανομένης της κατανομής πόρων, με βάση τα αποτελέσματα της αξιολόγησης.

Η Επιτροπή θα πρέπει να είναι υπεύθυνο για τη διατήρηση μιας διαδικασίας για την επίσημη συζήτηση και εκτίμηση των πιθανών δαπανών που σχετίζονται με περιστατικά κυβερνοασφάλειας και παραβιάσεις δεδομένων ως μέρος της διαδικασίας κατάρτισης προϋπολογισμού. Θα πρέπει επίσης να διασφαλίζει ότι η διοίκηση λαμβάνει τις κατάλληλες ενέργειες για την αντιμετώπιση μεταβαλλόμενων κινδύνων στον κυβερνοχώρο ή σημαντικών ζητημάτων ασφάλειας στον κυβερνοχώρο.

# Συμμόρφωση με Νομικές και Κανονιστικές Υποχρεώσεις

Ο [Όνομα Οργανισμού] να διατηρεί κεντρικό μητρώο νομικών, κανονιστικών ρυθμιστικών και συμβατικών υποχρεώσεων όσον αφορά την ασφάλεια δικτύων και πληροφοριών.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Α/Α** | **Νομοθεσία/Κανονισμός/Οδηγία** | **Αριθμός νομοθετήματος (πιο πρόσφατου)** | **Είδος** | **Ημερομηνία τελευταίας τροποποίησης** |
| **1** | ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2016/679 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών | 2016/679 | Νομοθεσία | 04/05/2016 |
| **2** | Ο ΠΕΡΙ ΑΣΦΑΛΕΙΑΣ ΔΙΚΤΥΩΝ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΩΝ ΝΟΜΟΣ ΤΟΥ 2020 | Κ.Δ.Π. 389/2020 | Νομοθεσία | 21/08/2020 |
| **3** | ΟΔΗΓΙΑ (ΕΕ) 2022/2555 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, την τροποποίηση του κανονισμού (ΕΕ) αριθ. 910/2014 και της οδηγίας (ΕΕ) 2018/1972, και για την κατάργηση της οδηγίας (ΕΕ) 2016/1148 (οδηγία NIS 2) | 2022/2555 | Οδηγία | 14/12/2022 |

Πρέπει να διενεργείται εσωτερικός έλεγχος, τουλάχιστον σε ετήσια βάση, για την διαπίστωση της συμμόρφωσης με όλες τις σχετικές νομοθετικές, κανονιστικές και ρυθμιστικές απαιτήσεις, και συμβατικές απαιτήσεις όσον αφορά την ασφάλεια δικτύων και πληροφοριών

2.2.3 Ο [Όνομα Οργανισμού] πρέπει να δημιουργεί πλάνο ενεργειών συμμόρφωσης σε περίπτωση που αναγνωριστεί απόκλιση σε μία ή περισσότερες απαιτήσεις.

# Αναθεώρηση

Ιδιοκτήτης της υφιστάμενης πολιτικής είναι ο/η [Τίτλος Ιδιοκτήτη] , ο/η οποίος/α είναι υπεύθυνος/η για την εφαρμογή, τήρηση και αναθεώρηση της πολιτικής αυτής, σύμφωνα με τις ακόλουθες κατευθυντήριες γραμμές:

* Σημαντικές αλλαγές στον Οργανισμό.
* Περιστατικά ασφάλειας πληροφοριών ή κανονιστικές αλλαγές.
* Ετήσια αναθεώρηση, εφόσον προκύπτει η ανάγκη για:
  + Βελτίωση της αποτελεσματικότητας της πολιτικής.
  + Ενημέρωση της για αλλαγές στην τεχνολογία.

# Αναφορές

|  |  |  |  |
| --- | --- | --- | --- |
| **Κατηγορία** | **ID** | **Μέτρο** | **Στόχος 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. |
| 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. |
| 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. |
| 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 τη στρατηγική ασφάλειας πληροφοριών. |