Όνομα Οργανισμού

Στρατηγική Ασφάλειας Πληροφοριών

|  |  |
| --- | --- |
| **Περιεχόμενο:** | Στρατηγική 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 Περιεχομένων

[Πίνακας Περιεχομένων 3](#_Toc157764361)

[1. Εισαγωγή 5](#_Toc157764362)

[2. Σκοπός 5](#_Toc157764363)

[3. Όραμα και Περιορισμοί 6](#_Toc157764364)

[4. Στόχοι Στρατηγικής Ασφάλειας Πληροφοριών 6](#_Toc157764365)

[5. Ευθυγράμμιση της Στρατηγικής Ασφάλειας Πληροφοριών με την Επιχειρησιακή Στρατηγική: 8](#_Toc157764366)

[6. Βασικές Πρωτοβουλίες σε Σχέση με την Κυβερνοασφάλεια 9](#_Toc157764367)

[6.1. Πλάνο Υλοποίησης Στρατηγικών Παρεμβάσεων Κυβερνοασφάλειας (Παράδειγμα) 10](#_Toc157764368)

[7. Αιτιολογημένη Κατανομή Προϋπολογισμού και Πόρων για την Κυβερνοασφάλεια: 10](#_Toc157764369)

[8. Δήλωση Πεδίου Εφαρμογής Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών 11](#_Toc157764370)

[9. Υποστηρικτικοί Οργανισμοί 11](#_Toc157764371)

[10. Στοιχεία Ενεργητικού 11](#_Toc157764372)

[11. Άτομα 12](#_Toc157764373)

[12. Πλαίσιο Διαχείρισης 12](#_Toc157764374)

[12.1. Διευθυντής 14](#_Toc157764387)

[12.2. Καθοδηγητική Επιτροπή Ασφάλειας Πληροφοριών 14](#_Toc157764388)

[Συχνότητα συσκέψεων / συνεδριάσεων 14](#_Toc157764391)

[Μέλη της Καθοδηγητικής Επιτροπής 15](#_Toc157764392)

[Ενημέρωση της Διεύθυνσης 15](#_Toc157764393)

[12.3. Προϊστάμενος Ασφάλειας Πληροφοριών 16](#_Toc157764401)

[12.4. Λειτουργός Ασφάλειας Πληροφοριών 17](#_Toc157764402)

[12.5. Άλλοι υπάλληλοι του Οργανισμού 18](#_Toc157764403)

[12.5.1 Προϊστάμενοι Τμημάτων 18](#_Toc157764404)

[12.5.2 Όλο το Προσωπικό 18](#_Toc157764405)

[12.5.3 Ιδιοκτήτες Πληροφοριών 18](#_Toc157764406)

[13. Μηχανισμός Υποβολής Εκθέσεων προς την Ανώτατη Διοίκηση (Top Management) 19](#_Toc157764407)

[14. Εκθέσεις Ασφάλειας Πληροφοριών / Μετρήσεις Απόδοσης 19](#_Toc157764408)

[15. Προσέγγιση Διαχείρισης Κινδύνου 19](#_Toc157764409)

[16. Εκπαίδευση και Ενημέρωση 20](#_Toc157764410)

[17. Πόροι 21](#_Toc157764411)

[18. Δέσμευση Διοίκησης 21](#_Toc157764412)

[19. Διαχείριση Συμβάντων Ασφαλείας Πληροφοριών 22](#_Toc157764413)

[20. Εποπτεία και Αναθεώρηση του Συστήματος 22](#_Toc157764414)

[21. Αξιολογήσεις της Συμμόρφωσης 22](#_Toc157764415)

[22. Διορθωτικές / Προληπτικές Ενέργειες 23](#_Toc157764416)

[23. Διαχείριση Κύκλου Ζωής του Εγγράφου της Στρατηγικής 24](#_Toc157764417)

[24. Νομοθετικές Πράξεις 25](#_Toc157764418)

# Εισαγωγή

Σύμφωνα με τον Κανονισμό Κ.Δ.Π. 389/2020, ο [Όνομα Οργανισμού]υ θεσπίζει την Στρατηγική Ασφάλειας Πληροφοριών στην οποία να αναλύονται οι στόχοι και η προσέγγιση υψηλού επιπέδου, με σκοπό τον μετριασμό των κινδύνων για την ασφάλεια πληροφοριών. Περιγράφονται λεπτομερώς συγκεκριμένοι στόχοι αναφορικά με την ασφάλεια, καθώς η 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.

Έχουν συνταχθεί πολιτικές ώστε να παρέχουν κατευθυντήριες γραμμές σε συγκεκριμένα ζητήματα όπως την αναφορά περιστατικών και την επιχειρησιακή συνέχεια, καθώς και δικλείδες ασφαλείας για την τήρηση των επιχειρησιακών στόχων. Οι πληροφορίες αυτές θα πρέπει να είναι διαθέσιμες στα Τμήματα / Υπηρεσίες ανά πάσα στιγμή και να διασφαλίζεται η ακεραιότητα και η εμπιστευτικότητα των πληροφοριών.

# Σκοπός

Η Στρατηγική Ασφάλειας Πληροφοριών έχει ως στόχο να διασφαλίσει την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα των πληροφοριών του [Όνομα Οργανισμού]. Αυτό επιτυγχάνεται μέσω της υλοποίησης προηγμένων πρακτικών κυβερνοασφάλειας, της εκπαίδευσης του προσωπικού, της συνεχούς ανάλυσης κινδύνων και της συνεχούς βελτίωσης των μέτρων ασφαλείας. Κάποιες από τις στρατηγικές επιδιώξεις είναι:

* Ανάπτυξη μέτρων ασφαλείας για την προστασία ευαίσθητων πληροφοριών και προσωπικών δεδομένων.
* Καθορισμός στρατηγικών για τον εντοπισμό, την πρόληψη και την αντιμετώπιση κυβερνοαπειλών.
* Εκπαίδευση του προσωπικού για την αναγνώριση και αντίδραση σε κυβερνοαπειλές.
* Διασφάλιση συμμόρφωσης με την ισχύουσα νομοθεσία, όπως η οδηγία NIS2 και άλλες σχετικές νομοθετικές απαιτήσεις.
* Εφαρμογή ευέλικτων και καινοτόμων λύσεων ασφαλείας για αντιμετώπιση νέων απειλών και τεχνολογικών εξελίξεων.
* Ανάπτυξη στενών σχέσεων και συνεργασία με εταίρους και προμηθευτές για την ενίσχυση της κυβερνοασφάλειας σε ολόκληρη την αλυσίδα.
* Εγκατάσταση ενός αποτελεσματικού, τεκμηριωμένου Σύστηματος Διαχείρισης Ασφάλειας Πληροφοριών για να προστατεύσει τις πληροφορίες του από απειλές (εσωτερικές ή εξωτερικές, σκόπιμες ή τυχαίες).

Σκοπός του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών είναι να:

* μειωθεί σε αποδεκτό επίπεδο ο κίνδυνος που διατρέχει ο [Όνομα Οργανισμού] σε σχέση με την ασφάλεια πληροφοριών
* διαφυλαχθεί η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα των πληροφοριών, σε ταύτιση με τις επιχειρησιακές ανάγκες του [Όνομα Οργανισμού]
* διασφαλιστεί ότι τα περιουσιακά στοιχεία και οι πληροφορίες του προστατεύονται κατάλληλα και παραμένουν διαθέσιμα σύμφωνα με τις απαιτήσεις του [Όνομα Οργανισμού] παρέχονται τα κατάλληλα τεκμήρια ότι εφαρμόζονται οι διαδικασίες.

# Όραμα και Περιορισμοί

Το όραμα της στρατηγικής ασφάλειας πληροφοριών εντάσσεται στο ευρύτερο πλαίσιο της ασφάλειας του [Όνομα Οργανισμού]. Στο μέλλον, ο [Όνομα Οργανισμού] οραματίζεται να διακρίνεται για την υψηλή τεχνική εμπειρογνωμοσύνη της και την άρτια εφαρμογή μέτρων ασφαλείας πληροφοριών.

Το επιθυμητό στάδιο περιλαμβάνει την πλήρη ενσωμάτωση των προηγμένων μέτρων ασφαλείας πληροφοριών σε όλες τις πτυχές των επιχειρηματικών δραστηριοτήτων του [Όνομα Οργανισμού], για την αντιμετώπιση των κυβερνοαπειλών και τη διασφάλιση της εμπιστευτικότητας, της διαθεσιμότητας και της ακεραιότητας των πληροφοριών του οργανισμού.

Οι στόχοι της στρατηγικής ασφάλειας πληροφοριών συνδέονται άμεσα με την επιχειρηματική μας δραστηριότητα:

* Προστασία Ευαίσθητων Δεδομένων: Εξασφάλιση της εμπιστευτικότητας των πελατών και εταίρων μέσω αποτελεσματικών μέτρων προστασίας δεδομένων.
* Αντιμετώπιση Κινδύνων Κυβερνοασφάλειας: Ανάπτυξη στρατηγικών για την αντιμετώπιση επιθέσεων και την προληπτική προστασία από κυβερνοεπιθέσεις.
* Συνεχής Λειτουργικότητα: Διασφάλιση της συνεχούς λειτουργίας των πληροφοριακών συστημάτων, επιτρέποντας την ομαλή διεξαγωγή των επιχειρηματικών δραστηριοτήτων.

Οι βασικοί περιορισμοί είναι:

* Νομικές Υποχρεώσεις: Συμμόρφωση με τους νόμους περί προστασίας δεδομένων και άλλες σχετικές νομικές υποχρεώσεις.
* Φυσικοί και Περιβαλλοντικοί Παράγοντες: Αντιμετώπιση των φυσικών κινδύνων (π.χ., φυσικές καταστροφές) και περιβαλλοντικών παραγόντων που μπορεί να επηρεάσουν την ασφάλεια των πληροφοριών.
* Οργανωτική Δομή και Κουλτούρα: Ενσωμάτωση των μέτρων ασφαλείας στην οργανωτική δομή και προώθηση μιας κουλτούρας ασφάλειας σε όλα τα επίπεδα του προσωπικού.

# Στόχοι Στρατηγικής Ασφάλειας Πληροφοριών

Η ιεράρχηση των προτεραιοτήτων της Στρατηγικής Κυβερνοασφάλειας και οι στόχοι σε σχέση με την ασφάλεια πληροφοριών και οι σχετικές ενέργειες για υλοποίηση τους σε επίπεδο executive level παρατίθενται ως εξής:

1. Ανάπτυξη και Εφαρμογή Πολιτικής Κυβερνοασφάλειας
* Δημιουργία ενός πλαισίου πολιτικής κυβερνοασφάλειας.
* Καθορισμός απαιτήσεων και προτύπων για τη συμμόρφωση με τους στόχους της κυβερνοασφάλειας.
* Ενίσχυση της παρακολούθησης και αναφοράς πολιτικών σχετικά με την κυβερνοασφάλεια.

*Ευκαιρίες:* Συνεργασία με κορυφαίους προμηθευτές κυβερνοασφάλειας, Ενίσχυση του επιπέδου εμπειρογνωμοσύνης, πιθανή συμμόρφωση με το πρότυπο ISO 27001 ή με άλλα διεθνές πρότυπα και η ενίσχυση εμπιστοσύνης πελατών.

*Περιορισμοί:* Περιορισμένος προϋπολογισμός για επενδύσεις σε νέες τεχνολογίες*,* Υψηλό κόστος συμμόρφωσης

1. Ανάπτυξη Κρίσιμης Εποπτείας και Αντίδρασης σε Περιστατικά
* Δημιουργία κέντρου εποπτείας για την παρακολούθηση και άμεση αντίδραση σε κυβερνοεπιθέσεις.
* Εκπαίδευση εξειδικευμένου προσωπικού για τη διαχείριση περιστατικών ασφαλείας.
* Δημιουργία εκτελεστικής ομάδας για την αποτελεσματική αντίδραση σε κρίσεις.

*Ευκαιρίες:* Εφαρμογή προηγμένων εργαλείων και τεχνικών για τον εντοπισμό και την αντιμετώπιση συμβάντων κυβερνοασφάλειας.

*Περιορισμοί:* Έλλειψη εξειδικευμένου προσωπικού για τη διαχείριση προηγμένων εργαλείων.

* Ενίσχυση της Κυβερνοασφάλειας Εφαρμογών και Δεδομένων
* Αξιολόγηση των εφαρμογών και των βάσεων δεδομένων για εντοπισμό ευπαθειών.
* Εφαρμογή μέτρων ενίσχυσης της ασφάλειας σε επίπεδο κώδικα.
* Εκπαίδευση των αναπτυξιακών ομάδων για την ασφαλή ανάπτυξη εφαρμογών.

*Ευκαιρίες:* Ανάπτυξη ειδικών ομάδων για την προστασία των νέων τεχνολογιών.

*Περιορισμοί:* Ανάγκη για συνεχείς εκπαιδεύσεις του προσωπικού.

1. Προώθηση της Συνειδητοποίησης Ασφάλειας στο Προσωπικό
* Ανάπτυξη εκπαιδευτικών προγραμμάτων για την ασφάλεια πληροφοριών.
* Διεξαγωγή εκστρατειών ευαισθητοποίησης για τους κινδύνους της κυβερνοασφάλειας.
* Καθορισμός ανταμοιβών για τη συμμετοχή του προσωπικού σε δράσεις ασφάλειας.

*Ευκαιρίες:* Αυξημένη ευαισθητοποίηση του προσωπικού σχετικά με θέματα κυβερνοασφάλειας, εκπαίδευση προσωπικού για αναγνώριση και αντιμετώπιση απειλών κυβερνοασφάλειας.

*Περιορισμοί:* Περιορισμένος προϋπολογισμός για εκπαιδευτικά προγράμματα, αντίσταση του προσωπικού για τη συμμετοχή σε εκπαιδευτικά προγράμματα.

1. Εφαρμογή Τεχνολογικών Καινοτομιών για την Κυβερνοασφάλεια
* Έρευνα και εφαρμογή των τελευταίων τεχνολογικών τάσεων στην κυβερνοασφάλεια.
* Ενσωμάτωση της τεχνητής νοημοσύνης και της ανάλυσης μεγάλων όγκων δεδομένων για τον εντοπισμό κυβερνοεπιθέσεων.
* Ανάπτυξη συστημάτων Zero Trust για την ενίσχυση της ασφάλειας δικτύων.

*Ευκαιρίες:* Υποστήριξη από εθνικούς πόρους για την ανθεκτικότητα, συνεργασία με κρίσιμες υποδομές για ανταλλαγή βέλτιστων πρακτικών, ανάπτυξη ειδικών ομάδων για την προστασία των νέων τεχνολογιών, ενίσχυση της ικανότητας αντιμετώπισης επιθέσεων σε κρίσιμες υποδομές.

*Περιορισμοί:* Συνεχείς απειλές κυβερνοεπιθέσεων, κόστος υλοποίησης προηγμένων τεχνολογιών, ανάγκη για συνεχείς εκπαιδεύσεις του προσωπικού.

Για τη μέτρηση της αποτελεσματικότητας της ασφάλειας στον κυβερνοχώρο, ορίζουμε συγκεκριμένα Key Performance Indicators (KPIs) που θα συνδέονται με τους προηγουμένως καθορισμένους βασικούς στόχους. Αυτό θα διευκολύνει την παρακολούθηση της προόδου και την αξιολόγηση της επίτευξης των επιδιωκόμενων αποτελεσμάτων.

1. Ανάπτυξη και Εφαρμογή Πολιτικής Κυβερνοασφάλειας
* Επίπεδο συμμόρφωσης με την εσωτερική πολιτική κυβερνοασφάλειας.
* Χρόνος αντίδρασης σε νέες απειλές κυβερνοασφάλειας.
1. Ανάπτυξη Κρίσιμης Εποπτείας και Αντίδρασης σε Περιστατικά
* Επιτυχία στην αποκατάσταση κρίσιμων υποδομών μετά από επίθεση.
* Χρόνος ανίχνευσης και αντίδρασης σε κρίσιμα περιστατικά κυβερνοασφάλειας.
1. Ενίσχυση της Κυβερνοασφάλειας Εφαρμογών και Δεδομένων
* Ποσοστό μείωσης των επιτυχημένων κυβερνοεπιθέσεων σε εφαρμογές και δεδομένα.
* Επίπεδο συμμόρφωσης των εφαρμογών με τις προτεινόμενες πολιτικές κυβερνοασφάλειας.
1. Προώθηση της Συνειδητοποίησης Ασφάλειας στο Προσωπικό
* Ποσοστό συμμετοχής του προσωπικού σε εκπαιδευτικά προγράμματα κυβερνοασφάλειας.
* Ποσοστό επιτυχούς εξέτασης ασφάλειας για το προσωπικό.
1. Εφαρμογή Τεχνολογικών Καινοτομιών για την Κυβερνοασφάλεια
* Επιτυχία στην εφαρμογή καινοτομιών, όπως ΙοΤ και AI, για την ενίσχυση της κυβερνοασφάλειας.

# Ευθυγράμμιση της Στρατηγικής Ασφάλειας Πληροφοριών με την Επιχειρησιακή Στρατηγική:

Η Στρατηγική Ασφάλειας Πληροφοριών αποτελεί κρίσιμο κομμάτι της επιχειρησιακής στρατηγικής του οργανισμού και πρέπει να ευθυγραμμίζεται με τους γενικούς στόχους και τις αξίες του οργανισμού. Η ενσωμάτωση της κυβερνοασφάλειας στην επιχειρησιακή στρατηγική εξασφαλίζει τον συντονισμό και τη συνοχή των προσπαθειών, ενισχύοντας έτσι τη συνολική ανθεκτικότητα και ασφάλεια του οργανισμού.

1. Ευθυγράμμιση με Στρατηγικούς Στόχους:

• Η Στρατηγική Ασφάλειας Πληροφοριών πρέπει να αντικατοπτρίζει τους στρατηγικούς στόχους του οργανισμού. Οι στόχοι κυβερνοασφάλειας θα πρέπει να συμβάλλουν στην επίτευξη των γενικότερων στόχων του οργανισμού.

1. Ενσωμάτωση στη Διαδικασία Στρατηγικού Σχεδιασμού:
* Η διαδικασία σχεδιασμού της επιχειρησιακής στρατηγικής θα πρέπει να συμπεριλαμβάνει την αξιολόγηση των κινδύνων κυβερνοασφάλειας και την καθορισμό στρατηγικών απαντήσεων.
1. Συνεργασία με Επιχειρησιακά Τμήματα:
* Η Στρατηγική Ασφάλειας Πληροφοριών πρέπει να αναπτύσσεται σε συνεργασία με τα επιχειρησιακά τμήματα του οργανισμού, ώστε να εξασφαλίζεται η αμοιβαία υποστήριξη και καλύτερη συνολική απόδοση.
1. Αξιολόγηση και Ενημέρωση:
* Περιοδική αξιολόγηση της ευθυγράμμισης της Στρατηγικής Ασφάλειας Πληροφοριών με την επιχειρησιακή στρατηγική και ανανέωση σε περίπτωση αλλαγών.
1. Ενημέρωση Διοίκησης:
* Αναφορά στη διοίκηση για την πρόοδο και τη συμμόρφωση με τους στόχους κυβερνοασφάλειας κατά τη διάρκεια των ετήσιων αναθεωρήσεων.

Αυτή η ευθυγράμμιση διασφαλίζει ότι η κυβερνοασφάλεια αντιμετωπίζεται ως ολοκληρωμένο μέρος του οργανισμού και ενσωματώνεται στην πυραμίδα των επιχειρησιακών προτεραιοτήτων.

# Βασικές Πρωτοβουλίες σε Σχέση με την Κυβερνοασφάλεια

1. Διακυβέρνηση & Ηγεσία:
* Καταγραφή: Συστατικά στοιχεία που αφορούν τη διακυβέρνηση και την ηγεσία για την κυβερνοασφάλεια.
* Σύνδεση: Αναφορά στην "Πολιτική Διακυβέρνησης Ασφάλειας Πληροφοριών."
1. Διαχείριση Κινδύνων:
* Καταγραφή: Προσέγγιση για τον προσδιορισμό, την αξιολόγηση και τη διαχείριση κυβερνοασφαλειακών κινδύνων.
* Σύνδεση: Σύνδεση με την "Πολιτική Διαχείρισης Συμβάντων και Περιστατικών."
1. Εκπαίδευση και Ενημέρωση:
* Καταγραφή: Συγκεκριμένα μέτρα για την εκπαίδευση και ενημέρωση του προσωπικού.
* Σύνδεση: Σύνδεση με την "Πλάνο Εκπαιδεύσεων Ευαισθητοποίησης."
1. Διαχείριση Συμβάντων:
* Καταγραφή: Δράσεις για τον αντίδραση και την αποκατάσταση κατά την εμφάνιση περιστατικών κυβερνοασφάλειας.
* Σύνδεση: Σύνδεση με την "Πολιτική Διαχείρισης Συμβάντων και Περιστατικών."
1. Διαχείριση Κινδύνων από Προμηθευτές και Τρίτους:
* Καταγραφή: Πολιτικές που καθορίζουν τον τρόπο αντιμετώπισης κυβερνοασφαλειακών κινδύνων που προκύπτουν από προμηθευτές.
* Σύνδεση: Σύνδεση με την "Πολιτική Διαχείρισης Προμηθευτών."

# Πλάνο Υλοποίησης Στρατηγικών Παρεμβάσεων Κυβερνοασφάλειας (Παράδειγμα)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Αριθμός** | **Έργο Κυβερνοασφάλειας** | **Ημερομηνία Εκκίνησης** | **Ημερομηνία Ολοκλήρωσης** | **Υπεύθυνος** | **Απαιτούμενοι Πόροι** | **Μέθοδος Αξιολόγησης** |
| 1 | Ενίσχυση Αντι-Phishing Προγραμμάτων |  |  | Τμήμα Πληροφορικής | Προϋπολογισμός, Προσωπικό, Εκπαίδευση | Καταγραφή Επιδόσεων, Κριτήρια Αξιολόγησης |
| 2 | Εκπαίδευση Προσωπικού για Κυβερνοαπειλές |  |  | Ανθρώπινο Δυναμικό | Κατάρτιση Εκπαιδευτικού Υλικού, Εκπαιδευτές | Έλεγχος Συμμετοχής, Εκτίμηση Εκπαιδευτικού Υλικού |
| 3 | Αναβάθμιση Ασφάλειας Δικτύου |  |  | Τμήμα Δικτύων | Εργαλεία Εντοπισμού, Τεχνικό Προσωπικό | Επίτευξη Καθορισμένων Στόχων, Εκτίμηση Ασφαλείας Δικτύου |
| 4 | Αξιολόγηση Συμμόρφωσης με ISO 27001 |  |  | Τμήμα Κυβερνοασφάλειας | Ειδικοί Επαγγελματίες, Εργαλεία Αξιολόγησης | Επαλήθευση Συμμόρφωσης, Ανάδειξη Κενών |
| 5 | Εφαρμογή Συστημάτων Zero Trust |  |  | Τμήμα Κυβερνοασφάλειας | Τεχνολογικοί Πόροι, Εκπαίδευση Προσωπικού | Ανάλυση Εφαρμογής, Αξιολόγηση Αποτελεσμάτων |
|  |  |  |  |  |  |  |

# Αιτιολογημένη Κατανομή Προϋπολογισμού και Πόρων για την Κυβερνοασφάλεια:

Η κατανομή του προϋπολογισμού και των πόρων για πρωτοβουλίες κυβερνοασφάλειας θα πρέπει να γίνεται μέσω αιτιολογημένων επενδύσεων με βάση τις προτεραιότητες στους στόχους που τέθηκαν πιο πάνω και τυχόν αξιολόγηση των κινδύνων.

1. Ανάλυση Προτεραιοτήτων:
* Εκτίμηση της κρισιμότητας και της επιρροής κάθε στόχου κυβερνοασφάλειας.
* Κατανόηση του επιπέδου κινδύνου και των απαιτούμενων πόρων για κάθε στόχο.
1. Επενδύσεις:
* Κατανομή προϋπολογισμού με βάση τη σημασία κάθε στόχου για την κυβερνοασφάλεια.
* Προτεραιοποίηση επενδύσεων σε στόχους με υψηλότερο επίπεδο κινδύνου ή κρισιμότητας.
1. Αξιολόγηση Κινδύνων:
* Αξιολόγηση των κινδύνων που σχετίζονται με κάθε στόχο κυβερνοασφάλειας.
* Καταγραφή των απαιτούμενων πόρων για τη μείωση των κινδύνων.
1. Αξιολόγηση Αποδοτικότητας:
* Καθορισμός μετρήσιμων επιδόσεων και ορισμός κλειδιών επιδόσεων (KPIs) για κάθε επένδυση.
* Συνεχής αξιολόγηση της αποδοτικότητας των επενδύσεων και προσαρμογή της κατανομής πόρων ανάλογα.
1. Ευελιξία στην Αντιμετώπιση Εκτάκτων Συμβάντων:
* Διατήρηση ευελιξίας στον προϋπολογισμό για αντιμετώπιση έκτακτων κυβερνοασφαλειακών περιστατικών.
* Διαμόρφωση εφεδρικών σχεδίων για την ταχεία ανταπόκριση σε νέους κινδύνους.
1. Συνεχής Αναθεώρηση και Ενημέρωση:
* Αναθεώρηση των απαιτήσεων και των προτεραιοτήτων σε τακτικά χρονικά διαστήματα.
* Ενημέρωση της κατανομής πόρων με βάση την εξέλιξη του κυβερνοασφαλειακού τοπίου.

# Δήλωση Πεδίου Εφαρμογής Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών

Η ασφαλής διαχείριση των εταιρικών πληροφοριών και ατομικών στοιχείων πληροφοριών που κατέχονται, λαμβάνονται, επεξεργάζονται και αποθηκεύονται σε χώρους του Οργανισμού και περιλαμβάνουν όλα τα Τμήματα / Υπηρεσίες και γραφεία του Οργανισμού.

# Υποστηρικτικοί Οργανισμοί

*[Προσθέστε τους Οργανισμούς που υποστηρίζουν τον Οργανισμό σας μαζί και τι υπηρεσίες σας παρέχουν]*

# Στοιχεία Ενεργητικού

Τα στοιχεία ενεργητικού του [Όνομα Οργανισμού] δύναται να είναι ιδιόκτητα, να μισθώνονται, να αναπτύσσονται εσωτερικά ή να αγοράζονται και περιλαμβάνουν όλες τις εγκαταστάσεις στις οποίες γίνεται επεξεργασία πληροφοριών.

Τα στοιχεία που καλύπτονται από αυτό το πεδίο βρίσκονται ως ακολούθως:

* Κατάλογος στοιχείων του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών
* Κατάλογος εξοπλισμού
* Κατάλογος λογισμικών.

Για περισσότερες πληροφορίες σχετικά με τη λίστα στοιχείων ενεργητικού ανατρέξτε στο Asset based Risk Assessment Workbook.

# Άτομα

Το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών εφαρμόζεται σε όλο το προσωπικό και τους εξωτερικούς συνεργάτες του Οργανισμού.

Κάθε ξεχωριστό μέλος του προσωπικού εντός του [Όνομα Οργανισμού] είναι υπεύθυνο για την εφαρμογή της παρούσας στρατηγικής και φέρει ευθύνη αναφορικά με τη συμμόρφωσή του με την παρούσα πολιτική.

Ο Προϊστάμενος του Τμήματος και ο Υπεύθυνος Ασφάλειας Πληροφοριών θα πρέπει να έχουν την ευθύνη για την ασφάλεια πληροφοριών εντός του αντίστοιχου τμήματος, εφαρμόζοντας επαρκής δικλείδες ασφάλειας που πληρούν τους στόχους ασφάλειας πληροφοριών που ορίζονται σε αυτή την πολιτική.

Οι χρήστες θα πρέπει να γνωρίζουν τις καθημερινές υποχρεώσεις τους με βάση την παρούσα πολιτική και των λοιπών λειτουργικών πολιτικών και διαδικασιών που εφαρμόζονται.

Όλες οι παραβιάσεις της ασφάλειας των πληροφοριών, πραγματικές ή πιθανές, θα αναφέρονται και θα διερευνώνται από τον Υπεύθυνο Ασφάλειας Πληροφοριών με τη βοήθεια του αρμόδιου προσωπικού και των προϊσταμένων των εκάστοτε τμημάτων (κατά περίπτωση).

# Πλαίσιο Διαχείρισης

Η ακόλουθη δομή έχει δημιουργηθεί για την εφαρμογή, διαχείριση, αναθεώρηση, ενημέρωση και βελτίωση του Συστήματος:

*[Προσθέστε το διάγραμμα με τα άτομα που απαρτίζουν την ομάδα εφαρμογής, διαχείρισης, αναθεώρησης, ενημέρωσης και βελτίωσης του Συστήματος μαζί με συνοπτική περιγραφή του ρόλου του κάθε ατόμου]*

**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.

1.
2.
3.
4.
5.
6.
7.
8.
9.
10.
11.
12.

# Διευθυντής

Ο Διευθυντής είναι o τελικός υπεύθυνος για την ασφάλεια πληροφοριών στον [Όνομα Οργανισμού]. Ο Διευθυντής υποστηρίζει τον Προϊστάμενο Ασφάλειας Πληροφοριών στην εκτέλεση του ρόλου του και διασφαλίζει ότι διατίθενται επαρκείς πόροι για τη διαχείριση και τη συντήρηση του Συστήματος.

# Καθοδηγητική Επιτροπή Ασφάλειας Πληροφοριών

Η Καθοδηγητική Επιτροπή Ασφάλειας Πληροφοριών έχει την ευθύνη για

* τον καθορισμό της στρατηγικής στα θέματα ασφάλειας πληροφοριών
* την παρακολούθηση της συμμόρφωσης του Οργανισμού με το πρότυπο και τις πολιτικές που απορρέουν από αυτό
* τη βελτίωση του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών
* να προάγει τη δέσμευση του Οργανισμού για το εν λόγω θέμα.

Η Επιτροπή υποβάλλει εισηγήσεις στον Διευθυντή για τη λήψη αποφάσεων σε σχέση με τα πιο πάνω.

Η Επιτροπή εφαρμόζει τις αρχές και τα πρότυπα της ασφάλειας πληροφοριών και διασφαλίζει ένα διευρυμένο πρόγραμμα ασφάλειας πληροφοριών.

Η Επιτροπή ορίζει πολιτική πάνω στα θέματα ασφάλειας πληροφοριών που επηρεάζουν τον Οργανισμό. Αυτό περιλαμβάνει τη φυσική ασφάλεια, την ασφάλεια των συστημάτων πληροφορικής κ.α.

Το πλαίσιο εργασιών της Επιτροπής περιλαμβάνει μεταξύ άλλων, τα ακόλουθα:

* Εφόσον ενημερωθεί για σημαντικές παραβιάσεις, υποβοηθά εάν απαιτείται ώστε οι παραβιάσεις αυτές να μην επαναλαμβάνονται
* Προώθηση της ευαισθητοποίησης σε θέματα ασφάλειας πληροφοριών σε όλο τον Οργανισμό
* Έγκριση και παρακολούθηση των μέτρων ασφάλειας πληροφοριών για νέα έργα
* Συμμόρφωση με νέα νομοθεσία που άπτεται θεμάτων ασφάλειας πληροφοριών
* Παρακολούθηση και αναφορά νέων ή ήδη καταγεγραμμένων θεμάτων ασφαλείας
* Εξετάζει την πρόοδο από τους ελέγχους ασφάλειας
* Παρακολούθηση της αποτελεσματικότητας των πολιτικών ασφάλειας των πληροφοριών.
	1.
	2.

### Συχνότητα συσκέψεων / συνεδριάσεων

Η Καθοδηγητική Επιτροπή Ασφάλειας Πληροφοριών συνεδριάζει σε τακτά χρονικά διαστήματα.

Κατόπιν εισήγησης του Προϊσταμένου Ασφάλειας Πληροφοριών, η Επιτροπή μπορεί να συνεδριάσει εκτάκτως εφόσον προκύψει σημαντικό θέμα ασφάλειας πληροφοριών.

Μετά το πέρας 15 λεπτών από την ώρα καθορισμού της συνάντησης της Επιτροπής, η Επιτροπή θεωρείται ότι βρίσκεται σε απαρτία με τα παρόντα μέλη της.

Επιπρόσθετα η ομάδα μελών της Επιτροπής μπορεί να συνέλθει για να μελετήσει και να υποβάλει εισηγήσεις για συγκεκριμένα θέματα ασφάλειας πληροφοριών. Οι εισηγήσεις της επί μέρους Επιτροπής κοινοποιούνται στη συνέχεια και στα υπόλοιπα μέλη της Επιτροπής (μέσω ηλεκτρονικού ταχυδρομείου).

### Μέλη της Καθοδηγητικής Επιτροπής

Η Επιτροπή απαρτίζεται από τους:

* Άτομο 1 – Ρόλος
* Άτομο 2 – Ρόλος
* Άτομο 3 – Ρόλος
* …

### Ενημέρωση της Διεύθυνσης

Μία φορά το χρόνο η Καθοδηγητική Επιτροπή Ασφάλειας Πληροφοριών συνεδριάζει με σκοπό την ανασκόπηση του Συστήματος. Για σκοπούς ενημέρωσης, ο Προϊστάμενος Ασφάλειας Πληροφοριών, διανέμει έκθεση στα μέλη της Επιτροπής, η οποία δύναται να περιλαμβάνει τις ακόλουθες πληροφορίες:

1.
2.
3.
4.
5.
6. 1.

**Αποτελέσματα Ελέγχων**

* Αξιολόγηση / εκτίμηση του κινδύνου
* Εισηγήσεις από προσωπικό
* Σχόλια από τα ενδιαφερόμενα μέρη
* Προληπτικές και διορθωτικές δράσεις
* Επιπρόσθετες απειλές και ευπάθειες
* Κατάσταση ενεργειών από προηγούμενες αξιολογήσεις
* Τεχνικές, προϊόντα ή διαδικασίες που θα μπορούσαν να χρησιμοποιηθούν στον [Όνομα Οργανισμού] για τη βελτίωση του Συστήματος.

Τα αποτελέσματα της ενημέρωσης καταγράφονται από τον Προϊστάμενο Ασφάλειας Πληροφοριών και διανέμονται στα μέλη της Επιτροπής. Η έκθεση για ενημέρωση της διεύθυνσης δύναται να περιλαμβάνει τα ακόλουθα:

* Οποιεσδήποτε συστάσεις σχετίζονται με την αποτελεσματικότητα του Συστήματος
* Συστάσεις για την τροποποίηση των διαδικασιών, ως αποτέλεσμα περιστατικών
* Ενημέρωση της αξιολόγησης κινδύνου και του σχεδίου αντιμετώπισης του κινδύνου
* Εξέταση οποιωνδήποτε αλλαγών στη λειτουργία, ασφάλεια, ρυθμιστικές ή νομικές απαιτήσεις
* Επισήμανση οποιωνδήποτε αλλαγών στους κινδύνους και αναγνώριση τομέων με αυξημένους κινδύνους που χρήζουν αποδοχής κινδύνου
* Προσδιορισμός οποιωνδήποτε επιπρόσθετων αναγκαίων πόρων (συστήματα, εργαλεία ή άτομα).

**Μέτρα Ασφαλείας**

 Τα μέτρα ασφαλείας που έχουν επιλεγεί από την νομοθεσία ΚΔΠ 389/2020 για την αντιμετώπιση των κινδύνων, συνδέονται, όπου είναι δυνατόν με τις προσδιοριζόμενες ή υποτιθέμενες απειλές και ευπάθειες που εντοπίστηκαν κατά τη διαδικασία εκτίμησης του κινδύνου. Εάν έχει επιλεγεί μια σειρά ~~μέτρων~~ ασφαλείας για την αντιμετώπιση ενός κινδύνου, ο [Όνομα Οργανισμού] μπορεί να υποστηρίξει το σχέδιο αντιμετώπισης του κινδύνου με τα σχέδια του έργου ή πρόσθετη τεκμηρίωση της εφαρμογής.

Η διαδικασία αξιολόγησης του κινδύνου επιτρέπει στον [Όνομα Οργανισμού] να εντοπίζει τα μέτρα ασφαλείας που χρησιμοποιούνται (τεκμηριωμένα ή άτυπα) και να καθορίζει επιπρόσθετα μέτρα ασφαλείας ώστε να μειωθεί ο κίνδυνος σε επιτρεπτό επίπεδο.

Ο [Όνομα Οργανισμού] μπορεί να εφαρμόσει επιπρόσθετες δικλείδες ασφαλείας που δεν συνδέονται άμεσα με αναγνωρισμένο κίνδυνο αλλά έχουν εμπορική ή οικονομική λογική.

Όπου δεν είναι εφικτό να εφαρμοστεί μία δικλείδα ασφαλείας ή ένας κίνδυνος δεν δύναται να μετριαστεί, η αιτιολογία και ο προτεινόμενος υπολειπόμενος κίνδυνος εγκρίνεται από τη Διεύθυνση ή/και την Επιτροπή Ασφάλειας Πληροφοριών.

# Προϊστάμενος Ασφάλειας Πληροφοριών

Ο Οργανισμός ορίζει τον Προϊστάμενο Ασφάλειας Πληροφοριών. Ο Προϊστάμενος Ασφάλειας Πληροφοριών είναι υπεύθυνος για την εφαρμογή της πολιτικής εντός του Οργανισμού

Οι κυριότερες αρμοδιότητες του Προϊστάμενου Ασφάλειας Πληροφοριών είναι η:

* εφαρμογή ελάχιστων απαιτήσεων και συμμόρφωση με τη σχετική νομοθεσία
* πρακτική και ευέλικτη προσέγγιση, προκειμένου να προσαρμοστεί στις μεταβαλλόμενες νομοθεσίες και τις εθνικές απαιτήσεις για την ασφάλεια πληροφοριών. Προωθεί και αναλαμβάνει πρωτοβουλία στις αλλαγές της πολιτικής και των διαδικασιών ασφάλειας πληροφοριών του [Όνομα Οργανισμού] ώστε να ενσωματώνει τις εξελίξεις στην εθνική πολιτική και αλλαγές στο περιβάλλον του Οργανισμού
* λήψη στρατηγικών μέτρων ώστε να εξασφαλίζεται η συμμόρφωση με την πολιτική της ασφάλειας πληροφοριών και τις νομοθετικές απαιτήσεις
* παροχή κατευθυντήριων γραμμών για τη λήψη αποφάσεων που αφορούν την πολιτική ασφάλειας πληροφοριών, κατόπιν συμβουλών από αρμόδιες εθνικές αρχές
* ενσωμάτωση των απαιτήσεων ασφάλειας πληροφοριών στις δραστηριότητες του [Όνομα Οργανισμού] και διαχείριση της ασφάλειας των πληροφοριών
* ανάπτυξη, καθορισμός ή παροχή συμβουλών (και / ή πρότυπα), για τη διαχείριση κινδύνου, για την πολιτική ασφάλειας πληροφοριών και για την επίτευξη των στόχων του [Όνομα Οργανισμού]
* ανάπτυξη και τήρηση της πολιτικής ασφάλειας πληροφοριών και των διαδικασιών για την προστασία των απαιτήσεων του [Όνομα Οργανισμού]
* διασφάλιση ότι τα αναπτυξιακά έργα, ή άλλες εργασίες σύμφωνα με σχετικές συμβάσεις, συμμορφώνονται με τις απαιτήσεις για την ασφάλεια των πληροφοριών
* τήρηση ενός σχεδίου αντιμετώπισης κινδύνου, προκειμένου να επιτευχθούν οι στόχοι ασφάλειας. Οι ενέργειες του σχεδίου αντιμετώπισης κινδύνου προτεραιοποιούνται με βάση τον πιθανό κίνδυνο και καταγράφονται η χρηματοδότηση (εάν χρειάζεται), οι υπεύθυνοι και η αναμενόμενη ημερομηνία ολοκλήρωσης.
* παραγωγή ή έγκριση σχεδίων για τη γενική διαχείριση της ασφάλειας των επικοινωνιών και κατάρτιση σχεδίων έκτακτης δράσης για την προστασία των συστημάτων ασφάλειας πληροφοριών, σύμφωνα με τις κυβερνητικές πολιτικές και/ή πολιτικές του [Όνομα Οργανισμού]
* χρήση κατάλληλων μηχανισμών και διαδικασιών, ώστε να επιτευχθούν οι στόχοι ασφάλειας του [Όνομα Οργανισμού]
* παροχή της απαιτούμενης τεκμηρίωσης για υποστήριξη των διαδικασιών
* συνεργασία με το προσωπικό και τους εξωτερικούς συνεργάτες, ώστε να διατηρούνται τα κατάλληλα επίπεδα ασφάλειας μέσα στον [Όνομα Οργανισμού] και στους συμβαλλόμενους του
* παροχή καθοδήγησης στο προσωπικό έτσι που να επιτυγχάνεται συμμόρφωση με τις πολιτικές ασφάλειας πληροφοριών,
* υποστήριξη των απαιτήσεων της ασφάλειας πληροφοριών, παρέχοντας ειδικές κατευθυντήριες γραμμές, και πιο γενικά, μεταδίδοντας τα θέματα ασφάλειας πληροφοριών στους λήπτες αποφάσεων εντός και εκτός του [Όνομα Οργανισμού]
* υποστήριξη της προώθησης της αποδοχής των απαιτήσεων της ασφάλειας πληροφοριών από τους ιεραρχικά ανώτερους λήπτες αποφάσεων, εντός και εκτός του [Όνομα Οργανισμού]
* προβολή των ωφελειών από την τήρηση της ασφάλειας των πληροφοριών, μέσω γενικών ενημερώσεων
* προώθηση της γνώσης και εμπειρίας στα θέματα ασφάλειας πληροφοριών, μέσω εκπαιδευτικών προγραμμάτων
* αναγνώριση ευκαιριών και ανάληψη πρωτοβουλιών για επαγγελματική ανάπτυξη και τήρηση επαγγελματικής γνώσης σε σχέση με την ασφάλεια των πληροφοριών.

# Λειτουργός Ασφάλειας Πληροφοριών

Ο Οργανισμός ορίζει τον Λειτουργό Ασφάλειας Πληροφοριών. Ο Λειτουργός Ασφάλειας Πληροφοριών ο οποίος υποστηρίζει τον Προϊστάμενο είναι υπεύθυνος για την εφαρμογή της πολιτικής εντός του Οργανισμού. Ο Λειτουργός Ασφάλειας Πληροφοριών είναι επίσης υπεύθυνος για τα ακόλουθα (ο κατάλογος δεν είναι εξαντλητικός):

* Να εισηγείται προτάσεις ή άλλα σχέδια ασφάλειας που θα βελτιώσουν την αποτελεσματικότητα του Συστήματος
* Να συντονίζει την αξιολόγηση κινδύνου
* Να ταξινομεί και να αναθεωρεί τις εκθέσεις ελέγχου που σχετίζονται με την ασφάλεια πληροφοριών
* Να τηρεί ενημερωμένο το σχέδιο αντιμετώπισης του κινδύνου
* Να καταγράφει τις αποδοχές των κινδύνων
* Να συλλέγει και να αναθεωρεί τις μετρήσεις απόδοσης
* Να βοηθά στη διαχείριση και στην έρευνα των περιστατικών ασφάλειας
* Να κρατά αρχείο με τα στοιχεία ενεργητικού
* Να βοηθά στην εφαρμογή της πολιτικής
* Να διαχειρίζεται το πρόγραμμα εκπαίδευσης και ενημέρωσης του προσωπικού.
* Να διαχειρίζεται το πρόγραμμα εκπαίδευσης των νεοεισερχομένων.
* Να τηρεί τα έγγραφα του Συστήματος
* Να τηρεί αρχείο με τις διορθωτικές και προληπτικές ενέργειες
* Να αρχειοθετεί έγγραφα του Συστήματος ως τεκμηρίωση της πολιτικής
* Να τηρεί πρακτικά των συνεδριάσεων της Επιτροπής Ασφάλειας Πληροφοριών
* Να βοηθά και να συμβουλεύει σε θέματα ασφάλειας πληροφοριών το υπόλοιπο προσωπικό του Οργανισμού
* Να διενεργεί ολοκληρωμένη αξιολόγηση των κινδύνων ασφάλειας πληροφοριών.

# Άλλοι υπάλληλοι του Οργανισμού

### 12.5.1 Προϊστάμενοι Τμημάτων

Όλοι οι Προϊστάμενοι Τμημάτων είναι άμεσα υπεύθυνοι για την εφαρμογή των πολιτικών και των διαδικασιών που τους αφορούν και για την τήρηση τους από το προσωπικό τους. Είναι υπεύθυνοι να ενημερώνουν τον Προϊστάμενο Ασφάλειας Πληροφοριών για νέα έργα που αναλαμβάνουν και να ενσωματώνουν πρόνοιες ασφάλειας πληροφοριών κατά τη διάρκεια της διαχείρισης των έργων αυτών.

### 12.5.2 Όλο το Προσωπικό

Το προσωπικό οφείλει να εφαρμόζει τις πολιτικές και διαδικασίες του Συστήματος που σχετίζονται με τα καθήκοντα τους και να αναφέρει τα συμβάντα / περιστατικά ασφάλειας πληροφοριών.

### 12.5.3 Ιδιοκτήτες Πληροφοριών

Όλες οι πληροφορίες και συστήματα πληροφορικής θα πρέπει να έχουν ιδιοκτήτη της πληροφορίας, υπεύθυνο για τα εξής:

* τον καθορισμό κατάλληλου επιπέδου προστασίας της πληροφορίας
* τον καθορισμό των ατόμων που θα έχουν πρόσβαση στην πληροφορία σύμφωνα με την αρχή της ανάγκης γνώσης
* τον προσδιορισμό των απαιτήσεων για αντίγραφα ασφαλείας και για επιχειρησιακή συνέχεια
* την εξασφάλιση ότι οι πληροφορίες τηρούνται και φυλάσσονται σύμφωνα με την πολιτική και τη νομοθεσία
* την παροχή κατευθυντήριων γραμμών στους διαχειριστές του συστήματος σχετικά με τις απαιτήσεις για πρόσβαση
* την περιοδική επανεξέταση των δικαιωμάτων πρόσβασης σε κρίσιμα συστήματα.

Ο [Όνομα Οργανισμού] καθορίζει τις αρμοδιότητες που απαιτούνται για την εφαρμογή, διαχείριση και τήρηση του Συστήματος, ενώ όπου απαιτείται παρέχει εξειδικευμένη εκπαίδευση για τα θέματα ασφάλειας πληροφοριών. Επιπλέον, ο Οργανισμός τηρεί μητρώα εκπαίδευσης.

# Μηχανισμός Υποβολής Εκθέσεων προς την Ανώτατη Διοίκηση (Top Management)

Για να διασφαλιστεί η συστηματική αναφορά των αποτελεσμάτων σχετικά με την κυβερνοασφάλεια προς το Top Management, προτείνεται η δημιουργία ενός ολοκληρωμένου μηχανισμού υποβολής εκθέσεων.

* Δημιουργία περιοδικών εκθέσεων που καλύπτουν τους βασικούς στόχους κυβερνοασφάλειας και τα σχετικά KPIs.
* Ορισμός συγκεκριμένων περιόδων υποβολής εκθέσεων, π.χ., τριμηνιαία, εξαμηνιαία και ετήσια.
* Χρήση γραφημάτων, γραφημάτων Gantt, και άλλων οπτικών μέσων για την ευκολότερη κατανόηση των αποτελεσμάτων από το Top Management.
* Συμπερίληψη σαφούς σημειολόγησης για τυχόν προβλήματα ή περιοχές που απαιτούν ειδική προσοχή.
* Παροχή προτεινόμενων ενεργειών για τη βελτίωση της κυβερνοασφάλειας.
* Οργάνωση περιοδικών συνεδριάσεων με το Top Management για την ανάλυση των αποτελεσμάτων και των προτεινόμενων ενεργειών.
* Παροχή σχολίων και ανάδρασης από τη διοίκηση για την αποτελεσματικότητα των ληφθέντων μέτρων και τις προοπτικές βελτίωσης.
* Ανάπτυξη συστημάτων αναφοράς που επιτρέπουν στο Top Management την πρόσβαση σε πραγματικό χρόνο σε δεδομένα ασφάλειας.

# Εκθέσεις Ασφάλειας Πληροφοριών / Μετρήσεις Απόδοσης

Ο [Όνομα Οργανισμού] λαμβάνει μια σειρά πρωτοβουλιών ώστε να μετρηθεί η απόδοση του Συστήματος και των εφαρμοστέων δικλείδων ασφαλείας. Επίσης, ο Οργανισμός δύναται να αναθεωρεί τις διεργασίες που παρακολουθεί, ώστε να αντικατοπτρίζονται τα ακόλουθα:

* Αλλαγές ή ενημερώσεις στις διαδικασίες και στους στόχους
* Πληροφορίες που ανακαλύφθηκαν κατά τη διαδικασία της έρευνας περιστατικών ασφάλειας
* Έλεγχοι συμμόρφωσης
* Εισηγήσεις από το προσωπικό
* Συστάσεις της Καθοδηγητικής Επιτροπής Ασφάλειας Πληροφοριών
* Συστάσεις από την Ενημέρωση της Διεύθυνσης
* Νομικές / κανονιστικές απαιτήσεις
* Απαιτήσεις των αιτητών.

# Προσέγγιση Διαχείρισης Κινδύνου

Η βασική προσέγγιση που έχει υιοθετηθεί για την αξιολόγηση της επικινδυνότητας σε σχέση με την ασφάλεια βασίζεται στις ακόλουθες δραστηριότητες:

* Αναγνώριση του στοιχείου ενεργητικού
* Ανάλυση επιχειρησιακών επιπτώσεων
* Συνοπτικό ‘Gap Assessment’
* Αξιολόγηση τρωτότητας
* Αξιολόγηση κινδύνου
* Αντιμετώπιση κινδύνου

Η συχνή αναθεώρηση του καταλόγου των στοιχείων και το προφίλ κινδύνου του Οργανισμού αποτελούν μέρος της προσέγγισης της διαχείρισης κινδύνου. Αυτό επιτρέπει τη συμμόρφωση με την πολιτική ασφάλειας και τη συνεχή αποτελεσματικότητα στην εφαρμογή των ελέγχων.

Για περισσότερες πληροφορίες, μελετήστε το έγγραφο ‘Μεθοδολογία Διαχείρισης Κινδύνου’.

# Εκπαίδευση και Ενημέρωση

Ο [Όνομα Οργανισμού] καταρτίζει, σε ετήσια βάση, πρόγραμμα εκπαίδευσης και ενημέρωσης για το προσωπικό του.

Εκπαίδευση / ενημέρωση παρέχεται στο νέο-εισερχόμενο προσωπικό, στο πλαίσιο της αρχικής εκπαίδευσης. Οι υφιστάμενοι υπάλληλοι (και οι εξωτερικοί συνεργάτες που εργάζονται στα γραφεία του Οργανισμού, αντίστοιχα) έχουν στη διάθεση τους έγγραφα με οδηγίες, στα οποία γίνεται επεξήγηση των ευθυνών τους σε σχέση με την Πολιτική και Στρατηγική Ασφάλειας Πληροφοριών του Οργανισμού.

Οι στόχοι της εκπαίδευσης και ενημέρωσης στα θέματα ασφάλειας πληροφοριών είναι:

* Να κατανοήσει το προσωπικό την αξία και τη σημαντικότητα των δεδομένων και των στοιχείων ενεργητικού
* Να μειωθεί ο κίνδυνος ανθρώπινου σφάλματος που πιθανόν να προκαλέσει αποτυχία των μέτρων ασφάλειας
* Να αντιληφθεί και να κατανοήσει το προσωπικό τις ευθύνες του.

Η εκπαίδευση περιλαμβάνει μεταξύ άλλων:

* Βασική εκπαίδευση του προσωπικού στα θέματα ασφάλειας ως μέρος της εκπαίδευσης των νεοεισερχομένων
* Ενημέρωση με σχετικά ενδο-υπηρεσιακά προγράμματα
* Ενημέρωση από Προϊσταμένους Τμημάτων / Υπεύθυνους Υπηρεσιών, κατά τη διάρκεια συναντήσεων με το προσωπικό τους
* Διανομή / αποστολή αφισών, φυλλαδίων, βίντεο και άλλων ηλεκτρονικών ενημερώσεων σε τακτα χρονικά διαστήματα,
* Ανάπτυξη και συντήρηση τοποθεσιών εντός του δικτύου του Οργανισμού και άλλα βοηθήματα για υπενθυμίσεις, με σκοπό την εύκολη ανεύρεση ενημερωτικού υλικού,

Όταν κριθεί αναγκαίο, ή / και μετά από σύσταση της Καθοδηγητικής Επιτροπής Ασφάλειας Πληροφοριών, παρέχεται επιπρόσθετη εκπαίδευση στους υφιστάμενους χρήστες.

Ο Προϊστάμενος Ασφάλειας Πληροφοριών τηρεί αρχείο με τις πραγματοποιηθείσες εκπαιδεύσεις. Ως μέρος της εκπαίδευσης, οι χρήστες ενημερώνονται για τη σημαντικότητα της ασφάλειας πληροφοριών και τις επιπτώσεις που θα μπορούσε να έχει οποιαδήποτε παραβίαση της στον Οργανισμό, στους υπαλλήλους και στους συνεργάτες του.

# Πόροι

Η Καθοδηγητική Επιτροπή Ασφάλειας Πληροφοριών έχει εξουσιοδοτήσει τον Προϊστάμενο Ασφάλειας Πληροφοριών να διαχειρίζεται τους πόρους και τις απαιτήσεις / ανάγκες έτσι ώστε το Σύστημα να εφαρμόζεται, να τηρείται και να αναθεωρείται.

Ο Προϊστάμενος Ασφάλειας Πληροφοριών διαχειρίζεται τους πόρους με τρόπο ώστε οι διαδικασίες ασφάλειας πληροφοριών να υποστηρίζουν τις απαιτήσεις του Οργανισμού και να διατηρείται επαρκής ασφάλεια με τη σωστή εφαρμογή των δικλείδων ασφαλείας.

Ο Προϊστάμενος και η Καθοδηγητική Επιτροπή Ασφάλειας Πληροφοριών διασφαλίζουν ότι το προσωπικό που εφαρμόζει τις δικλείδες ασφαλείας και τις απαιτήσεις του Συστήματος είναι κατάλληλα εκπαιδευμένο.

Επιπρόσθετοι πόροι και απαιτήσεις ίσως να είναι αναγκαίοι για συγκεκριμένα θέματα ή για την αντιμετώπιση νέων περιστατικών ή για τη βελτίωση και αναθεώρηση του Συστήματος, οι οποίοι τυγχάνουν αναθεώρησης και διαχείρισης από τον Προϊστάμενο ή / και την Επιτροπή Ασφάλειας Πληροφοριών.

Στην περίπτωση όπου απαιτούνται επιπρόσθετοι πόροι ή χρηματοδότηση, ο Προϊστάμενος Ασφάλειας Πληροφοριών επανεξετάζει και συμφωνεί τις απαιτήσεις με την Καθοδηγητική Επιτροπή Ασφάλειας Πληροφοριών.

# Δέσμευση Διοίκησης

Η διοίκηση του οργανισμού δεσμεύεται σθεναρά να προωθήσει και να υποστηρίξει την υλοποίηση της Στρατηγικής Κυβερνοασφάλειας με σκοπό την προστασία των πληροφοριών και τη διασφάλιση της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητας των πληροφοριών. Η διοίκηση δηλώνει την αφοσίωσή της προς την κυβερνοασφάλεια μέσω των παρακάτω βασικών δεσμεύσεων:

1. Υποστήριξη και Πόροι:

Παροχή αναγκαίων πόρων (οικονομικών, ανθρώπινου δυναμικού, τεχνολογικών) για την εφαρμογή πολιτικών και μέτρων κυβερνοασφάλειας.

1. Προώθηση Πολιτικών Κυβερνοασφάλειας:

Δημιουργία και εφαρμογή πολιτικών κυβερνοασφαλείας και συμμόρφωση με αυτές.

1. Ευαισθητοποίηση Προσωπικού:

Παροχή εκπαίδευσης στο προσωπικό και ευαισθητοποίηση σχετικά με τις απειλές κυβερνοασφάλειας.

1. Συνεχής Αξιολόγηση και Ενίσχυση:

Τακτική αξιολόγηση των μέτρων κυβερνοασφάλειας και εφαρμογή βελτιώσεων όπου απαιτείται.

1. Διαχείριση Κρίσεων:

Ανάπτυξη και διατήρηση ισχυρής ικανότητας διαχείρισης κρίσεων σε περίπτωση κυβερνοεπίθεσης.

1. Συνεργασία με Εξωτερικούς Φορείς:

Επιδίωξη στενής συνεργασίας με εξωτερικούς φορείς και αρχές για την ανταλλαγή πληροφοριών και την κοινή αντιμετώπιση προκλήσεων κυβερνοασφάλειας.

Αυτή η δέσμευση αποτελεί αναγκαίο πυλώνα για τη διασφάλιση ενός αξιόπιστου, ασφαλούς και ανθεκτικού περιβάλλοντος πληροφοριών για τον οργανισμό μας και όλα τα εμπλεκόμενα μέρη.

# Διαχείριση Συμβάντων Ασφαλείας Πληροφοριών

Τα περιστατικά ασφάλειας πληροφοριών διερευνώνται σύμφωνα με τη Διαδικασία Διαχείρισης Συμβάντων και Περιστατικών Ασφάλειας Πληροφοριών του [Όνομα Οργανισμού].

Ο Προϊστάμενος Ασφάλειας Πληροφοριών συλλέγει πληροφορίες σχετικά με τα περιστατικά ασφάλειας και τις αδυναμίες του συστήματος. Περαιτέρω, αναλύει τις τάσεις και συστήνει την εφαρμογή επιπρόσθετων δικλείδων ασφαλείας, εάν απαιτείται.

Για περισσότερες πληροφορίες σχετικά με την αναφορά περιστατικών, δείτε τη σχετική πολιτική και διαδικασία του [Όνομα Οργανισμού].

# Εποπτεία και Αναθεώρηση του Συστήματος

Η Καθοδηγητική Επιτροπή Ασφάλειας Πληροφοριών παρακολουθεί το Σύστημα τακτικά.

Τα πιο κάτω έγγραφα είναι διαθέσιμα για θεώρηση:

* Εξωτερικές εκθέσεις ελέγχου
* Αξιολογήσεις κίνδυνου
* Εκθέσεις εσωτερικού ελέγχου
* Εκθέσεις μη συμμόρφωσης
* Περιστατικά ασφαλείας

Ο Προϊστάμενος Ασφάλειας Πληροφοριών τηρεί ένα χρονοδιάγραμμα αξιολόγησης κινδύνου. Το χρονοδιάγραμμα εξασφαλίζει ότι οι σημαντικότερες πληροφορίες υπόκεινται σε εκτίμηση του κινδύνου τουλάχιστον μια φορά κάθε [ορίστε χρονικό διάστημα σε χρόνια]. Το χρονοδιάγραμμα αξιολόγησης κινδύνου υποστηρίζεται από τμηματικές αξιολογήσεις κινδύνου, εάν κριθεί αναγκαίο. Οι ενέργειες που απορρέουν από τις τμηματικές αξιολογήσεις κινδύνου ενσωματώνονται στο πλάνο αντιμετώπισης κινδύνου και δύναται να θεωρούνται στις συνεδριάσεις της Επιτροπής Ασφάλειας Πληροφοριών.

# Αξιολογήσεις της Συμμόρφωσης

Ο Προϊστάμενος Ασφάλειας Πληροφοριών είναι υπεύθυνος για τη δημιουργία ενός προγράμματος ελέγχου. Αναμένεται ότι μία φορά κάθε [ορίστε χρονικό διάστημα σε χρόνια] θα ελεγχθεί κάθε δικλείδα ασφαλείας.

Οι εσωτερικοί έλεγχοι εντός του [Όνομα Οργανισμού] πραγματοποιούνται από την Υπηρεσία Εσωτερικού Ελέγχου, ή άλλο σύμβουλο. Η Διεύθυνση και η Επιτροπή Ασφάλειας Πληροφοριών ενημερώνεται για τα αποτελέσματα των ελέγχων αυτών.

Το πλάνο ελέγχου περιλαμβάνει σχέδια για τους ελέγχους που απαιτούνται με στόχο την επιτυχή εφαρμογή του Συστήματος.

Ο Προϊστάμενος Ασφάλειας Πληροφοριών διασφαλίζει ότι κάθε τμήμα του Συστήματος επαληθεύεται και τηρεί ένα πλάνο ελέγχου.

Οι έλεγχοι μπορεί να διεξαχθούν πιο συχνά ανάλογα με τη σπουδαιότητα των δραστηριοτήτων που ελέγχονται.

Οι παρακάτω πηγές πληροφοριών αναθεωρούνται για τον προσδιορισμό του προγράμματος ελέγχου:

* Προηγούμενες εκθέσεις ελέγχου (εσωτερικές ή εξωτερικές)
* Σχόλια από τους χρήστες / προσωπικό
* Οδηγίες της Επιτροπής Ασφάλειας Πληροφοριών που πιθανόν να επηρεάσουν οποιεσδήποτε πολιτικές
* Αλλαγές στα λειτουργικά συστήματα
* Αλλαγές στα σχετικές νομοθεσίες.

Το πρόγραμμα καλύπτει τους ελέγχους που διεξάγονται:

* Εντός του Οργανισμού
* Από εξωτερικούς συνεργάτες
* Σε τεχνικό επίπεδο, όπως για παράδειγμα ‘penetration testing’

Το πρόγραμμα ενδεχομένως να αναθεωρείται εντός του έτους κατόπιν ελέγχου της προόδου και εξέτασης τυχόν αλλαγών π.χ. στην πολιτική, στο σύστημα.

# Διορθωτικές / Προληπτικές Ενέργειες

Οι διορθωτικές ενέργειες εφαρμόζονται στις περιπτώσεις μη συμμόρφωσης με το Σύστημα. Εφαρμόζονται επίσης ώστε να εξαλειφθεί η κύρια αιτία που προκάλεσε τη μη-συμμόρφωση και να αποτραπεί τυχόν επανάληψη της.

Οι προληπτικές ενέργειες εφαρμόζονται όταν εντοπιστεί πιθανή μη-συμμόρφωση με το Σύστημα. Μια προληπτική ενέργεια σχεδιάζεται για να αποτραπεί η εμφάνιση οποιασδήποτε μη-συμμόρφωσης.

Η μη-συμμόρφωση ορίζεται ως εξής:

* Η απουσία, ή η αποτυχία εφαρμογής και τήρησης μίας ή περισσοτέρων εκ των απαιτήσεων του Συστήματος
* Περίπτωση η οποία, βάσει διαθέσιμων αντικειμενικών αποδεικτικών στοιχείων, αυξάνει σημαντικά τις αμφιβολίες, ως προς την ικανότητα του Συστήματος να ικανοποιήσει την Πολιτική Ασφάλειας Πληροφοριών και τους στόχους ασφάλειας του Οργανισμού.

Η πραγματική ή πιθανή μη-συμμόρφωση, μπορεί να αναγνωριστεί από τα ακόλουθα:

* Ελέγχους
* Αναθεωρήσεις
* Παρακολούθηση
* Περιστατικά και συμβάντα ασφάλειας
* Παρατηρήσεις από μέλη του προσωπικού κατά τις καθημερινές δραστηριότητες.

Όλες οι πραγματικές ή πιθανές μη-συμμορφώσεις κοινοποιούνται στον Προϊστάμενο Ασφάλειας Πληροφοριών. Ο Προϊστάμενος Ασφάλειας Πληροφοριών τις αναφέρει και συνεργάζεται με το αρμόδιο τμήμα/προσωπικό για την επίλυση/πρόληψη της μη-συμμόρφωσης.

Ο Προϊστάμενος Ασφάλειας Πληροφοριών τηρεί κατάλογο με τις διορθωτικές/προληπτικές δράσεις, που περιέχει τουλάχιστον:

* Ημερομηνία που εγέρθηκε και χρονικό πλαίσιο επίλυσης
* Ευθύνη υλοποίησης
* Εισηγήσεις διορθωτικών μέτρων / προληπτικών δράσεων
* Ενέργειες που έγιναν και κατάσταση ενεργειών

Τα αποτελέσματα και η κατάσταση με τις διορθωτικές / προληπτικές δράσεις δύναται να παρουσιάζονται κατά τη διευθυντική ενημέρωση. Τα αποτελέσματα των διορθωτικών / προληπτικών δράσεων ενδέχεται να δημιουργήσουν προσθήκες στο πλάνο αντιμετώπισης κινδύνου και να επιφέρουν αλλαγές στο πλάνο ελέγχου για θεώρηση των σχετικών δράσεων που πραγματοποιήθηκαν.

# Διαχείριση Κύκλου Ζωής του Εγγράφου της Στρατηγικής

Για τη διασφάλιση της επιτυχημένης υλοποίησης και διαχείρισης της Στρατηγικής Ασφάλειας Πληροφοριών, απαιτείται η εφαρμογή ενός συστηματικού και διαρκούς κύκλου ζωής του εγγράφου.

1. Ανασκόπηση και Ενημέρωση Στόχων:
* Περιοδική ανασκόπηση των στόχων κυβερνοασφάλειας, προκειμένου να διαπιστωθεί η συνέχιση της συμμόρφωσης με τις εξελίξεις στον τομέα της κυβερνοασφάλειας.
1. Υπεύθυνοι και Ρόλοι:
* Καθορισμός υπευθύνων και ρόλων για την ανασκόπηση και ενημέρωση, με επισήμανση των αρμοδιοτήτων κάθε εμπλεκόμενου.
1. Επικύρωση Αποτελεσματικότητας Ενεργειών:
* Αξιολόγηση της αποτελεσματικότητας των επιμέρους ενεργειών της στρατηγικής, με χρήση κριτηρίων που ενδέχεται να περιλαμβάνουν τη συμμόρφωση, την αντίδραση σε περιστατικά, και το επίπεδο ευαισθητοποίησης του προσωπικού.
1. Εξαγωγή Δεικτών Επίδοσης:
* Καθορισμός και εξαγωγή βασικών δεικτών επίδοσης (KPIs) που συνδέονται άμεσα με τους στόχους του οργανισμού, προκειμένου να παρέχουν ουσιαστική πληροφορία για την κυβερνοασφάλεια.
1. Αναθεώρηση Στρατηγικής:
* Καθορισμός περιόδων για την αναθεώρηση της στρατηγικής, προκειμένου να εξασφαλιστεί η επικαιρότητα και η συμμόρφωση με τις εξελίξεις του κυβερνοχώρου.
1. Ενημέρωση Top Management:
* Υλοποίηση μηχανισμού ενημέρωσης του Top Management για τα αποτελέσματα των ανασκοπήσεων, τις επιδόσεις των ενεργειών και τους εξαγόμενους δείκτες.

# Νομοθετικές Πράξεις

Για την επιτυχή υλοποίηση της Στρατηγικής Ασφάλειας Πληροφοριών, είναι ουσιώδες να λαμβάνονται υπόψη οι κυριότερες νομοθετικές πράξεις που διέπουν τον τομέα της κυβερνοασφάλειας και της προστασίας των πληροφοριών. Συγκεκριμένα, καταγράφονται οι εξής νομοθετικές πράξεις:

* Οδηγία NIS 2 (Οδηγία (EU) 2016/1148, όπως τροποποιήθηκε από την Οδηγία (EU) 2019/881)
* Εθνική Νομοθεσία (π.χ., Νόμος 4577/2018, "Προστασία των Πληροφοριών και της Ασφάλειας των Δικτύων")
* Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR - Κανονισμός (EU) 2016/679)
* Εθνική Νομοθεσία (π.χ., Νόμος 4624/2019, "Προστασία Φυσικών Προσώπων από τη Μεταχείριση των Δεδομένων Προσωπικού Χαρακτήρα και την Ελεύθερη Κυκλοφορία των Δεδομένων")
* Νόμος 4577/2018 (DORA - Διαχείριση Οργάνων και Ροών της Διακυβέρνησης και της Δημόσιας Διοίκησης)
* Εθνική Νομοθεσία που αφορά την κυβερνοασφάλεια και την προστασία των κρίσιμων υποδομών (Νόμος 389/2020)

Η συνεχής παρακολούθηση των εν λόγω νομοθετικών εξασφαλίζει τη συμμόρφωση του οργανισμού με τις νέες απαιτήσεις και θα παρέχει την αναγκαία προστασία και ευελιξία στον τομέα της κυβερνοασφάλειας.