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](#_Toc189654345)

[1. Εισαγωγή 4](#_Toc189654346)

[1.1. Σκοπός 4](#_Toc189654347)

[2. Πεδίο Εφαρμογής 5](#_Toc189654348)

[3. Ευθυγράμμιση της Στρατηγικής Ασφάλειας Πληροφοριών με την Επιχειρησιακή Στρατηγική 5](#_Toc189654349)

[4. Βασικοί Στρατηγικοί πυλώνες Ασφάλειας Πληροφοριών 6](#_Toc189654350)

[4.1. Διακυβέρνηση και συμμόρφωση 6](#_Toc189654351)

[4.2. Διαδικασία διαχείρισης κινδύνου 7](#_Toc189654352)

[4.3. Πλαίσιο Ασφάλειας Πληροφοριών 7](#_Toc189654353)

[4.4. Εποπτεία και Αντίδραση σε Περιστατικά 7](#_Toc189654354)

[4.5. Εκπαίδευση και ευαισθητοποίηση 8](#_Toc189654355)

[4.6. Εφαρμογή Τεχνολογικών Καινοτομιών στην Κυβερνοασφάλεια 8](#_Toc189654356)

[4.7. Διαχείριση Προμηθευτών και Τρίτων Οργανισμών: 9](#_Toc189654357)

[5. Νομοθετικές Πράξεις 10](#_Toc189654358)

[6. Μετρήσεις επιδόσεων και παρακολούθηση 10](#_Toc189654359)

[7. Πλάνο Υλοποίησης Στρατηγικών Παρεμβάσεων Ασφάλειας Πληροφοριών/Κυβερνοασφάλειας (Παράδειγμα) 11](#_Toc189654360)

[7.1. Αιτιολογημένη Κατανομή Προϋπολογισμού και Πόρων για την υλοποίηση του πλάνου: 12](#_Toc189654361)

[8. Δέσμευση Ανώτατης Διοίκησης 13](#_Toc189654362)

[9. Αναθεώρηση 13](#_Toc189654363)

[10. Αναφορές 15](#_Toc189654364)

# Εισαγωγή

# Σκοπός

Σύμφωνα με την Απόφαση Κ.Δ.Π. 389/2020, ο [Όνομα Οργανισμού] θεσπίζει μία Στρατηγική Ασφάλειας Πληροφοριών στην οποία να αναλύονται οι μαρκοπρόθεσμοι στόχοι και η προσέγγιση σε ανώτερο επίπεδο για τη διαχείριση της ασφάλειας πληροφοριών, με σκοπό τον μετριασμό των σχετικών κινδύνων. Διασφαλίζει ότι οι προσπάθειες ασφάλειας πληροφοριών ευθυγραμμίζονται με την αποστολή, τους στόχους, τις κανονιστικές και άλλες απαιτήσεις του [Όνομα Οργανισμού], ενώ παράλληλα ενισχύει την ανθεκτικότητα έναντι των εξελισσόμενων απειλών.

Αυτό επιτυγχάνεται μέσω της υλοποίησης προηγμένων πρακτικών κυβερνοασφάλειας, της εκπαίδευσης και ευαισθητοποίησης του προσωπικού, της συνεχούς ανάλυσης κινδύνων και της συνεχούς βελτίωσης των οργανωτικών και τεχνικών μέτρων ασφαλείας πληροφοριών.

Πιο συγκεκριμένα, οι στρατηγικές επιδιώξεις είναι:

* Η ευθυγράμμιση της στρατηγικής ασφάλειας πληροφοριών με τους οργανωτικούς στόχους του [Όνομα Οργανισμού] μέσω της ενσωμάτωσης σχετικών μέτρων ασφαλείας στις επιχειρησιακές διαδικασίες ώστε να εξασφαλίζεται η υποστήριξη των στρατηγικών στόχων του [Όνομα Οργανισμού].
* Ο μετριασμός των κινδύνων μέσω διαδικασίας αξιολόγησης κινδύνων ώστε να προσδιορίζονται, να αξιολογούνται και να ιεραρχούνται οι κίνδυνοι ασφάλειας πληροφοριών και να εφαρμόζονται επαρκή μέτρα για τη μείωση των επιπτώσεων των κινδύνων αυτών στις λειτουργίες του [Όνομα Οργανισμού].
* Η συμμόρφωση σχετικών νομοθεσιών, κανονισμών (π.χ. οδηγία NIS2) και άλλων καλών πρακτικών και προτύπων.
* Η προώθηση μιας κουλτούρας εκπαίδευσης και ευαισθητοποίησης με στόχο την ανάπτυξη της απαραίτητης υπευθυνότητας σε θέματα ασφάλειας σε ολόκληρο τον [Όνομα Οργανισμού].
* Η αξιοποίηση προηγμένων τεχνολογιών και μεθοδολογιών για τη βελτίωση της αποτελεσματικότητας των ελέγχων ασφαλείας. Το επιθυμητό στάδιο περιλαμβάνει την πλήρη ενσωμάτωση των προηγμένων μέτρων ασφαλείας πληροφοριών σε όλες τις πτυχές των επιχειρηματικών δραστηριοτήτων του [Όνομα Οργανισμού].
* Η συνεχής λειτουργικότητα μέσω της ανάπτυξης ικανοτήτων για τον αποτελεσματικό εντοπισμό, την αντιμετώπιση και την ανάκαμψη από περιστατικά ασφαλείας.
* Η καθιέρωση μηχανισμών για την συχνή επανεξέταση και βελτίωση των οργανωτικών και τεχνικών μέτρων ασφαλείας με στόχο την αντιμετώπιση αναδυόμενων απειλών και τρωτών σημείων των συστημάτων του [Όνομα Οργανισμού].
* Ανάπτυξη στενών σχέσεων και συνεργασία με τρίτα μέρη (π.χ. προμηθευτές) για την ενίσχυση της κυβερνοασφάλειας σε ολόκληρη την εφοδιαστική αλυσίδα του [Όνομα Οργανισμού].

# Πεδίο Εφαρμογής

Η στρατηγική αυτή εφαρμόζεται σε όλα τα περιουσιακά στοιχεία, τις υποδομές, το προσωπικό και τις διαδικασίες του οργανισμού, συμπεριλαμβανομένων των πιο κάτω:

* Ανθρώπινοι πόροι (εργαζόμενοι και τρίτα μέρη-προμηθευτές) που έχουν πρόσβαση ή αλληλεπιδρούν με τα συστήματα πληροφοριών.
* Πληροφοριακά περιουσιακά στοιχεία που αφορούν σημαντικά είδη δεδομένων, είτε αποθηκεύονται, είτε βρίσκονται σε επεξεργασία, είτε διαβιβάζονται, συμπεριλαμβανομένων των ευαίσθητων, προσωπικών και κρίσιμων για την επιχείρηση πληροφοριών.
* Πολιτικές, διαδικασίες, και άλλες ροές εργασίας που σχετίζονται με τη διαχείριση πληροφοριών.
* Τεχνολογική υποδομή: υλισμικά, λογισμικά, άλλα συστήματα και εφαρμογές πληροφορικής, δίκτυα, και άλλα περιβάλλοντα που βασίζονται σε υπηρεσίες cloud κτλ.
* Προστασία των φυσικών περιουσιακών στοιχείων που στεγάζουν κρίσιμες πληροφορίες, όπως τα κέντρα δεδομένων και άλλες κτηριακές τοποθεσίες και εγκαταστάσεις στις οποίες λειτουργεί ο [Όνομα Οργανισμού].

# Ευθυγράμμιση της Στρατηγικής Ασφάλειας Πληροφοριών με την Επιχειρησιακή Στρατηγική

Η Στρατηγική Ασφάλειας Πληροφοριών αποτελεί κρίσιμο κομμάτι της επιχειρησιακής στρατηγικής του οργανισμού και πρέπει να διασφαλίζεται η ευθυγράμμιση της με την αποστολή και τους στρατηγικούς και γενικότερων στόχων του [Όνομα Οργανισμού]. Η ενσωμάτωση της ασφάλεια των πληροφοριών και κυβερνοασφάλειας στην επιχειρησιακή στρατηγική εξασφαλίζει την ενίσχυση της παραγωγικότητας τον συντονισμό και τη συνοχή των προσπαθειών, ενισχύοντας έτσι τη συνολική ανθεκτικότητα και ασφάλεια του οργανισμού.

Η ασφάλεια των πληροφοριών δεν πρέπει να αντιμετωπίζεται ως μια μεμονωμένη λειτουργία, αλλά ως βασικός παράγοντας για την επιτυχία του [Όνομα Οργανισμού]. Πρέπει να προστατεύει τα κρίσιμα δεδομένα και συστήματα, ενώ παράλληλα να προάγει την καινοτομία και τη λειτουργική αποδοτικότητα.

Κατά τη διαδικασία του στρατηγικού σχεδιασμού θα πρέπει να λαμβάνονται υπόψη τα αποτελέσματα της αξιολόγησης των κινδύνων σε σχέση με την ασφάλεια πληροφοριών και κυβερνοασφάλειας με στόχο το καλύτερο σχεδιασμό μελλοντικών αναγκών και πρωτοβουλιών.

Με σκοπό να παραμένει πάντοτε ενημερωμένη θα πρέπει να γίνεται περιοδική αξιολόγηση της ευθυγράμμισης της Στρατηγικής Ασφάλειας Πληροφοριών με την επιχειρησιακή στρατηγική και ανανέωση σε περίπτωση αλλαγών. Επιπρόσθετα 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.

# Βασικοί Στρατηγικοί πυλώνες Ασφάλειας Πληροφοριών

Η στρατηγική που υπάρχει καταγεγραμμένη, 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. Με στόχο τη καταγραφή και προτεραιοποίηση των στόχων, ο [Όνομα Οργανισμού] έχει επιλέξει το μοντέλο ωριμότητας κυβερνοασφάλειας όπως αυτό δημοσιεύθηκε στην Απόφαση Κ.Δ.Π 245/2024, ως ένα χρήσιμο εργαλείο για σκοπούς καθοδήγησης, αυτό-αξιολόγησης, σχεδιασμού και συνεχόμενης βελτίωσης των επιπέδων ασφάλειας του Οργανισμού, το οποίο θα τον βοηθήσει να προσδιορίσει που αναμένεται να βρίσκεται ο [Όνομα Οργανισμού] τα επόμενα τρία έως πέντε χρόνια όσον αφορά την ωριμότητα για καθεμία από αυτές τις κατηγορίες και υποκατηγορίες του Μοντέλου.

Η ιεράρχηση των προτεραιοτήτων της Στρατηγικής Ασφάλειας Πληροφοριών και οι στόχοι σε σχέση με την ασφάλεια πληροφοριών και οι σχετικές ενέργειες για υλοποίηση τους σε ανώτερο επίπεδο είναι ως εξής:

# Διακυβέρνηση και συμμόρφωση

* Καθορισμός ρόλων και αρμοδιοτήτων σε σχέση με την ασφάλεια των πληροφοριών/κυβερνοασφάλειας στον [Όνομα Οργανισμού].
* Ανάπτυξη και εφαρμογή ενός πλαισίου πολιτικής κυβερνοασφάλειας. Η στρατηγική ασφάλειας πληροφοριών αντικατοπτρίζεται στην πολιτική ασφάλειας πληροφοριών, όπως περιγράφεται στο μέτρο [GOV3] της Απόφασης Κ.Δ.Π 389/2020.
* Ανάπτυξη και συμμόρφωση με σχετικές πολιτικές, διαδικασίες, πρότυπα και άλλες κατευθυντήριες γραμμές.
* Παρακολούθηση της συμμόρφωσης με τις κανονιστικές και άλλες υποχρεώσεις.
* Ενίσχυση της παρακολούθησης και αναφοράς πολιτικών σχετικά με την κυβερνοασφάλεια.

*Ευκαιρίες:* Συνεργασία με έμπειρους προμηθευτές στο τομέα ασφάλειας πληροφοριών/κυβερνοασφάλειας, ενίσχυση του επιπέδου εμπειρογνωμοσύνης εντός του Οργανισμού, πιθανή συμμόρφωση με διεθνής πρότυπα όπως ISO 27001 ή με άλλα διεθνές πρότυπα και η ενίσχυση εμπιστοσύνης των πελατών του [Όνομα Οργανισμού].

*Περιορισμοί*: Περιορισμένος προϋπολογισμός για συνεχείς επενδύσεις σε νέες τεχνολογίες, Υψηλό κόστος συμμόρφωσης, δυσκολία στην εξεύρεση εμπειρογνωμόνων στο τομέα και το συνεχές εναλλασσόμενο τοπίο κυβερνοαπειλών.

*Σύνδεση*: Αναφορά στην «Πολιτική Διακυβέρνησης Ασφάλειας Πληροφοριών».

# Διαδικασία διαχείρισης κινδύνου

* Ανάπτυξη ενός πλαισίου αξιολόγησης και διαχείρισης κινδύνων του [Όνομα Οργανισμού] στο οποίο περιλαμβάνονται διαδικασίες εντοπισμού, ανάλυσης, αξιολόγησης και μετριασμού των πιθανών απειλών και τρωτών σημείων.
* Καθορισμός των βασικών εργαλείων και μεθοδολογιών που χρησιμοποιούνται για τη διαχείριση κινδύνων.

*Ευκαιρίες: τεκμηριωμένη και γρηγορότερη λήψη αποφάσεων, ανταγωνιστικό πλεονέκτημα, βελτιωμένη αποδοτικότητα με καλύτερο εξορθολογισμό των διαδικασιών, ενθάρρυνση της καινοτομίας και της ανάπτυξης.*

*Περιορισμοί: περιορισμούς όσον αφορά τον προϋπολογισμό, το προσωπικό και την εμπειρογνωμοσύνη, ελλιπή, ανακριβή ή μη διαθέσιμα δεδομένα, διατήρηση της συνάφειας λόγο του συνεχούς μεταβαλλόμενου τοπίου κυβερνοασφάλειας/κυβερνοαπειλών, αντίσταση στην αλλαγή.*

*Σύνδεση: Αναφορά στη «Πολιτική Διαχείρισης Κινδύνων & στο Μητρώο Στοιχείων Ενεργητικού “Asset based Risk Assessment Workbook».*

# Πλαίσιο Ασφάλειας Πληροφοριών

* Εγκατάσταση ενός αποτελεσματικού, τεκμηριωμένου Σύστηματος Διαχείρισης Ασφάλειας Πληροφοριών για να προστατεύσει τις πληροφορίες του από απειλές (εσωτερικές ή εξωτερικές, σκόπιμες ή τυχαίες).

*Ευκαιρίες: δομημένη προσέγγιση για τον εντοπισμό, την αξιολόγηση και τον μετριασμό των κινδύνων στον κυβερνοχώρο, καλύτερη προστασία των κρίσιμων περιουσιακών στοιχείων και μειωμένη ευπάθεια σε επιθέσεις, Βελτιωμένη συμμόρφωση.*

*Περιορισμοί: περιορισμούς στους πόρους για διατήρηση ενός ολοκληρωμένου πλαισίου ασφάλειας, πολυπλοκότητα, αντίσταση στην αλλαγή, διατήρηση της συνάφειας λόγο του μεταβαλλόμενο τοπίου κυβερνοασφάλειας/κυβερνοαπειλών.*

*Σύνδεση: Αναφορά* *στην* «*Πολιτική* Ασφάλειας Πληροφοριών».

# Εποπτεία και Αντίδραση σε Περιστατικά

* Ανάπτυξη ολοκληρωμένου σχεδίου αντιμετώπισης περιστατικών και δημιουργία κέντρου εποπτείας για την παρακολούθηση και άμεση αντίδραση σε κυβερνοεπιθέσεις.
* Εκπαίδευση ομάδων ώστε να εντοπίζουν και να ανταποκρίνονται αποτελεσματικά σε περιστατικά ασφαλείας.
* Εκπαίδευση εξειδικευμένου προσωπικού και καταρτισμός ομάδων για την αποτελεσματική διαχείριση περιστατικών ασφαλείας.
* Πραγματοποίηση ανασκοπήσεων μετά το συμβάν για τη βελτίωση των μελλοντικών αντιδράσεων.

*Ευκαιρίες: Ελαχιστοποίηση των επιχειρησιακών διαταραχών, εφαρμογή προηγμένων εργαλείων και τεχνικών για τον εντοπισμό και την αντιμετώπιση συμβάντων κυβερνοασφάλειας, βελτιωμένη εμπιστοσύνη μεταξύ των ενδιαφερόμενων του Οργανισμού.*

*Περιορισμοί: Έλλειψη εξειδικευμένου προσωπικού για τη διαχείριση προηγμένων εργαλείων και δεξιοτήτων ελαχιστοποίησης επιχειρησιακών διαταραχών, χρονοβόρες δοκιμές και εκπαίδευση, μεγάλος όγκο ειδοποιήσεων, πολλές από τις οποίες είναι ψευδώς θετικές(false positive).*

*Σύνδεση: Αναφορά στη* *«Πολιτική Διαχείρισης Συμβάντων και Περιστατικών»*

# Εκπαίδευση και ευαισθητοποίηση

* Διεξαγωγή περιοδικών εκπαιδευτικών σεμιναρίων για τους εργαζόμενους και τους άλλους ενδιαφερόμενους φορείς.
* Διεξαγωγή εκστρατειών ευαισθητοποίησης για τους κινδύνους της κυβερνοασφάλειας και θέματα ασφάλειας για την προώθηση βέλτιστων πρακτικών.
* Ασκήσεις δοκιμών με στόχο την οργανωτική ετοιμότητα μέσω προσομοιώσεων phishing και άλλων ασκήσεων.
* Καταγραφή: Συγκεκριμένα μέτρα για την εκπαίδευση και ενημέρωση του προσωπικού.

*Ευκαιρίες: Αυξημένη ευαισθητοποίηση του προσωπικού σχετικά με θέματα κυβερνοασφάλειας, εκπαίδευση προσωπικού για αναγνώριση και αντιμετώπιση απειλών κυβερνοασφάλειας, καλύτερη απόδοση στην εργασία και παραγωγικότητα, καλύτερη αποδοχή και προσαρμογή στις αλλαγές, καλλιέργεια μελλοντικών επαγγελματιών με εξειδικευμένες γνώσεις εντός του οργανισμού.*

*Περιορισμοί: Περιορισμένος προϋπολογισμός για εκπαιδευτικά προγράμματα, αντίσταση του προσωπικού για τη συμμετοχή σε εκπαιδευτικά προγράμματα, ενημέρωση περιεχομένου για να παραμένει πάντα επίκαιρο.*

*Σύνδεση: Αναφορά στη* *«Πολιτική Ανθρώπινου Δυναμικού & Εκπαίδευσης».*

# Εφαρμογή Τεχνολογικών Καινοτομιών στην Κυβερνοασφάλεια

* Επένδυση και εφαρμογή των τελευταίων τεχνολογικών τάσεων στην κυβερνοασφάλεια με χρήση προηγμένων εργαλείων ανίχνευσης και πρόληψης απειλών.
* Ενσωμάτωση της τεχνητής νοημοσύνης (AI) και της μηχανικής μάθησης (ML) για την ανάλυση μεγάλων όγκων δεδομένων (big data) με στόχο τον εντοπισμό κυβερνοεπιθέσεων.
* Ανάπτυξη αρχιτεκτονικών όπως Zero Trust, **Defense in Depth** για την ενίσχυση της ασφάλειας δικτύων.
* Ενσωμάτωση των αρχών της ασφάλειας κατά το σχεδιασμό στην ανάπτυξη συστημάτων και εφαρμογών.

*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.*

# Διαχείριση Προμηθευτών και Τρίτων Οργανισμών:

* Καταγραφή πολιτικών που καθορίζουν τον τρόπο αντιμετώπισης των κινδύνων κυβερνοασφάλειας που προκύπτουν από προμηθευτές και άλλους τρίτους οργανισμούς.
* Καθορισμός συμβατικών απαιτήσεων, συμπεριλαμβανομένης της συμμόρφωσης με τις πολιτικές ασφάλειας πληροφοριών του οργανισμού.
* Διεξαγωγή τακτικών αξιολογήσεων και ελέγχων των πρακτικών ασφάλειας τρίτων.
* Παρακολούθηση της πρόσβασης τρίτων στα συστήματα και τα δεδομένα του οργανισμού για τη διασφάλιση της συνεχούς συμμόρφωσης και τον μετριασμό των κινδύνων.

*Ευκαιρίες: Βελτιωμένη τεχνογνωσία και αποτελεσματικότητα μέσω αξιοποίησης τρίτων παρόχων με παροχή εξειδικευμένων δεξιοτήτων και τεχνολογιών, εξοικονόμηση κόστους, χωρίς την ανάγκη για αρχική επένδυση σε πόρους εκ μέρους του Οργανισμού, ευέλικτες και επεκτάσιμες λύσεις.*

*Περιορισμοί: Κίνδυνοι ασφάλειας δεδομένων και απορρήτου, εξάρτηση σε ένα πάροχο, περιορισμένος έλεγχος και μειωμένη ορατότητα των διαδικασιών και των μέτρων ασφαλείας από τους εξωτερικούς πάροχους, συμβατικές και νομικές προκλήσεις.*

*Σύνδεση: Αναφορά στη* *«Πολιτική Διαχείρισης Προμηθευτών».*

# 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 και NIS2 (Οδηγία (EU) 2016/1148 & 2022/2555)
* Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR - Κανονισμός (EU) 2016/679)
* Νομοθεσία 89/2020 που αφορά την κυβερνοασφάλεια και την προστασία των κρίσιμων υποδομών και όλες σχετικές Αποφάσεις (π.χ. Αποφάσεις Κ.Δ.Π 389/2020, Κ.Δ.Π 39/2022, Κ.Δ.Π 245/2024 κτλ.)

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 ασφάλειας πληροφοριών και κυβερνοασφάλειας.

# Μετρήσεις επιδόσεων και παρακολούθηση

Για τη μέτρηση της αποτελεσματικότητας της ασφάλειας στον κυβερνοχώρο, ο [Όνομα Οργανισμού] ορίζει συγκεκριμένες μετρήσεις επιδόσεων (Key Performance Indicators - KPIs) που θα συνδέονται με τους προηγουμένως καθορισμένους βασικούς στόχους.

Μέσω τακτικών εκθέσεων οι οποίες θα κοινοποιούνται στην ανώτερη διοίκηση θα παρέχεται η απαραίτητη ορατότητα όσον αφορά την απόδοση της ασφάλειας πληροφοριών και τους τομείς που χρήζουν βελτίωσης. Αυτό θα διευκολύνει την παρακολούθηση της προόδου και την αξιολόγηση της επίτευξης των επιδιωκόμενων αποτελεσμάτων.

Για τη μέτρηση της αποτελεσματικότητας της στρατηγικής για την ασφάλεια των πληροφοριών, δύναται να παρακολουθούνται οι ακόλουθες μετρήσεις:

1. Ανάπτυξη και Εφαρμογή Πολιτικής Κυβερνοασφάλειας

* Επίπεδο συμμόρφωσης με την εσωτερική πολιτική κυβερνοασφάλειας.
* Χρόνος αντίδρασης σε νέες απειλές κυβερνοασφάλειας.
* Αποτελέσματα ελέγχων συμμόρφωσης.

1. Ανάπτυξη Κρίσιμης Εποπτείας και Αντίδρασης σε Περιστατικά

* Ποσοστό μείωσης των επιτυχημένων κυβερνοεπιθέσεων σε εφαρμογές και δεδομένα.
* Επιτυχία στην αποκατάσταση κρίσιμων υποδομών μετά από επίθεση.
* Χρόνος ανίχνευσης και αντίδρασης σε κρίσιμα περιστατικά κυβερνοασφάλειας.
* Χρόνος διαθεσιμότητας του συστήματος και χρόνος αποκατάστασης μετά από διαταραχές.

1. Προώθηση της εκπαίδευσης και της ευαισθητοποίησης του προσωπικού

* Ποσοστό συμμετοχής και ολοκλήρωσης 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.

# Πλάνο Υλοποίησης Στρατηγικών Παρεμβάσεων Ασφάλειας Πληροφοριών/Κυβερνοασφάλειας (Παράδειγμα)

Ακολουθεί το πλάνο υλοποίησης στρατηγικών παρεμβάσεων σε σχέση με την Ασφάλεια Πληροφοριών/κυβερνοασφάλειας το οποίο έτυχε έγκρισης από την Ανώτατη Διεύθυνση του [Όνομα Οργανισμού] και το οποίο αναθεωρείται τουλάχιστο σε ετήσια βάση.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **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 αρχιτεκτονικής Zero Trust |  |  | Τμήμα Κυβερνοασφάλειας | Τεχνολογικοί Πόροι, Εκπαίδευση Προσωπικού | Ανάλυση Εφαρμογής, Αξιολόγηση Αποτελεσμάτων |
|  |  |  |  |  |  |  |

# Αιτιολογημένη Κατανομή Προϋπολογισμού και Πόρων για την υλοποίηση του πλάνου:

Η κατανομή του προϋπολογισμού και των πόρων για υλοποίηση των πρωτοβουλιών του Πλάνου Υλοποίησης Στρατηγικών Παρεμβάσεων Ασφάλειας Πληροφοριών/Κυβερνοασφάλειας, θα πρέπει να γίνεται μέσω αιτιολογημένων επενδύσεων με βάση τις προτεραιότητες στους στόχους που τέθηκαν πιο πάνω και τυχόν αξιολόγηση των κινδύνων. Πιο συγκεκριμένα για κάθε παρέμβαση καταγράφονται σε σχετική έκθεση τουλάχιστο τα ακόλουθα:

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 τοπίου κυβερνοασφάλειας.

# Δέσμευση Ανώτατης Διοίκησης

Οι ενέργειες που έχουν προκύψει για υλοποίηση από την στρατηγική υποστηρίζονται από την ανώτατη διοίκηση με την παροχή πόρων, γνώσεων και χρόνου. Η διοίκηση του [Όνομα Οργανισμού] δεσμεύεται να προωθήσει και να υποστηρίξει την υλοποίηση της Στρατηγικής Ασφάλειας Πληροφοριών με σκοπό την προστασία των πληροφοριών και τη διασφάλιση της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητας των πληροφοριών. Όπως αναφέρθηκε και πιο πάνω, η ανώτατη διοίκηση δηλώνει την αφοσίωση της προς τα θέματα κυβερνοασφάλειας 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.

# Αναθεώρηση

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

* Περιοδική ανασκόπηση των στόχων κυβερνοασφάλειας, προκειμένου να διαπιστωθεί η συνέχιση της συμμόρφωσης με τις εξελίξεις στον τομέα της κυβερνοασφάλειας. Στα πλαίσια της διαδικασίας προβλέπεται η ανασκόπηση για την καταλληλότητα των σχετικών στοιχείων τουλάχιστον μια φορά το χρόνο και οι αλλαγές που προκύπτουν υλοποιούνται στα πλαίσια της διαδικασίας διαχείρισης αλλαγών.
* Καθορισμός υπευθύνων και ρόλων για την ανασκόπηση και ενημέρωση, με επισήμανση των αρμοδιοτήτων κάθε εμπλεκόμενου.
* Επικύρωση Αποτελεσματικότητας Ενεργειών μέσω εξαγωγή δεικτών επίδοσης, που συνδέονται άμεσα με τους στόχους του οργανισμού.
* Ενημέρωση της Ανώτατης Διεύθυνσης μέσω υλοποίησης μηχανισμού ενημέρωσης για τα αποτελέσματα των ανασκοπήσεων, τις επιδόσεις των ενεργειών και τους εξαγόμενους δείκτες.

# 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. |