Όνομα Οργανισμού

Πολιτική Ασφάλειας Πληροφοριών

|  |  |
| --- | --- |
| **Περιεχόμενο:** | Πολιτική 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](#_Toc189830362)

[1. Εισαγωγή 4](#_Toc189830363)

[1.1. Σκοπός 4](#_Toc189830364)

[1.2. Πεδίο Εφαρμογής 4](#_Toc189830365)

[2. Πολιτική Ασφάλειας Πληροφοριών 5](#_Toc189830366)

[2.1. Ρόλοι και Αρμοδιότητες Ασφάλειας Πληροφοριών 5](#_Toc189830367)

[2.2. Συμμόρφωση με Νομικές και Κανονιστικές Υποχρεώσεις 5](#_Toc189830368)

[2.3. Πολιτικές, πρότυπα, κατευθυντήριες γραμμές και διαδικασίες ασφάλειας πληροφοριών 6](#_Toc189830369)

[2.4. Έλεγχος Πρόσβασης 6](#_Toc189830370)

[2.5. Διαχείριση Κινδύνου 7](#_Toc189830371)

[2.6. Αποδεκτή Χρήση 7](#_Toc189830372)

[2.7. Καταγραφή και Παρακολούθηση 7](#_Toc189830373)

[2.8. Ασφάλεια Ανθρώπινου Δυναμικού 8](#_Toc189830374)

[2.9. Ασφάλεια Δικτύου 8](#_Toc189830375)

[2.10. Προστασία Δεδομένων 9](#_Toc189830376)

[2.11. Διαχείριση Αλλαγών και Διαμόρφωσης 10](#_Toc189830377)

[2.12. Διαχείριση Ευπαθειών 10](#_Toc189830378)

[2.13. Διαχείριση Προμηθευτών 10](#_Toc189830379)

[2.14. Ασφάλεια Συστημάτων και Εφαρμογών 10](#_Toc189830380)

[2.15. Διαχείριση Στοιχείων Ενεργητικού 11](#_Toc189830381)

[2.16. Διαχείριση Συμβάντων και Περιστατικών 11](#_Toc189830382)

[2.17. Επιχειρησιακή Συνέχεια 12](#_Toc189830383)

[2.18. Φυσική Ασφάλεια 13](#_Toc189830384)

[2.19. Στόχοι και Απόδοση Ασφάλειας Πληροφοριών 13](#_Toc189830385)

[2.20. Κυρώσεις 14](#_Toc189830386)

[2.21. Εξαιρέσεις 15](#_Toc189830387)

[3. Αναθεώρηση 16](#_Toc189830388)

[4. Αναφορές 17](#_Toc189830389)

# Εισαγωγή

# Σκοπός

Το παρόν έγγραφο περιλαμβάνει ενδεικτικούς Όρους Πολιτικής σχετικά με τη θέσπιση ενός πλαισίου για την προστασία των περιουσιακών στοιχείων του [Όνομα Οργανισμού] από κυβερνοαπειλές σε σχέση με την ασφάλεια πληροφοριών και τη συμμόρφωση με σχετικές απαιτήσεις της Απόφασης Κ.Δ.Π 389/2020.

Σκοπός της παρούσας Πολιτικής Διακυβέρνησης Ασφάλειας Πληροφοριών είναι η καθιέρωση ενός ολοκληρωμένου πλαισίου που θα εξασφαλίζει την προστασία των πληροφοριών του [Όνομα Οργανισμού] από απειλές και κινδύνους, διασφαλίζοντας την ακεραιότητα, την εμπιστευτικότητα, τη διαθεσιμότητα και την αυθεντικότητα τους. Η Πολιτική αυτή αποσκοπεί στην προάσπιση των δεδομένων και των συστημάτων πληροφορικής, που αποτελούν κρίσιμα στοιχεία για την επιτυχή λειτουργία και την επίτευξη των στόχων του [Όνομα Οργανισμού] μέσω:

* Καταγραφής κατευθυντήριων γραμμών για την αποτροπή μη εξουσιοδοτημένης πρόσβασης, χρήσης, γνωστοποίησης, τροποποίησης ή καταστροφής των πληροφοριών.
* Διασφάλισης της συμμόρφωσης με τις νομικές και άλλες κανονιστικές υποχρεώσεις.
* Προώθησης μιας κουλτούρας με επίγνωση της ασφάλειας πληροφοριών εντός του [Όνομα Οργανισμού].

Στόχοι του πλαισίου Ασφάλειας πληροφοριών είναι μεταξύ άλλων:

* Προστασία των κρίσιμων περιουσιακών στοιχείων πληροφοριών από εσωτερικές και εξωτερικές απειλές.
* Καθορισμός ρόλων και αρμοδιοτήτων για τη διατήρηση και επιβολή της ασφάλειας των πληροφοριών εντός του [Όνομα Οργανισμού].
* Καθιέρωση μεθοδολογίας διαχείρισης κινδύνων για τον εντοπισμό, την αξιολόγηση και τον μετριασμό των κινδύνων.
* Διασφάλιση της συνέχειας των επιχειρηματικών λειτουργιών με την εφαρμογή αποτελεσματικών ελέγχων ασφαλείας.
* Παροχή πλαισίου για την αποτελεσματική αντιμετώπιση περιστατικών και παραβιάσεων.
* Υποστήριξη της συμμόρφωσης με τη σχετική νομοθεσία, κανονισμούς και άλλες βέλτιστες πρακτικές.
* Προώθηση της εκπαίδευσης και ευαισθητοποίησης και της κατάρτισης μεταξύ των εργαζομένων, των εργολάβων και των ενδιαφερομένων μερών.
* Ενεργοποίηση της ασφαλούς συνεργασίας μεταξύ ομάδων, τμημάτων και τρίτων μερών του [Όνομα Οργανισμού].

# Πεδίο Εφαρμογής

Το πεδίο εφαρμογής της Πολιτικής Ασφάλειας Πληροφοριών καλύπτει όλες τις πληροφορίες που διαχειρίζεται ο [Όνομα Οργανισμού], ανεξαρτήτως του μέσου αποθήκευσης ή της μορφής τους, καθώς και όλα τα συστήματα πληροφορικής και τις διαδικασίες που σχετίζονται με τη χρήση των πληροφοριών αυτών. Επίσης, περιλαμβάνει το προσωπικό του [Όνομα Οργανισμού], τους συνεργάτες, τους προμηθευτές και κάθε άλλο ενδιαφερόμενο μέρος που έχει πρόσβαση ή διαχειρίζεται πληροφορίες του [Όνομα Οργανισμού].

# Πολιτική Ασφάλειας Πληροφοριών

Τα μέτρα ασφάλειας πληροφοριών και η λεπτομερής περιγραφή της εφαρμογής τους, έχουν καθοριστεί στα πλαίσια της Πολιτικής Ασφάλειας Πληροφοριών. Η Πολιτική Ασφάλειας Πληροφοριών αντικατοπτρίζει τους στόχους που περιγράφονται στην Στρατηγική Ασφάλειας Πληροφοριών.

# Ρόλοι και Αρμοδιότητες Ασφάλειας Πληροφοριών

Η Ανώτερη Διεύθυνση του [Όνομα Οργανισμού] είναι υπεύθυνη για την καθιέρωση και την υποστήριξη του πλαισίου ασφάλειας πληροφοριών και αναμένει ότι όλο το προσωπικό θα συμμορφωθεί με τις οδηγίες που παρουσιάζονται στο πλαίσιο αυτής της πολιτικής. Προς επίτευξη του στόχου, 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.

Ο Υπεύθυνος για την Ασφάλεια Δικτύων και Συστημάτων Πληροφοριών (ΥΑΠ) επιβλέπει την ανάπτυξη, την εφαρμογή και την παρακολούθηση των πολιτικών και πρακτικών ασφάλειας. Οι επικεφαλής των τμημάτων και άλλων υπηρεσιών του [Όνομα Οργανισμού] διασφαλίζουν τη συμμόρφωση των τμημάτων τους, ενώ οι εργαζόμενοι είναι υπεύθυνοι για την τήρηση των κατευθυντήριων γραμμών ασφαλείας, την αναφορά περιστατικών και τη διαφύλαξη των οργανωτικών πόρων σε σχέση με την ασφάλεια πληροφοριών.

Για περισσότερες πληροφορίες βλέπε «Πολιτική Διακυβέρνησης Ασφάλειας Πληροφοριών».

# Συμμόρφωση με Νομικές και Κανονιστικές Υποχρεώσεις

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

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

Επιπρόσθετα αναμένεται να πραγματοποιούνται έλεγχοι συμμόρφωσης από εξωτερικούς συνεργάτες ή/και άλλους φορείς για ανασκόπηση της αποτελεσματικότητας της εφαρμογής του πλαισίου.

Ο [Όνομα Οργανισμού] δημιουργεί πλάνο ενεργειών συμμόρφωσης (action plan) σε περίπτωση που αναγνωριστεί απόκλιση σε μία ή περισσότερες απαιτήσεις.

# Πολιτικές, πρότυπα, κατευθυντήριες γραμμές και διαδικασίες ασφάλειας πληροφοριών

Πέραν της υφιστάμενης πολιτικής, o [Όνομα Οργανισμού] υιοθετεί πολιτικές, οδηγίες και τυποποιημένες διαδικασίες λειτουργίας οι οποίες και εφαρμόζονται για την ασφάλεια πληροφοριών σε σχέση με συγκεκριμένες επεξεργασίες, συστήματα ή δραστηριότητες, ανάλογα με τις ανάγκες και το προσωπικό έχει ενημερωθεί και εκπαιδευτεί σχετικά.

Όλες οι πολιτικές και οι διαδικασίες πρέπει να εγκρίνονται από τη διοίκηση του οργανισμού.

Το προσωπικό πρέπει να ενημερώνεται και να εκπαιδεύεται σχετικά με τις πολιτικές και τις διαδικασίες.

Όλες οι πολιτικές και διαδικασίες θα πρέπει να ανασκοπούνται για την καταλληλόλητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών ή σε περίπτωση σημαντικών αλλαγών.

# Έλεγχος Πρόσβασης

Η πρόσβαση στους πόρους του [Όνομα Οργανισμού] πρέπει να καθορίζεται βάσει ρόλων και ευθυνών, διασφαλίζοντας ότι μόνο εξουσιοδοτημένοι χρήστες έχουν τη δυνατότητα να εκτελούν συγκεκριμένες ενέργειες.

Η εξωτερική πρόσβαση στους πόρους του [Όνομα Οργανισμού] πρέπει να ελέγχεται αυστηρά, με τη χρήση ισχυρών μηχανισμών επαλήθευσης και ασφαλών πρωτοκόλλων.

Οι προνομιούχοι χρήστες πρέπει να υπόκεινται σε αυξημένα μέτρα ασφαλείας, με περιορισμένη πρόσβαση βάσει αναγκαιότητας γνώσης και τακτικές αναθεωρήσεις των προνομίων τους.

Όλοι οι χρήστες πρέπει να επαληθεύουν την ταυτότητά τους πριν αποκτήσουν πρόσβαση στους κρίσιμους πόρους του [Όνομα Οργανισμού].

Τα διαπιστευτήρια πρέπει να δημιουργούνται, να διανέμονται και να διαχειρίζονται με ασφαλή τρόπο.

Πρέπει να εφαρμόζονται επαρκή μέτρα διαχείρισης και προστασίας της ταυτότητας του κάθε χρήστη καθ’ όλη την διάρκεια του κύκλου ζωής της ταυτότητας.

Για περισσότερες πληροφορίες βλέπε «Πολιτική Ελέγχου Πρόσβασης».

# Διαχείριση Κινδύνου

Ο [Όνομα Οργανισμού] ακολουθεί μια επίσημη μεθοδολογία διαχείρισης κινδύνων σύμφωνα με την οποία πρέπει να εντοπίζει, να αναλύει και να αντιμετωπίζει τους κινδύνους, βάσει της διάθεσης ανάληψης κινδύνων του [Όνομα Οργανισμού].

Όλοι οι κίνδυνοι πρέπει να καταγράφονται λεπτομερώς σε ένα μητρώο κινδύνων, το οποίο θα ενημερώνεται τακτικά και θα χρησιμοποιείται για την παρακολούθηση και τη διαχείριση των κινδύνων σε όλο τον [Όνομα Οργανισμού].

Για κάθε αναγνωρισμένο κίνδυνο, πρέπει να αναπτύσσονται και να εφαρμόζονται σχέδια αντιμετώπισης που θα περιγράφουν τις ενέργειες για τη μείωση ή την εξάλειψη των επιπτώσεων του κινδύνου με βάση την πολιτική ανάληψης κινδύνων του οργανισμού.

Για περισσότερες πληροφορίες βλέπε «Πολιτική & Μεθοδολογία Διαχείρισης Κινδύνου».

# Αποδεκτή Χρήση

Οι εργαζόμενοι του [Όνομα Οργανισμού] ακολουθούν τις κατευθυντήριες οδηγίες σχετικά με την αποδεκτή χρήση των πόρων που χρησιμοποιούν.

Η πλοήγηση στο διαδίκτυο να γίνεται με υπευθυνότητα, αποφεύγοντας την πρόσβαση σε κακόβουλους ή αμφιβόλου προέλευσης ιστότοπους, και σύμφωνα με τις πολιτικές ασφάλειας και αποδεκτής χρήσης του [Όνομα Οργανισμού].

Οι κωδικοί πρόσβασης πρέπει να είναι ισχυροί και να αλλάζουν τακτικά, με την υποχρέωση των χρηστών να διασφαλίζουν την εμπιστευτικότητα των κωδικών τους και να μην τους μοιράζονται με τρίτους.

Όλες οι ευαίσθητες πληροφορίες πρέπει να αποθηκεύονται με ασφάλεια, χρησιμοποιώντας κατάλληλες μεθόδους κρυπτογράφησης και προστασίας δεδομένων.

Για περισσότερες πληροφορίες βλέπε «Πολιτική Αποδεκτής Χρήσης».

# Καταγραφή και Παρακολούθηση

Όλες οι δραστηριότητες που σχετίζονται με τα στοιχεία ενεργητικού του [Όνομα Οργανισμού] πρέπει να καταγράφονται και να παρακολουθούνται με σκοπό τον εντοπισμό μη εξουσιοδοτημένων δραστηριοτήτων.

Για περισσότερες πληροφορίες βλέπε «Πολιτική Αποδεκτής Χρήσης».

# Ασφάλεια Ανθρώπινου Δυναμικού

Ο [Όνομα Οργανισμού] υλοποιεί επαρκή μέτρα για την εξασφάλιση ότι τα στελέχη που εργάζονται για λογαριασμό του οργανισμού, τα οποία έχουν πρόσβαση σε οργανωτικούς πόρους, υποστηρίζουν την πολιτική ασφάλειας πληροφοριών και τους στόχους του οργανισμού.

Πρέπει να εξασφαλίζεται ότι τα στελέχη που εργάζονται για λογαριασμό του οργανισμού συμμορφώνονται με την πολιτική ασφάλειας πληροφοριών και τηρούν τις ευθύνες ασφάλειας τους καθ’ όλη τη διάρκεια του κύκλου ζωής της απασχόλησης.

Πρέπει να εξασφαλίζεται ότι τα στελέχη που εργάζονται για λογαριασμό του οργανισμού, είναι υπεύθυνα για τις εκούσιες ή ακούσιες δραστηριότητες που επηρεάζουν τους στόχους ασφάλειας πληροφοριών του οργανισμού.

Πρέπει να εξασφαλίζεται ότι οι εξωτερικοί συνεργάτες που εργάζονται για λογαριασμό του οργανισμού τηρούν την πολιτική ασφάλειας πληροφοριών και τους στόχους ασφάλειας του οργανισμού.

Ο [Όνομα Οργανισμού] υλοποιεί επαρκή μέτρα για την εξασφάλιση από απειλές κατά της ασφάλειας δικτύων και πληροφοριών από το εσωτερικό του οργανισμού.

Πρέπει να εξασφαλίζεται ότι οι ευθύνες που αφορούν την ασφάλεια πληροφοριών και την αποδεκτή χρήση των στοιχείων ενεργητικού, ενσωματώνονται στις συμφωνίες εργοδότησης και στις διαδικασίες έναρξης απασχόλησης, για την επίτευξη υπευθυνότητας και ευαισθητοποίησης.

Ο [Όνομα Οργανισμού] υλοποιεί πρόγραμμα ενημέρωσης και ευαισθητοποίησης σχετικά με την ασφάλεια πληροφοριών για όλα τα στελέχη εντός του οργανισμού, λαμβάνοντας υπόψη τα στοιχεία που περιγράφονται στις πολιτικές, τα πρότυπα, τις κατευθυντήριες γραμμές και τις διαδικασίες ασφάλειας πληροφοριών.

Για περισσότερες πληροφορίες βλέπε «Πολιτική Ανθρώπινου Δυναμικού & Εκπαίδευσης».

# Ασφάλεια Δικτύου

Η διεπαφή του εσωτερικού δικτύου με το εξωτερικό δίκτυο πρέπει να προστατεύεται μέσω κατάλληλων τεχνικών και οργανωτικών μέτρων από επιθέσεις, απειλές και άλλες εκούσιες ή ακούσιες ενέργειες με δυνητικά αρνητικές επιπτώσεις.

Το δίκτυο πρέπει να διαχωρίζεται και να τμηματοποιείται σε ζώνες ασφαλείας βάσει των αναγκών ασφαλείας και της ευαισθησίας των δεδομένων, ώστε να περιορίζεται η εξάπλωση πιθανών επιθέσεων και να διασφαλίζεται η ασφάλεια των κρίσιμων πόρων.

Πρέπει να εφαρμόζονται μέτρα προστασίας από επιθέσεις άρνησης παροχής υπηρεσιών (DDoS) για να εξασφαλίζεται η διαθεσιμότητα των υπηρεσιών του [Όνομα Οργανισμού].

Πρέπει να εφαρμόζονται κατάλληλα πρωτόκολλα επικοινωνίας προκειμένου να επιτευχθεί ασφαλής επικοινωνία μεταξύ των πόρων του δικτύου.

Πρέπει να εξασφαλίζεται η ανίχνευση και η πρόληψη από εξωτερικές απόπειρες εισβολής στο εσωτερικό δίκτυο.

Για περισσότερες πληροφορίες βλέπε «Πολιτική Ασφάλειας Δικτύου».

# Προστασία Δεδομένων

Όλοι οι υπαλλήλοι εντός του [Όνομα Οργανισμού] είναι υπεύθυνα για τη διασφάλιση της προστασίας των προσωπικών και ευαίσθητων δεδομένων σύμφωνα με την ισχύων  νομοθεσία και κανονισμούς. Ο υπεύθυνος προστασίας δεδομένων (DPO) είναι υπεύθυνος για την εποπτεία των στρατηγικών προστασίας δεδομένων, τη διασφάλιση της τήρησης των κανονιστικών απαιτήσεων και ως κύριος σύνδεσμος για θέματα προστασίας δεδομένων.

Οι επικεφαλής των τμημάτων του [Όνομα Οργανισμού] εφαρμόζουν μέτρα προστασίας δεδομένων στις ομάδες τους, ενώ οι εργαζόμενοι αναμένεται να χειρίζονται τα δεδομένα με υπευθυνότητα, να αναφέρουν αμέσως τις παραβιάσεις και να ακολουθούν τις καθιερωμένες κατευθυντήριες γραμμές. Οι τρίτοι πάροχοι υπηρεσιών στον [Όνομα Οργανισμού] οφείλουν να τηρούν τις συμβατικές υποχρεώσεις και τα ισχύοντα πρότυπα προστασίας δεδομένων για τη διασφάλιση των δεδομένων του οργανισμού και των πελατών.

Ο [Όνομα Οργανισμού] διασφαλίζει την προστασία δεδομένων καθ’ όλο τον κύκλο ζωής των πληροφοριών, συμπεριλαμβανομένης της συλλογής, καταχώρησης, οργάνωσης, δομής, αποθήκευσης, προσαρμογής ή μεταβολής, ανάκτησης, αναζήτησης, χρήσης, κοινοποίησης με διαβίβαση, διάδοσης ή κάθε άλλη μορφή διάθεσης, συσχέτισης ή συνδυασμού, περιορισμού, διαγραφής ή καταστροφής

Όλες οι πληροφορίες ταξινομούνται και να επισημαίνονται ανάλογα με το επίπεδο ευαισθησίας τους, χρησιμοποιώντας καθορισμένα κριτήρια ταξινόμησης, ώστε να διασφαλίζεται η κατάλληλη προστασία και διαχείρισή τους

Ο [Όνομα Οργανισμού] διασφαλίζει ότι είναι δυνατή η αποκατάσταση των πληροφοριών σε περίπτωση απώλειας ή αλλοίωσής τους.

Η μεταφορά και η ανταλλαγή πληροφοριών εσωτερικά και με τρίτα μέρη, πρέπει να πραγματοποιούνται με ασφαλείς μεθόδους, διασφαλίζοντας την προστασία των δεδομένων κατά τη διακίνηση.

Πρέπει να εφαρμόζονται τεχνικά και οργανωτικά μέτρα για την πρόληψη της απώλειας και της διαρροής δεδομένων, διασφαλίζοντας ότι οι πληροφορίες παραμένουν ασφαλείς από μη εξουσιοδοτημένη πρόσβαση, αλλοίωση ή καταστροφή.

Πρέπει να μπορεί να διασφαλιστεί η εμπιστευτικότητα, ακεραιότητα και αυθεντικότητα των πληροφοριών με την υιοθέτηση κατάλληλων κρυπτογραφικών λύσεων.

Για περισσότερες πληροφορίες βλέπε «Πολιτική Προστασίας Δεδομένων».

# Διαχείριση Αλλαγών και Διαμόρφωσης

Όλες οι αλλαγές στις διαδικασίες και τα συστήματα πληροφοριών πρέπει να εφαρμόζονται με ασφάλεια, χωρίς να θίγεται το απόρρητο, η ακεραιότητα, η διαθεσιμότητα και η αυθεντικότητα των πληροφοριών.

Για όλες τις διαμορφώσεις των πόρων του [Όνομα Οργανισμού] πρέπει να μπορούν να εντοπίζονται, να διατηρούνται και να επαληθεύονται οι πληροφορίες για τα στοιχεία ενεργητικού και τις διαμορφώσεις του οργανισμού.

Για περισσότερες πληροφορίες βλέπε «Πολιτική & Διαδικασία Διαχείρισης Αλλαγών και Διαμόρφωσης».

# Διαχείριση Ευπαθειών

Όλα τα συστήματα και η πληροφοριακή υποδομή του [Όνομα Οργανισμού] πρέπει να υποβάλλονται σε τακτικούς ελέγχους και σαρώσεις για την ανίχνευση και τον εντοπισμό ευπαθειών, διασφαλίζοντας ότι οι πιθανές απειλές αναγνωρίζονται εγκαίρως.

Οι ευπάθειες που εντοπίζεται καταγράφονται και αναφέρονται άμεσα, προκειμένου να αξιολογηθεί ο κίνδυνος και να καθοριστούν οι απαραίτητες ενέργειες αποκατάστασης.

Πρέπει να υιοθετούνται διαδικασίες για την έγκαιρη αποκατάσταση των εντοπισμένων ευπαθειών μέσω κατάλληλων διορθωτικών ενεργειών και ενημερώσεων ασφάλειας, διασφαλίζοντας ότι τα συστήματα και η πληροφοριακή υποδομή παραμένουν προστατευμένα από γνωστές απειλές και επιθέσεις.

Για περισσότερες πληροφορίες βλέπε «Πολιτική Διαχείρισης Ευπαθειών και Τρωτότητας».

# Διαχείριση Προμηθευτών

Ο [Όνομα Οργανισμού] πρέπει να επιδεικνύει τη δέουσα επιμέλεια σχετικά με τρίτα μέρη και προμηθευτές

Ο [Όνομα Οργανισμού] πρέπει να διασφαλίζει ότι ενσωματώνονται οι κατάλληλες συμβατικές ρήτρες ασφάλειας πληροφοριών στις σχέσεις με τρίτα μέρη και προμηθευτές.

Για περισσότερες πληροφορίες βλέπε «Πολιτική Διαχείρισης Προμηθευτών».

# Ασφάλεια Συστημάτων και Εφαρμογών

Όλα τα στοιχεία ενεργητικού πρέπει να είναι ασφαλή καθ’ όλη τη διάρκεια του κύκλου ζωής τους, συμπεριλαμβανομένης της προμήθειας, της ανάπτυξης, της συντήρησης και της διάθεσης τους

Όλα τα στοιχεία ενεργητικού πρέπει να καταγράφονται σε κατάλογο και η ιδιοκτησία πρέπει να καθορίζεται με σκοπό την επίτευξη της ιχνηλασιμότητας και της ευθύνης για τα στοιχεία.

Όλα τα στοιχεία ενεργητικού πρέπει να είναι υπό παρακολούθηση για επιθέσεις, ύποπτη συμπεριφορά χρηστών και απειλές κατά της ασφάλειας, προκειμένου να ενεργοποιηθούν οι διαδικασίες για την αντιμετώπιση συμβάντων και περιστατικών

Πρέπει να μπορεί να διασφαλιστεί η διαθεσιμότητα δικτύων και συστημάτων πληροφοριών με την επίτευξη επαρκούς διαθεσιμότητας πόρων, εφεδρείας και συστημάτων / διαδικασιών υψηλής διαθεσιμότητας.

Πρέπει να μπορεί να εξασφαλιστεί η κατάλληλη χωρητικότητα και επίδοση των υπηρεσιών των συστημάτων και εφαρμογών.

Όλα τα στοιχεία ενεργητικού θα πρέπει να προστατεύονται από κακόβουλο λογισμικό και κώδικα.

Θα πρέπει να ελαχιστοποιηθεί, στο μέτρο του δυνατού, η επιφάνεια επίθεσης των συστημάτων και εφαρμογών.

Θα πρέπει να εξασφαλιστεί η κατάλληλη ασφάλεια των κινητών συσκευών που έχουν πρόσβαση σε οργανωτικούς πόρους.

Θα πρέπει να μπορεί να διασφαλιστεί η κατάλληλη διαχείριση των εφαρμογών που χρησιμοποιούνται για την πρόσβαση ή επεξεργασία οργανωτικών πόρων.

Θα πρέπει να διασφαλιστούν επαρκή μέτρα ασφάλειας στο πλαίσιο των δραστηριοτήτων ανάπτυξης λογισμικού που αναπτύσσει ο [Όνομα Οργανισμού].

Για περισσότερες πληροφορίες βλέπε «Πολιτική Ασφάλειας Συστημάτων και\_Εφαρμογών».

# Διαχείριση Στοιχείων Ενεργητικού

Ο [Όνομα Οργανισμού] πρέπει να καταγράφει και να παρακολουθεί όλα τα στοιχεία ενεργητικού του, εξασφαλίζοντας ότι αυτά προστατεύονται κατάλληλα και ότι διαχειρίζονται αποτελεσματικά καθ' όλη τη διάρκεια ζωής τους.

Ο [Όνομα Οργανισμού] πρέπει να εφαρμόζει μεθόδους κρυπτογράφησης για την προστασία ευαίσθητων δεδομένων τόσο κατά τη μεταφορά όσο και κατά την αποθήκευση.

Για περισσότερες πληροφορίες βλέπε «Πολιτική Διαχείρισης Στοιχείων Ενεργητικού».

# Διαχείριση Συμβάντων και Περιστατικών

Ο [Όνομα Οργανισμού] πρέπει να διαθέτει διαδικασίες για την έγκαιρη αναγνώριση, αναφορά και αντιμετώπιση συμβάντων και περιστατικών που αφορούν την ασφάλεια πληροφοριών.

Κάθε συμβάν και περιστατικό ασφαλείας πρέπει να αναλύεται λεπτομερώς για να αξιολογηθεί η φύση, η έκταση και ο αντίκτυπος του, βοηθώντας στην κατανόηση των αιτιών και των συνεπειών του.

Πρέπει να εφαρμόζονται άμεσα μέτρα περιορισμού για να μειωθεί η επίδραση των συμβάντων και περιστατικών ασφαλείας, καθώς και να υιοθετούνται διαδικασίες αποκατάστασης των συστημάτων και των υπηρεσιών στην κανονική τους λειτουργία.

Μετά την επίλυση ενός συμβάντος ή περιστατικού ασφαλείας, πρέπει να διεξάγονται ανασκοπήσεις και αναλύσεις για να αναγνωριστούν τα αίτια και να υιοθετηθούν βελτιώσεις στις διαδικασίες και στα συστήματα ασφαλείας.

Ο [Όνομα Οργανισμού] πρέπει να τηρεί όλες τις ρυθμιστικές απαιτήσεις για την κοινοποίηση συμβάντων και περιστατικών ασφαλείας στις αρμόδιες αρχές και να συνεργάζεται με αυτές για την επίλυση τους.

Ο [Όνομα Οργανισμού] πρέπει να κοινοποιεί πληροφορίες σχετικά με συμβάντα και περιστατικά ασφάλειας δικτύων και πληροφοριών σε εσωτερικούς και εξωτερικούς ενδιαφερόμενους φορείς.

Για περισσότερες πληροφορίες βλέπε «Πολιτική Διαχείρισης Συμβάντων και Περιστατικών».

# Επιχειρησιακή Συνέχεια

Ο [Όνομα Οργανισμού] πρέπει να διεξάγει ανάλυση επιχειρησιακών επιπτώσεων για να αναγνωριστούν οι κρίσιμες λειτουργίες του και οι πιθανές επιπτώσεις από διακοπές λειτουργίας.

Ο [Όνομα Οργανισμού] πρέπει να αναπτύσσει, να εφαρμόζει και να δοκιμάζει σχέδια επιχειρησιακής συνέχειας για να διασφαλίσει την απρόσκοπτη λειτουργία των κρίσιμων υπηρεσιών σε περίπτωση διακοπής.

Πρέπει να διεξάγονται τακτικές ασκήσεις και προσομοιώσεις επιχειρησιακής συνέχειας για να διασφαλίζεται ότι το προσωπικό είναι προετοιμασμένο να ανταποκριθεί αποτελεσματικά σε καταστάσεις έκτακτης ανάγκης και να επιβεβαιωθεί η αποτελεσματικότητα των σχεδίων.

Ο [Όνομα Οργανισμού] πρέπει να διαθέτει ένα ολοκληρωμένο σχέδιο αποκατάστασης από καταστροφή, το οποίο να περιγράφει τις διαδικασίες για την αποκατάσταση των κρίσιμων συστημάτων και λειτουργιών μετά από μια καταστροφή.

Πρέπει να δημιουργούνται τακτικά εφεδρικά αντίγραφα των δεδομένων και να διασφαλίζεται ότι τα δεδομένα μπορούν να ανακτηθούν γρήγορα και αποτελεσματικά σε περίπτωση απώλειας ή καταστροφής.

Η διαθεσιμότητα των κρίσιμων συστημάτων και υπηρεσιών πρέπει να διασφαλίζεται μέσω της εφαρμογής κατάλληλων μέτρων και διαδικασιών, όπως η παρακολούθηση της απόδοσης, η προληπτική συντήρηση και η χρήση εφεδρικών συστημάτων.

Η διαχείριση της χωρητικότητας των συστημάτων πρέπει να πραγματοποιείται μέσω της τακτικής αξιολόγησης των απαιτήσεων και της προσαρμογής των πόρων για να διασφαλιστεί ότι οι συστημικές υποδομές μπορούν να υποστηρίξουν την αυξανόμενη ζήτηση και να λειτουργούν αποδοτικά

Πρέπει να εξασφαλίζεται η διαθεσιμότητα πληροφοριών και δικτύων πληροφοριών με την επίτευξη επαρκούς διαθεσιμότητας πόρων, εφεδρικού εξοπλισμού, συστημάτων και συνδέσεων υψηλής διαθεσιμότητας.

Για περισσότερες πληροφορίες βλέπε «Πολιτική Επιχειρησιακής Συνέχειας».

# Φυσική Ασφάλεια

Ο [Όνομα Οργανισμού] πρέπει να εφαρμόζει μέτρα φυσικής ασφάλειας και ελέγχου πρόσβασης για την προστασία των εγκαταστάσεων του και των εσωτερικών του χώρων, εξασφαλίζοντας ότι μόνο εξουσιοδοτημένο προσωπικό έχει πρόσβαση σε κρίσιμα σημεία και εξοπλισμό.

Για την καλωδίωση και τον εξοπλισμό που υποστηρίζουν την επεξεργασία των πληροφοριών, πρέπει να εξασφαλίζεται η φυσική προστασία από παρεμβολές, υποκλοπή ή ζημιά.

Οι εσωτερικοί χώροι και οι εγκαταστάσεις του Οργανισμού που φιλοξενούν Πληροφοριακά Συστήματα ή/και υποδομή τεχνολογίας, προστατεύονται από φυσικές ζημιές.

Πρέπει να υπάρχουν επαρκή μέτρα για την προστασία του οργανισμού από τις επιπτώσεις φυσικών καταστροφών, όπως οι πλημμύρες, οι σεισμοί και οι πυρκαγιές.

Για περισσότερες πληροφορίες βλέπε «Πολιτική Φυσικής και Περιβαλλοντικής Ασφάλειας».

# Στόχοι και Απόδοση Ασφάλειας Πληροφοριών

Ο Υπεύθυνος Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών είναι υπεύθυνος για την ετοιμασία ετήσιων στόχων σε σχέση με την ασφάλεια πληροφοριών οι οποίοι εγκρίνονται από την Διεύθυνση του [Όνομα Οργανισμού].

Ο βαθμός επίτευξης τους μετριέται και παρουσιάζεται στην Διεύθυνση του Οργανισμού σε ετήσια βάση.

Ο Υπεύθυνος Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών αξιολογεί τους στόχους και, όπου συστήνεται, τους αναθεωρεί με βάση την πληροφόρηση για την αποτελεσματικότητα και την αποδοτικότητα του συστήματος και την πρόοδο στην αντιμετώπιση των κινδύνων.

# Κυρώσεις

Μη συμμόρφωση με τη υφιστάμενη πολιτική αλλά και το υπόλοιπο πλαίσιο, ορίζεται ως ένα ή περισσότερα από τα εξής:

* Οποιαδήποτε παράβαση των μέτρων που περιλαμβάνονται σε αυτή την πολιτική
* Μη εξουσιοδοτημένη αποκάλυψη ή προβολή των διαβαθμισμένων δεδομένων ή πληροφοριών που ανήκουν στον [Όνομα Οργανισμού].
* Μη εξουσιοδοτημένη αλλαγή πληροφοριών, λογισμικών ή λειτουργιών συστημάτων.
* Η χρήση υλικού, λογισμικών, δικτύων επικοινωνίας και εξοπλισμού, δεδομένων ή πληροφοριών για παράνομο σκοπό, ο οποίος μπορεί να περιλαμβάνει παραβιάσεις νόμου, κανονισμών ή απαιτήσεις για ενημέρωση νομικών ή κυβερνητικών φορέων.
* Έκθεση του [Όνομα Οργανισμού] σε πραγματική ή δυνητική χρηματική απώλεια η οποία θα προέλθει από συμβιβασμό των μέτρων ασφαλείας.
* Οποιοδήποτε πρόσωπο γνωρίζει ή υποπτεύεται παραβίαση αυτής της πολιτικής πρέπει να αναφέρει τα γεγονότα στον Υπεύθυνο Ασφάλειας Δικτύων και Συστημάτων Πληροφορίων.

Κάθε παραβίαση ή μη τήρηση αυτής της πολιτικής δύναται να αντιμετωπιστεί ως σοβαρό πειθαρχικό παράπτωμα.

Για περισσότερες πληροφορίες βλέπε ««Πολιτική Ανθρώπινου Δυναμικού & Εκπαίδευσης».

# Εξαιρέσεις

Εξαιρέσεις από την Πολιτική Ασφάλειας Πληροφοριών μπορούν να δοθούν υπό συγκεκριμένες συνθήκες, εφόσον αιτιολογούνται, τεκμηριώνονται και εγκρίνονται μέσω της κατάλληλης διαδικασίας διακυβέρνησης. Πιθανά παραδείγματα τέτοιων εξαιρέσεων περιλαμβάνουν:

* Σε περίπτωση που η συμμόρφωση με την πολιτική αυτή δύναται να οδηγήσει σε σωματική βλάβη ή τραυματισμό κάποιου εργοδοτουμένου.
* Σε περίπτωση που η συμμόρφωση με την πολιτική αυτή μπορεί να προκαλέσει σοβαρές ζημιές στη φήμη του [Όνομα Οργανισμού] ή στην δυνατότητα του να λειτουργήσει τις κρίσιμες επιχειρηματικές λειτουργίες ή στόχους και εφαρμόζονται αντισταθμιστικά μέτρα μετριασμού του κινδύνου.
* Σε περίπτωση τεχνικών περιορισμών όταν αυτοί δύναται να εμποδίζουν την πλήρη τήρηση της πολιτικής, υπό την προϋπόθεση ότι εφαρμόζονται αντισταθμιστικά μέτρα μετριασμού του κινδύνου.

Όλες οι εξαιρέσεις θα πρέπει:

* Να έχουν ζητηθεί επίσημα με λεπτομερή αιτιολόγηση.
* Να έχουν υποβληθούν σε διαδικασία αξιολόγησης κινδύνου με σκοπό την εκτίμηση των πιθανών επιπτώσεων.
* Να εξετάζονται και να εγκρίνονται από τον Υπεύθυνο Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών ή από άλλη διορισμένη από την Διοίκηση του [Όνομα Οργανισμού] αρχή.
* Να περιλαμβάνουν καθορισμένο χρονοδιάγραμμα επίλυσης ή επανεξέτασης.

Αναμένεται να πραγματοποιούνται περιοδικοί έλεγχοι με στόχο να διασφαλίζεται ότι οι εξαιρέσεις εξακολουθούν να ισχύουν και ότι δεν ενέχουν αδικαιολόγητους κινδύνους για την ασφάλεια του οργανισμού.

# Αναθεώρηση

Η πολιτική αυτή επανεξετάζεται και επικαιροποιείται τουλάχιστον σε ετήσια βάση ή νωρίτερα, εάν υπάρχουν σχετικές νομοθετικές ή κανονιστικές απαιτήσεις ή / και σημαντικές αλλαγές στη λειτουργία του [Όνομα Οργανισμού], ώστε να διασφαλίζεται η συνεχής καταλληλόλητα και αποτελεσματικότητά της. Επιπλέον, οι αναθεωρήσεις θα διεξάγονται υπό τις ακόλουθες συνθήκες:

Τεχνολογικές εξελίξεις: Όταν υιοθετούνται νέες τεχνολογίες, συστήματα ή διαδικασίες που επηρεάζουν το περιβάλλον ασφάλειας πληροφοριών του [Όνομα Οργανισμού].

Ανάλυση περιστατικών: Μετά από σημαντικά περιστατικά ασφάλειας ή παραβιάσεις για την αντιμετώπιση των εντοπισμένων τρωτών σημείων και τη βελτίωση της ανθεκτικότητας.

Συστάσεις ελέγχου: Με βάση τα ευρήματα και τις συστάσεις από εσωτερικούς ή εξωτερικούς ελέγχους ασφαλείας.

Όλες οι ενημερώσεις εγκρίνονται από τη διοίκηση του [Όνομα Οργανισμού] και οι εργαζόμενοι πρέπει να ενημερώνονται και να εκπαιδεύονται σχετικά με τις σημαντικές αλλαγές, ώστε να διασφαλίζεται η συνεχής συμμόρφωση και ευαισθητοποίηση.

# 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. |