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](#_Toc153435267)

[1. Εισαγωγή 4](#_Toc153435268)

[2. Αποστολή 4](#_Toc153435269)

[2.1. Πεδίο Εφαρμογής 4](#_Toc153435270)

[3. Σκοπός Ασφάλειας Πληροφοριών 4](#_Toc153435271)

[3.1. Στόχοι και Απόδοση Ασφάλειας Πληροφοριών 4](#_Toc153435272)

[3.2. Πρόγραμμα Δράσης 5](#_Toc153435273)

[3.3. Αναθεώρηση 5](#_Toc153435274)

[4. Οδηγίες και Τυποποιημένες Διαδικασίες Ασφάλειας Πληροφοριών 6](#_Toc153435275)

[5. Πολιτική Ασφάλειας Πληροφοριών 7](#_Toc153435276)

[6. Ρόλους και Αρμοδιότητες 13](#_Toc153435277)

[7. Οδηγίες για τυποποιημένες διαδικασίες λειτουργίες 16](#_Toc153435278)

[8. Συμμόρφωση 16](#_Toc153435279)

[8.1. Συμμόρφωση με την Πολιτική Ασφάλειας Πληροφοριών 16](#_Toc153435280)

[8.2. Εξαιρέσεις 17](#_Toc153435281)

[8.3. Κυρώσεις 17](#_Toc153435282)

# Εισαγωγή

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

# Αποστολή

Η αποστολή του [Όνομα Οργανισμού] σε σχέση με την ασφάλεια πληροφοριών είναι η συμμόρφωση του με τις σχετικές απαιτήσεις του Κανονισμού Κ.Δ.Π 389/2020, για την εκπλήρωση της ευρύτερης αποστολής του [Όνομα Οργανισμού].

# Πεδίο Εφαρμογής

Ο [Όνομα Οργανισμού] έχει εγκαταστήσει ένα αποτελεσματικό, τεκμηριωμένο Πλαίσιο Μέτρων Ασφάλειας για να προστατεύσει τις πληροφορίες του από απειλές (εσωτερικές ή εξωτερικές, σκόπιμες ή τυχαίες).

Παραδείγματα τέτοιων πληροφοριών είναι:

* Πληροφορίες υπαλλήλων, πελατών και άλλων ενδιαφερόμενων μερών
* Πληροφορίες που του εμπιστεύονται οι πολίτες και οι επιχειρήσεις
* Πληροφορίες που του εμπιστεύονται οι κυβερνητικές υπηρεσίες

Οι εν λόγω πληροφορίες είναι σημαντικές για την εκτέλεση των εργασιών του [Όνομα Οργανισμού] και στηρίζουν τη λειτουργία του.

# Σκοπός Ασφάλειας Πληροφοριών

Σκοπός του Πλαισίου Μέτρων Ασφάλειας 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

# Στόχοι και Απόδοση Ασφάλειας Πληροφοριών

Οι στόχοι της ασφάλειας πληροφοριών εγκρίνονται από τον Υπεύθυνο Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών, και 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.

# Πρόγραμμα Δράσης

Για την εκπλήρωση της αποστολής της ασφάλειας πληροφοριών, του σκοπού και των στόχων της:

* Διενεργούνται αξιολογήσεις κινδύνου για να ληφθούν τα κατάλληλα μέτρα διαφύλαξης της εμπιστευτικότητας, της ακεραιότητας, της διαθεσιμότητας και της αυθεντικότητας των πληροφοριών σύμφωνα με τις επιχειρησιακές ανάγκες του οργανισμού.
* Δημιουργούνται, εγκρίνονται, εφαρμόζονται και αναθεωρούνται επί μέρους πολιτικές και διαδικασίες ώστε να υποστηρίζουν την πολιτική ασφάλειας πληροφοριών.
* Καταγράφονται ανάγκες εκπαίδευσης και υλοποιείται το σχετικό πρόγραμμα εκπαίδευσης.
* Αναφέρονται και διερευνούνται τα περιστατικά μη συμμόρφωσης και διασφαλίζεται η έγκαιρη λήψη των κατάλληλων μέτρων ώστε να ελαχιστοποιηθεί τυχόν επιχειρησιακή ζημιά.
* Όπου η αγορά προϊόντων ή υπηρεσιών ανατίθεται σε εξωτερικούς συνεργάτες, επιβεβαιώνεται η τήρηση των απαιτήσεων του Κ.Δ.Π. 389/2020 μέσω συμβάσεων, ελέγχων και πιθανών άλλων μέτρων.
* Δημιουργούνται, ενημερώνονται και ελέγχονται τα Σχέδια Επιχειρησιακής Συνέχειας και Αποκατάστασης από Καταστροφές.

# Αναθεώρηση

Η πολιτική αυτή θεωρείται από τον Υπεύθυνο Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών μια φορά ανά έτος ή νωρίτερα, εάν υπάρχουν σχετικές νομοθετικές ή κανονιστικές απαιτήσεις ή / και σημαντικές αλλαγές στη λειτουργία του [Όνομα Οργανισμού]. Επικαιροποιείται όποτε κριθεί αναγκαίο.

* Τα στοιχεία που θα πρέπει να περιλαμβάνει η ανασκόπηση της πολιτικής είναι τα εξής: Διατυπώνεται σαφώς ο σκοπός της πολιτικής;
* Η προτεινόμενη αναθεώρηση πολιτικής συμμορφώνεται με:
	+ Νομοθεσίες που διέπουν τον [Όνομα Οργανισμού];
	+ Την διεύθυνση του [Όνομα Οργανισμού];
	+ Άλλες Πολιτικές του [Όνομα Οργανισμού];
* Υπάρχουν οι απαραίτητες αναφορές σε άλλες Πολιτικές;
* Θεωρήθηκαν οι βέλτιστες πρακτικές;
* Είναι κατανοητά αυτά που αναγράφονται στην Πολιτική;
* Είναι ξεκάθαρο ποιοι πρέπει να συμμορφώνονται με την Πολιτική;
* Όροι και ορισμοί είναι σωστά και απλά γραμμένα;
* Έγινε κάποιος έλεγχος για σύγκρουση δεδομένων μεταξύ αυτής της Πολιτικής και άλλων Πολιτικών;
* Υπήρξε κάποια μορφή σχόλιων από Προϊσταμένους τμημάτων;

# Οδηγίες και Τυποποιημένες Διαδικασίες Ασφάλειας Πληροφοριών

Η πολιτική ασφάλειας πληροφοριών αποτελεί θεμέλιο λίθο για τη διασφάλιση της εμπιστευτικότητας, της διαθεσιμότητας και της ακεραιότητας των πληροφοριακών συστημάτων ενός οργανισμού. Οι παρακάτω οδηγίες και τυποποιημένες διαδικασίες [GOV3] έχουν σχεδιαστεί για να διασφαλίσουν την αποτελεσματική υλοποίηση της πολιτικής ασφάλειας πληροφοριών στον οργανισμό μας.

1. Καθορισμός Αρμοδιοτήτων:

Κάθε τμήμα και μέλος του προσωπικού πρέπει να γνωρίζει τις αρμοδιότητές του σχετικά με την ασφάλεια πληροφοριών. Οι ρόλοι και οι ευθύνες πρέπει να καθορίζονται ξεκάθαρα, ενισχύοντας έτσι την αποτελεσματική διαχείριση του κινδύνου.

1. Εκπαίδευση και Ευαισθητοποίηση:

Όλοι οι εργαζόμενοι πρέπει να υποβάλλονται σε τακτικά προγράμματα εκπαίδευσης σχετικά με τις βασικές αρχές ασφάλειας πληροφοριών και τη συμμόρφωση με τις πολιτικές του οργανισμού.

1. Προστασία Δεδομένων:

Ορίζονται τεχνικά μέτρα προστασίας, όπως κρυπτογραφία, firewalls, και antivirus λογισμικά, για την εξασφάλιση της ακεραιότητας και της εμπιστευτικότητας των δεδομένων.

1. Παρακολούθηση και Ανίχνευση:

Συστήματα παρακολούθησης και ανίχνευσης προστίθενται για την άμεση ανίχνευση και αντιμετώπιση ενδεχόμενων απειλών στην ασφάλεια πληροφοριών.

1. Αντιμετώπιση Περιστατικών:

Προκαθορισμένες διαδικασίες αντιμετώπισης και αποκατάστασης καθορίζονται για κάθε είδος επιθέσεων ή παραβίασης της ασφάλειας.

1. Στρατηγική Ασφάλειας [STR1]:

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.

# Πολιτική Ασφάλειας Πληροφοριών

Η Πολιτική Ασφάλειας Πληροφοριών περιλαμβάνει σειρά πολιτικών που στην ολότητα τους καλύπτουν τις απαιτήσεις που καθορίζει το ισχύον νομοθετικό και κανονιστικό πλαίσιο.

Οι πολιτικές αποτελούν βέλτιστες πρακτικές που ρυθμίζουν την υπό αναφορά θεματολογία. Ο [Όνομα Οργανισμού] υιοθετεί τις πολιτικές ως τέτοιες βέλτιστες πρακτικές και αποσκοπεί προς την κατεύθυνση της μέγιστης δυνατής συμμόρφωσης με αυτές.

Νοείται ότι ο βαθμός συμμόρφωσης επηρεάζεται / εξαρτάται από το επίπεδο αξιολόγησης των σχετικών κινδύνων και συναφών ελέγχων αναλογικά με το επίπεδο έκθεσης σε κίνδυνο και της σημαντικότητας των λειτουργικών δραστηριοτήτων του οργανισμού.

Η διοίκηση του οργανισμού δεσμεύεται για την εφαρμογή, τη συντήρηση και τη συνεχή βελτίωση της ασφάλειας πληροφοριών με βάση το Πλαίσιο Κ.Δ.Π. 389/2020. Έτσι, υιοθετήθηκε η ακόλουθη πολιτική ασφάλειας πληροφοριών:

* Ο [Όνομα Οργανισμού] υιοθετεί τις απαιτήσεις του κανονισμού Κ.Δ.Π. 389/2020, ως βάση για τη δομή και τη διατήρηση ενός πλαισίου μέτρων για τη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας, της διαθεσιμότητας και της ανθεκτικότητας δεδομένων και συστημάτων πληροφοριών.
* Οι πολιτικές και οι διαδικασίες για την ασφάλεια πληροφοριών είναι δεσμευτικές για όλους τους εργαζομένους.
* Ο [Όνομα Οργανισμού] θα συμμορφώνεται με τον Γενικό Κανονισμό Προσωπικών Δεδομένων (GDPR) και με τους συμβατικούς όρους που έχουν συμφωνηθεί μεταξύ του οργανισμού και των πελατών του σχετικά με τα προσωπικά στοιχεία ταυτοποίησης (PII).
* Όλοι οι εργαζόμενοι υποχρεούνται να συμμορφώνονται με τις ισχύουσες νομικές απαιτήσεις, όπως τον Γενικό Κανονισμό Προστασίας Δεδομένων.
* Όλοι οι εργαζόμενοι και τρίτα μέρη του οργανισμού πρέπει να προστατεύουν τα δεδομένα και τα πληροφοριακά συστήματα από μη εξουσιοδοτημένη πρόσβαση, χρήση, τροποποίηση, αποκάλυψη, καταστροφή, απώλεια ή μεταφορά.
* Ο [Όνομα Οργανισμού] προωθεί ενεργά την ευαισθητοποίηση σχετικά με την ασφάλεια, των τρίτων μερών, των επισκεπτών, και των εργαζομένων της καθ’ όλη τη διάρκεια απασχόλησής τους.
* Όλοι οι εργαζόμενοι πρέπει να παρακολουθούν και να συμμετέχουν σε τυχόν εκπαιδεύσεις (ηλεκτρονικές ή φυσικές) που θα οργανώνονται από τον οργανισμό ή κάποιο εξωτερικό συνεργάτη εκ μέρους του [Όνομα Οργανισμού].
* Το δίκτυο του [Όνομα Οργανισμού] θα πληροί τις απαιτήσεις που σχετίζονται με τις πολιτικές και τις διαδικασίες ασφάλειας πληροφοριών.
* Όλα τα συστήματα πληροφοριών (συμπεριλαμβανομένου λογισμικών και υλικών) θα συμμορφώνονται με τις πολιτικές και τις διαδικασίες ασφάλειας πληροφοριών, συμπεριλαμβανομένης της διαχείρισης αλλαγών, της ανάπτυξης συστημάτων, της φυσικής ασφάλειας και του λογικού ελέγχου πρόσβασης.
* Ο [Όνομα Οργανισμού] αναπτύσσει σχέδια επιχειρησιακής συνέχειας και αποκατάστασης από καταστροφές για να εξασφαλίσει τη συνέχεια των ζωτικών λειτουργιών σε περίπτωση καταστροφής.
* Ο [Όνομα Οργανισμού] θεωρεί τα περιστατικά ασφάλειας υψηλής σημασίας και εφαρμόζει Σχέδιο και Διαδικασίες Αντιμετώπισης Συμβάντων.
* Ο [Όνομα Οργανισμού] καταγράφει και ταξινομεί τα κρίσιμα στοιχεία ενεργητικού (συμπεριλαμβανομένων ηλεκτρονικών δεδομένων, εντύπων αντιγράφων, λογισμικού και υλικού) και διενεργεί ετήσια αξιολόγηση κινδύνου για τον εντοπισμό πιθανών απειλών και τρωτών σημείων για τη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας, της διαθεσιμότητας και της ανθεκτικότητας των στοιχείων ενεργητικού.
* Ο [Όνομα Οργανισμού] αντιμετωπίζει τους κινδύνους όταν μοιράζεται πληροφορίες ή όταν εκτελεί δραστηριότητες επεξεργασίας πληροφοριών με εξωτερικούς φορείς μέσω συμφωνιών επιπέδου υπηρεσίας (SLA) και στενής παρακολούθησης.
* Η διοίκηση παρακολουθεί στενά τη συμμόρφωση με τις πολιτικές και τις διαδικασίες ασφάλειας πληροφοριών.
* Ο Υπεύθυνος Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών επανεξετάζει την πολιτική ασφάλειας πληροφοριών τουλάχιστον μια φορά τον χρόνο και την ενημερώνει όπως απαιτείται.
* Επιτρέπονται εξαιρέσεις από μέρη αυτής της πολιτικής, μόνο εάν έχουν εξουσιοδοτηθεί από την διοίκηση.

Στο πλαίσιο της Πολιτικής συμπεριλαμβάνονται οι υπευθυνότητες που οφείλει κάθε εργαζόμενος να τηρεί:

1. Καθορισμός Ρόλων και Ευθυνών: Κάθε μέλος του προσωπικού οφείλει να γνωρίζει και να συμμορφώνεται με τον καθορισμένο ρόλο και τις ευθύνες του σχετικά με την ασφάλεια πληροφοριών.

2. Εκπαίδευση και Ευαισθητοποίηση: Παρέχεται συστηματική εκπαίδευση σε όλους τους εργαζόμενους για την αναγνώριση, την αντιμετώπιση, και την πρόληψη απειλών στην ασφάλεια πληροφοριών.

Η συνεχής αναθεώρηση και εφαρμογή της Πολιτικής Ασφάλειας Πληροφοριών αποτελεί θεμελιώδη διαδικασία για τη διασφάλιση της ασφάλειας των πληροφοριών του Οργανισμού και την προάσπιση των συμφερόντων του. Έτσι επιτυγχάνονται:

1. Εξασφάλιση Εμπιστευτικότητας: Η προστασία της εμπιστευτικότητας των πληροφοριών του [Όνομα Οργανισμού] αποτελεί προτεραιότητα, εξασφαλίζοντας ότι οι πληροφορίες δεν διαρρέουν σε μη εξουσιοδοτημένα πρόσωπα.

2. Διαθεσιμότητα Πληροφοριών: Η πρόσβαση σε πληροφορίες πρέπει να είναι διαθέσιμη όταν απαιτείται, εξασφαλίζοντας τη συνεχή λειτουργία των επιχειρησιακών διαδικασιών.

Η συγκεκριμένη Πολιτική Ασφάλειας Πληροφοριών θα μπορούσε να συνδεθεί με τις ακόλουθες πολιτικές:

1. Πολιτική Διαχείρισης Κινδύνων: Καθορίζει τις διαδικασίες για την αναγνώριση, την αξιολόγηση και τον χειρισμό κινδύνων που ενδέχεται να επηρεάσουν την ασφάλεια πληροφοριών.

2. Πολιτική Αντιμετώπισης Παραβάσεων: Καθορίζει τις διαδικασίες για την ανίχνευση, την αντιμετώπιση και την αποκατάσταση παραβιάσεων της πολιτικής ασφάλειας πληροφοριών.

Πιο συγκεκριμένα, στον [Όνομα Οργανισμού] έχουν θεσπιστεί τα πιο κάτω μέτρα:

* Δημιουργήθηκε, εγκρίθηκε, εφαρμόζετε και αναθεωρείται στρατηγική ασφάλειας πληροφοριών στην οποία αναλύονται οι στόχοι και η προσέγγιση υψηλού επιπέδου με σκοπό τον μετριασμό των κινδύνων για την ασφάλεια πληροφοριών.
* Έχουν καθοριστεί οι ρόλοι και οι αρμοδιότητες σχετικά με την ασφάλεια πληροφοριών εντός του οργανισμού, όπου θα πρέπει να καθορίζεται από την διοίκηση, ώστε να εξασφαλίζεται η υπευθυνότητα για τις αποφάσεις της διοίκησης που σχετίζονται με την ασφάλεια δικτύων και συστημάτων πληροφοριών.
* Εξασφαλίζεται η συμμόρφωση με όλες τις εφαρμοστέες νομικές και κανονιστικές υποχρεώσεις όσον αφορά την ασφάλεια δικτύων και πληροφοριών.
* Δημιουργούνται, εγκρίνονται, εφαρμόζονται και αναθεωρούνται πολιτικές, πρότυπα, κατευθυντήριες γραμμές και διαδικασίες για την ασφάλεια πληροφοριών που να αντικατοπτρίζουν τη στρατηγική ασφάλειας πληροφοριών.
* Δημιουργούνται, εγκρίνονται, εφαρμόζονται και αναθεωρούνται επί μέρους πολιτικές και διαδικασίες ώστε να υποστηρίζουν την πολιτική ασφάλειας πληροφοριών
* Δημιουργήθηκε, εγκρίθηκε, εφαρμόζετε και αναθεωρείται μεθοδολογία διαχείρισης κινδύνων, η οποία αντικατοπτρίζει τη διαδικασία εκτίμησης κινδύνου του οργανισμού, τα κριτήρια ανάλυσης κινδύνου, τα κριτήρια αποδοχής κινδύνων και την πολιτική ανάληψης κινδύνων.
* Καταρτίσθηκε κατάλογος στοιχείων ενεργητικού, συστημάτων και διαδικασιών εντός του οργανισμού.
* Έχουν εντοπιστεί οι απειλές, ευπάθειες και κίνδυνοι στους οποίους εκτίθενται τα στοιχεία ενεργητικού, τα συστήματα και οι διαδικασίες του οργανισμού.
* Διενεργούνται αξιολογήσεις κινδύνου για να ληφθούν τα κατάλληλα μέτρα διαφύλαξης της εμπιστευτικότητας, της ακεραιότητας, της διαθεσιμότητας και της αυθεντικότητας των πληροφοριών σύμφωνα με τις επιχειρησιακές ανάγκες του οργανισμού.
* Καταγράφονται ανάγκες εκπαίδευσης και υλοποιείται το σχετικό πρόγραμμα εκπαίδευσης
* Όπου η αγορά προϊόντων ή υπηρεσιών ανατίθεται σε εξωτερικούς συνεργάτες, επιβεβαιώνεται η τήρηση των απαιτήσεων του Πλαισίου Μέτρων Ασφάλειας μέσω συμβάσεων, ελέγχων και πιθανών άλλων μέτρων
* Εξασφαλίζεται η προστασία δεδομένων καθ’ όλο τον κύκλο ζωής των πληροφοριών.
* Εξασφαλίζεται η ταξινόμηση και η επισήμανση των δεδομένων κατά τρόπο ώστε να αντικατοπτρίζεται η ευαισθησία τους ώστε να εξασφαλίζεται η κατάλληλη επεξεργασία τους.
* Έχει καταστεί δυνατή η αποκατάσταση των πληροφοριών στο πλαίσιο συμβάντων και περιστατικών ασφάλειας.
* Έχουν εφαρμοστεί επαρκή μέτρα στο πλαίσιο της διαβίβασης και ανταλλαγής πληροφοριών εσωτερικά ή με τρίτα μέρη, προκειμένου να διασφαλιστεί η ασφαλής μεταφορά δεδομένων.
* Έχει εξασφαλιστεί η προστασία των δεδομένων από εκούσια ή ακούσια απώλεια και διαρροή δεδομένων.
* Διασφαλίζεται ότι οι αλλαγές στις διαδικασίες και τα συστήματα πληροφοριών εφαρμόζονται με ασφάλεια, χωρίς να θίγεται το απόρρητο, η ακεραιότητα, η διαθεσιμότητα, ή η αυθεντικότητα των πληροφοριών.
* Εντοπίζονται, διατηρούνται και επαληθεύονται οι πληροφορίες για τα στοιχεία ενεργητικού και τις διαμορφώσεις του [Όνομα Οργανισμού].
* Διασφαλίζεται ότι τα στοιχεία ενεργητικού είναι ασφαλή καθ’ όλη τη διάρκεια του κύκλου ζωής τους, συμπεριλαμβανομένης της προμήθειας, της ανάπτυξης, της συντήρησης και της διάθεσης τους.
* Διασφαλίζεται ότι τα στοιχεία ενεργητικού καταγράφονται σε κατάλογο και ότι η ιδιοκτησία καθορίζεται με σκοπό την επίτευξη της ιχνηλασιμότητας και της ευθύνης για τα στοιχεία.
* Διασφαλίζεται ότι τα στοιχεία ενεργητικού είναι υπό παρακολούθηση για επιθέσεις, ανωμαλίες και απειλές κατά της ασφάλειας, προκειμένου να ενεργοποιηθούν οι διαδικασίες για την αντιμετώπιση συμβάντων και περιστατικών.
* Διασφαλίζεται η διαθεσιμότητα δικτύων και συστημάτων πληροφοριών με την επίτευξη επαρκούς διαθεσιμότητας πόρων, εφεδρείας και συστημάτων / διαδικασιών υψηλής διαθεσιμότητας.
* Διασφαλίζεται η εμπιστευτικότητα, ακεραιότητα και αυθεντικότητα των πληροφοριών με την υιοθέτηση κατάλληλων κρυπτογραφικών λύσεων.
* Εξασφαλίζεται η κατάλληλη χωρητικότητα και επίδοση των υπηρεσιών των συστημάτων και διαδικασιών πληροφοριών.
* Επαληθεύει την αυθεντικότητα και εξουσιοδότηση χρηστών, με βάση το ελάχιστο προνόμιο και τους οργανωτικούς ρόλους και αρμοδιότητες.
* Εξασφαλίζονται επαρκή μέτρα στο πλαίσιο της εξωτερικής πρόσβασης σε οργανωτικούς πόρους.
* Εξασφαλίζονται επαρκή μέτρα για τους χρήστες που έχουν προνομιακή πρόσβαση σε οργανωτικούς πόρους, συστήματα και δίκτυα.
* Εξασφαλίζεται ότι γίνεται η επαλήθευση της ταυτότητας των εξουσιοδοτημένων ατόμων με ασφάλεια και με τη χρήση μέτρων ισχυρής επαλήθευσης ταυτότητας.
* Διασφαλίζεται η ασφαλής διαχείριση διαπιστευτηρίων για πρόσβαση σε εταιρικούς πόρους, και ότι επαληθεύεται η ταυτότητα των χρηστών με ασφάλεια για χρήση υπηρεσιών του [Όνομα Οργανισμού].
* Διασφαλίζεται η μη-άρνηση ανιχνευσιμότητας των ενεργειών των χρηστών που εκτελούνται στο πλαίσιο των οργανωτικών πόρων, ώστε να είναι δυνατή η ανίχνευση και η διερεύνηση εκούσιων ή ακούσιων δραστηριοτήτων που έχουν αρνητικό αντίκτυπο.
* Διασφαλίζεται ότι οι ρόλοι και η έγκριση της ταυτότητας αντικατοπτρίζουν τον κύκλο ζωής της ταυτότητας του χρήστη.
* Διασφαλίζεται ότι οι ευπάθειες συστημάτων είναι γνωστές στον οργανισμό, προκειμένου να τυχαίνουν κατάλληλου χειρισμού.
* Διασφαλίζεται ότι οι ευπάθειες καταγράφονται και υποβάλλονται σε σχετικές εκθέσεις, ώστε να είναι δυνατή η λήψη τεκμηριωμένων αποφάσεων από τη διοίκηση όσον αφορά τον χειρισμό τους.
* Εξασφαλίζεται η αποκατάσταση των ευπαθειών συστημάτων και η εφαρμογή ενημερώσεων ασφάλειας, κατόπιν απόφασης της διοίκησης.
* Διασφαλίζεται ότι η διεπαφή του τοπικού δικτύου με το εξωτερικό δίκτυο προστατεύεται από επιθέσεις, απειλές και άλλες εκούσιες ή ακούσιες ενέργειες με δυνητικά αρνητικές επιπτώσεις.
* Εξασφαλίζεται ο διαχωρισμός του λογικού δικτύου, σύμφωνα με τις επιχειρηματικές λειτουργίες, και αποφεύγεται η εξάπλωση κακόβουλων στοιχείων.
* Διασφαλίζεται η προστασία των οργανωτικών πόρων από επιθέσεις άρνησης παροχής υπηρεσιών, και ότι δεν επηρεάζονται οι νόμιμες δραστηριότητες παροχής υπηρεσιών.
* Διασφαλίζονται κατάλληλα πρωτόκολλα επικοινωνίας προκειμένου να επιτευχθεί ασφαλής επικοινωνία μεταξύ των πόρων του δικτύου.
* Εξασφαλίζεται ότι η πρόσβαση στο λογικό δίκτυο από εξωτερικά και εσωτερικά συστήματα ασφαλίζεται κατάλληλα, ώστε μόνο τα εξουσιοδοτημένα πρόσωπα να μπορούν να έχουν πρόσβαση σε οργανωτικούς πόρους.
* Εξασφαλίζεται η διαθεσιμότητα πληροφοριών και δικτύων πληροφοριών με την επίτευξη επαρκούς διαθεσιμότητας πόρων, εφεδρικού εξοπλισμού, συστημάτων και συνδέσεων υψηλής διαθεσιμότητας.
* Διασφαλίζεται η ανίχνευση και η πρόληψη από εξωτερικές απόπειρες εισβολής και επιθέσεις ασφάλειας.
* Διασφαλίζεται ότι δεν θα επηρεαστούν οργανωτικοί πόροι από κακόβουλο λογισμικό και κώδικα.
* Ελαχιστοποιείται, στο μέτρο του δυνατού, η επιφάνεια επίθεσης των συστημάτων πληροφοριών, μέσω της μείωσης της λειτουργικότητας και των χαρακτηριστικών τους.
* Εξασφαλίζεται η κατάλληλη ασφάλεια των κινητών συσκευών που έχουν πρόσβαση σε οργανωτικούς πόρους.
* Διασφαλίζεται η κατάλληλη διαχείριση των εφαρμογών που χρησιμοποιούνται για την πρόσβαση ή επεξεργασία οργανωτικών πόρων.
* Διασφαλίζεται επαρκή μέτρα ασφάλειας στο πλαίσιο των δραστηριοτήτων ανάπτυξης λογισμικού που αναπτύσσει ο [Όνομα Οργανισμού].
* Υλοποιούνται επαρκή μέτρα για την εξασφάλιση ότι τα στελέχη που εργάζονται για λογαριασμό του οργανισμού, τα οποία έχουν πρόσβαση σε οργανωτικούς πόρους, υποστηρίζουν την πολιτική ασφάλειας πληροφοριών και τους στόχους του οργανισμού.
* 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.
* 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 [Όνομα Οργανισμού].
* Εξασφαλίζεται ότι οι εξωτερικοί συνεργάτες που εργάζονται για λογαριασμό του οργανισμού τηρούν την πολιτική ασφάλειας πληροφοριών και τους στόχους ασφάλειας του [Όνομα Οργανισμού].
* Εξασφαλίζεται η προστασία από απειλές κατά της ασφάλειας δικτύων και πληροφοριών από το εσωτερικό του [Όνομα Οργανισμού].
* Διασφαλίζεται 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.
* Εξασφαλίζονται επαρκή μέτρα για την προστασία του [Όνομα Οργανισμού] από τις επιπτώσεις φυσικών καταστροφών, όπως οι πλημμύρες, οι σεισμοί και οι πυρκαγιές.
* Διασφαλίζεται η φυσική περίμετρος του οργανισμού, με την εξασφάλιση και αποτροπή της μη εξουσιοδοτημένης πρόσβασης.
* Εξασφαλίζεται έλεγχος της πρόσβασης σε εσωτερικούς χώρους εργασίας και τις εγκαταστάσεις, ώστε να διασφαλίζεται ότι η φυσική πρόσβαση περιορίζεται κατόπιν ανάγκης.
* Εξασφαλίζεται ότι για την καλωδίωση και τον εξοπλισμό που υποστηρίζουν την επεξεργασία των πληροφοριών, εξασφαλίζεται η φυσική προστασία από παρεμβολές, υποκλοπή ή ζημιά.
* Εξασφαλίζεται ότι οι εσωτερικοί χώροι και οι εγκαταστάσεις του οργανισμού προστατεύονται από φυσικές ζημιές.
* Διασφαλίζεται ότι ο [Όνομα Οργανισμού] είναι σε θέση να εντοπίζει συμβάντα και περιστατικά που ενδέχεται να συνιστούν απειλή για τους στόχους της ασφάλειας πληροφοριών του οργανισμού και να ενεργοποιεί τις αντίστοιχες διαδικασίες αντιμετώπισης περιστατικών.
* Διασφαλίζεται ότι ο [Όνομα Οργανισμού] είναι σε θέση να αναλύει και να αξιολογεί συμβάντα και περιστατικά που αφορούν την ασφάλεια πληροφοριών, ούτως ώστε να ενεργοποιεί κατάλληλες διαδικασίες περιορισμού και ανάκτησης.
* Εξασφαλίζεται επαρκής περιορισμός και αποκατάσταση από συμβάντα και περιστατικά ασφάλειας που επηρεάζουν αρνητικά τους στόχους ασφάλειας πληροφοριών του [Όνομα Οργανισμού].
* Διασφαλίζεται ότι ο [Όνομα Οργανισμού] μαθαίνει από συμβάντα και περιστατικά ασφάλειας, προκειμένου να αποτρέπονται παρόμοια συμβάντα και περιστατικά στο μέλλον.
* Διασφαλίζεται ότι ο [Όνομα Οργανισμού] ενημερώνει τα σχετικά ενδιαφερόμενα μέρη στην περίπτωση συμβάντων ή περιστατικών ασφάλειας, όπως περιγράφεται σε νομικές και ρυθμιστικές υποχρεώσεις.
* Εξασφαλίζεται ότι ο [Όνομα Οργανισμού] κοινοποιεί πληροφορίες σχετικά με συμβάντα και περιστατικά ασφάλειας δικτύων και πληροφοριών σε εσωτερικούς και εξωτερικούς ενδιαφερόμενους φορείς.
* Δημιουργούνται, ενημερώνονται και ελέγχονται το Πλάνο Επιχειρησιακής Συνέχειας και το Πλάνο Αποκατάστασης από Καταστροφή
* Εξασφαλίζεται ότι ο οργανισμός έχει αναλύσει και αξιολογήσει τις κρίσιμες επιχειρηματικές διαδικασίες που πρέπει να ληφθούν υπόψη στο σχέδιο επιχειρησιακής συνέχειας, ώστε να μπορέσει ο οργανισμός να αποκαταστήσει τις επιχειρηματικές διαδικασίες σε αποδεκτό επίπεδο το συντομότερο δυνατόν, σε περίπτωση συμβάντος ή περιστατικού.
* Εξασφαλίζεται ότι ο [Όνομα Οργανισμού] διαθέτει σχέδιο για τη διατήρηση της συνέχειας των κρίσιμων επιχειρηματικών διαδικασιών και την αποκατάσταση κατά τη διάρκεια συμβάντος ή περιστατικού και μετά από αυτό.
* Διασφαλίζεται ότι ο [Όνομα Οργανισμού] και τα στελέχη του γνωρίζουν τις ευθύνες τους κατά τη διάρκεια ενός συμβάντος ή περιστατικού που ενεργοποιεί το σχέδιο επιχειρησιακής συνέχειας.
* Εξασφαλίζεται ότι ο [Όνομα Οργανισμού] διαθέτει σχέδιο για την αποκατάσταση των συστημάτων κρίσιμων πληροφοριών σε αποδεκτό επίπεδο κατά τη διάρκεια ή μετά από περιστατικό.
* Αξιολογούνται η αποτελεσματικότητα και η αποδοτικότητα του Πλαισίου Μέτρων Ασφάλειας μέσω των ελέγχων και της διαδικασίας παρουσίασης στην Διεύθυνση.
* Αναφέρονται και διερευνώνται τα περιστατικά μη συμμόρφωσης και διασφαλίζεται η έγκαιρη λήψη των κατάλληλων μέτρων ώστε να ελαχιστοποιηθεί τυχόν επιχειρησιακή ζημιά.

# Ρόλους και Αρμοδιότητες

* Διοικητικό συμβούλιο(Board of Directors):
* Επίβλεψη/κατανόηση κινδύνων και θεμάτων για την ασφάλεια στον κυβερνοχώρο.
* Συμβουλευτείτε την ομάδα Εκτελεστική Ηγεσία για να κατανοήσετε την όρεξη για κινδύνους και την ωριμότητα ασφάλειας.
* Εκτελεστική Ηγεσία(Executive Leadership):
* Άριστη κατανόηση των κινδύνων ασφαλείας και των πιθανών αδύνατων σημείων.
* Να αξιολογείτε συνεχώς την όρεξη για κινδύνους έναντι πιθανών απειλών.
* Ενσωματώστε την ασφάλεια στη στρατηγική της εταιρείας.
* Διαδρομή επικοινωνίας για θέματα ασφαλείας στο Διοικητικό Συμβούλιο.
* Προϊστάμενος Ασφαλείας(Head of Security):
* Ευθυγραμμίζει τις πολιτικές και τις πρακτικές Ασφάλειας Πληροφοριών με βάση την αποστολή του [Όνομα Οργανισμού], τους στρατηγικούς στόχους και την ανάληψη κινδύνου.
* Εξυπηρετεί ως πρεσβευτής ασφαλείας τον [Όνομα Οργανισμού] και στις εξωτερικές δεσμεύσεις (π.χ. σύνδεσμος με την εκτελεστική ομάδα, το Διοικητικό Συμβούλιο, τις δεσμεύσεις που αντιμετωπίζουν πελάτες για θέματα ασφάλειας).
* Καθορίζει και εκτελεί το πρόγραμμα ασφάλειας σε ολόκληρο τον οργανισμό.
* Δημιουργήστε ένα σε βάθος προφίλ κινδύνου και ωριμότητας για τον [Όνομα Οργανισμού] και χρησιμοποιήστε το για να σχεδιάσετε πρωτοβουλίες.
* Υπεύθυνος για την επίβλεψη των πολιτικών ασφαλείας.
* Υπεύθυνος για την παρακολούθηση κινδύνων ασφαλείας και τη δημιουργία σχεδίων αποκατάστασης.
* Κοινοποιεί τους κινδύνους για την ασφάλεια των πληροφοριών στην εκτελεστική ηγεσία.

Υπεύθυνος Συμμόρφωσης (Compliance Manager):

* Συνεργάζεται με την κατάλληλη εκτελεστική ηγεσία για τη δημιουργία ενός πλαισίου ασφάλειας πληροφοριών και ενός προγράμματος ευαισθητοποίησης.
* Δημιουργεί και διατηρεί ένα Πλαίσιο Διαχείρισης Κινδύνων Ασφάλειας Πληροφοριών και Επιχειρήσεων.
* Εκτίμηση και διαχείριση κινδύνου: Προσδιορισμός και αξιολόγηση πιθανών κινδύνων και τρωτών σημείων για τα πληροφοριακά συστήματα και τα περιουσιακά στοιχεία του οργανισμού. Ανάπτυξη και εφαρμογή στρατηγικών και ελέγχων μετριασμού του κινδύνου για την ελαχιστοποίηση των επιπτώσεων συμβάντων ασφαλείας ή παραβιάσεων.
* Ανάπτυξη και επιβολή πολιτικής: Καθιερώστε πολιτικές, πρότυπα και διαδικασίες ασφάλειας πληροφοριών που ευθυγραμμίζονται με τις βέλτιστες πρακτικές του κλάδου και τις κανονιστικές απαιτήσεις.
* Ευαισθητοποίηση και εκπαίδευση σε θέματα ασφάλειας: Αναπτύξτε και παραδώστε προγράμματα ευαισθητοποίησης για την ασφάλεια των πληροφοριών για την εκπαίδευση των εργαζομένων σχετικά με πιθανούς κινδύνους ασφάλειας, τις βέλτιστες πρακτικές και τους ρόλους και τις ευθύνες τους στη διαφύλαξη των πληροφοριών.
* Έλεγχοι και αξιολογήσεις ασφάλειας: Διεξάγετε περιοδικούς ελέγχους και αξιολογήσεις ασφάλειας για την αξιολόγηση της αποτελεσματικότητας των ελέγχων ασφαλείας και τον εντοπισμό περιοχών προς βελτίωση. Συνεργαστείτε με εσωτερικούς και εξωτερικούς ελεγκτές για τη διασφάλιση της συμμόρφωσης με τις κανονιστικές απαιτήσεις και τα πρότυπα του κλάδου.
* Διαχείριση κινδύνων προμηθευτών και τρίτων: Αξιολογήστε τη στάση ασφαλείας τρίτων προμηθευτών και συνεργατών για να αξιολογήσετε τους πιθανούς κινδύνους για τον οργανισμό. Καθιερώστε κατευθυντήριες γραμμές και διαδικασίες για την αξιολόγηση, την επιλογή και την παρακολούθηση των προμηθευτών με βάση τις δυνατότητες ασφαλείας τους και τη συμμόρφωσή τους με τα πρότυπα ασφάλειας πληροφοριών.
* Διακυβέρνηση ασφάλειας και παρακολούθηση συμμόρφωσης: Παρακολουθήστε και μετρήστε τη συμμόρφωση με τις πολιτικές ασφαλείας, τους ελέγχους και τις κανονιστικές απαιτήσεις. Διεξάγετε τακτικές εσωτερικές αξιολογήσεις και ελέγχους για τη διασφάλιση της τήρησης των καθιερωμένων πλαισίων και προτύπων ασφαλείας.
* Συνεχής βελτίωση και τάσεις του κλάδου: Μείνετε ενημερωμένοι για τις πιο πρόσφατες απειλές ασφαλείας, τάσεις και ρυθμιστικές αλλαγές. Συνεχής βελτίωση των πρακτικών και των διαδικασιών ασφάλειας πληροφοριών με βάση τις εξελίξεις του κλάδου και τα διδάγματα που αντλήθηκαν από συμβάντα ασφαλείας.

Ιδιοκτήτες ελέγχου(Control Owners):

* Έλεγχος σχεδιασμού σε συνεργασία με την ομάδα συμμόρφωσης και ασφάλειας.
* Έλεγχος συλλογής αποδεικτικών στοιχείων και υποβολής για επανεξέταση.
* Συντήρηση ελέγχου (δηλαδή καθώς αλλάζουν οι διαδικασίες της εταιρείας, τυχόν αξιόπιστοι έλεγχοι πρέπει να προσαρμοστούν).
* Εκπροσώπηση ελέγχου για τυχόν εσωτερικούς και εξωτερικούς ελέγχους.

 Ιδιοκτήτες Συστήματος(System Owners):

* Διαχειρίζονται την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των πληροφοριακών συστημάτων για τα οποία είναι υπεύθυνα, σύμφωνα με τις πολιτικές του [Όνομα Οργανισμού] για την ασφάλεια των πληροφοριών και το απόρρητο.
* Έγκριση αιτημάτων τεχνικής πρόσβασης και αλλαγής για μη τυπική πρόσβαση (ετήσιες αναθεωρήσεις).

Εργαζόμενοι του [Όνομα Οργανισμού], Εργολάβοι, έκτακτοι εργαζόμενοι(Employees,Contractors):

* Ενεργώντας ανά πάσα στιγμή με τρόπο που δεν θέτει σε κίνδυνο τα περιουσιακά στοιχεία του [Όνομα Οργανισμού].
* Βοηθά στον εντοπισμό του κινδύνου ως μέρος της διαδικασίας διαχείρισης κινδύνου και στην εφαρμογή επανορθώσεων.
* Τήρηση των πολιτικών και των προτύπων συμπεριφοράς της εταιρείας.
* Αναφορά περιστατικών και παρατηρούμενων ανωμαλιών ή αδυναμιών.

# Οδηγίες για τυποποιημένες διαδικασίες λειτουργίες

Ο [Όνομα Οργανισμού] θα πρέπει να διαθέτει μια διαδικασία για τον καθορισμό των διαδικασιών. Αυτές οι SOP [τυποποιημένες διαδικασίες λειτουργίας] θα πρέπει στη συνέχεια να γραφτούν από ιδιώτες που γνωρίζουν τη δραστηριότητα και την εσωτερική δομή του οργανισμού.

Τα SOP [τυποποιημένες διαδικασίες λειτουργίας] θα πρέπει να είναι γραμμένα με επαρκή λεπτομέρεια, έτσι ώστε κάποιος με περιορισμένη εμπειρία ή γνώση της διαδικασίας, αλλά με βασική κατανόηση, μπορεί να αναταράξει με επιτυχία τη διαδικασία όταν δεν υπάρχει επίβλεψη. Η απαίτηση εμπειρίας για την εκτέλεση μιας δραστηριότητας θα πρέπει να σημειωθεί στην ενότητα για τα προσόντα του προσωπικού.

# Συμμόρφωση

# Συμμόρφωση με την 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.

Πέραν της Πολιτικής Ασφάλειας Πληροφοριών, έχουν εφαρμοστεί συγκεκριμένες πολιτικές και διαδικασίες για την ασφάλεια πληροφοριών σε σχέση με συγκεκριμένες επεξεργασίες, συστήματα ή δραστηριότητες, ανάλογα με τις ανάγκες.

Επιπρόσθετα, έχουν καθοριστεί επιχειρησιακές κατευθυντήριες γραμμές για την ασφάλεια πληροφοριών καθώς και τυποποιημένες διαδικασίες λειτουργίας για συγκεκριμένες δραστηριότητες που σχετίζονται με πληροφορίες ή συστήματα επεξεργασίας πληροφοριών σε επιχειρησιακό επίπεδο.

Η Διεύθυνση και οι Προϊστάμενοι αναμένουν ότι όλο το προσωπικό θα συμμορφωθεί με τις οδηγίες που παρουσιάζονται στο πλαίσιο αυτής της πολιτικής. Θα πραγματοποιούνται επίσης έλεγχοι συμμόρφωσης για ανασκόπηση της αποτελεσματικότητας της εφαρμογής.

# Εξαιρέσεις

Στις ακόλουθες έκτακτες περιπτώσεις, για ορισμένα μέρη της πολιτικής, ενδέχεται να μην απαιτείται αυστηρή συμμόρφωση. Τα μέρη για τα οποία μπορεί να συμβεί το πιο πάνω εξαρτώνται από τις συγκεκριμένες συνθήκες του περιστατικού που διερευνάται.

* Εάν συμμόρφωση με την πολιτική μπορεί να οδηγήσει σε σωματική βλάβη ή τραυματισμό υπαλλήλου
* Εάν συμμόρφωση με την πολιτική μπορεί να προκαλέσει σοβαρές ζημιές στη φήμη του Οργανισμού ή στην δυνατότητα του να λειτουργήσει
* Εάν προκύψει έκτακτη ανάγκη

Στις υπό αναφορά περιπτώσεις, ο ενδιαφερόμενος υπάλληλος πρέπει να λαμβάνει τα ακόλουθα μέτρα:

* Βεβαιωθείτε ότι κάποιος Προϊστάμενος γνωρίζει την κατάσταση και τις ενέργειες που πρέπει να ληφθούν
* Βεβαιωθείτε ότι η κατάσταση και οι ενέργειες, καταγράφονται με όσο περισσότερη λεπτομέρεια είναι δυνατόν, σε μία έκθεση μη-συμμόρφωσης
* Βεβαιωθείτε ότι η κατάσταση αναφέρθηκε το συντομότερο δυνατό στον Υπεύθυνο Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών

Αποτυχία στη λήψη των πιο πάνω ενεργειών ενδέχεται να έχει ως αποτέλεσμα να αναληφθούν πειθαρχικά μέτρα.

Επιπλέον, ο Υπεύθυνος Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών διατηρεί ένα κατάλογο των γνωστών εξαιρέσεων και μη συμμορφώσεων στην πολιτική. Αυτός ο κατάλογος περιλαμβάνει:

* Γνωστές παραβιάσεις που βρίσκονται στο στάδιο να διορθωθούν
* Μικρότερης σημασίας παραβιάσεις που δεν θεωρούνται να αξίζουν οποιουδήποτε χειρισμού
* Περιπτώσεις στις οποίες η πολιτική δεν θεωρείται ότι εφαρμόζεται

# Κυρώσεις

Μη συμμόρφωση 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.

Οι κυρώσεις μπορεί να περιλαμβάνουν τερματισμό της απασχόλησης ή ρυθμίσεις στη σύμβαση (εάν υπάρχει) ή αστική ή ποινική δίωξη.