Όνομα Οργανισμού

Πλάνο Εκπαιδεύσεων Ευαισθητοποίησης

|  |  |
| --- | --- |
| **Περιεχόμενο:** | Πλάνο Εκπαιδεύσεων Ευαισθητοποίησης |
| **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

[1. Εισαγωγή 4](#_Toc154573037)

[2. Σκοπός 4](#_Toc154573038)

[3. Πεδίο Εφαρμογής 4](#_Toc154573039)

[4. Σχέδιο Ευαισθητοποίησης και Εκπαίδευσης 4](#_Toc154573040)

[5. Χρόνος 6](#_Toc154573041)

[6. Ευθύνες 6](#_Toc154573042)

[6.1. Προϊστάμενος Ασφάλειας Πληροφοριών 7](#_Toc154573043)

[6.2. Προϊστάμενοι Τμημάτων / Υπεύθυνοι Υπηρεσιών: 7](#_Toc154573044)

[6.3. Υπάλληλοι: 7](#_Toc154573045)

[7. Έγγραφα Ελέγχου Ποιότητας 7](#_Toc154573046)

[8. Δράση 9](#_Toc154573047)

# Εισαγωγή

Το έγγραφο αυτό καθορίζει το Πλάνο Εκπαιδεύσεων Ευαισθητοποίησης για την Ασφάλεια Πληροφοριών και την Κυβερνοασφάλεια του [Όνομα Οργανισμού].

Το Πλάνο αυτό έχει θεσπιστεί λαμβάνοντας υπόψη τα στοιχεία που περιγράφονται στις πολιτικές, τα πρότυπα, τις κατευθυντήριες γραμμές και τις διαδικασίες ασφάλειας πληροφοριών.

Ο [Όνομα Οργανισμού] παρέχει εκπαίδευση προς όλα τα στελέχη του, όπως ορίζεται στο πλάνο ασφάλειας πληροφοριών που ακολουθεί.

# Σκοπός

Σκοπός είναι ο καθορισμός του πλάνου εκπαιδεύσεων ευαισθητοποίησης όσον αφορά την ασφάλεια των πληροφοριών, ώστε να υπάρχει επαρκής ευαισθητοποίηση των στελεχών σχετικά με τους ρόλους και τις ευθύνες όσον αφορά την ασφάλεια δικτύων και πληροφοριών.

Επίσης, η επαρκής ενημέρωση των στελεχών σχετικά με τους ρόλους και τις αρμοδιότητες τους όσον αφορά την ασφάλεια δικτύων και πληροφοριών, μέσω της κατάλληλης εκπαίδευσης και κατάρτισης που προσφέρεται με την υποστήριξη της διοίκησης ανώτατου επιπέδου.

Οι εκπαιδεύσεις σχετικά με την ασφάλεια πληροφοριών περιλαμβάνουν συγκεκριμένες πληροφορίες σχετικά με τις επιχειρησιακές δραστηριότητες των στελεχών για λογαριασμό του [Όνομα Οργανισμού] στο πλαίσιο της επεξεργασίας πληροφοριών ή της πρόσβασης σε συστήματα επεξεργασίας πληροφοριών.

# Πεδίο Εφαρμογής

Αυτό το πλάνο καλύπτει όλες τις δραστηριότητες για αναγνώριση και ικανοποίηση των απαιτήσεων εκπαίδευσης και ενημέρωσης του προσωπικού του [Όνομα Οργανισμού] σε θέματα ασφάλειας πληροφοριών.

# Σχέδιο Ευαισθητοποίησης και Εκπαίδευσης

Ο Κανονισμός Κ.Δ.Π. 389/2020 προτείνει ο [Όνομα Οργανισμού] να:

* θεσπιστεί πρόγραμμα ενημέρωσης σχετικά με την ασφάλεια πληροφοριών για όλα τα στελέχη εντός του [Όνομα Οργανισμού], λαμβάνοντας υπόψη τα στοιχεία που περιγράφονται στις πολιτικές, τα πρότυπα, τις κατευθυντήριες γραμμές και τις διαδικασίες ασφάλειας πληροφοριών. Οφείλει να καθορίσει πρόγραμμα ευαισθητοποίησης όσον αφορά την ασφάλεια των πληροφοριών, ώστε να υπάρχει επαρκής ευαισθητοποίηση των στελεχών σχετικά με τους ρόλους και τις ευθύνες όσον αφορά την ασφάλεια δικτύων και πληροφοριών [ΤΑ1].
* Παρέχει εκπαίδευση προς όλα τα στελέχη του [Όνομα Οργανισμού], όπως ορίζεται στο πρόγραμμα ασφάλειας πληροφοριών. Οφείλει να ενημερώνει επαρκώς τα στελέχη σχετικά με τους ρόλους και τις αρμοδιότητες τους όσον αφορά την ασφάλεια δικτύων και πληροφοριών, μέσω κατάλληλης εκπαίδευσης και κατάρτισης που προσφέρεται με την υποστήριξη της διοίκησης ανώτατου επιπέδου. Οι εκπαιδεύσεις σχετικά με την ασφάλεια πληροφοριών περιλαμβάνουν συγκεκριμένες πληροφορίες για τις επιχειρησιακές δραστηριότητες των στελεχών για λογαριασμό του [Όνομα Οργανισμού] στο πλαίσιο της επεξεργασίας πληροφοριών ή της πρόσβασης σε συστήματα επεξεργασίας πληροφοριών [ΤΑ2].

Η προστασία των πληροφοριών και η αντιμετώπιση κυβερνοαπειλών αποτελούν κρίσιμο μέλημα για την επιτυχία και την ακεραιότητα του [Όνομα Οργανισμού]. Η δημιουργία ενός σχεδίου ευαισθητοποίησης και εκπαίδευσης θα ενισχύει την αντίληψη των εργαζομένων μας σε θέματα ασφάλειας πληροφοριών και κυβερνοασφάλειας.

Στόχος του πλάνου είναι η κατανόηση των βασικών αρχών ασφάλειας πληροφοριών και κυβερνοασφάλειας, η ευαισθητοποίηση σε σχέση με τις σύγχρονες κυβερνοαπειλές καθώς και η εκπαίδευση στην αντιμετώπιση κυβερνοεπιθέσεων και αντιδράσεις σε περιστατικά.

Τα βήματα που περιλαμβάνονται στο σχέδιο είναι:

1. Βασικές Αρχές Ασφάλειας Πληροφοριών:
* Ορισμός και σημασία ασφάλειας πληροφοριών
* Αναγνώριση και προστασία ευαίσθητων δεδομένων
* Διαχείριση πρόσβασης και προσωπικών στοιχείων
1. Κυβερνοασφάλεια:
* Εννοιολογία και σημασία της κυβερνοασφάλειας
* Κυβερνοαπειλές και τρέχουσες τάσεις
* Προληπτικά μέτρα και πρακτικές ασφαλούς συμπεριφοράς
1. Κυβερνοεπιθέσεις και Αντίδραση:
* Phishing και Social Engineering
* Κακόβουλο Λογισμικό και Επιθέσεις σε Δίκτυα
* Διαχείριση περιστατικών και αποκατάσταση μετά την επίθεση
1. Υποχρεώσεις Εργαζομένων και Αντίδραση σε Περιστατικά:
* Συμμόρφωση με τις πολιτικές ασφάλειας του οργανισμού
* Αναφορά ανωμαλιών και παραβιάσεων
* Προετοιμασία για αντίδραση σε περίπτωση κυβερνοεπίθεσης
1. Ευαισθητοποίηση Προσωπικού:
* Ενημέρωση για τις επιπτώσεις παραβιάσεων ασφάλειας
* Σενάρια και προσομοιωμένες καταστάσεις
* Προσωπική ευθύνη και συμβολή στην ασφάλεια

Για την εφαρμογή του πλάνου ευαισθητοποίησης και εκπαίδευσης ο [Όνομα Οργανισμού] μπορεί να:

* Παρέχει εκπαιδευτικό υλικό και πλατφόρμες
* Πραγματοποιεί εκπαιδεύσεις με παρουσιάσεις, σεμινάρια, και προσομοιωμένες ασκήσεις
* Πραγματοποιεί περιοδικούς ελέγχους κατανόησης του περιεχομένου του προγράμματος
* Ενημερώνει διαρκώς για νέες απειλές και τεχνικές

Η αποτελεσματικότητα του προγράμματος θα αξιολογείται μέσω:

* Αξιολογήσεων συμμετοχής και κατανόησης
* Περιοδικών αξιολογήσεων από το προσωπικό
* Ανάλυσης στατιστικών περιστατικών κυβερνοεπιθέσεων και αντιμετώπισης περιστατικών
* Συλλογή ανατροφοδοτήσεων από τους συμμετέχοντες

Η διαρκής βελτίωση του σχεδίου θα εξασφαλίζει την προστασία του [Όνομα Οργανισμού] από τις σύγχρονες κυβερνοαπειλές και τη συμμετοχή όλων των εργαζομένων στον ενιαίο στόχο της κυβερνοασφάλειας.

# Χρόνος

Οι ανάγκες των αρμόδιων ατόμων για εκπαίδευση και ενημέρωση σε θέματα ασφάλειας πληροφοριών αναγνωρίζονται:

* Κατά την εκπόνηση του ετήσιου προγράμματος εκπαίδευσης και ενημέρωσης σε θέματα ασφάλειας πληροφοριών
* Κατά την εκπόνηση του ετήσιου προϋπολογισμού
* Κατά τη συμπλήρωση των ετήσιων αξιολογήσεων εκπαίδευσης και των ετήσιων αξιολογήσεων απόδοσης
* Ως αποτέλεσμα ενεργειών από διάφορες δραστηριότητες του [Όνομα Οργανισμού] π.χ. Εσωτερικό έλεγχο, Διαχείριση περιστατικών ασφάλειας
* Ως αποτέλεσμα αλλαγής στις επιχειρησιακές ανάγκες του [Όνομα Οργανισμού].

# Ευθύνες

Ο [Όνομα Οργανισμού] πρέπει να ορίσει μια Καθοδηγητική Επιτροπή Ασφάλειας Πληροφοριών η οποία θα απαρτίζεται από όλους τους Προϊσταμένους τμημάτων του Οργανισμού. Τα κριτήρια επιλογής ατόμων που θα απαρτίζουν την Επιτροπή, είναι άτομα τα οποία γνωρίζουν καλά τις διαδικασίες λειτουργίας του [Όνομα Οργανισμού] και είναι σε θέση να παίρνουν διοικητικές αποφάσεις σε κρίσιμες στιγμές χωρίς την προβλεπόμενη έγκριση.

Στην περίπτωση όπου ο [Όνομα Οργανισμού] είναι μικρός και η σύσταση αυτής της επιτροπής είναι αδύνατη, ο Προϊστάμενος Ασφάλειας Πληροφοριών δύναται να εκτελεί και τα καθήκοντα της επιτροπής εφόσον δεν οδηγούν σε σύγκρουση συμφερόντων και λαμβάνοντας υπόψη το επίπεδο κρισιμότητας του οργανισμού, με την έγκριση της Αρχής Ψηφιακής Ασφάλειας.

Η Καθοδηγητική Επιτροπή Ασφάλειας Πληροφοριών: έχει τη ευθύνη για έγκριση του ετήσιου προγράμματος εκπαίδευσης και ενημέρωσης σε θέματα ασφάλειας πληροφοριών ώστε να προάγεται η δέσμευση και η κουλτούρα ασφάλειας για τις πληροφορίες του [Όνομα Οργανισμού].

# Προϊστάμενος Ασφάλειας Πληροφοριών

* Υποστηρίζει τους Προϊσταμένους Τμημάτων και Υπεύθυνων Υπηρεσιών στην εκτέλεση του ρόλου τους όπως πιο κάτω, αναπτύσσοντας το ετήσιο πρόγραμμα με τις ανάγκες εκπαίδευσης που έχουν και εκπονώντας τον ανάλογο προϋπολογισμό
* Δίνει επανατροφοδότηση στην Καθοδηγητική Επιτροπή Ασφάλειας Πληροφοριών για εκπαιδευτικές ανάγκες, σύμφωνα με τις υφιστάμενες και μελλοντικές επιχειρησιακές ανάγκες
* Εγκρίνει το εκπαιδευτικό υλικό σε γενικής φύσης θέματα ασφάλειας πληροφοριών
* Εφαρμόζει λογισμικές εφαρμογές για την εκπαίδευση και ανάπτυξη του προσωπικού
* Μελετά και αξιολογά συστήματα και καλές πρακτικές για την εκπαίδευση και ενημέρωση του προσωπικού

Η/Ο Λειτουργός Ασφάλειας Πληροφοριών υποστηρίζει τον Προϊστάμενο Ασφάλειας Πληροφοριών σε όλες τις ευθύνες του/της (ετοιμάζει αναφορές, εκπαιδευτικό υλικό κ.α. και δίνει εξειδικευμένη καθοδήγηση και συμβουλές για τον κατάλληλο χειρισμό και τις καλές πρακτικές των θεμάτων ασφάλειας πληροφοριών). Για περαιτέρω πληροφορίες σχετικά με τις αρμοδιότητες του Προϊσταμένου Ασφάλειας Πληροφοριών, ανατρέξτε στην Πολιτική Διακυβέρνησης Ασφάλειας Πληροφοριών.

# Προϊστάμενοι Τμημάτων / Υπεύθυνοι Υπηρεσιών:

* Αναγνωρίζουν ανάγκες για εκπαίδευση και ενημέρωση σε θέματα ασφάλειας πληροφοριών
* Εφαρμόζουν τις υφιστάμενες πρακτικές για την εκπαίδευση και ενημέρωση του προσωπικού, καθώς και, όπου προνοείται, φροντίζουν για τη συμμετοχή του προσωπικού του Τμήματος/Υπηρεσίας τους στις δραστηριότητες του εκπαιδευτικού προγράμματος του οργανισμού
* Σε συνεργασία με το προσωπικό τους, αξιολογούν την ποιότητα ενός παροχέα εκπαιδευτικής δραστηριότητας.

# Υπάλληλοι:

* Αναγνώριση των αναγκών τους σε εκπαίδευση
* Συμμετοχή σε εκπαιδευτικές δραστηριότητες.
* Συμμετοχή σε πρακτικές εκπαιδευτικές δραστηριότητες.
* Συμμετοχή σε απρόοπτες δοκιμασίες γνώσεων διαφόρων διαδικασιών.
* Αξιολόγηση της ποιότητας ενός παροχέα εκπαιδευτικής δραστηριότητας.

Η/Ο Προϊστάμενη/ος του Τμήματος Διοίκησης και Ανθρώπινου Δυναμικού, οι Προϊστάμενοι Τμημάτων/Υπεύθυνοι Υπηρεσιών και οι υπάλληλοι έχουν επίσης ευθύνη για όλα όσα προσδιορίζονται στην ‘Πολιτική Ανθρώπινου Δυναμικού (Human Resources Policy) και στις σχετικές διαδικασίες.

# Έγγραφα Ελέγχου Ποιότητας

* Ετήσιο πρόγραμμα εκπαίδευσης και ενημέρωσης προσωπικού
* Ετήσια έκθεση απόδοσης για τα θέματα εκπαίδευσης και ενημέρωσης του προσωπικού
* Παρουσιολόγιο παρακολούθησης των εκπαιδεύσεων
* Όλα τα υπόλοιπα αρχεία εκπαίδευσης όπως αναλύονται στην ‘Πολιτική Ανθρώπινου Δυναμικού’.

# Δράση

|  |  |  |  |
| --- | --- | --- | --- |
| **Ενέργεια** | **Ιδιοκτήτης Ενέργειας** | **Λεπτομερής περιγραφή της ενέργειας της διαδικασίας** | **Πρότυπα Διαδικασίας** |
| Εκπόνηση ετήσιου προγράμματος Εκπαίδευσης |  |  |  |
| Έγκριση ετήσιου προγράμματος Εκπαίδευσης |  |  |  |
| Προγραμματισμός των δραστηριοτήτων εκπαίδευσης και ενημέρωσης |  |  |  |
| Σχεδιασμός δραστηριότητας εκπαίδευσης και ενημέρωσης |  |  |  |
| Διεξαγωγή εκπαιδευτικής δραστηριότητας |  |  |  |
| Αναθεώρηση προγράμματος εκπαίδευσης και ενημέρωσης σε θέματα ασφάλειας πληροφοριών |  |  |  |
| Ετοιμασία της Έκθεσης ετήσιας απόδοσης της εκπαίδευσης και ενημέρωσης σε θέματα ασφάλειας πληροφοριών |  |  |  |
| Θεώρηση έκθεσης ετήσιας απόδοσης, προγράμματος επόμενου έτους |  |  |  |