Όνομα Οργανισμού

Πολιτική Φυσικής και Περιβαλλοντικής Ασφάλειας

|  |  |
| --- | --- |
| **Περιεχόμενο:** | Πολιτική Φυσικής και Περιβαλλοντικής Ασφάλειας |
| **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. Σκοπός 4](#_Toc154732866)

[2. Φυσική Περίμετρος – Γενικές Αρχές 4](#_Toc154732867)

[3. Εσωτερικά Περιβαλλοντικά Μέτρα 4](#_Toc154732868)

[4. Περιμετρική Ασφάλεια - Γενικά 5](#_Toc154732869)

[5. Ασφάλεια Εγκαταστάσεων και Εξοπλισμού 7](#_Toc154732870)

[5.1. Γενικές Αρχές Διασφάλισης Φυσικής Ασφάλειας Κτηρίων 9](#_Toc154732871)

[5.2. Πυροπροστασία Κτηρίων – Γενικές Αρχές 10](#_Toc154732872)

[6. Εξασφάλιση Παροχών και Διασυνδέσεων 10](#_Toc154732873)

[7. Ασφάλεια Καλωδίωσης, Εξοπλισμού και Εγκαταστάσεων 11](#_Toc154732874)

[8. Ασφάλεια Κρίσιμων στοιχείων του Οργανισμού 11](#_Toc154732875)

[9. Έλεγχος Φυσικής Πρόσβασης 12](#_Toc154732876)

[10. Ενημέρωση/Εκπαίδευση του Κατάλληλου Προσωπικού 13](#_Toc154732877)

[11. Επιχειρησιακή Συνέχεια και Ανάκαμψη από Καταστροφή 13](#_Toc154732878)

# Σκοπός

Η Πολιτική Φυσικής και Περιβαλλοντική Ασφάλειας θέτει τις προστατευτικές δικλίδες που πρέπει να υπάρχουν ως πρώτη γραμμή άμυνας για την εταιρία ενάντια σε κλοπές, βανδαλισμούς, φυσικές καταστροφές, σκόπιμες ή τυχαίες καταστροφές.

Ο σκοπός της Πολιτικής Φυσικής και Περιβαλλοντικής Ασφάλειας είναι να καθορίσει τις απαιτήσεις και τεχνικές για την περιμετρική ασφάλεια καθώς και την ασφάλεια των εγκαταστάσεων και εξοπλισμού του [Όνομα Οργανισμού].

# Φυσική Περίμετρος – Γενικές Αρχές

* Σύμφωνα με τον Νόμο Κ.Δ.Π. 389/2020, ο [Όνομα Οργανισμού] διασφαλίζει τη φυσική περίμετρο του, με την εξασφάλιση και αποτροπή της μη εξουσιοδοτημένης πρόσβασης, με σκοπό την προστασία των εγκαταστάσεων επεξεργασίας πληροφοριών. πρέπει να καθιερώσει κατάλληλα μέτρα ελέγχου της περιμετρικής πρόσβασης με την εφαρμογή φυσικών συνόρων, όπως φράχτες, πόρτες και τοίχοι. Απαιτεί από τους υπαλλήλους και τους επισκέπτες να αποδεικνύουν την ταυτότητά τους στους φρουρούς ασφαλείας προκειμένου να εισέλθουν (σε κάποιο μέρος) στον [Όνομα Οργανισμού]. Θα πρέπει να εξετάσει την εγκατάσταση καμερών κλειστού κυκλώματος με σκοπό τον εντοπισμό εισβολέων στα όρια του [PS3]. Συγκεκριμένα:

1. Συνοριακή Ασφάλεια:

* Καθορισμός και συντήρηση φυσικών ή τεχνολογικών συστημάτων για την ενίσχυση της συνοριακής ασφάλειας του οργανισμού.

1. Περιμετρικά Σύνορα:

* Καθορισμός και συντήρηση σαφών φυσικών ή εικονικών περιμετρικών ορίων του οργανισμού.

1. Έλεγχος Εισόδων:

* Εγκατάσταση συστημάτων ελέγχου πρόσβασης σε εισόδους και εξόδους των κτιρίων και του χώρου εργασίας.

1. Παρακολούθηση Περιμέτρου:

* Εφαρμογή συστημάτων παρακολούθησης της περιμέτρου με τη χρήση καταγραφικών καμερών και αισθητήρων κίνησης.

1. Έλεγχος Οχημάτων:

* Θέσπιση πολιτικών για τον έλεγχο της πρόσβασης οχημάτων, συμπεριλαμβανομένων των συστημάτων αναγνώρισης κυκλοφορίας.

# Εσωτερικά Περιβαλλοντικά Μέτρα

Να εξασφαλιστεί ότι οι εσωτερικοί χώροι και οι εγκαταστάσεις του οργανισμού προστατεύονται από φυσικές ζημιές. Για αυτό και είναι αναγκαία η θέσπιση, εφαρμογή και διατήρηση μέτρων φυσικής ασφάλειας και προστασίας, ώστε να αποφεύγεται η φυσική ζημία στους εσωτερικούς χώρους και τις εγκαταστάσεις του οργανισμού. Κατά την εφαρμογή εσωτερικών περιβαλλοντικών μέτρων, ο [Όνομα Οργανισμού] θα πρέπει να εξετάζει τους κινδύνους που σχετίζονται με τη φωτιά και τη θερμοκρασία, την υγρασία, την ηλεκτρική ενέργεια, τη χρήση του νερού και άλλα στοιχεία που θα μπορούσαν να επηρεάσουν αρνητικά τη φυσική ασφάλεια των στοιχείων ενεργητικού. Ο [Όνομα Οργανισμού] πρέπει να εξετάζει την πυρόσβεση, τον έλεγχο της υγρασίας και άλλα μέτρα ανάλογα με τα χαρακτηριστικά των εσωτερικών φυσικών χώρων, όπως είναι τα κέντρα δεδομένων ή άλλους χώρους όπου βρίσκεται εξοπλισμός επεξεργασίας πληροφοριών [PS5].

Συγκεκριμένα προτείνεται:

1. Η θερμοκρασία και η υγρασία στα κέντρα δεδομένων και σε άλλες περιοχές επεξεργασίας πληροφοριών πρέπει να ελέγχονται, να παρακολουθούνται και να διατηρούνται χρησιμοποιώντας κατάλληλο εξοπλισμό ελέγχου αέρα και υγρασίας.
2. Επαρκείς συσκευές ασφαλείας π.χ. συναγερμός πυρκαγιάς, ανιχνευτής διαρροής νερού, ανιχνευτής καπνού, κλπ. πρέπει να τοποθετούνται σε γραφεία, αποθήκες και κέντρα δεδομένων.
3. Όλος ο εξοπλισμός περιβαλλοντικής ασφάλειας πρέπει να υποβάλλεται σε τακτικές δοκιμές (τουλάχιστον μία φορά το χρόνο) και τα αποτελέσματα των δοκιμών καθορίζουν την αποτελεσματικότητα και την επάρκεια αυτού του εξοπλισμού.

# Περιμετρική Ασφάλεια - Γενικά

* Ο [Όνομα Οργανισμού] έχει θεσπίσει, εφαρμόζει και διατηρεί μέτρα για την ασφάλεια της περιμέτρου του οργανισμού με σκοπό την προστασία των εγκαταστάσεων επεξεργασίας πληροφοριών
* Η περίμετρος ασφάλειας των κτιρίων και εγκαταστάσεων του οργανισμού πρέπει να οριοθετηθεί και να προστατευθεί με την εγκατάσταση φράκτη.
* Ο οργανισμός θα πρέπει να εγκαταστήσει σύστημα συναγερμού αλλά και σύστημα ελέγχου πρόσβασης για την είσοδο του προσωπικού στις εγκαταστάσεις του [Όνομα Οργανισμού].
* Πρέπει να υπάρχει ένας επανδρωμένος χώρος υποδοχής για τον έλεγχο της φυσικής πρόσβασης και του εξουσιοδοτημένου προσωπικού.
* Ο [Όνομα Οργανισμού] διατηρεί λίστα στην είσοδο των εγκαταστάσεων με τα άτομα που έχουν μπει στον οργανισμό. Ο οργανισμός έχει θεσπίσει, εφαρμόζει και διατηρεί εσωτερικά μέτρα πρόσβασης, τα οποία είναι ευθυγραμμισμένα με τους ρόλους που περιγράφονται στο [ΙΑΜ1], προκειμένου να διασφαλιστεί ότι μόνο τα στελέχη με έννομο συμφέρον έχουν πρόσβαση σε (συγκεκριμένα μέρη) του οργανισμού.
* Πρέπει να χρησιμοποιούνται θύρες και παράθυρα υψηλής ασφάλειας στις εγκαταστάσεις του οργανισμού
* Σε άκρως προστατευόμενες εγκαταστάσεις (όπως server room, αρχειοφυλάκιο) του οργανισμού, πρέπει να χρησιμοποιούνται πόρτες με μηχανισμούς εξακρίβωσης ταυτότητας (όπως smart cards και PINS).
* Για τους προμηθευτές, επισκέπτες και τρίτους, πρέπει να διατηρείται ιστορικό εισόδου/εξόδου από τις εγκαταστάσεις του οργανισμού. Οι προμηθευτές, επισκέπτες και τρίτοι πρέπει να συνοδεύονται σε όλη τη διάρκεια που βρίσκονται εντός των εγκαταστάσεων του οργανισμού. Εξαιρούνται οι χώροι αναμονής πελατών.
* Πρέπει να εφαρμόζονται συστήματα ανίχνευσης εισβολών (π.χ. συστήματα συναγερμού) σε όλες τις εξωτερικές πόρτες και παράθυρα (εφόσον είναι προσβάσιμες και βάσει εκτίμησης κινδύνου). Θα πρέπει επίσης να περιλαμβάνει υψηλής ευαισθησίας περιοχές, όπως server rooms, power rooms.
* Κάμερες ασφάλειας και συστήματα συναγερμού πρέπει να τοποθετηθούν περιμετρικά των εγκαταστάσεων και σε προστατευόμενες εγκαταστάσεις. Το κλειστό κύκλωμα παρακολούθησης πρέπει να συμμορφώνεται με τις πρόνοιες του Γενικού Κανονισμού για την Προστασία των Δεδομένων και τυχόν Οδηγίες που εκδίδονται τόσο από την Επίτροπο Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, όσο και με τις οδηγίες του [Όνομα Οργανισμού]:
* Οι κάμερες πρέπει να έχουν υψηλή ευκρίνεια (τουλάχιστο 2k ή 4k).
* Οι καταγραφές από το κλειστό κύκλωμα παρακολούθησης πρέπει να διατηρούνται για τουλάχιστο 1 μήνα. Σε περίπτωση περιστατικού/συμβάντος το υλικό πρέπει να διατηρείται για 10 χρόνια. Σημειώνεται ότι οι πιο πάνω περίοδος διατήρησης, ενδέχεται να διαφοροποιείται σε περίπτωση όπου καθορίζεται διαφορετικά με βάση το κανονιστικό πλαίσιο του οργανισμού.
* Όσο αφορά την πρόσβαση και τη διαχείριση του κλειστού κυκλώματος παρακολούθησής / βίντεο -παρακολούθησης, έχει καταγραφεί και ακολουθείται διαδικασία που περιλαμβάνει τα ακόλουθα:
  + Την πρόσβαση / διερεύνηση στα μαγνητοσκοπημένα βίντεο.
  + Την παράδοση των μαγνητοσκοπημένων βίντεο προς αρχές για διερεύνηση.
  + Τη φύλαξη των μαγνητοσκοπημένων βίντεο για θέματα τα οποία τυγχάνουν διερεύνησης.
  + Τη διευθέτηση των μαγνητοσκοπημένων βίντεο.
* Η παραλαβή και παράδοση πληροφοριακών συστημάτων ή/και άλλων αναλώσιμων των πληροφοριακών συστημάτων πρέπει να γίνεται σε ελεγχόμενο χώρο.
* Οι πληροφορίες πρέπει να τυγχάνουν της απαιτούμενης φυσικής φύλαξης ανάλογα με την ευαισθησία και διαβάθμιση τους (βλέπε Πολιτική και Διαδικασία Διαχείρισης Στοιχείων Ενεργητικού).
* Η φυσική Ασφάλεια πρέπει να αξιολογείται σε τακτά χρονικά διαστήματα και να αναθεωρείται όποτε χρειάζεται. (βλέπε *Μεθοδολογία Διαχείρισης Κινδύνου).*
* Ο [Όνομα Οργανισμού] πρέπει να τηρεί αρχεία για όλες τις βλάβες και για κάθε προληπτική και διορθωτική συντήρηση.
* Να γίνεται αναφορά στο ότι ο [Όνομα Οργανισμού] φιλοξενεί τα κρίσιμα στοιχεία του οργανισμού όπως έχουν αναγνωριστεί στο [DS2] και στο [AM2] σε διακριτούς χώρους που εφαρμόζεται έλεγχος πρόσβασης.

# Ασφάλεια Εγκαταστάσεων και Εξοπλισμού

* Οι εγκαταστάσεις του [Όνομα Οργανισμού] πρέπει να είναι πιστοποιημένες ως αντισεισμικές από εγκεκριμένους οργανισμούς πιστοποίησης.
* Ο [Όνομα Οργανισμού] έχει θεσπίσει, εφαρμόζει και διατηρεί κατάλληλα μέτρα για την προστασία του οργανισμού από τις επιπτώσεις φυσικών καταστροφών, όπως οι πλημμύρες, οι σεισμοί και οι πυρκαγιές.
* Οι εγκαταστάσεις του [Όνομα Οργανισμού] πρέπει να υποστηρίζονται με συστήματα πυρόσβεσης. Η λειτουργία των συστημάτων αυτών θα πρέπει να ελέγχεται τακτικά (πρέπει να υπάρχει μητρώο ελέγχου). Επίσης το προσωπικό πρέπει να είναι εκπαιδευμένο σχετικά με θέματα πυρόσβεσης.
* Ο [Όνομα Οργανισμού] διενεργεί δοκιμές εκκένωσης σε τακτική βάση για σενάρια κινδύνων που ανήκουν στην συγκεκριμένη κατηγορία. Τα στοιχεία από τις δοκιμές να λαμβάνονται υπόψη στον σχεδιασμό των σχεδίων επιχειρησιακής συνέχειας και ανάκαμψης από καταστροφή
* Η κατανάλωση φαγητού και ποτού καθώς και το κάπνισμα κοντά στα πληροφοριακά συστήματα απαγορεύεται.
* Στους χώρους πρέπει να απαγορεύεται η φορτοεκφόρτωση και η είσοδος μη εξουσιοδοτημένου προσωπικού.
* Για τους χώρους της γεννήτριας και του σημείου αποθήκευσης καυσίμου θα πρέπει να υπάρχουν κατάλληλα μέτρα πυρανίχνευσης και πυρόσβεσης σύμφωνα με την κείμενη νομοθεσία.
* Η πρόσβαση σε κάθε όροφο θα πρέπει να ελέγχεται με κάρτες πρόσβασης.
* Οι επισκέπτες, οι προμηθευτές και τα τρίτα μέρη θα πρέπει να έχουν πρόσβαση μόνο στους συγκεκριμένους χώρους που σχετίζονται με τα καθήκοντά / την εργασία τους.
* Κατά το τέλος της ημέρας, δεν πρέπει να υπάρχουν έντυπες πληροφορίες πάνω στα γραφεία (βλέπε Πολιτική Αποδεκτής Χρήσης) ή να εκτίθενται με οποιοδήποτε άλλο τρόπο.
* Ο φορητός εξοπλισμός πρέπει να κλειδώνεται ή να τοποθετείται σε ασφαλισμένα ντουλάπια. (βλέπε Πολιτική Ασφάλειας Συστημάτων).
* Πρέπει να τηρείται κατάσταση εξοπλισμού και να είναι ενημερωμένη. Επίσης πρέπει να τηρείται μητρώο με τα συμβόλαια εξοπλισμού.
* Οι γραμμές τροφοδοσίας ηλεκτρισμού και τηλεπικοινωνιών συνιστάται να είναι υπόγειες.
* Πρέπει να υπάρχει εγκατεστημένο αλεξικέραυνο σε όλες τις εγκαταστάσεις του [Όνομα Οργανισμού] για την αποφυγή αυξομείωσης της τάσης του ρεύματος σε περιπτώσεις κακοκαιρίας. Το αλεξικέραυνο πρέπει να επιθεωρείται συχνά.
* Ο [Όνομα Οργανισμού] πρέπει να εξασφαλίζει ότι οι βασικές παροχές (π.χ. ρεύμα, δίκτυο) και οι κρίσιμες διασυνδέσεις με τρίτα μέρη όπου απαιτούνται έχουν τουλάχιστον 2 διαφορετικές οδεύσεις και αν είναι δυνατό, διαφορετικούς παρόχους. Ο [Όνομα Οργανισμού] πρέπει να καταγράψει και να επικαιροποιεί όπως απαιτείται σχετικά σχέδια που αποτυπώνουν τις σχετικές οδεύσεις
* Η δικτυακή και η τηλεφωνική καλωδίωση (βλέπε Πολιτική Ασφάλειας Δικτύου):
  + πρέπει να προστατεύεται από μη εξουσιοδοτημένη παρεμπόδιση, υποκλοπή, ή ζημιά.
  + πρέπει να είναι ανεξάρτητη από οποιαδήποτε άλλα καλώδια.
  + πρέπει να τερματίζεται σε κατανεμητές, καμπίνες. Οι κατανεμητές, καμπίνες πρέπει να κλειδώνονται και να έχουν σταθερή, ελεγχόμενη θερμοκρασία.
  + συστήνεται η χρήση οπτικών ινών.
* Οι εγκαταστάσεις που φιλοξενούν πληροφοριακά συστήματα μεσαίου και υψηλού κινδύνου:
  + πρέπει να τοποθετούνται σε δωμάτια που δεν είναι εύκολα προσβάσιμα από το κοινό.
  + πρέπει να ασφαλίζονται με πυρίμαχες πόρτες υψηλής ασφάλειας και μηχανισμούς εξακρίβωσης ταυτότητας.
  + πρέπει να ασφαλίζονται όταν δεν είναι υπό επίβλεψη.
  + πρέπει να είναι σε συνεχή παρακολούθηση από το κλειστό κύκλωμα παρακολούθησης.
  + αποτυπωμένο σχέδιο του χώρου με αναγνώριση των σημείων που βρίσκεται ο εξοπλισμός.
  + πρέπει να προστατεύονται με συστήματα σταθεροποίησης κλιματισμού και υγρασίας. Η θερμοκρασία πρέπει να είναι 10-16 βαθμούς Κελσίου και το επίπεδο υγρασίας 40–60%. Επιπρόσθετα, φίλτρα αέρος πρέπει να χρησιμοποιούνται για την προστασία από τη σκόνη.
  + πρέπει να προστατεύονται με αυτόματα συστήματα ανίχνευσης καπνού και πυρόσβεσης για προστασία από φωτιά.
  + πρέπει να προστατεύονται με αυτόματα συστήματα ανίχνευσης νερού για προστασία από πλημμύρες ή άλλες καταστροφές από νερό.
  + πρέπει να τροφοδοτούν τα πληροφοριακά συστήματα με αρκετή ισχύ ρεύματος. Εξοπλισμός αντιμετώπισης αυξομείωσης της τάσης του ρεύματος πρέπει επίσης να χρησιμοποιείται.
  + πρέπει να τροφοδοτούν με ρεύμα τα πληροφοριακά συστήματα μέσω UPS.
  + πρέπει να υποστηρίζουν εφεδρικές γεννήτριες ρεύματος. Σε περίπτωση διακοπής ρεύματος τα πληροφοριακά συστήματα πρέπει αυτόματα να τροφοδοτούνται από αυτά.
  + πρέπει να υποστηρίζουν εφεδρικές γραμμές διαδικτύου και αν είναι εφικτό από διαφορετικούς παρόχους. Σε περίπτωση βλάβης στις γραμμές διαδικτύου του ενός παρόχου, η εφεδρική γραμμή πρέπει αυτόματα να τροφοδοτούνται από αυτή.
* Η διευθέτηση (disposal) πληροφοριών και πληροφοριακών συστημάτων πρέπει να συμμορφώνεται με την Πολιτική και Διαδικασία Διαχείρισης Στοιχείων Ενεργητικού*.*
* Ο [Όνομα Οργανισμού] θεσπίζει, εφαρμόζει και διατηρεί μέτρα φυσικής ασφάλειας και προστασίας, ώστε να αποφεύγεται η φυσική ζημία στους εσωτερικούς χώρους και τις εγκαταστάσεις του οργανισμού. Κατά την εφαρμογή εσωτερικών περιβαλλοντικών μέτρων, ο οργανισμός θα πρέπει να εξετάσει τους κινδύνους που σχετίζονται με τη φωτιά και τη θερμοκρασία, την υγρασία, την ηλεκτρική ενέργεια, τη χρήση του νερού και άλλα στοιχεία που θα μπορούσαν να επηρεάσουν αρνητικά τη φυσική ασφάλεια των στοιχείων ενεργητικού
* Πρέπει να οριστούν σχετικοί κανόνες για την ενημέρωση του κατάλληλου προσωπικού σε περίπτωση που οι τιμές βρεθούν εκτός των προδιαγεγραμμένων αποδεκτών ορίων.

# Γενικές Αρχές Διασφάλισης Φυσικής Ασφάλειας Κτηρίων

* Τα κτήρια που στεγάζουν, λειτουργούν, και εξυπηρετούν τον οργανισμό έχουν σχεδιαστεί και δομηθεί με τρόπο που ανταποκρίνεται στα υψηλότερα πρότυπα ασφάλειας, σύμφωνα με τους κατάλληλους κανονισμούς, κώδικες πρακτικής και τον αντισεισμικό κώδικα που ίσχυε κατά την ημερομηνία κατασκευής.

1. Σχεδιασμός Κτηρίων:

* Όλα τα κτήρια θα υποβληθούν σε σχεδιασμό που να συμμορφώνεται με τους ισχύοντες αντισεισμικούς κώδικες και πρότυπα ασφάλειας κτιρίων.

1. Κατασκευή Κτηρίων:

* Η κατασκευή θα πραγματοποιείται με τη χρήση υλικών και μεθόδων που είναι σύμφωνα με τους αντίστοιχους κανονισμούς ασφάλειας.
* Συντήρηση και Επιθεώρηση:
* Προγράμματα συντήρησης θα διασφαλίζουν τη συνεχή ασφάλεια των κτηρίων.
* Περιοδικές επιθεωρήσεις θα διενεργούνται για να ελεγχθεί η συμμόρφωση με τα πρότυπα ασφάλειας.

1. Αντισεισμική Προστασία:

* Οργάνωση επαναλαμβανόμενων εκπαιδευτικών προγραμμάτων για το προσωπικό σε θέματα αντισεισμικής ασφάλειας.
* Κατασκευή και διατήρηση αντισεισμικών μέτρων σύμφωνα με τους κατάλληλους κώδικες.

# Πυροπροστασία Κτηρίων – Γενικές Αρχές

1. Πρόληψη Πυρκαγιάς:

* Υλοποίηση πολιτικών και διαδικασιών για την πρόληψη πυρκαγιάς, συμπεριλαμβανομένης της σωστής αποθήκευσης εύφλεκτων υλικών.

1. Ανίχνευση και Ειδοποίηση:

* Εγκατάσταση συστημάτων ανίχνευσης πυρκαγιάς και συστημάτων ειδοποίησης για άμεση αντίδραση.

1. Κατάρτιση και Εκπαίδευση:

* Κατάρτιση προσωπικού για την ασφαλή αντίδραση σε περίπτωση πυρκαγιάς.
* Πραγματοποίηση πυροσβεστικών ασκήσεων.

1. Συστήματα Πυρόσβεσης:

* Εγκατάσταση και συντήρηση συστημάτων πυρόσβεσης, συμπεριλαμβανομένων αφυγραντήρων και αυτόματων συστημάτων πυροσβεστικών.

1. Ασφαλείς Διάδρομοι Εκκένωσης:

* Συντήρηση ανοικτών διαδρόμων εκκένωσης και διασφάλιση πρόσβασης για το πυροσβεστικό προσωπικό.

# Εξασφάλιση Παροχών και Διασυνδέσεων

Ο [Όνομα Οργανισμού] δεσμεύεται να διασφαλίσει την αξιοπιστία και την ανθεκτικότητα των βασικών παροχών, όπως το ρεύμα και το δίκτυο, καθώς και των κρίσιμων διασυνδέσεων με τρίτα μέρη. Αυτό επιτυγχάνεται μέσω της δημιουργίας τουλάχιστον δύο διαφορετικών οδών και, όπου είναι δυνατό, της χρήσης διαφορετικών παρόχων υπηρεσιών. Ο [Όνομα Οργανισμού] επίσης δεσμεύεται να καταγράφει και να επικαιροποιεί, κατά το δυνατό, τα σχετικά σχέδια που αποτυπώνουν τις διαφορετικές οδεύσεις.

1. Διπλές Διαφορετικές Οδεύσεις:

* Όλες οι βασικές παροχές και κρίσιμες διασυνδέσεις πρέπει να έχουν τουλάχιστον δύο διαφορετικές οδεύσεις για τη μείωση του κινδύνου αποτυχίας.

1. Διαφορετικοί Πάροχοι Υπηρεσιών:

* Εάν είναι δυνατό, οι βασικές παροχές πρέπει να εξασφαλίζονται από διαφορετικούς παρόχους υπηρεσιών για αυξημένη ανθεκτικότητα.

1. Καταγραφή και Επικαιροποίηση:

* Καταγραφή όλων των σχετικών σχεδίων που περιλαμβάνουν τις διαφορετικές οδεύσεις .
* Επικαιροποίηση των σχεδίων σε τακτική βάση, κυρίως κατά την εισαγωγή νέων τεχνολογιών ή αλλαγών στις υποδομές.

# Ασφάλεια Καλωδίωσης, Εξοπλισμού και Εγκαταστάσεων

Σύμφωνα με τον Νόμο Κ.Δ.Π. 389/2020, για την καλωδίωση και τον εξοπλισμό που υποστηρίζουν την επεξεργασία των πληροφοριών, εξασφαλίζεται η φυσική προστασία από παρεμβολές, υποκλοπή ή ζημιά οι οποίες θα προκαλούσαν διακοπή στις υπηρεσίες του οργανισμού. Ο [Όνομα Οργανισμού] πρέπει να εξασφαλίζει ότι τα καλώδια που παρέχουν ηλεκτρική ενέργεια σε κρίσιμες υποδομές προστατεύονται δεόντως και να εκπαιδεύει τους υπαλλήλους, ώστε να γνωρίζουν τη σημασία του εξοπλισμού που υποστηρίζει τις δραστηριότητες επεξεργασίας πληροφοριών. Η φυσική πρόσβαση στα λογικά δίκτυα θα πρέπει επίσης να προστατεύεται με κατάλληλα μέτρα ώστε να αποτρέπεται η μη εξουσιοδοτημένη φυσική πρόσβαση στο λογικό εξοπλισμό και το δίκτυο του [Όνομα Οργανισμού] [PS4]. Συγκεκριμένα προτείνονται τα εξής:

1. Ασφάλεια Εξοπλισμού Πληροφορικής

* Ο εξοπλισμός πρέπει να τοποθετείται σε μια τοποθεσία ανάλογα με την κρισιμότητα και την διαβάθμισή του.
* Ο εξοπλισμός δεν πρέπει να μετακινείται από την τοποθεσία του, εκτός εάν έχει εγκριθεί από τον Υπεύθυνο Ασφάλειας Πληροφοριών και τον αντίστοιχο Υπεύθυνο περιουσιακού αγαθού.
* Όλος ο εξοπλισμός πρέπει να υποβάλλεται σε διαδικασία συντήρησης μία φορά το χρόνο από τον προμηθευτή ή χρησιμοποιώντας εκπαιδευμένο εσωτερικό προσωπικό.

1. Ασφάλεια Καλωδίωσης

* Τα καλώδια τροφοδοσίας πρέπει να διαχωρίζονται από τα καλώδια επικοινωνίας για την αποφυγή παρεμβολών.
* Η καλωδίωση δικτύου πρέπει να προστατεύεται από μη εξουσιοδοτημένη παρέμβαση ή ζημιά.
* Οι πίνακες επιδιόρθωσης δικτύου πρέπει να βρίσκονται σε ασφαλή ερμάρια.

Όλα τα καλώδια που αφορά κρίσιμο εξοπλισμό θα πρέπει να διαθέτουν ετικέτα.

# Ασφάλεια Κρίσιμων στοιχείων του Οργανισμού

* Ασφάλιση Γραφείων, Κέντρων Δεδομένων και άλλων Ασφαλών Περιοχών:
* Το κέντρο δεδομένων, οι αίθουσες εξοπλισμού και οι ντουλάπες τηλεπικοινωνιών πρέπει να είναι κλειδωμένες όταν δεν παρακολουθούνται.
* Τα συρτάρια και τα ερμάρια σε χώρους γραφείων καθώς και στο εσωτερικό αρχείο του [Όνομα Οργανισμού] κλειδώνονται όταν δεν χρησιμοποιούνται και τα κλειδιά φυλάσσονται από τον Προϊστάμενο του σχετικού Τμήματος.
* Οι δικτυακές συσκευές πρέπει να τοποθετούνται σε ζώνες περιορισμένης πρόσβασης που παρέχουν προστασία από μη εξουσιοδοτημένη πρόσβαση.
* Όλες οι εφαρμογές, οι διακομιστές βάσεων δεδομένων και οι συσκευές ασφαλείας δικτύου πρέπει να τοποθετούνται στα κέντρα δεδομένων του [Όνομα Οργανισμού].
* Όλα τα μέσα προέλευσης για λογισμικό λειτουργικού συστήματος, εφαρμογές, εφεδρικές ταινίες/ συσκευές και κλειδιά άδειας πρέπει να ετικετοποιούνται  κατάλληλα και να αποθηκεύονται σε βιβλιοθήκες λογισμικού σε ζώνη περιορισμένης πρόσβασης - με πρόσβαση που παρέχεται μόνο σε εξουσιοδοτημένο προσωπικό.
* Όλος ο εξοπλισμός τρίτων και τα περιουσιακά αγαθά πληροφοριών μπορούν να εισαχθούν στο κέντρο δεδομένων μετά από κατάλληλη εξουσιοδότηση από τον υπεύθυνο ασφάλειας πληροφοριών.

# Έλεγχος Φυσικής Πρόσβασης

* Οι ασφαλείς περιοχές πρέπει να προστατεύονται με συνδυασμό ελέγχου πρόσβασης, εξοπλισμού καταγραφής πρόσβασης, εξοπλισμού παρακολούθησης δραστηριότητας και φύλακες ασφαλείας, κατά περίπτωση.
* Κάθε φυσική πρόσβαση και μεταφορά περιουσιακών αγαθών πρέπει να εγκριθεί, να παρακολουθείται και να αναθεωρείται.
* Η πρόσβαση σε ευαίσθητες ή κρίσιμες εγκαταστάσεις επεξεργασίας πληροφοριών εκτός των κανονικών ωρών εργασίας πρέπει να εγκριθεί, να παρακολουθείται και να καταγράφεται.
* Τα δικαιώματα φυσικής πρόσβασης πρέπει να ενημερώνονται τακτικά με βάση την κρίσιμη σημασία των συστημάτων πληροφοριών.
* Η πρόσβαση κάθε επισκέπτη στις εγκαταστάσεις του [Όνομα Οργανισμού] πρέπει να εγκριθεί από τον Υπεύθυνο Ασφάλειας Πληροφοριών, συνοδευόμενος από ένα μέλος του προσωπικού, μαζί με την εφαρμογή κατάλληλων μηχανισμών καταγραφής και παρακολούθησης.
* Η πρόσβαση κάθε επισκέπτη στο κέντρο δεδομένων του [Όνομα Οργανισμού] πρέπει να έχει εγκριθεί από τον Υπεύθυνο Ασφάλειας Πληροφοριών, συνοδευόμενος από ένα μέλος του προσωπικού από το Τμήμα Πληροφορικής, μαζί με την εφαρμογή κατάλληλων μηχανισμών καταγραφής και παρακολούθησης.
* Η φυσική πρόσβαση στο κέντρο δεδομένων του [Όνομα Οργανισμού] πρέπει να επιτρέπεται βάσει των επιχειρησιακών αναγκών, να καταγράφεται και να παρακολουθείται συνεχώς. Αυτό μπορεί να γίνει ηλεκτρονικά ή χρησιμοποιώντας ένα φυσικό μητρώο.
* Τα δικαιώματα φυσικής πρόσβασης πρέπει να ανακαλούνται αμέσως μετά τον τερματισμό/ παραίτηση των εργαζομένων ή την ολοκλήρωση της συμφωνίας τρίτων.
* Τα αρχεία καταγραφής ελέγχου πρόσβασης πρέπει να διατηρούνται τουλάχιστον για περίοδο τριών μηνών.

# Ενημέρωση/Εκπαίδευση του Κατάλληλου Προσωπικού

Πρέπει να οριστούν σχετικοί κανόνες για την ενημέρωση/εκπαίδευση του κατάλληλου προσωπικού σε περίπτωση που οι τιμές βρεθούν εκτός των προδιαγεγραμμένων αποδεκτών ορίων. Τα ελάχιστα μέτρα περιλαμβάνουν:

1. Αυτόματο Σύστημα Πυρανίχνευσης:

* Εγκατάσταση αυτόματου συστήματος πυρανίχνευσης για άμεση αντίδραση σε περίπτωση πυρκαγιάς

1. Έλεγχος Πρόσβασης:

* Τοποθέτηση εξοπλισμού εντός rack με ελεγχόμενη πρόσβαση, εξασφαλίζοντας την ασφαλή φύλαξη του.

1. Αποτυπωμένο Σχέδιο:

* Δημιουργία αποτυπωμένου σχεδίου του χώρου, συμπεριλαμβανομένων των σημείων τοποθέτησης του εξοπλισμού.

1. Σήμανση και Ασφαλής Εκκένωση:

* Σήμανση και ύπαρξη μεγάφωνου ή άλλου μέσου για αναγγελία έκτακτης ανάγκης.
* Κουμπί εκκένωσης για άμεση αντίδραση σε περίπτωση κινδύνου.
* Κατάλληλος φωτισμός ασφαλείας για εξασφάλιση ορατότητας.

1. Υπερυψωμένο Πάτωμα:

* Εγκατάσταση υπερυψωμένου πατώματος για προστασία των καλωδίων και εξοπλισμού.

1. Περιορισμός Πρόσβασης:

* Απαγόρευση φορτοεκφόρτωσης και εισόδου μη εξουσιοδοτημένου προσωπικού.

1. Πυρανίχνευση και Πυρόσβεση:

* Εφαρμογή κατάλληλων μέτρων πυρανίχνευσης και πυρόσβεσης για χώρους γεννήτριας και αποθήκευσης καυσίμου, σύμφωνα με τη νομοθεσία.

# Επιχειρησιακή Συνέχεια και Ανάκαμψη από Καταστροφή

Η παρούσα πολιτική έχει ως στόχο τη διασφάλιση της φυσικής ασφάλειας των κτηρίων και την αποτελεσματική αντιμετώπιση σεναρίων φυσικών καταστροφών, με εστίαση στον σχεδιασμό σχεδίων επιχειρησιακής συνέχειας και ανάκαμψης από καταστροφή.

1. Σχεδιασμός Καταστροφικών Σεναρίων:

* Αναγνώριση και αξιολόγηση πιθανών καταστροφικών σεναρίων που μπορεί να επηρεάσουν τα κτίρια και τις επιχειρήσεις.

1. Σχεδίαση για Επιχειρησιακή Συνέχεια:

* Ανάπτυξη εκτενούς σχεδίου επιχειρησιακής συνέχειας που να περιλαμβάνει διαδικασίες για την άμεση αντιμετώπιση των επιπτώσεων καταστροφής.

1. Ενίσχυση Δομικής Αντοχής:

* Ενίσχυση της δομικής αντοχής των κτιρίων κατά των καταστροφικών επιπτώσεων, όπως σεισμοί, πλημμύρες, και πυρκαγιές.

1. Ανίχνευση και Προειδοποίηση:

* Εγκατάσταση προηγμένων συστημάτων ανίχνευσης και προειδοποίησης για να ενημερώνουν άμεσα το προσωπικό και να ενεργοποιούν τα σχέδια επιχειρησιακής συνέχειας.