Όνομα Οργανισμού

Πολιτική Φυσικής και Περιβαλλοντικής Ασφάλειας

|  |  |
| --- | --- |
| **Περιεχόμενο:** | Πολιτική Φυσικής και Περιβαλλοντικής Ασφάλειας |
| **Δημιουργός:** | **Author** |
| **Έκδοση:** | 1. |
| **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 Περιεχομένωνκ

[1. Εισαγωγή 4](#_Toc184801938)

[2.1 Σκοπός 4](#_Toc184801939)

[2.2 Πεδίο Εφαρμογής 4](#_Toc184801940)

[2. Πολιτική Φυσικής Ασφάλειας 5](#_Toc184801941)

[2.1. Έλεγχος περιμετρικής πρόσβασης 5](#_Toc184801942)

[2.2. Έλεγχος Εσωτερικής Πρόσβασης 5](#_Toc184801943)

[2.3 Περιβαλλοντικα Μετρα 7](#_Toc184801944)

[2.4 Ασφάλεια Εγκαταστάσεων, καλωδίωσης και Εξοπλισμού 8](#_Toc184801945)

[2.5 Ασφάλεια εγκαταστάσεων υψηλότερης κατηγορία διαβάθμισης 9](#_Toc184801946)

[3. Ενημέρωση/Εκπαίδευση του Κατάλληλου Προσωπικού 12](#_Toc184801947)

[4. Αναθεώρηση 13](#_Toc184801948)

[5. Αναφορές 14](#_Toc184801949)

# Εισαγωγή

## Σκοπός

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

Ρυθμίζει την προστασία των φυσικών και περιβαλλοντικών πτυχών που θα μπορούσαν να επηρεάσουν την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των περιουσιακών στοιχείων πληροφοριών.

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 που χειρίζονται ευαίσθητες πληροφορίες του [Όνομα Οργανισμού].

## Πεδίο Εφαρμογής

Η παρούσα Πολιτική εφαρμόζεται σε όλες τις εγκαταστάσεις και υποδομές στις οποίες δραστηριοποιείται ο [Όνομα Οργανισμού], ανεξαρτήτως γεωγραφικής τοποθεσίας συμπεριλαμβανομένου της περιμετρική ασφάλειας, των κέντρων δεδομένων, των υποκαταστημάτων και άλλων εγκαταστάσεων.

Περιλαμβάνει μεταξύ άλλων:

1. Ελέγχους φυσικής πρόσβασης.
2. Περιβαλλοντικές διασφαλίσεις (π.χ. παροχή ηλεκτρισμού, έλεγχος θερμοκρασίας κτλ).
3. Ασφαλής αποθήκευση και διάθεση των περιουσιακών στοιχείων πληροφοριών.
4. Προστασία εξοπλισμού, καλωδίωσης και εγκαταστάσεων.

Όλοι οι εργαζόμενοι και συνεργάτες του [Όνομα Οργανισμού] είναι υποχρεωμένοι να κατανοούν και να ακολουθούν τις διαδικασίες και τα πρωτόκολλα που προβλέπονται από την παρούσα πολιτική, ώστε να διασφαλίζεται η αποτελεσματική διαχείριση των απειλών και η διατήρηση ενός ασφαλούς περιβάλλοντος εργασίας.

# Πολιτική Φυσικής Ασφάλειας

## Έλεγχος περιμετρικής πρόσβασης

Σύμφωνα με την Απόφαση 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. Τα κατάλληλα μέτρα ελέγχου της περιμετρικής πρόσβασης με την εφαρμογή φυσικών συνόρων, όπως φράχτες, πόρτες και τοίχοι, την εγκατάσταση συστημάτων παρακολούθησης και συναγερμών θα πρέπει να υλοποιηθούν με σκοπό την προστασία των εγκαταστάσεων επεξεργασίας πληροφοριών.

Προς αυτό το σκοπό:

* Ο οργανισμός έχει εγκαταστήσει σύστημα συναγερμού αλλά και σύστημα ελέγχου πρόσβασης για την είσοδο του προσωπικού στις εγκαταστάσεις του [Όνομα Οργανισμού].
* Ο [Όνομα Οργανισμού] διαθέτει μέτρα ασφαλείας και διαδικασίες που αφορούν την είσοδο στους χώρους του [Όνομα Οργανισμού], όπως σύστημα καμερών κλειστού κυκλώματος και λίστα στην είσοδο των εγκαταστάσεων με τα άτομα που έχουν εισέλθει στον [Όνομα Οργανισμού].
* Ο [Όνομα Οργανισμού] παρακολουθεί το σύστημα συναγερμού και το σύστημα καμερών κλειστού κυκλώματος(CCTV) και να λαμβάνει σχετικές ενημερώσεις σε περίπτωση που παρουσιαστεί οποιαδήποτε κίνηση.
* Ο [Όνομα Οργανισμού] πρέπει να διατηρεί logs σχετικά με την καταγραφή των καμερών(CCTV) σύμφωνα με τη σχετική νομοθεσία για τα προσωπικά δεδομένα.
* Όπου είναι δυνατό ο [Όνομα Οργανισμού] πρέπει να διαθέτει 2 επίπεδα ελέγχου, ο πρώτος έλεγχος πραγματοποιείται στην περίμετρο των εγκαταστάσεων και ο δεύτερος στην είσοδο του κτιρίου.

## Έλεγχος Εσωτερικής Πρόσβασης

Ο [Όνομα Οργανισμού] εφαρμόζει εσωτερικά μέτρα ασφάλειας που αφορούν την προέλευση και την είσοδο των υπαλλήλων βάση του ρόλου τους, ώστε να διασφαλίζεται ότι μόνο οι εξουσιοδοτημένοι υπάλληλοι έχουν πρόσβαση σε συγκεκριμένους χώρους και πληροφορίες του [Όνομα Οργανισμού]. Οι ασφαλείς περιοχές πρέπει να προστατεύονται με συνδυασμό ελέγχου πρόσβασης, εξοπλισμού καταγραφής πρόσβασης, εξοπλισμού παρακολούθησης δραστηριότητας και φύλακες ασφαλείας, κατά περίπτωση.

Πιο συγκεκριμένα:

* Η πρόσβαση σε κάθε όροφο ελέγχεται με κάρτες πρόσβασης.
* Οι επισκέπτες του [Όνομα Οργανισμού] πρέπει να έχουν κάρτες που επιτρέπουν την πρόσβαση μόνο στην κεντρική είσοδο. Κατά τη διάρκεια παραμονής τους στις εγκαταστάσεις πρέπει να συνοδεύονται υποχρεωτικά από εξουσιοδοτημένο προσωπικό.
* Ο [Όνομα Οργανισμού] ελέγχει την πρόσβαση σε χώρους εργασίας και οι προσβάσεις των υπαλλήλων πρέπει να αναθεωρούνται ετησίως.
* Η πρόσβαση κάθε επισκέπτη στις εγκαταστάσεις του [Όνομα Οργανισμού] πρέπει να εγκριθεί από τον Υπεύθυνο Ασφάλειας Πληροφοριών ή εκπρόσωπο, συνοδευόμενος από ένα μέλος του προσωπικού, μαζί με την εφαρμογή κατάλληλων μηχανισμών καταγραφής και παρακολούθησης.
* Η πρόσβαση κάθε επισκέπτη στο Data Center/computer room του [Όνομα Οργανισμού] πρέπει να έχει εγκριθεί από τον Υπεύθυνο Ασφάλειας Πληροφοριών ή άλλο εκπρόσωπο του Οργανισμού, συνοδευόμενος από ένα μέλος του προσωπικού από το Τμήμα Πληροφορικής του [Όνομα Οργανισμού], μαζί με την εφαρμογή κατάλληλων μηχανισμών καταγραφής και παρακολούθησης.
* 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.
* Η φυσική πρόσβαση στο Data Center/computer room του [Όνομα Οργανισμού] πρέπει να επιτρέπεται βάσει των επιχειρησιακών αναγκών, να καταγράφεται και να παρακολουθείται συνεχώς. Αυτό γίνεται είτε ηλεκτρονικά είτε χρησιμοποιώντας ένα φυσικό μητρώο.
* Τα δικαιώματα φυσικής πρόσβασης πρέπει να ανακαλούνται αμέσως μετά τον τερματισμό/ παραίτηση των εργαζομένων ή την ολοκλήρωση της συμφωνίας τρίτων.
* Πρέπει να πραγματοποιούνται ετησίως δοκιμές παρείσδυσης που περιλαμβάνουν απροειδοποίητες προσπάθειες παράκαμψης των ελέγχων ασφαλείας που σχετίζονται με τα φυσικά σημεία πρόσβασης στις εγκαταστάσεις του [Όνομα Οργανισμού].
* Ο [Όνομα Οργανισμού] πρέπει να διατηρεί logs από το σύστημα ελέγχου φυσικής πρόσβασης (access control) και να ενημερώνεται μέσω ειδοποιήσεων για τυχόν παραβιάσεις.
* Η πρόσβαση σε ευαίσθητες ή κρίσιμες εγκαταστάσεις επεξεργασίας πληροφοριών εκτός των κανονικών ωρών εργασίας πρέπει να εγκριθεί, να παρακολουθείται και να καταγράφεται.

## Περιβαλλοντικα Μετρα

Ο [Όνομα Οργανισμού] εξασφαλίζει ότι οι χώροι (εσωτερικοί & εξωτερικοί) και άλλες εγκαταστάσεις του προστατεύονται από φυσικές καταστροφές και άλλες ζημιές.. Ο [Όνομα Οργανισμού] εφαρμόζει κατάλληλα μέτρα φυσικής ασφάλειας και προστασίας στους, περιλαμβάνοντας μονάδες κλιματισμού, υπερυψωμένα πατώματα, σήμανση και μέσα εκκένωσης, κατάλληλο φωτισμό ασφαλείας καθώς και συστήματα αναγνώρισης και σήμανσης καλωδίων.

* Ο [Όνομα Οργανισμού] στα πλαίσια της Διαδικασίας Αξιολόγησης Κινδύνου, διενεργεί αξιολόγηση κινδύνου σε σχέση με τους περιβαλλοντικούς κινδύνους (π.χ. πλημμύρες, σεισμοί και πυρκαγιές). Για τους κινδύνους αυτούς πρέπει να γίνεται ανάλυση και σχεδιασμός βασικών προληπτικών μέτρων τόσο στο εξωτερικό του κτηρίου όσο και στο εσωτερικό, λαμβάνοντας υπόψη ιστορικά στοιχεία και διαθέσιμες μελέτες ανά περιοχή (Π.χ. κατά πόσο ένα κτήριο βρίσκεται σε περιοχή δυνητικού Κινδύνου Πλημμύρας ή σεισμού).
* Βάσει της αξιολόγησης κινδύνου ο [Όνομα Οργανισμού] εφαρμόζει και διατηρεί κατάλληλα μέτρα για την προστασία από επιπτώσεις φυσικών καταστροφών (π.χ. πλημμύρες, σεισμοί και πυρκαγιές).
* Ως ελάχιστο μέτρο ο [Όνομα Οργανισμού] έχει εγκαταστήσει αυτόματο σύστημα πυρανίχνευσης στις εγκαταστάσεις του.
* Ο [Όνομα Οργανισμού] διενεργεί σε τακτική βάση δοκιμές εκκένωσης βάση σεναρίων κινδύνων που ανήκουν στην συγκεκριμένη κατηγορία και τα αποτελέσματα τους πρέπει να λαμβάνονται υπόψη στον σχεδιασμό των σχεδίων επιχειρησιακής συνέχειας και ανάκαμψης από καταστροφή.
* Ο [Όνομα Οργανισμού] λαμβάνει υπόψη τη γεωγραφική θέση κατά τη δημιουργία της υποδομής δικτύου και να εξασφαλίζει ότι τα κρίσιμα στοιχεία υποδομής και συστήματα είναι γεωγραφικά διάσπαρτα.
* Ο [Όνομα Οργανισμού] 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 δυνατόν, διαφορετικούς παρόχους. Ο [Όνομα Οργανισμού] καταγράφει και να επικαιροποιεί, όπως απαιτείται, σχετικά σχέδια που αποτυπώνουν τις σχετικές οδεύσεις.

Σε περίπτωση αποκλίσεων, πρέπει να υπάρχουν διαδικασίες για την άμεση ενημέρωση του αρμόδιου προσωπικού.

Διασφαλίζει την ύπαρξη κατάλληλων μέτρων πυρανίχνευσης, πυρόσβεσης και ελέγχου υγρασίας, συμπεριλαμβανομένων των χώρων που φιλοξενούνται οι γεννήτριες.

* Ο [Όνομα Οργανισμού] πρέπει να έχει πραγματοποιήσει μελέτη για τα περιβαλλοντικά μέτρα που υλοποιήθηκαν σύμφωνα και με την κείμενη νομοθεσία.
* Ο [Όνομα Οργανισμού] πρέπει να αποτυπώσει ένα σχέδιο του χώρου με αναγνώριση των σημείων που βρίσκεται ο εξοπλισμός

## Ασφάλεια Εγκαταστάσεων, καλωδίωσης και Εξοπλισμού

Η παρούσα ενότητα αφορά την ασφάλεια και την προστασία των εγκαταστάσεων, των καλωδιώσεων και του εξοπλισμού με στόχο τη προστασία του προσωπικού, των περιουσιακών στοιχείων και των πληροφοριών από κινδύνους που σχετίζονται με ακατάλληλη εγκατάσταση, καλωδίωση ή άλλες βλάβες του εξοπλισμού φυσικής ασφάλειας. Πιο συγκεκριμένα:

* Οι εγκαταστάσεις του [Όνομα Οργανισμού] πρέπει να είναι πιστοποιημένες ως αντισεισμικές από εγκεκριμένους οργανισμούς πιστοποίησης ή άλλη αρμόδια κυβερνητική αρχή.
* Ο [Όνομα Οργανισμού] πρέπει να προστατεύει την καλωδίωση και τον υπόλοιπο εξοπλισμό από παρεμβολές, υποκλοπές ή ζημιές, οι οποίες θα προκαλούσαν διακοπή στις υπηρεσίες του [Όνομα Οργανισμού].
* Τα καλώδια τροφοδοσίας πρέπει να θωρακίζονται και να διαχωρίζονται από τα καλώδια επικοινωνίας για την αποφυγή παρεμβολών.
* 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.
* Συστήνεται όπως 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. Χρησιμοποιείται μόνο εξουσιοδοτημένο προσωπικό συντήρησης για τις επισκευές και τον πιθανό εξοπλισμό συντήρησης.
* Η φυσική πρόσβαση στα λογικά δίκτυα πρέπει να προστατεύεται με κατάλληλα μέτρα ώστε να αποτρέπεται η μη εξουσιοδοτημένη φυσική πρόσβαση στο λογικό εξοπλισμό και το δίκτυο του [Όνομα Οργανισμού].
* Οι χώροι όπου υπάρχει πιθανότητα πρόσβασης σε οποιοδήποτε δικτυακό εξοπλισμό πρέπει να προστατεύονται (π.χ. χρήση racks που κλειδώνουν).
* Ο [Όνομα Οργανισμού] πρέπει να διασφαλίζει την ακεραιότητα και την τακτική συντήρηση των εγκαταστάσεων δικτύου.
* Ο [Όνομα Οργανισμού] πρέπει να διατηρεί αρχεία καταγραφής για όλες τις βλάβες και για κάθε προληπτική και διορθωτική συντήρηση καθώς και να πραγματοποιεί ελέγχους κατά την διάρκεια αυτών.
* Η απομακρυσμένη συντήρηση των περιουσιακών στοιχείων του [Όνομα Οργανισμού] καταγράφεται, εγκρίνεται, και εκτελείται με τρόπο που αποτρέπει τη μη εξουσιοδοτημένη πρόσβαση.
* Πρέπει να εφαρμόζονται έλεγχοι όταν ο εξοπλισμός προγραμματίζεται για συντήρηση, λαμβάνοντας υπόψη εάν αυτή η συντήρηση εκτελείται από προσωπικό στο χώρο του [Όνομα Οργανισμού] ή εκτός αυτού. Όπου είναι απαραίτητο, οι εμπιστευτικές πληροφορίες διαγράφονται από τον εξοπλισμό.
* Ο [Όνομα Οργανισμού] πρέπει να εκτελεί τεχνικές σαρώσεις και φυσικές επιθεωρήσεις για μη εξουσιοδοτημένες συσκευές που βρίσκονται εντός των εγκαταστάσεων του.]
* Ο [Όνομα Οργανισμού] τηρεί μία κατάσταση εξοπλισμού η οποία είναι πάντα ενημερωμένη. Επίσης τηρείται μητρώο με τα συμβόλαια(SLAs - Servive Level Agreements) εξοπλισμού/υπηρεσιών και διασφαλίζει ότι οι προμηθευτές τηρούν όλες τις απαιτήσεις που επιβάλλονται από τα συμβόλαια αυτά όσον αφορά την συντήρηση και υποστήριξη τους.
* Απαγορεύεται η φορτοεκφόρτωση και η είσοδος μη εξουσιοδοτημένου προσωπικού στις εγκαταστάσεις του [Όνομα Οργανισμού].

## Ασφάλεια εγκαταστάσεων υψηλότερης κατηγορία διαβάθμισης

* Ο [Όνομα Οργανισμού] πρέπει να έχει θεσπίσει και εφαρμόσει πλάνο και διαδικασίες για τον διαχωρισμό, διαβάθμιση και καταγραφή των μέτρων ασφαλείας για κάθε κατηγορία χώρου επεξεργασίας πληροφοριών. Η διαβάθμιση των χώρων πρέπει να λαμβάνει υπόψη την κρισιμότητα των διεργασιών, την ευαισθησία των πληροφοριών και τα αποτελέσματα της διαδικασίας διαχείρισης διακινδύνευσης.
* Οι πιο κρίσιμοι χώροι, όπως το data center/computer room, διαθέτουν αυτόματα συστήματα πυρανίχνευσης και πυρόσβεσης, ενημέρωσης για περιστατικά πλημμύρας, και ο [Όνομα Οργανισμού] πρέπει να διατηρεί σχετικό σχέδιο για την αντιμετώπιση των αντίστοιχων κινδύνων σύμφωνα με την απαίτηση PS5 της Απόφασης 389/2020.
* Πιο συγκεκριμένα για τα data center/computer room πρέπει να ληφθούν υπόψη τα ακόλουθα:

1. Οι συνθήκες θερμοκρασίας και υγρασίας στο data center/computer room και σε άλλες κρίσιμες περιοχές επεξεργασίας πληροφοριών πρέπει να παρακολουθούνται αυτόματα.
2. Η ύπαρξη επαρκών συσκευών ασφαλείας π.χ. συναγερμός πυρκαγιάς, ανιχνευτής διαρροής νερού, ανιχνευτής καπνού, υγρασίας κλπ. πρέπει να τοποθετούνται σε γραφεία, αποθήκες και κέντρα δεδομένων.
3. Όλος ο εξοπλισμός περιβαλλοντικής ασφάλειας να υποβάλλεται σε τακτικές δοκιμές/επιθεωρήσεις (τουλάχιστον μία φορά το χρόνο) και τα αποτελέσματα των δοκιμών καθορίζουν την αποτελεσματικότητα και την επάρκεια αυτού του εξοπλισμού και επιβεβαιώνουν το επίπεδο φυσικής ασφάλειας που κατέχουν.
4. Ο [Όνομα Οργανισμού] έχει ορίσει υπεύθυνα άτομα για την παρακολούθηση και διαχείριση των συνθηκών περιβάλλοντος (θερμοκρασία, υγρασία) στους κρίσιμους χώρους, και διασφαλίσει ότι τα μέτρα προστασίας είναι επαρκή για τη διατήρηση των αποδεκτών ορίων.
5. Η κατανάλωση φαγητού και ποτού καθώς και το κάπνισμα κοντά στα πληροφοριακά συστήματα απαγορεύεται.

* Επιπρόσθετα ο [Όνομα Οργανισμού] δύναται να εφαρμόζει τα ακόλουθα για τους χώρους που ανήκουν στην υψηλότερη κατηγορία διαβάθμισης:
* Εγκατάσταση αυτόματου συστήματος πυρόσβεσης με κατάλληλο μέσο ώστε να εξασφαλίζεται η μικρότερη επίπτωση στους ανθρώπους, τον εξοπλισμό και τις πληροφορίες.
* Παροχή διπλών (εφεδρικών) συστημάτων για τη διατήρηση σταθερής θερμοκρασίας εντός των χώρων.
* Διασφάλιση εφεδρικών διασυνδέσεων σε επίπεδο ενέργειας και δικτύου.
* Ύπαρξη τουλάχιστον τριών ειδών παροχής ενέργειας (δίκτυο, UPS, γεννήτρια).
* Λήψη κατάλληλων μέτρων για την φυσική προστασία των καλωδίων από τρωκτικά και άλλους παράγοντες.
* Χρήση ειδικών power strips για κάθε rack που φιλοξενεί εξοπλισμό, τα οποία συνδέονται με τουλάχιστον δύο διακριτές πηγές ενέργειας.
* Ανάθεση της παρακολούθησης, συντήρησης, ορθής λειτουργίας και άμεσης ανταπόκρισης σε εξουσιοδοτημένο προσωπικό για τα φυσικά μέσα προστασίας.
* Εγκατάσταση συστήματος αναγνώρισης και σήμανσης των σχετικών καλωδίων.
* Διενέργεια μελέτης και σχεδιασμού του χώρου και του πατώματος για το μέγιστο βάρος που μπορεί να αντέξει και τη σχετική κατανομή του.
* Διασφάλιση παροχής ρεύματος σε συστήματα ελέγχου θερμοκρασίας, φωτισμού και πρόσβασης, καθώς και σε όλα τα σημεία δικτύου που απαιτούνται για την λειτουργική διασύνδεση και παροχή κρίσιμων υπηρεσιών, σε περίπτωση ενεργοποίησης της γεννήτριας.
* Οι γραμμές ηλεκτρικού ρεύματος και τηλεπικοινωνιών στις εγκαταστάσεις επεξεργασίας πληροφοριών είναι υπόγειες, όπου είναι δυνατόν.
* Τήρηση διαδικασιών για τη συντήρηση, τον έλεγχο και τη δοκιμή των στοιχείων παροχής ενέργειας σε τακτική βάση.
* Μέτρηση του χρόνου και του τρόπου εκκίνησης της γεννήτριας και ενσωμάτωσή τους στον σχεδιασμό για την ικανότητα του UPS και την αυτοματοποίηση των ενεργειών.
* Εγκατάσταση αυτοματοποιημένου συστήματος by-pass για την απομόνωση στοιχείων ενέργειας σε περίπτωση συντήρησης, αντικατάστασης στοιχείων ή μπαταριών, ή αστοχίας.
* Τήρηση διαδικασιών για τη συντήρηση, τον έλεγχο και τη δοκιμή των στοιχείων πυροπροστασίας και διατήρησης θερμοκρασίας σε τακτική βάση.
* Χρήση κατάλληλης σήμανσης και ανιχνευτών που υποδεικνύουν την απελευθέρωση αερίου που δεν είναι κατάλληλο για ανθρώπους στον χώρο.
* Λήψη επαρκών μέτρων για την γείωση του συνόλου της εγκατάστασης ή του εξοπλισμού.
* Για τους χώρους της γεννήτριας και του σημείου αποθήκευσης καυσίμου θα πρέπει να υπάρχουν κατάλληλα μέτρα πυρανίχνευσης και πυρόσβεσης σύμφωνα με την κείμενη νομοθεσία.

Είναι σημαντικό να τονιστεί ότι ο [Όνομα Οργανισμού] πρέπει να εφαρμόζει και να τηρεί όλα τα παραπάνω μέτρα και στις περιπτώσεις που χρησιμοποιεί χώρους και εγκαταστάσεις τρίτων (π.χ πάροχοι υπηρεσιών νέφους) για τη φιλοξενία του σχετικού εξοπλισμού, ώστε να διασφαλίζεται η συμμόρφωση με τις απαιτήσεις ασφάλειας.

# Ενημέρωση/Εκπαίδευση του Κατάλληλου Προσωπικού

Ως μέρος της αύξησης της ευαισθητοποίησης του προσωπικού και της ικανότητας του να προστατεύει τα φυσικά περιουσιακά στοιχεία πληροφοριών, o [Όνομα Οργανισμού] διασφαλίζει ότι όλο το σχετικό προσωπικό είναι επαρκώς εκπαιδευμένο και ενήμερο για τα μέτρα φυσικής ασφάλειας πληροφοριών και τις καλές πρακτικές προστασίας των εγκαταστάσεων και εξοπλισμού, ώστε να ελαχιστοποιούνται οι σχετικοί κίνδυνοι.

Το σχετικό προσωπικό που εμπλέκεται θα πρέπει να γνωρίζει επαρκώς θέματα που αφορούν:

* Διαχείριση και λειτουργία εγκαταστάσεων.
* Εγκατάσταση, συντήρηση ή χειρισμό συστημάτων φυσικής ασφάλειας.
* Περιβαλλοντικούς ελέγχους συστημάτων πυρόσβεσης, κλιματισμού και παροχής ενέργειας. Θα πρέπει να οριστούν σχετικοί κανόνες για την ενημέρωση του κατάλληλου προσωπικού σε περίπτωση που η μέτρηση κάποιου συστήματος βρεθεί εκτός των προδιαγεγραμμένων αποδεκτών ορίων.
* Χρήση συστημάτων καταστολής πυρκαγιάς και διαδικασίες εκκένωσης προσαρμοσμένες στις εγκαταστάσεις που φιλοξενούν ευαίσθητα δεδομένα.
* Διαδικασίες για τον περιορισμό της πρόσβασης σε εγκαταστάσεις υψηλότερης κατηγορία διαβάθμισης (ευαίσθητες περιοχές) και άλλα περιουσιακά στοιχεία πληροφοριών.
* Για την αντιμετώπιση περιστατικών, τα βήματα που πρέπει να ακολουθηθούν σε περίπτωση μη εξουσιοδοτημένης πρόσβασης, κλοπής ή παραβίασης ή άλλου περιβαλλοντικού κινδύνου.
* Πρέπει να τηρείται κατάσταση εξοπλισμού και να είναι ενημερωμένη. Επίσης πρέπει να τηρείται μητρώο με τα συμβόλαια εξοπλισμού και να ανανεώνετε αναλόγως.

# Αναθεώρηση

Τα έγγραφα σχετικά με την Φυσική και Περιβαλλοντικής Ασφάλειας θα πρέπει να επανεξετάζονται και να αναθεωρούνται τουλάχιστον ετησίως ή σε περίπτωση σημαντικών αλλαγών στο περιβάλλον του [Όνομα Οργανισμού] ώστε να διασφαλίζει ότι παραμένει αποτελεσματική, συναφές και συμβατή με τις εξελισσόμενες απειλές(π.χ ακραίες φυσικές καταστροφές), τις οργανωτικές αλλαγές και τυχόν κανονιστικές απαιτήσεις.

# Αναφορές

|  |  |  |  |
| --- | --- | --- | --- |
| **Κατηγορία** | **ID** | **Μέτρο** | **Στόχος Μέτρου** |
| Φυσική Ασφάλεια | PS1 | Περιβαλλοντικά μέτρα | Να εξασφαλιστούν επαρκή μέτρα για την προστασία του οργανισμού από τις επιπτώσεις φυσικών καταστροφών, όπως οι πλημμύρες, οι σεισμοί και οι πυρκαγιές. |
| Φυσική Ασφάλεια | PS2 | Έλεγχος περιμετρικής πρόσβασης | Να διασφαλιστεί η φυσική περίμετρος του οργανισμού, με την εξασφάλιση και αποτροπή της μη εξουσιοδοτημένης πρόσβασης. |
| Φυσική Ασφάλεια | PS3 | Έλεγχος εσωτερικής πρόσβασης | Να εξασφαλιστεί ο έλεγχος της πρόσβασης σε εσωτερικούς χώρους εργασίας και τις εγκαταστάσεις, ώστε να διασφαλίζεται ότι η φυσική πρόσβαση περιορίζεται κατόπιν ανάγκης. |
| Φυσική Ασφάλεια | PS4 | Ασφάλεια καλωδίωσης, εξοπλισμού και εγκαταστάσεων | Να εξασφαλιστεί ότι για την καλωδίωση και τον εξοπλισμό που υποστηρίζουν την επεξεργασία των πληροφοριών, εξασφαλίζεται η φυσική προστασία από παρεμβολές, υποκλοπή ή ζημιά |
| Φυσική Ασφάλεια | PS5 | Εσωτερικά περιβαλλοντικά μέτρα | Να εξασφαλιστεί ότι οι εσωτερικοί χώροι και οι εγκαταστάσεις του οργανισμού προστατεύονται από φυσικές ζημιές. |