KASSINAKIS

TÜV AUSTRIA HELLAS
EN ISO 9001:2015
EN ISO 14001:2015
EN ISO 45001:2018

# ΠΟΛΙΤΙΚΕΣ ΑΣΦΑΛΕΙΑΣ

# Π.Ε ΚΑΣΙΝΑΚΗΣ Α.Ε

**Πληροφορίες Έκδοσης**

| | |
|---|---|
| Έκδοση: | 01 |
| Ημ. Έκδοσης: | 25.04.2025 |
| Ιδιοκτήτης: | Διοίκηση |
| Κατάσταση Εγγράφου: | Τελικό |

# 1. Ασφάλεια πληροφοριών

## Σκοπός

Σκοπός της παρούσας Πολιτικής είναι να περιγράψει τον τρόπο με τον οποίο η εταιρεία διατηρεί αντίγραφα ασφαλείας (back-up) για όλα τα συστήματα της, ώστε να διασφαλίζει τα δεδομένα καθώς και τη διαδικασία επαναφοράς δεδομένων από αυτά.

## Εμπλεκόμενοι – Ευθύνες

Υποχρέωση εφαρμογής της παρούσας πολιτικής έχει το σύνολο του ανθρώπινου δυναμικού και των εξωτερικών συνεργατών της εταιρείας.

## Πολιτική Αντιγράφων Ασφαλείας

### Εισαγωγή

Η παρούσα πολιτική περιέχει πληροφορίες και κανόνες για τη τήρηση αντιγράφων ασφαλείας των πληροφοριακών συστημάτων της εταιρείας.

### Γενικοί Κανόνες

- Οι πληροφορίες σε επίπεδο συστήματος περιλαμβάνουν, για παράδειγμα, πληροφορίες κατάστασης συστήματος (System - State), λειτουργικό σύστημα (Operating System), λογισμικό εφαρμογών (Application Software) και άδειες χρήσης. Οι πληροφορίες σε επίπεδο χρήστη περιλαμβάνουν οποιεσδήποτε άλλες πληροφορίες εκτός από τις πληροφορίες σε επίπεδο συστήματος.
- Σε επίπεδο σχεδιασμού των αντιγράφων ασφαλείας της εταιρείας, έχει ληφθεί υπόψη ο κανόνας δημιουργίας αντιγράφων σε δύο (2) διαφορετικά επίπεδα, τα οποία είναι φυσικά και τεχνικά ανεξάρτητα και ως εκ τούτου δεν υπόκειται στους ίδιους κινδύνους αναφορικά με την ασφάλεια πληροφοριών.
- Οι μηχανισμοί που χρησιμοποιούνται για την προστασία της ακεραιότητας των αντιγράφων ασφαλείας του συστήματος πληροφοριών περιλαμβάνουν, για παράδειγμα, ψηφιακές υπογραφές ή κρυπτογράφηση.
- Τα αντίγραφα ασφαλείας του συστήματος πληροφοριών αντικατοπτρίζουν τις απαιτήσεις σε σχέδια έκτακτης ανάγκης καθώς και άλλες οργανωτικές απαιτήσεις για τη δημιουργία αντιγράφων ασφαλείας πληροφοριών.

## Λήψη Αντιγράφων Ασφαλείας

Η εταιρεία εφαρμόζει τα κατάλληλα αντίγραφα ασφαλείας για να διασφαλίζεται ότι όλες οι βασικές πληροφορίες και το λογισμικό μπορεί να ανακτηθεί μετά από καταστροφή ή αποτυχία μέσων. Κατά το σχεδιασμό του εφεδρικού σχεδίου εφαρμόζονται τα εξής:

- Με ευθύνη του IT Admin τηρούνται ακριβή και πλήρη αρχεία των αντιγράφων ασφαλείας και τεκμηριωμένων διαδικασιών αποκατάστασης. Το σύστημα λήψης αντιγράφων ασφαλείας, λαμβάνει με αυτοματοποιημένο τρόπο, αντίγραφα ασφαλείας των σημαντικών συστημάτων και αρχείων σύμφωνα με τον προγραμματισμό που έχει πραγματοποιηθεί.
- Τηρούνται αντίγραφα ασφαλείας εντός των χώρων της εταιρείας αλλά και σε δευτερεύοντα χώρο για λόγους επιχειρησιακής συνέχειας.
- Τα αντίγραφα ασφαλείας αποθηκεύονται σε κρυπτογραφημένα αποθηκευτικά μέσα.
- Διασφάλιση ότι οι εφεδρικές πληροφορίες έχουν κατάλληλο επίπεδο φυσικής και περιβαλλοντικής ασφάλειας.
- Ο IT Admin μεριμνά για τη δοκιμή των διαδικασιών αποκατάστασης για να επιτύχει τον απαιτούμενου χρόνο αποκατάστασης. Έχουν ενεργοποιηθεί ειδοποιήσεις για την έκβαση της διαδικασίας του αντιγράφου ασφαλείας. Αποστέλλεται αυτόματη ειδοποίηση για την αποτυχημένη λήψη αντιγράφου ασφαλείας.
- Η εταιρεία εξετάζει τη διαγραφή πληροφοριών που τηρούνται σε αντίγραφα ασφαλείας μόλις λήξει η περίοδος διατήρησης των πληροφοριών. Λαμβάνεται υπόψιν η σχετική νομοθεσία και οι κανονισμοί τήρησης πληροφοριών.

### Έλεγχος και Διατήρηση Αντιγράφων Ασφαλείας

- Οι ρυθμίσεις δημιουργίας αντιγράφων ασφαλείας για μεμονωμένα συστήματα και υπηρεσίες ελέγχονται τακτικά για να διασφαλίζεται ότι πληρούν τις απαιτήσεις των σχεδίων επιχειρηματικής συνέχειας και της γενικότερης στρατηγικής της εταιρείας.

- Στην περίπτωση κρίσιμων συστημάτων και υπηρεσιών, οι ρυθμίσεις αντιγράφων ασφαλείας θα πρέπει να καλύπτουν όλες τις πληροφορίες συστημάτων, τις εφαρμογές και τα δεδομένα που είναι απαραίτητα για την ανάκτηση ολόκληρου του συστήματος σε περίπτωση καταστροφής.

## Διαδικασία Λήψης Αντιγράφων Ασφαλείας

Η διαδικασία λήψης και διαχείρισης αντιγράφων ασφάλειας ακολουθεί τα παρακάτω βήματα:

- Το σύστημα λήψης αντιγράφων ασφαλείας, λαμβάνει με αυτοματοποιημένο τρόπο πλήρη και καθημερινά αντίγραφα ασφαλείας των συστημάτων σύμφωνα με τον προγραμματισμό που έχει γίνει από τους διαχειριστές των συστημάτων. Το αντίγραφο ασφαλείας αποθηκεύεται σε NAS Storage, το οποίο χρησιμοποιείται καθημερινά για Full/Incremental λήψη αντιγράφων.

- Εκτελούνται δειγματοληπτικά ενέργειες επιβεβαίωσης της ορθής λήψης των αντιγράφων, η οποία περιλαμβάνει τον έλεγχο των αρχείων που έχουν μεταφερθεί.
- Σε περίπτωση μη επιτυχούς ολοκλήρωσης της διαδικασίας, εξετάζεται το πρόβλημα.

### Ενημέρωση Αποτυχίας Αντιγράφων Ασφαλείας

Έχουν υλοποιηθεί προσαρμοσμένες εργασίες οι οποίες να πληροφορούν τον IT Admin για πιθανή βλάβη της διαδικασίας δημιουργίας αντιγράφων ασφαλείας, γράφοντας το κατάλληλο αρχείο καταγραφής, συμπεριλαμβανομένων πληροφοριών σχετικά με το σφάλμα, την ημερομηνία και την ώρα της δημιουργίας αντιγράφων ασφαλείας.

### Δοκιμή Αντιγράφων Ασφαλείας

Τα αντίγραφα ασφαλείας πρέπει να δοκιμάζονται ανά τακτά χρονικά διαστήματα μία φορά τον χρόνο ώστε να διασφαλίζεται η ακεραιότητα και η πληρότητα των περιεχόμενών τους. Έπειτα από κάθε δοκιμή των αντιγράφων ασφαλείας πρέπει να είναι σαφές αν:

- Η ολική επαναφορά των συστημάτων είναι εφικτή.
- Η διαδικασία επαναφοράς καλύπτει τους στόχους επαναφοράς.
- Τα δεδομένα μπορούν να εγκατασταθούν με επιτυχία σε εναλλακτικά συστήματα.
- Το προσωπικό το οποίο συμμετέχει στις διαδικασίες λήψης αντιγράφων ασφαλείας, δοκιμών και επαναφοράς έχουν πλήρη επίγνωση όλων των βημάτων που απαιτούνται στις διαδικασίες αυτές.

## Διαδικασία Επαναφοράς Δεδομένων από Αντίγραφα Ασφαλείας

Η διαδικασία επαναφοράς δεδομένων από αντίγραφα ασφάλειας ακολουθεί τα παρακάτω βήματα:

- Ο ιδιοκτήτης των δεδομένων που πρέπει να ανακτηθούν από τα αντίγραφα ασφαλείας αιτείται την ανάκτησή τους και δίνει όλα τα στοιχεία που μπορούν να οδηγήσουν στην ανεύρεση και ανάκτηση των δεδομένων, όπως περιγραφή των δεδομένων, ημερομηνία, ώρα κλπ.
    - Ανάλογα με τη φύση των δεδομένων προς ανάκτηση, το αίτημα γίνεται κατευθείαν από το χρήστη / ιδιοκτήτη των δεδομένων ή απαιτείται και η έγκριση του προϊσταμένου του.
    - Η αίτηση μπορεί να γίνει και μέσω ηλεκτρονικού ταχυδρομείου.
- Ο IT Admin αναζητά τα προς ανάκτηση δεδομένα στα αντίγραφα ασφαλείας.
- Επαναφέρουν τα δεδομένα από τα αντίγραφα ασφαλείας και βεβαιώνουν την επιτυχία της διαδικασίας επαναφοράς.
    - Σε περίπτωση μη επιτυχούς ολοκλήρωσης της διαδικασίας, ο IT Admin εξετάζει το πρόβλημα. Αν το πρόβλημα δεν επιλυθεί ή δημιουργήθηκε από βλάβη του συστήματος λήψης αντιγράφων ασφάλειας λαμβάνονται διορθωτικά μέτρα.
- Ο IT Admin ενημερώνει τον ιδιοκτήτη των δεδομένων για την επαναφορά τους.

| Διαδικασία Λήψης Αντιγράφων Ασφάλειας | |
|---|---|
| **Βήμα 1** | Δημιουργία πλάνου λήψης αντιγράφων ασφαλείας. |
| **Βήμα 2** | Ενημέρωση αποτυχίας αντιγράφων ασφαλείας. |
| **Βήμα 3** | Δοκιμή αντιγράφων ασφαλείας. |
| **Βήμα 4** | Αξιολόγηση της επαναφοράς αντιγράφων ασφάλειας. |

# 2. Φορητές συσκευές

## Σκοπός

Στο έγγραφο αυτό καλύπτονται οι βασικές απαιτήσεις ασφάλειας για τη διαχείριση φορητών συσκευών και καθορίζονται τα μέτρα προστασίας που πρέπει να εφαρμόζονται κατά τη χρήση τους.

## Εμπλεκόμενοι – Ευθύνες

Η πολιτική εφαρμόζεται σε όλους τους τομείς και τις εγκαταστάσεις της εταιρείας, όπως επίσης και στο προσωπικό των εξωτερικών συνεργατών, εφόσον απαιτείται, στους οποίους παρέχονται φορητές συσκευές για την άσκηση των εργασιών τους.

## Πολιτική Φορητών Συσκευών

### Εισαγωγή

Ως φορητές συσκευές ορίζονται, αλλά δεν περιορίζονται, οι παρακάτω:

- Φορητοί υπολογιστές (Laptops).
- Κινητά τηλέφωνα.
- Tablets.

Η συγκεκριμένη πολιτική καθορίζει τα μέτρα προστασίας που πρέπει να υπάρχουν κατά τη χρήση φορητών συσκευών, με στόχο το μετριασμό των ακόλουθων κινδύνων:

- Απώλεια ή κλοπή των φορητών συσκευών, συμπεριλαμβανομένων και των δεδομένων τους.
- Διαρροή διαβαθμισμένων πληροφοριών ή προσωπικών δεδομένων.
- Εισαγωγή ιών και κακόβουλου λογισμικού στο δίκτυο.

Τα μέτρα που προβλέπονται στην παρούσα πολιτική πρέπει να τηρούνται συνεχώς κατά τη χρήση και μεταφορά των φορητών συσκευών.

## Κανόνες Χρήσης Φορητών Συσκευών

Η εταιρεία υιοθετεί και υποστηρίζει μέτρα ασφαλείας για τη διαχείριση των κινδύνων που εισάγονται με τη χρήση φορητών συσκευών.

Η πολιτική για τις κινητές συσκευές λαμβάνει υπόψη τους κινδύνους που συνεπάγεται η εργασία με φορητές συσκευές σε μη προστατευμένα περιβάλλοντα.

Η πολιτική για τις φορητές συσκευές εξετάζει:

- Καταχώριση φορητών συσκευών.
- Απαιτήσεις για φυσική προστασία.
- Περιορισμός της σύνδεσης με τις υπηρεσίες πληροφοριών.
- Προστασία από κακόβουλα προγράμματα.
- Απομακρυσμένη απενεργοποίηση, διαγραφή ή κλείδωμα.
- Δημιουργία αντιγράφων ασφαλείας.
- Χρήση υπηρεσιών ιστού και εφαρμογών ιστού.
- Απομακρυσμένη διαχείριση συσκευών αν είναι εφικτό.

Λαμβάνεται μέριμνα για αποφυγή χρήσης κινητών συσκευών σε κοινόχρηστα μη ασφαλή δίκτυα όπως σε δημόσιους χώρους, αίθουσες συνεδριάσεων και άλλες μη προστατευόμενες περιοχές.

Σε περίπτωση που παραστεί ανάγκη χρήσης προσωπικής συσκευής αυτή γίνεται αποδεκτή εφόσον τηρούνται μέτρα ασφαλείας. Ενδεικτικά:

- Κλείδωμα με PIN ή Μοτίβο για τα κινητά τηλέφωνα και με κωδικό ασφαλείας για laptop σύμφωνα με την πολιτική κωδικών.
- Κρυπτογράφηση δίσκου σε περίπτωση laptop.
- Χρήση εφαρμογής προστασίας από κακόβουλο λογισμικό.
- Διαχωρισμό της ιδιωτικής και επαγγελματικής χρήσης των συσκευών, συμπεριλαμβανομένης της χρήσης λογισμικού για την υποστήριξη αυτών πραγματοποιώντας διαχωρισμό και προστασία επιχειρηματικών δεδομένων σε ιδιωτική συσκευή.
- Την παροχή πρόσβασης σε επιχειρηματικές πληροφορίες μόνο αφού οι χρήστες έχουν αναγνωρίσει τα καθήκοντά τους (φυσική προστασία, ενημέρωση λογισμικού κ.λπ.), έχουν παραιτηθεί από την ιδιοκτησία των επιχειρηματικών δεδομένων, επιτρέποντας την απομακρυσμένη διαγραφή δεδομένων από τον οργανισμό σε περίπτωση κλοπής ή απώλειας συσκευής ή όταν δεν είναι πλέον εξουσιοδοτημένοι να χρησιμοποιούν την υπηρεσία.

## Φορητοί Υπολογιστές

Οι φορητοί υπολογιστές που παρέχονται από την εταιρεία, προορίζονται για επαγγελματική και μόνο χρήση. Δεν προβλέπεται η χρήση τους για προσωπικούς σκοπούς.

Γενικότερα θα πρέπει να:

- Εφαρμόζεται ισχυρή κρυπτογράφηση σύμφωνα με την Πολιτική Κρυπτογράφησης.
- Είναι μέλη του Active Directory.
- Ενεργοποίηση απομακρυσμένης διαχείρισης αν είναι εφικτό.
- Κατά την χρήση αποσπώμενων μέσων γίνεται έλεγχος από αντιϊκό λογισμικό (Antivirus).
- Προστατεύονται φυσικά από κλοπή, ιδίως όταν παραμένουν, για παράδειγμα, σε αυτοκίνητα και άλλα μέσα ή τύπους μεταφοράς, δωμάτια ξενοδοχείων, συνεδριακά κέντρα και χώρους συνάντησης.
- Μην παραμένουν χωρίς επίβλεψη και όπου είναι δυνατόν, πρέπει να προστατεύονται συσκευές οι οποίες περιέχουν σημαντικές, ευαίσθητες ή κρίσιμες επιχειρηματικές πληροφορίες.

## Έλεγχος Πρόσβασης

- Δεν επιτρέπεται η σύνδεση σε μη ασφαλείς συνδέσεις και μη αξιόπιστες σελίδες. Οι χρήστες πρέπει να επιλέγουν την πρόσβαση σε σελίδες ασφαλών πρωτοκόλλων (πχ https).
- Δεν επιτρέπεται η σύνδεση μέσω των εταιρικών φορητών συσκευών σε περιεχόμενο σελίδων που δεν είναι επιτρεπτό από την εταιρεία.
- Ο χρήστης θα πρέπει να συνδέεται στις υποδομές της εταιρείας μέσω ασφαλών εικονικών δικτύων (VPN).
- Ο χρήστης όταν απομακρύνεται από τον φορητό υπολογιστή θα πρέπει να τον κλειδώνει και για την επανασύνδεσή του να απαιτείται κωδικός πρόσβασης.
- Πρέπει να είναι ενεργοποιημένες οι αυτόματες ενημερώσεις και εγκατεστημένες οι διορθώσεις ασφαλείας του κατασκευαστή.

**Συντομογραφίες**

| | |
|---|---|
| **https** | Hypertext Transfer Protocol Secure |
| **PIN** | Personal Identification Number |
| **VPN** | Virtual Private Network |

# 3. Προστασία και ορθή χρήση των πόρων

## Σκοπός

Η Πολιτική αυτή καθορίζει τους στόχους/αρχές για όλες τις πτυχές της Χρήσης Σταθμών Εργασίας εντός της εταιρείας **«Π.Ε. ΚΑΣΙΝΑΚΗΣ Α.Ε.»** και έχει ως σκοπό, την

κάλυψη των βασικών απαιτήσεων ασφάλειας για την ορθή χρήση του διαδικτύου, αλλά και για τις αρμοδιότητες των χρηστών.

# Εμπλεκόμενοι – Ευθύνες

Υποχρέωση εφαρμογής της παρούσας πολιτικής έχει το σύνολο του ανθρώπινου δυναμικού και των εξωτερικών συνεργατών της εταιρείας.

# Πολιτική Προστασίας Hardware-Software

## Εισαγωγή

Η παρούσα πολιτική διασφαλίζει την ορθή και αποδοτική λειτουργία του φυσικού εξοπλισμού και του λογισμικού (Software) που είναι εγκατεστημένο στους σταθμούς εργασίας και στους εξυπηρετητές, ώστε να διασφαλιστεί η ασφάλεια των δεδομένων που βρίσκονται στο δίκτυο της εταιρείας και να μειωθεί ο κίνδυνος μόλυνσης των συστημάτων με κακόβουλο λογισμικό.
Επιπλέον, θέτει κανόνες ορθής χρήσης του ηλεκτρονικού ταχυδρομείου, διαχείρισης κωδικών ασφαλείας καθώς και τις επιτρεπτές ενέργειες των εξουσιοδοτημένων χρηστών της εταιρείας, αλλά και καλύπτει τις βασικές απαιτήσεις ασφάλειας πληροφοριών για την ορθή χρήση του διαδικτύου και για τις προσωπικές ευθύνες των χρηστών. Τέλος, περιγράφει την πολιτική της **«Π.Ε. ΚΑΣΙΝΑΚΗΣ Α.Ε.»** όσον αφορά την εξ αποστάσεως εργασία του προσωπικού της και την υλοποίηση των μέτρων ασφάλειας ώστε να προστατευτούν οι πληροφορίες στις οποίες το προσωπικό έχει πρόσβαση, επεξεργάζεται και αποθηκεύει.

## Φυσική Προστασία Εξοπλισμού

Τα μέτρα για την διασφάλιση της καλής λειτουργίας των συστημάτων περιλαμβάνουν:

- Συστήματα Αδιάλειπτης Τάσης (UPS) και πολύμπριζα ασφαλείας για πρόληψη διακυμάνσεων ή πτώσης τάσης του ηλεκτρικού ρεύματος.
- Διατήρηση ιδανικών συνθηκών θερμοκρασίας και υγρασίας.
- Πυροσβεστήρες για αντιμετώπιση πυρκαγιάς.
- Κάμερες Εισόδου / Εξόδου για καταγραφή μη εξουσιοδοτημένης πρόσβασης στο χώρο.

### Επισκευή Βλαβών

Σε περίπτωση βλάβης hardware η αντικατάσταση γίνεται από τους διαχειριστές των συστημάτων ενώ το σύστημα βρίσκεται σε λειτουργία, εφόσον υπάρχει εφεδρικό ανταλλακτικό και εφόσον είναι εφικτό. Σε διαφορετική περίπτωση ενημερώνεται το επηρεαζόμενο τμήμα για διακοπή λειτουργίας του συστήματος για συγκεκριμένο χρονικό διάστημα. Σε κάθε περίπτωση η επισκευή ή αντικατάσταση γίνεται πάντα από αρμόδιο προσωπικό ή από εξουσιοδοτημένο συνεργάτη του κατασκευαστή ή από εξωτερικό συνεργάτη.

### Computer Room - Datacenter

Τα ικριώματα στα οποία φυλάσσεται ο δικτυακός εξοπλισμός όπως switches, Firewall, UPS, τηλεφωνία κ.α. βρίσκονται σε ξεχωριστό χώρο (Computer Room), ενώ πρόσβαση έχει μόνο το αρμόδιο προσωπικό. Απαγορεύεται η πρόσβαση του προσωπικού στο χώρο του Computer Room χωρίς εξουσιοδότηση.

Για την προστασία του υλικού εξοπλισμού από διακυμάνσεις ή πτώσεις ηλεκτρικού ρεύματος χρησιμοποιείται Σύστημα Αδιάλειπτης Τάσης (UPS). Σε περίπτωση μη επαναφοράς του ηλεκτρικού ρεύματος για μεγάλο χρονικό διάστημα γίνεται τερματισμός των συστημάτων για αποφυγή απώλειας δεδομένων και βλαβών.

Περιβαλλοντικές συνθήκες, όπως η θερμοκρασία και η υγρασία, παρακολουθούνται όπου κρίνεται απαραίτητο από τους διαχειριστές των συστημάτων, ώστε να μην επηρεάσουν δυσμενώς τη λειτουργία του εξοπλισμού.

Κάθε 6 μήνες πραγματοποιείται έλεγχος των μπαταριών στα Συστήματα Αδιάλειπτης Τάσης (UPS), αλλά και συντήρηση του δικτυακού εξοπλισμού.

## Προστασία Software

### Προστασία Δεδομένων από Κακόβουλο Λογισμικό

Η Διοίκηση ορίζει την πολιτική που θα εφαρμοστεί στην εταιρεία προκειμένου να διασφαλιστούν τα Πληροφοριακά Συστήματα από την απειλή κακόβουλου λογισμικού.

Τρόποι αντιμετώπισης των απειλών:

- Εγκατάσταση αντιϊκού λογισμικού (Antivirus) με προστασία πραγματικού χρόνου (real-time) σε όλους τους σταθμούς εργασίας και τους εξυπηρετητές.
- Το αντιϊκό λογισμικό έχει ρυθμιστεί ώστε να ελέγχει υποχρεωτικά τα αποσπώμενα μέσα, όταν εισάγονται στον σταθμό εργασίας για κακόβουλο λογισμικό. Ο χρήστης δεν μπορεί να παρακάμψει τον συγκεκριμένο έλεγχο.
- Αλλαγές στο αντιϊκό λογισμικό μπορεί να πραγματοποιήσει μόνο εξουσιοδοτημένο προσωπικό. Οι ρυθμίσεις είναι κλειδωμένες με κωδικό ασφαλείας για τον τελικό χρήστη.
- Υφίσταται τεχνικός περιορισμός που αποτρέπει την εγκατάσταση λογισμικού στους σταθμούς εργασίας από μη εξουσιοδοτημένο προσωπικό.
- Απαγόρευση εγκατάστασης και χρήσης προγραμμάτων που δεν έχουν εγκριθεί ή δεν διαθέτουν νόμιμη άδεια.
- Οι αναβαθμίσεις των λειτουργικών συστημάτων των εξυπηρετητών της εταιρείας πραγματοποιούνται μετά την παρέλευση ενός καθορισμένου χρονικού διαστήματος από την κυκλοφορία τους, με ευθύνη του IT Admin, ώστε να λαμβάνονται εγκαίρως οι

απαραίτητες ενημερώσεις ασφαλείας, ενώ ταυτόχρονα να διασφαλίζεται πως δεν θα προκύψουν διακοπές στην εύρυθμη λειτουργία τους εξαιτίας προβληματικών ενημερώσεων.

- Στους χρήστες των σταθμών εργασίας είναι ενεργοποιημένες οι αυτόματες ενημερώσεις του λειτουργικού συστήματος και του αντιϊκού λογισμικού.

## Πολιτική Κωδικών

Η διαχείριση κωδικών πρόσβασης θα πρέπει να είναι αλληλεπιδραστική και θα πρέπει να εξασφαλίζει το αποδεκτό επίπεδο κωδικών.

Η διαχείριση των κωδικών πρόσβασης ορίζεται από τους ακόλουθους κανόνες:

- Επιβάλλεται η χρήση ατομικών αναγνωριστικών χρήστη και κωδικών πρόσβασης για τη διατήρηση της λογοδοσίας.
- Υποχρεώνονται οι χρήστες να αλλάξουν τον προσωρινό κωδικό που τους έχει αποδοθεί από το σύστημα κατά την πρώτη είσοδό τους σε αυτό.
- Επιτρέπεται στους χρήστες να επιλέγουν και να αλλάζουν τους δικούς τους κωδικούς πρόσβασης και να περιλαμβάνεται μια διαδικασία επιβεβαίωσης που να αναγνωρίζει και να κάνει εμφανή στους χρήστες και διαχειριστές τα σφάλματα εισόδου.
- Επιβάλλεται η επιλογή πολύπλοκων κωδικών από τους χρήστες.
- Επιβάλλεται η τακτική αλλαγή των κωδικών πρόσβασης ανάλογα με τις ανάγκες και τις παραμέτρους χρήσης του εκάστοτε πληροφοριακού πόρου.
- Δεν επιτρέπεται η εμφάνιση των κωδικών πρόσβασης στην οθόνη κατά την εισαγωγή.
- Εξασφαλίζεται ότι τα προσωρινά συνθηματικά παρέχονται στους χρήστες με ασφαλή τρόπο.

### *Οδηγίες Κωδικών Πρόσβασης*

Η πρόσβαση σε σταθμούς εργασίας και το πληροφοριακό σύστημα της εταιρείας πραγματοποιείται έπειτα από ταυτοποίηση και αυθεντικοποίηση του χρήστη. Αυτό επιτυγχάνεται μέσω του μοναδικού ονόματος χρήστη και του κωδικού πρόσβασης που έχει ο κάθε χρήστης του αντίστοιχου πληροφοριακού πόρου:

Τα συνθηματικά των χρηστών πρέπει να αποτελούνται από τουλάχιστον Οκτώ (8) αλφαριθμητικούς χαρακτήρες, μεταξύ των οποίων θα υπάρχουν χαρακτήρες από τουλάχιστον τρεις από τις παρακάτω κατηγορίες:

- Πεζοί λατινικοί χαρακτήρες (a έως z).
- Κεφαλαίοι χαρακτήρες (A έως Z).
- Αριθμοί (0 έως 9).
- Ειδικοί χαρακτήρες (π.χ. !, $, #, %).

Τα συνθηματικά λήγουν κάθε 180 ημέρες.
Ο χρήστης δεν επιτρέπεται να επαναχρησιμοποιήσει τα προηγούμενα πέντε (5) συνθηματικά που εφάρμοζε κατά την είσοδό του, ενώ επιτρέπεται να αλλάξει συνθηματικό πέντε (5) ημέρες μετά από την τελευταία αλλαγή του.

Οι χρήστες είναι υποχρεωμένοι να χρησιμοποιούν την λειτουργία πιστοποίησης πολλαπλών παραγόντων (MFA) εάν είναι διαθέσιμη.

*Περιορισμοί στη Δημιουργία Κωδικών Πρόσβασης*

Κατά τη δημιουργία και αλλαγή κωδικού πρόσβασης **απαγορεύεται**:

- Η χρήση ίδιων συνθηματικών που εφαρμόζονται σε πληροφοριακά συστήματα της εταιρείας με τα συνθηματικά που χρησιμοποιούνται σε συστήματα εκτός αυτής (π.χ. προσωπικοί υπολογιστές στην οικία των εργαζομένων κ.ο.κ.).
- Να περιέχουν:
    - Μέρος του ονόματος χρήστη.
    - Λέξεις που σχετίζονται με την επωνυμία ή υπηρεσιών της εταιρείας.
    - Οποιαδήποτε πληροφορία που αφορά τον χρήστη, όπως η ημερομηνία γέννησης, τον αριθμό τηλεφώνου, κλπ.
- Η χρήση λειτουργιών αυτόματης συμπλήρωσης συνθηματικού «Remember Password», καθώς και η αποθήκευση των συνθηματικών σε υπολογιστές ή συσκευές χωρίς κρυπτογράφηση.
- Να κοινοποιούνται σε τρίτους.

*Πρόσβαση σε Υπηρεσίες Microsoft 365*

Για πρόσβαση στις υπηρεσίες της Microsoft 365 εφαρμόζεται επιπρόσθετα το μέτρο της Ταυτοποίησης 2 Παραγόντων (2FA).

*Μέτρα Προστασίας Κωδικών Πρόσβασης*

- Οι χρήστες αλλάζουν τακτικά τον κωδικό πρόσβασης στις περιπτώσεις που δεν δύναται να εφαρμοστεί αυτόματα.
- Σε περίπτωση πέντε (5) διαδοχικών αποτυχημένων προσπαθειών πρόσβασης, αδρανοποιείται ο λογαριασμός του χρήστη που επιχειρεί την πρόσβαση για δεκαπέντε (15) λεπτά.
- Μετά από την αποχώρηση οποιουδήποτε υπαλλήλου θα πρέπει να απενεργοποιούνται άμεσα τα στοιχεία πρόσβασής του στους πληροφοριακούς πόρους.
- Οι χρήστες πρέπει να αλλάζουν το συνθηματικό τους σε κάθε περίπτωση που θεωρούν ότι μπορεί να έχει αποκαλυφθεί.

- Σε περίπτωση καταγραφής συνθηματικών σε ηλεκτρονικό αρχείο, το αρχείο αυτό θα είναι αποθηκευμένο ως κρυπτογραφημένο και θα απαιτείται κωδικός πρόσβασης για την ανάγνωσή του.
- Οι κωδικοί πρόσβασης ελέγχονται αυτόματα από το σύστημα για την τήρηση των κανόνων το οποίο έχει τη δυνατότητα να απορρίπτει όσους δεν ακολουθούν τους κανόνες διαχείρισης και οδηγίες διαμόρφωσής τους.
- Οι κωδικοί πρόσβασης πρέπει να θεωρούνται εμπιστευτικές πληροφορίες.

## Κανόνες Ηλεκτρονικών Μηνυμάτων

Οι εκτιμήσεις ασφάλειας πληροφοριών για τα ηλεκτρονικά μηνύματα πρέπει να περιλαμβάνουν τα εξής:

- Την προστασία των μηνυμάτων από μη εξουσιοδοτημένη πρόσβαση, τροποποίηση ή άρνηση παροχής υπηρεσιών.
- Εξασφάλιση της σωστής διεύθυνσης αποστολής και μεταφοράς του μηνύματος.
- Την επιλογή αξιόπιστου παρόχου.
- Μέριμνα για νομικά ζητήματα, για παράδειγμα απαιτήσεις για ηλεκτρονικές υπογραφές.
- Αξιολόγηση του κινδύνου πριν από τη χρήση εξωτερικών δημόσιων υπηρεσιών όπως η άμεση ανταλλαγή μηνυμάτων, μέσα κοινωνικής δικτύωσης ή κοινή χρήση αρχείων.
- Ισχυρότερα επίπεδα ελέγχου ταυτότητας από δημόσια προσβάσιμα δίκτυα.

## Οδηγίες Χρήσης Υπηρεσιών Μηνυμάτων (E-mails)

- Απαγορεύεται η χρήση του εταιρικού ηλεκτρονικού ταχυδρομείου για την αποστολή ή προώθηση αυτόκλητων μηνυμάτων (Unsolicited E-mail / Spam).
- Οι υπηρεσίες ηλεκτρονικού ταχυδρομείου παρέχονται στο προσωπικό της Εταιρείας για να χρησιμοποιούνται αποκλειστικά και μόνο για τους σκοπούς της Εταιρείας.
- Η Εταιρεία δεν είναι υποχρεωμένη να προστατεύει τα ηλεκτρονικά μηνύματα ως προσωπικά δεδομένα των υπαλλήλων.
- Οι χρήστες γνωρίζουν ότι ο παραλήπτης ενός μηνύματος μπορεί να το διατηρήσει για απροσδιόριστο χρόνο, να το προωθήσει σε τρίτους ή ακόμα να αλλοιώσει το περιεχόμενό του και έπειτα να το προωθήσει σε τρίτους.
- Οι χρήστες γνωρίζουν ότι η πραγματική ταυτότητα του αποστολέα ενός μηνύματος μπορεί να είναι διαφορετική από την αναγραφόμενη στο μήνυμα.
- Οι χρήστες δεν χρησιμοποιούν τους λογαριασμούς ηλεκτρονικού ταχυδρομείου συναδέλφων τους. Αν απαιτείται περισσότερα του ενός πρόσωπα να χρησιμοποιούν ένα λογαριασμό, τότε δημιουργείται ειδικός λογαριασμός με όνομα που δε συνδέεται με κάποιο πρόσωπο.
- Απαγορεύεται η επισύναψη διαβαθμισμένων αρχείων μέσω ηλεκτρονικού ταχυδρομείου, εκτός αν το αρχείο αυτό είναι κρυπτογραφημένο.

- Γίνεται χρήση 2FA για τη διασφάλιση της πρόσβασης με αυτό.

## Επιτρεπόμενη Χρήση Ηλεκτρονικού Ταχυδρομείου

Ο λογαριασμός ηλεκτρονικού ταχυδρομείου που παρέχεται σε κάθε υπάλληλό της εταιρείας, χρησιμοποιείται μόνο για επιχειρησιακούς σκοπούς. Για την αποστολή διαβαθμισμένων πληροφοριών μέσω ηλεκτρονικού ταχυδρομείου, πρέπει να ακολουθούνται συγκεκριμένες οδηγίες, σύμφωνα με την Πολιτική Διαβάθμισης Πληροφοριών. Όλα τα μηνύματα που αποστέλλονται από διεύθυνση ηλεκτρονικού ταχυδρομείου της εταιρείας, παραμένουν στην κυριότητα της «**Π.Ε. ΚΑΣΙΝΑΚΗΣ Α.Ε.**» και θεωρούνται μέρος των εταιρικών δεδομένων.

Ο IT Admin είναι υπεύθυνος για τη ρύθμιση και επίβλεψη της λειτουργίας του συστήματος Ηλεκτρονικού Ταχυδρομείου. Η εταιρεία διατηρεί το δικαίωμα να παρακολουθεί και να ελέγχει τα αρχεία καταγραφών για τη χρήση του ηλεκτρονικού ταχυδρομείου, προκειμένου να αξιολογεί τη συμμόρφωσή τους με την πολιτική. Αυτό γίνεται πάντα, σύμφωνα με τις διατάξεις της σχετικής νομοθεσίας.

## Ανάλυση Πολιτικής Ορθής Χρήσης των Σταθμών Εργασίας

Οι εργαζόμενοι της εταιρείας είναι υποχρεωμένοι να τηρούν τους παρακάτω κανόνες κατά τη χρήση των σταθμών εργασίας:

- Κάθε εργαζόμενος συνδέεται με δικό του μοναδικό όνομα χρήστη (Username) και συνθηματικό (Password).
- Οι εργαζόμενοι δεν πρέπει σε καμία περίπτωση να γνωστοποιούν τους κωδικούς τους.
- Η χρήση των σταθμών εργασίας γίνεται αποκλειστικά και μόνο για την εκπλήρωση των σκοπών της εταιρείας. Η προσωπική χρήση δεν επιτρέπεται.
- Κάθε υπάλληλος είναι υπεύθυνος για τον σταθμό εργασίας του καθώς και την καλωδίωση αυτού και οφείλει να τον προσέχει και να μην τα κακομεταχειρίζεται.
- Οι εργαζόμενοι κλειδώνουν τον υπολογιστή τους όταν απομακρύνονται από τη θέση τους.
- Όταν εκτυπώνονται ευαίσθητες ή διαβαθμισμένες πληροφορίες, πρέπει να αφαιρούνται από τους εκτυπωτές αμέσως.
- Απαγορεύεται η εγκατάσταση προγραμμάτων με σκοπό την προσωπική χρήση, εκτός από αυτών που έχει ορίσει η εταιρεία για την εκπλήρωση των εργασιών της εταιρείας.
- Κατά το πέρας της εργασίας έγγραφα και ευαίσθητα δεδομένα φυλάσσονται κλειδωμένα στους αντίστοιχους αποθηκευτικούς χώρους και οι σταθμοί εργασίας κλειδώνονται.

## Ανάλυση Πολιτικής Ορθής Χρήσης του Διαδικτύου

Η πρόσβαση στο διαδίκτυο επιτρέπεται σε όλους τους εργαζομένους. Η πρόσβαση είναι ελεγχόμενη μέσω του Τείχους Προστασίας (Firewall) και γίνεται καταγραφή όλων των δραστηριοτήτων σε αρχεία καταγραφής (Log Files). Τα αρχεία καταγραφής (Log Files) ελέγχονται

δειγματοληπτικά για παραβάσεις των εργαζομένων, είτε για ύποπτη κίνηση προς το δίκτυο της εταιρείας από εξωτερικό παράγοντα αλλά και από το εσωτερικό δίκτυο προς τα έξω.

Κάθε εργαζόμενος οφείλει να είναι ιδιαίτερα προσεκτικός όσον αφορά τις ιστοσελίδες που ανοίγει στις εφαρμογές πλοήγησης, προτιμώντας γνωστές και έγκυρες. Σε περίπτωση που παρατηρήσει κάτι ασυνήθιστο πρέπει να το αναφέρει. Σε καμία περίπτωση δεν επισκέπτεται αμφιβόλου εγκυρότητας ιστότοπους.

Οι ίδιοι κανόνες ισχύουν και για τους επισκέπτες / συνεργάτες της εταιρείας, οι οποίοι συνδέονται σε ξεχωριστό δίκτυο το οποίο δεν επικοινωνεί με το παραγωγικό δίκτυο της εταιρείας, για την διασφάλιση των δεδομένων από κακόβουλο λογισμικό που μπορεί να υπάρχει εγκατεστημένο στα laptop ή στα κινητά τηλέφωνα (Smartphone) των επισκεπτών / συνεργατών.

Για να καταστεί ασφαλής για τα δεδομένα και για τα υπολογιστικά συστήματα της Εταιρείας η περιήγηση στο διαδίκτυο, δεν επιτρέπεται η πρόσβαση σε ορισμένα είδη δικτυακών τόπων. Ενδεικτικά περιορίζονται μέσω Web / Application filtering:

- Δικτυακοί τόποι που φιλοξενούν διαμοιρασμούς αρχείων (torrent files).
- Δικτυακοί τόποι πορνογραφικού περιεχομένου.
- Δικτυακοί τόποι τζόγου.
- Δικτυακοί τόποι ηλεκτρονικών παιχνιδιών.
- Δικτυακοί τόποι κακόβουλου λογισμικού (Hacking, Phishing, Spams, Malware).

## Πολιτική Καθαρού Γραφείου

- Όπου είναι πρακτικά δυνατόν, τα έγγραφα και τα πολυμέσα των υπολογιστών, όταν δεν χρησιμοποιούνται και ιδιαίτερα εκτός των ωρών εργασίας, θα πρέπει να αποθηκεύονται σε κατάλληλα κλειδωμένα χρηματοκιβώτια, ερμάρια ή άλλες μορφές επίπλων που ασφαλίζονται.
- Όταν εκτυπώνονται ευαίσθητες ή διαβαθμισμένες πληροφορίες, αφαιρούνται από τους εκτυπωτές αμέσως και μετά την χρήση τους τοποθετούνται σε ασφαλή χώρο.
- Σημειώσεις και έγγραφα οργάνωσης αποθηκεύονται σε μη εμφανές σημείο όταν δεν χρησιμοποιούνται.

Τα έγγραφα που παραμένουν πάνω στο γραφείο είναι περισσότερο ευάλωτα στην περίπτωση επέλευσης κάποιου κινδύνου και οφείλουν άπαντες να μεριμνούν για την προστασία αυτών.

## Πολιτική Καθαρής Οθόνης

- Οι σταθμοί εργασίας όταν δεν χρησιμοποιούνται πρέπει να παραμένουν κλειδωμένοι.
- Οι οθόνες υπολογιστών εργαζομένων με εμπιστευτικά στοιχεία θα πρέπει να τοποθετούνται υπό κατάλληλες γωνίες ώστε να μην είναι ευκρινείς από μη εξουσιοδοτημένα άτομα.
- Να γίνεται χρήση του συνδυασμού πλήκτρου WIN+L για το άμεσο κλείδωμα της οθόνης του Η/Υ (σε συστήματα Windows).

- Το κλείδωμα ασφαλείας των Windows έχει ρυθμιστεί ώστε να ενεργοποιείται όταν δεν υπάρχει δραστηριότητα για προκαθορισμένο χρονικό διάστημα. Προβλέπεται αυτόματο κλείδωμα του υπολογιστή μετά το πέρας δεκαπέντε (15) λεπτών αδράνειας.

## Χρήση Πόρων κατά την Τηλεργασία

Η απομακρυσμένη πρόσβαση στις εσωτερικές υπηρεσίες, επιτρέπεται μόνο μέσω ασφαλών εικονικών δικτύων (VPN).

## Μέτρα Ασφαλείας

- Το προσωπικό της Εταιρείας μπορεί να έχει εξωτερική πρόσβαση μόνο μέσω χρήσης κρυπτογραφημένων καναλιών επικοινωνίας για την πρόσβαση στους υπολογιστικούς της πόρους.
- Σε κάθε περίπτωση, για την απομακρυσμένη σύνδεση σε πληροφοριακές υποδομές και πόρους της Εταιρείας, χρησιμοποιούνται μόνο εγκεκριμένες από την εταιρεία εφαρμογές.
- Κάθε εργαζόμενος ο οποίος συνδέεται απομακρυσμένα στις πληροφοριακές υποδομές της Εταιρείας έχει την υποχρέωση να συμμορφώνεται με τους κανόνες ορθής χρήσης των εταιρικών πόρων και πληροφοριών.
- Αποτελεί υποχρέωση των εξουσιοδοτημένων για εξ αποστάσεως πρόσβαση χρηστών, να τηρούν αυστηρά προσωπικούς τους κωδικούς πρόσβασης, να μην τους μοιράζονται με τρίτους και να διασφαλίζουν ότι μόνο αυτοί συνδέονται απομακρυσμένα σε πληροφοριακές υποδομές και πόρους της Εταιρείας.
- Οι ενέργειες που εκτελούν οι χρήστες, οι οποίοι συνδέονται εξ αποστάσεως στις πληροφοριακές υποδομές της εταιρείας καταγράφονται.

## Κατευθυντήριες Γραμμές της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα για τη Λήψη Μέτρων Ασφαλείας στο Πλαίσιο της Τηλεργασίας

Η Ελληνική Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, με στόχο την ευαισθητοποίηση των υπευθύνων επεξεργασίας, των εκτελούντων την επεξεργασία, των εργαζομένων και γενικότερα του κοινού αναφορικά με τους κινδύνους που αφορούν την προστασία των προσωπικών δεδομένων αλλά, ταυτόχρονα, και τις σχετικές υποχρεώσεις που απορρέουν από τον Γενικό Κανονισμό Προστασίας Δεδομένων και τον νόμο 4624/2019, παραθέτει τις ακόλουθες Κατευθυντήριες Γραμμές:

- Ο οργανισμός / επιχείρηση (εφεξής, φορέας) οφείλει να ορίσει και να υποστηρίξει συγκεκριμένες διαδικασίες για την τηλεργασία. Οι διαδικασίες αυτές πρέπει να λαμβάνουν υπόψη, για την κάθε περίπτωση, τη φύση και τη σοβαρότητα των κινδύνων ως προς την προστασία προσωπικών δεδομένων, οι οποίοι απορρέουν από την εξ αποστάσεως εργασία.
- Ο φορέας οφείλει να ενημερώνει επαρκώς, να εκπαιδεύει και να συνδράμει τους εργαζομένους του στην εφαρμογή των διαδικασιών αυτών, λαμβάνοντας υπόψη ότι πολλοί χρήστες δεν είναι εξοικειωμένοι με τις τεχνολογίες που υποστηρίζουν την τηλεργασία και

τους σχετικούς κινδύνους. Για τον σκοπό αυτό, είναι πολύτιμη η συμβολή του Υπεύθυνου Προστασίας Δεδομένων (DPO) όπου έχει ορισθεί.

- Επισημαίνεται ιδιαίτερα ότι οι υποχρεώσεις των φορέων αναφορικά με την προστασία των προσωπικών δεδομένων των εργαζομένων τους αποκτούν ιδιάζουσα βαρύτητα στην περίπτωση της τηλεργασίας. Και τούτο, διότι ο εργαζόμενος, λόγω του γεγονότος ότι βρίσκεται στο σπίτι του, έχει μεγαλύτερη προσδοκία για την προστασία της ιδιωτικής του ζωής.

Οι διαδικασίες για την τηλεργασία συστήνεται να περιλαμβάνουν μέτρα, όπως τα ακόλουθα:

- Διασφάλιση ότι δεν υπάρχει δυνατότητα μη ασφαλούς απομακρυσμένης πρόσβασης σε πόρους των πληροφοριακών συστημάτων του φορέα, όπως υπολογιστές εσωτερικού δικτύου και εσωτερικά αρχεία. Η ασφαλής σύνδεση μπορεί, ενδεικτικώς, να επιτευχθεί μέσω εικονικού ιδιωτικού δικτύου στο οποίο πραγματοποιείται κρυπτογράφηση των δεδομένων και αυθεντικοποίηση των χρηστών (π.χ. IPSec VPN).
    - Καθορισμός και περιορισμός των πόρων στους οποίους επιτρέπεται η απομακρυσμένη πρόσβαση στο απολύτως απαραίτητο, ανάλογα με τα καθήκοντα που επιτελεί ο τηλεργαζόμενος.
    - Σύνδεση σε υπολογιστικά συστήματα του φορέα μέσω υπηρεσίας «απομακρυσμένης επιφάνειας εργασίας» (RDP), μόνο εφόσον αυτή γίνεται μέσω ασφαλούς εικονικού ιδιωτικού δικτύου (VPN).
- Χρήση ασφαλούς πρωτοκόλλου WPA2 με ισχυρό κωδικό, όταν η σύνδεση της συσκευής του τηλεργαζόμενου στο Διαδίκτυο γίνεται μέσω ασύρματου δικτύου (Wi-Fi). Τούτο ισχύει ακόμα και όταν μετά τη σύνδεση στο Διαδίκτυο, γίνεται ασφαλής σύνδεση στο δίκτυο του φορέα π.χ. με χρήση VPN.
- Αποφυγή αποθήκευσης αρχείων με προσωπικά δεδομένα σε υπηρεσίες διαδικτυακής αποθήκευσης (π.χ. Dropbox, Google Drive), εκτός και αν υπάρχουν τα κατάλληλα εχέγγυα, όπως π.χ. να πρόκειται για υπηρεσία που παρέχεται, με κατάλληλα μέτρα ασφάλειας, από τον φορέα ή τα δεδομένα να αποθηκεύονται αποκλειστικά σε κατάλληλα κρυπτογραφημένη μορφή.

## Χρήση Εφαρμογών Ηλεκτρονικού Ταχυδρομείου / Ανταλλαγής Μηνυμάτων

- Αποφυγή χρήσης προσωπικού ηλεκτρονικού ταχυδρομείου (π.χ. Gmail, Yahoo, Hotmail) για αποστολή ή λήψη μηνυμάτων για σκοπούς τηλεργασίας, τα οποία σχετίζονται με προσωπικά δεδομένα. Αντ' αυτού, θα πρέπει να χρησιμοποιείται η επαγγελματική ηλεκτρονική διεύθυνση την οποία παρέχει ο φορέας. Εάν αυτό δεν είναι τεχνικά εφικτό (π.χ. μη δυνατότητα πρόσβασης στο εσωτερικό ηλεκτρονικό ταχυδρομείο από εξωτερικό του φορέα δίκτυο), τότε το περιεχόμενο των μηνυμάτων που αφορά προσωπικά δεδομένα πρέπει να κρυπτογραφείται κατάλληλα (π.χ. είτε ολόκληρο το μήνυμα είτε μόνο τα συνημμένα αρχεία).

- Αποφυγή χρήσης εφαρμογών ανταλλαγής μηνυμάτων (κείμενο ή / και βίντεο) για τους σκοπούς της τηλεργασίας, όταν τα μηνύματα αυτά περιέχουν προσωπικά δεδομένα, των οποίων τυχόν διαρροή θα επέφερε κινδύνους. Αν είναι πραγματικά απαραίτητο, να προτιμώνται υπηρεσίες των οποίων τα χαρακτηριστικά ασφάλειας (κρυπτογράφηση, ρυθμίσεις προστασίας δεδομένων) αξιολογούνται ως ισχυρά.

### Πραγματοποίηση Τηλεδιασκέψεων

- Στην περίπτωση τηλεδιασκέψεων, θα πρέπει να αξιοποιούνται πλατφόρμες που υποστηρίζουν υπηρεσίες ασφαλείας (κρυπτογράφηση). Για παράδειγμα, θα πρέπει να αποφεύγεται λογισμικό τηλεδιάσκεψης το οποίο δεν εξασφαλίζει κρυπτογράφηση από άκρη σε άκρη (end-to-end encryption).
- Σε περίπτωση προγραμματισμένης τηλεδιάσκεψης, προστασία του συνδέσμου (link) αυτής (π.χ. όχι δημοσιοποίησή του σε κοινωνικό δίκτυο).

Προσεκτική μελέτη των όρων χρήσης και των όρων προστασίας προσωπικών δεδομένων κατά την επιλογή της λύσης τηλεδιάσκεψης.

## Χρήση Τερματικής Συσκευής / Αποθηκευτικών Μέσων

Κατά τη χρήση σταθμών εργασίας ή αποθηκευτικών μέσων οι χρήστες σε συνεργασία με τον IT Admin, ενόσω βρίσκονται σε καθεστώς τηλεργασίας, οφείλουν να τηρούν τους παρακάτω κανόνες:

1. Εγκατάσταση και τακτική ενημέρωση Antivirus και Firewall στη συσκευή μέσω της οποίας πραγματοποιείται η τηλεργασία.
2. Εγκατάσταση των πλέον πρόσφατων ενημερώσεων του λογισμικού εφαρμογών και λειτουργικού συστήματος της συσκευής των εργαζομένων.
3. Σε περιπτώσεις σύνδεσης σε προγράμματα πλοήγησης στο Διαδίκτυο (π.χ. Firefox, Chrome κτλ.) ή σε web applications, ο χρήστης οφείλει να διασφαλίζει ότι:
   a. Αναφορικά με τα προγράμματα πλοήγησης που χρησιμοποιεί, αυτά να είναι ενημερωμένα με τις πλέον πρόσφατες, ανά περίπτωση, εκδόσεις τους.
   b. Κατά την σύνδεση μέσω προγραμμάτων πλοήγησης επιλέγει, κατά προτίμηση, το άνοιγμα καρτέλας ανώνυμης περιήγησης ή εναλλακτικά διαγράφει από το ιστορικό των συνδέσμων (history) τους συνδέσμους που δημιούργησε κατά την περιήγησή του.
   c. Δεν επιλέγει αποθήκευση των προσωπικών κωδικών πρόσβασης που χρησιμοποιεί κατά την σύνδεσή του στις εταιρικές υποδομές.
4. Σε περιπτώσεις σύνδεσης από μη εταιρικές συσκευές πρέπει να γίνεται διαχωρισμός των αρχείων που περιέχουν δεδομένα προσωπικού χαρακτήρα και εταιρικά δεδομένα, τα οποία σχετίζονται με την εργασία, από προσωπικά αρχεία τα οποία τηρεί ο εργαζόμενος στη συγκεκριμένη συσκευή (π.χ. σε σαφώς διακριτούς φακέλους, με κατάλληλη προσδιοριστική ονομασία).
5. Κατάλληλη κρυπτογράφησης συσκευών τηλεργασίας

6. Υποστήριξη διαδικασιών λήψης αντιγράφων ασφαλείας για αρχεία με προσωπικά δεδομένα, τα οποία υφίστανται επεξεργασία στο πλαίσιο δραστηριοτήτων τηλεργασίας.
7. «Κλείδωμα» της συσκευής από την οποία γίνεται η τηλεργασία εφόσον μένει, για κάποιο λόγο, χωρίς επιτήρηση.

**Συντομογραφίες**

| | |
|---|---|
| **H/Y** | Ηλεκτρονικός Υπολογιστής |
| **2FA** | Two-Factor Authentication |
| **IPS** | Intrusion Prevention System |
| **IPSec** | Internet Protocol Security |
| **MFA** | Multi-factor Authentication |
| **RDP** | Remote Desktop Protocol |
| **UPS** | Uninterruptible Power Supply |
| **USB** | Universal Serial Bus |
| **VPN** | Virtual Private Network |
| **Wi-Fi** | Wireless Fidelity |
| **WPA2** | Wi-Fi Protected Access 2 |

# 4. Πειθαρχικά Παραπτώματα

## Σκοπός

Η Πολιτική Πειθαρχικών Παραπτωμάτων είναι η απόδειξη πως όλοι οι εργαζόμενοι ακολουθούν τις πολιτικές ασφάλειας που τους έχουν δοθεί. Αυτή η Πολιτική καθορίζει τους στόχους/αρχές για όλες τις πτυχές της διαχείρισης των Πειθαρχικών Παραπτωμάτων εντός της εταιρείας και επιτυγχάνεται μέσα από μία σειρά ελέγχων και των αντίστοιχων κυρώσεων.

## Εμπλεκόμενοι – Ευθύνες

Υποχρέωση εφαρμογής της παρούσας πολιτικής έχει το σύνολο του ανθρώπινου δυναμικού της εταιρείας.

# Πολιτική Πειθαρχικών Παραπτωμάτων

## Εισαγωγή

Η Πολιτική Πειθαρχικών Παραπτωμάτων εξασφαλίζει την τήρηση των πολιτικών ασφαλείας καθώς και των σχετικών διαδικασιών και οδηγιών εργασίας από το σύνολο του προσωπικού της εταιρείας. Αυτή η Πολιτική επιτυγχάνεται μέσα από μία σειρά ελέγχων και των κυρώσεων που επιβάλλονται ανά είδος παραπτώματος ή παράβασης.
Πειθαρχικό παράπτωμα αποτελεί κάθε παράβαση υπαλληλικού καθήκοντος που συντελείται με υπαίτια πράξη ή παράλειψη και μπορεί να καταλογισθεί στον υπάλληλο είτε αυτή προκλήθηκε με δόλο είτε όχι.
Για την ασφάλεια και την προστασία πληροφοριών της εταιρείας απαιτούνται κανόνες που να οριοθετούν τις ευθύνες και τις υποχρεώσεις όλων των εργαζομένων στο πλαίσιο των αρμοδιοτήτων τους όπως αυτές ορίζονται μέσα από την περιγραφή της θέσης εργασίας τους. Αυτή η τακτική έχει ως αποτέλεσμα την αποφυγή πιθανών παραπτωμάτων στα οποία το προσωπικό μπορεί να υποπέσει.

Μέσω του ορισμού και της κατηγοριοποίησης των πιθανώς εκδηλούμενων παραπτωμάτων όλα τα στελέχη της εταιρείας, ανεξάρτητα από τη θέση που κατέχουν στην ιεραρχία αυτής, έχουν τη δυνατότητα να γνωρίζουν τα είδη των παραπτωμάτων, το επίπεδο τους, καθώς και τις αντίστοιχες συνέπειες τους.
Σε περίπτωση που εργαζόμενος διαπράξει οποιοδήποτε παράπτωμα τα στελέχη της εταιρείας ακολουθούν την σχετική διαδικασία διαχείρισης.

## Άμεσα Εμπλεκόμενα Μέρη

### Διοίκηση Εταιρείας

Έχει την πρωταρχική ευθύνη διαχείρισης, λήψης αποφάσεων ανά περίπτωση και επιβολής κυρώσεων για τα ενδεχόμενα παραπτώματα και παραβάσεις στα οποία μπορεί να υποπέσει το προσωπικό της εταιρείας, τους. Σε κάθε περίπτωση, η Διοίκηση αποφασίζει και ακολουθεί το προβλεπόμενο πλάνο ενεργειών σύμφωνα με την κατηγορία στην οποία εντάσσεται το εκάστοτε παράπτωμα.

### IT Admin

Ο IT Admin απαριθμεί στις κύριες υπευθυνότητές του την επίγνωση και τη διαχείριση καταστάσεων εντός του εργασιακού χώρου - στο πλαίσιο που του ορίζουν οι αρμοδιότητές του με βάση την θέσης εργασίας του - οι οποίες σχετίζονται με πιθανές παραβιάσεις ασφαλείας που απειλούν ή επιτυγχάνουν άμεσο πλήγμα στην ασφάλεια πληροφοριών της εταιρείας.

## Έλεγχος Παραπτωμάτων

Όταν εκδηλώνεται ένα παράπτωμα από το προσωπικό το οποίο απειλεί ή υποβαθμίζει άμεσα το επίπεδο της ασφάλειας πληροφοριών εντός της εταιρείας, ο IT Admin υποχρεούται να διεξάγει έλεγχο προκειμένου να το εντάξει στην κατάλληλη κατηγορία ανάλογα με τον βαθμό στον οποίο ανήκει και να το γνωστοποιήσει στον Τομέα Ανθρώπινου Δυναμικού και στη Διοίκηση, ώστε αυτή να αναλάβει δράση για τη διαχείριση του υποπίπτοντος στο παράπτωμα εργαζομένου.

**Ο έλεγχος ενδεικτικά πραγματοποιείται:**

- Βάσει των αναφορών ασφάλειας.
- Δειγματοληπτικά.
- Βάσει των αρχείων καταγραφής των συστημάτων ελέγχου της εταιρείας.
- Βάσει της εν γένει συμπεριφοράς του προσωπικού σχετικά με τη διαχείριση των υποθέσεων, του έργου και την εκτέλεση των καθηκόντων τους ιδίως σε ό,τι αφορά ζητήματα ασφάλειας πληροφοριών.

Ο IT Admin αξιολογεί τις πληροφορίες που έχει για τον εργαζόμενο σχετικά με την παραβίαση πολιτικών ασφάλειας πληροφοριών και αποσαφηνίζει το μέγεθος των επιπτώσεων που αυτή έχει επιφέρει στην ακεραιότητα, τη διαθεσιμότητα ή / και την εμπιστευτικότητα των πληροφοριών της εταιρείας προκειμένου να προβεί στις κατάλληλες διορθωτικές ενέργειες ώστε να τις επαναφέρει στο προγενέστερο στάδιο από την εκδήλωση της παραβίασης. Παράλληλα, ενημερώνει τη Διοίκηση, η οποία είναι αρμόδια να αποφασίζει την επιβολή των κυρώσεων στον εργαζόμενο που αντιστοιχούν στον βαθμό της εκδηλούμενης παράβασης.

## Διαδικασία Αξιολόγησης Παραπτωμάτων

Η διαδικασία της αξιολόγησης παραπτωμάτων, γίνεται βάσει κατηγοριοποίησης, στην οποία αναλύονται τα σφάλματα / παραβάσεις σε βαθμίδες. Τη διαδικασία αρχικά αξιολογεί ο IT Admin, ο οποίος παραπέμπει τον υπάλληλο που διέπραξε παράπτωμα στη Διοίκηση της εταιρείας.

## Κατηγορίες Παραπτωμάτων

Τα παραπτώματα χωρίζονται σε τρεις κατηγορίες, οι οποίες είναι οι εξής:

- 1ου βαθμού παραπτώματα (υψηλού επιπέδου).
- 2ου βαθμού παραπτώματα (μετρίου επιπέδου).
- 3ου βαθμού παραπτώματα (χαμηλού επιπέδου).

**1ου βαθμού παραπτώματα θεωρούνται:**

- Αναπαραγωγή και διακίνηση πληροφοριών από έγγραφα της εταιρείας.

- Σκόπιμη σύνταξη αναληθούς αναφοράς εγγράφων.
- Σκόπιμη καταστροφή διακινούμενων εγγράφων.
- Σκόπιμη αμέλεια παράδοσης εγγράφων υψηλής σημασίας στον Υπεύθυνο Διαχείρισης Εγγράφων.
- Παραβίαση πληροφοριακών συστημάτων.
- Κάλυψη προβλήματος ασφάλειας πληροφοριών.
- Καταστροφή ή παράλειψη αναφορών ασφάλειας.
- Παράβλεψη ενημέρωσης της Διοίκησης για υψηλής σημαντικότητας παράπτωμα.
- Κατά συρροή παραπτώματα 1ου και 2ου βαθμού, αγνοώντας τους κανόνες Πειθαρχικών Παραπτωμάτων.
- Είσοδος επισκέπτη στις εγκαταστάσεις της εταιρείας χωρίς έλεγχο ταυτότητας, επίβλεψης και συνοδείας του στους ενδεδειγμένους χώρους της εταιρείας.
- Πρόσβαση επισκέπτη σε εμπιστευτικές πληροφορίες.
- Ενημέρωση επισκέπτη σχετικά με έκθετα έγγραφα ή πληροφορίες των οργανωτικών ή επιχειρησιακών διεργασιών και δεδομένων που δεν τον αφορούν.
- Αποκάλυψη κωδικών σε επισκέπτη ή άλλο τρίτο μέρος χωρίς εξουσιοδότηση.
- Κλοπή κλειδιών / καρτών πρόσβασης.
- Παράλειψη ή αποφυγή ασφάλισης δικτύου όποτε και όταν χρειάζεται.
- Μεταφορά εμπιστευτικών αρχείων εκτός εταιρείας.
- Διαρροή προσωπικών δεδομένων πελατών ή δεδομένων έργων με απόρρητο ή εμπιστευτικό επίπεδο διαβάθμισης.
- Διαρροή προσωπικών δεδομένων εργαζομένων και εξωτερικών συνεργατών.

**2ου βαθμού παραπτώματα θεωρούνται:**

- Ανταλλαγή και γνωστοποίηση προσωπικών κωδικών μεταξύ των χρηστών.
- Αποφυγή τακτικών ελέγχων, σχετικά με τα έγγραφα, το παρεχόμενο έργο και τη διαχείριση τους.
- Καθυστέρηση ή αμέλεια περιορισμού κινδύνου σε πληροφοριακά συστήματα.
- Αμέλεια ενημέρωσης προϊστάμενου σε ζητήματα πληροφοριακών συστημάτων.
- Αποκάλυψη στοιχείων σύνδεσης.
- Άνοιγμα ύποπτων e-mail χωρίς αναφορά.
- Αναπαραγωγή πληροφοριών από έγγραφα που βρίσκονταν προσωρινά σε εκτυπωτικό μηχάνημα.
- Αποφυγή ή καθυστέρηση τακτικών ελέγχων σε θέματα φυσικής ασφάλειας.
- Παρεμπόδιση αναφοράς θέματος ασφάλειας.

- Παράβλεψη επίλυσης προβλήματος ασφάλειας από τον IT Admin.
- Αποφυγή εκπαιδευτικών συνεδρίων με θέμα που άπτεται της ασφάλειας πληροφοριών.
- Απώλεια κλειδιών / κάρτας πρόσβασης επανειλημμένα.

**3ου βαθμού παραπτώματα θεωρούνται:**

- Καθυστερημένη αρχειοθέτηση εγγράφων.
- Τοποθέτηση εγγράφων σε κάδο απορριμμάτων.
- Καταστροφή πληροφοριακών μέσων, λόγω απροσεξίας.
- Αμέλεια αλλαγής κωδικών όταν χρειάζεται.
- Αποθήκευση κωδικού χρήστη σε εμφανές σημείο.
- Συνεχής άρνηση ενέργειας κλειδώματος κατά την απομάκρυνση του χρήστη από τον Η/Υ.
- Εκτυπώσεις εκτός εργασιακών πλαισίων.
- Εκτύπωση σε πρόχειρα χαρτιά που περιέχουν ευαίσθητα δεδομένα της εταιρείας .
- Παρατημένα αρχεία από χρήστη σε κοινόχρηστους χώρους.
- Επιπολαιότητα σε ζητήματα φυσικής ασφάλειας.
- Παράτυπη συμπεριφορά σχετικά με τη διαδικασία αναφοράς θεμάτων ασφάλειας.
- Άσκοπη αναπαραγωγή και διακίνηση πληροφοριών μέσω τηλεφώνου.

Η Διοίκηση διατηρεί το δικαίωμα να εντάσσει και άλλα παραπτώματα, που δεν αναφέρονται παραπάνω, όταν ειδικές συνθήκες το απαιτούν.

## Κυρώσεις Παραπτωμάτων

Οι κυρώσεις παραπτωμάτων αποφασίζονται από τη Διοίκηση της εταιρείας. Σε περίπτωση χαμηλού επιπέδου παραπτώματος και ύστερα από αξιολόγηση, γίνεται στον εργαζόμενο που το διέπραξε προφορική επίπληξη.
Εάν κάποιος υπάλληλος διαπράττει παραπτώματα κατ' εξακολούθηση, του γίνεται γραπτή επίπληξη και προειδοποίηση για το όριο παραπτωμάτων που έχει διαπράξει.
Σε περίπτωση που εκφραστούν προφορικώς ή εγγράφως επανειλημμένες παρατηρήσεις, χωρίς τη συμμόρφωση του εργαζομένου, το θέμα γνωστοποιείται και μεταφέρεται στη Διοίκηση προς διαχείριση.

Σε υψηλού επιπέδου παραπτώματα και ύστερα από απόφαση της Διοίκησης, μπορεί να γίνει καταγγελία της σύμβασης συνεργασίας του εργαζομένου με την εταιρεία. Επιπλέον, η εταιρεία έχει δικαίωμα να προβεί σε νομικές διαδικασίες, εάν κριθεί απαραίτητο από το εφαρμοστέο νομοθετικό πλαίσιο στο οποίο υπάγεται.

**Συντομογραφίες**

| | |
|---|---|
| **Η/Υ** | Ηλεκτρονικός Υπολογιστής |

# 5. Κρυπτογράφηση

## Σκοπός

Ο σκοπός της Πολιτικής Κρυπτογράφησης είναι να καθορίσει τις διαδικασίες, τα πρότυπα και τις πρακτικές που αφορούν την ασφαλή χρήση της κρυπτογράφησης για την προστασία των δεδομένων. Η πολιτική αυτή αποσκοπεί στη διασφάλιση της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των δεδομένων, ενώ ταυτόχρονα συμβάλλει στην πρόληψη της μη εξουσιοδοτημένης πρόσβασης, της διαρροής ή της αλλοίωσης των πληροφοριών.

## Εμπλεκόμενοι – Ευθύνες

Υποχρέωση εφαρμογής της παρούσας πολιτικής έχει το σύνολο του ανθρώπινου δυναμικού και των εξωτερικών συνεργατών της εταιρείας.

## Πολιτική Κρυπτογράφησης

### Εισαγωγή

Η παρούσα πολιτική περιέχει πρακτικές οδηγίες για τη χρήση κρυπτογραφικών στοιχείων ελέγχου.

### Γενικοί Κανόνες

Η πολιτική χρήσης κρυπτογράφησης περιλαμβάνει γενικούς κανόνες, οι οποίοι πρέπει να ακολουθούνται ώστε να αποφεύγονται οι κίνδυνοι από την απουσία κρυπτογράφησης αλλά και τους κινδύνους εσφαλμένης χρήσης της κρυπτογράφησης. Οι γενικοί κανόνες συνοψίζονται στα κάτωθι:

- Εξετάζεται η χρήση της κρυπτογράφησης όποτε είναι σημαντική η εμπιστευτικότητα ενός στοιχείου. Η κρυπτογραφία μπορεί να χρησιμοποιηθεί κατά την αποστολή (μεταφορά) δεδομένων και κατά την αποθήκευση δεδομένων (τήρηση αντιγράφων ασφαλείας).

- Οι ευαίσθητες πληροφορίες που είναι αποθηκευμένες σε αφαιρούμενα μέσα πρέπει να προστατεύονται μέσω κρυπτογράφησης. Ο κωδικός πρόσβασης πρέπει να μοιράζεται μέσω ενός εναλλακτικού καναλιού από το αρχικό, όπως το κινητό τηλέφωνο.
- Προσδιορίζεται το απαιτούμενο επίπεδο προστασίας λαμβάνοντας υπόψη τον τύπο, την ισχύ και την ποιότητα του απαιτούμενου αλγορίθμου κρυπτογράφησης, βάσει της αξιολόγησης κινδύνων.
- Η εταιρεία χρησιμοποιεί ισχυρούς κρυπτογραφικούς αλγόριθμους.
- Η εταιρεία χρησιμοποιεί μόνο αλγορίθμους που έχουν δημοσιευθεί και έχουν εξεταστεί από ερευνητές. Δεν επινοεί ποτέ τους δικούς της αλγόριθμους και δεν χρησιμοποιεί μη επίσημους αλγορίθμους.
- Τα κλειδιά της κρυπτογράφησης δημιουργούνται με ασφάλεια, αποθηκεύονται με ασφαλή τρόπο και καταστρέφονται όταν δεν χρειάζονται πλέον.
- Τα κλειδιά συμμετρικού αλγορίθμου και τα ιδιωτικά κλειδιά είναι σαν τους κωδικούς πρόσβασης και ισχύουν οι κανόνες πολιτικής κωδικού πρόσβασης. Για παράδειγμα, αυτά τα κλειδιά δεν θα πρέπει ποτέ να επαναχρησιμοποιηθούν και θα πρέπει επίσης να τροποποιούνται τουλάχιστον ετησίως. Τα δημόσια κλειδιά είναι συνήθως μη εμπιστευτικά και μπορούν να τροποποιηθούν λιγότερο συχνά.
- Όλα τα κλειδιά παράγονται τυχαία χρησιμοποιώντας μια ασφαλή γεννήτρια τυχαίων αριθμών.
- Όταν αποφασίζεται να χρησιμοποιηθεί εμπορικό προϊόν με κρυπτογραφικά χαρακτηριστικά (π.χ. λογισμικό κρυπτογράφησης), πρέπει να ελέγχεται ότι το προϊόν χρησιμοποιεί ισχυρό κρυπτογραφικό αλγόριθμο. Πρέπει επίσης να ελέγχεται (π.χ. με αναζήτηση στο διαδίκτυο) αν αυτό το προϊόν έχει γνωστές αδυναμίες.

Κατά την εφαρμογή της κρυπτογραφικής πολιτικής, λαμβάνονται υπόψη οι κανονισμοί και οι εθνικοί περιορισμοί που ενδέχεται να ισχύουν για τη χρήση κρυπτογραφικών τεχνικών σε διάφορες χώρες και στα ζητήματα της διασυνοριακής ροής κρυπτογραφημένων πληροφοριών.
Οι κρυπτογραφικοί έλεγχοι μπορούν να χρησιμοποιηθούν για την επίτευξη διαφορετικών στόχων ασφάλειας πληροφοριών, όπως:

- **Εμπιστευτικότητα**: Χρήση κρυπτογράφησης πληροφοριών για την προστασία ευαίσθητων ή κρίσιμων πληροφοριών, είτε αποθηκευμένων είτε μεταδιδόμενων.
- **Ακεραιότητα /αυθεντικότητα:** Χρήση ψηφιακών υπογραφών ή κωδικών ελέγχου ταυτότητας μηνυμάτων για την επαλήθευση της γνησιότητας ή της ακεραιότητας των αποθηκευμένων ή μεταδιδόμενων ευαίσθητων ή κρίσιμων πληροφοριών.
- **Μη αποποίηση:** Χρήση κρυπτογραφικών τεχνικών για την παροχή αποδεικτικών στοιχείων για την εμφάνιση ή τη μη εμφάνιση ενός γεγονότος ή μιας ενέργειας.
- **Έλεγχος ταυτότητας:** Χρήση κρυπτογραφικών τεχνικών για τον έλεγχο ταυτότητας χρηστών και άλλων οντοτήτων συστήματος που ζητούν πρόσβαση ή συναλλάσσονται με χρήστες, οντότητες και πόρους του συστήματος.

## Διαχείριση Κλειδιών

Κατά τη χρήση της κρυπτογράφησης, η προστασία των ψηφιακών κλειδιών είναι πολύ σημαντική. Η πρώτη πτυχή της διαχείρισης κλειδιών είναι η ασφαλής δημιουργία τους. Οποιοδήποτε κλειδί χρησιμοποιείται δεν πρέπει να είναι προβλέψιμο. Η εταιρεία μπορεί να χρησιμοποιήσει ένα πρόγραμμα για την παραγωγή κλειδιών (Γεννήτρια Κωδικών), εφόσον αυτό το πρόγραμμα έχει σχεδιαστεί για τη δημιουργία ισχυρών για την πρόβλεψη κλειδιών.
Μια ακόμα σημαντική πτυχή είναι η ασφαλής αποθήκευση των κλειδιών. Το προσωπικό της εταιρείας αποθηκεύει τα κλειδιά με τέτοιο τρόπο ώστε η πρόσβαση σε αυτά να είναι περιορισμένη. Δεν επιτρέπεται η αποθήκευση κλειδιών σε δημόσιο χώρο ή η τοποθέτηση κλειδιών σε σημείο του File Server που είναι προσβάσιμα από άλλους μη εξουσιοδοτημένους χρήστες.

## Είδη Κρυπτογράφησης

Οι τύποι κρυπτογράφησης που χρησιμοποιεί η εταιρεία είναι οι παρακάτω:

- **Συμμετρική κρυπτογράφηση:** Ένας συμμετρικός αλγόριθμος κρυπτογράφησης χρησιμοποιεί ένα κλειδί (μικρή σειρά δεδομένων) για να ανακατεύει ένα κείμενο σε ένα κρυπτογραφικό κείμενο. Το κρυπτογράφημα δεν είναι αναγνώσιμο σε κανέναν που δεν έχει πρόσβαση στο κλειδί.
- **Ασύμμετρη κρυπτογράφηση (γνωστή και ως κρυπτογράφηση δημόσιου κλειδιού):** Ένας ασύμμετρος αλγόριθμος κρυπτογράφησης χρησιμοποιεί ένα ζεύγος κλειδιών που αποτελείται από ένα τμήμα δημόσιου κλειδιού και ένα τμήμα ιδιωτικού κλειδιού. Ο αλγόριθμος παίρνει το τμήμα του δημόσιου κλειδιού και ένα απλό κείμενο για να δημιουργήσει ένα κρυπτογραφικό κείμενο. Το κρυπτογράφημα είναι κατανοητό μόνο για τα μέρη που έχουν το ιδιωτικό κλειδί.

## Επιλογή Ισχυρών Κρυπτογραφικών Αλγορίθμων

Η εταιρεία επιλέγει τη δημιουργία ισχυρών αλγόριθμων. Παρακάτω παραθέτουμε αρκετούς ισχυρούς αλγόριθμους που μπορεί να χρησιμοποιεί η εταιρεία. Η επιλογή της εταιρείας βασίζεται στο «Algorithms, key size and parameters report» του ENISA. Ο αλγόριθμος πρέπει να είναι ανθεκτικός σε γνωστές επιθέσεις, όπως:

- **Επίθεση Brute Force:** Ο αλγόριθμος πρέπει να απαιτεί υψηλό υπολογιστικό κόστος για την παραβίαση του κλειδιού, ακόμη και με τις πιο σύγχρονες τεχνικές υπολογιστικής ισχύος.
- **Επίθεση Κρυπτοανάλυσης:** Πρέπει να είναι ανθεκτικός σε επιθέσεις που στοχεύουν στην ανάλυση του αλγορίθμου για την αποκάλυψη των κλειδιών ή των δεδομένων χωρίς τη γνώση του κλειδιού (π.χ. επίθεση με κείμενα γνωστά ή επίθεση με κείμενα επιλεγμένα).
- **Απώλεια Ασφάλειας σε Μακροπρόθεσμο Χρόνο:** Ο αλγόριθμος πρέπει να παραμένει ασφαλής ακόμη και σε περιβάλλοντα όπου η υπολογιστική ισχύς και οι μέθοδοι επιθέσεων εξελίσσονται.

Προτεινόμενοι ισχυροί αλγόριθμοι:

- **Συμμετρική κρυπτογράφηση:** Advanced Encryption Standard (AES). Το AES είναι ένας από τους πιο αξιόπιστους και ισχυρούς αλγόριθμους συμμετρικής κρυπτογράφησης, κατάλληλος για χρήση σε πολλούς τομείς. Η ευκολία εφαρμογής του, σε συνδυασμό με την εξαιρετική του ανθεκτικότητα σε επιθέσεις, το καθιστά την προτιμώμενη επιλογή για την προστασία των δεδομένων σε σύγχρονα συστήματα ασφαλείας.

Το AES υποστηρίζει τρία διαφορετικά μήκη κλειδιών: AES-128, AES-192 και AES-256.

- **Ασύμμετρη κρυπτογράφηση:** Rivest–Shamir–Adleman (RSA) (συνιστάται 4096 bits). Ο αλγόριθμος RSA χρησιμοποιείται σε πολλές κρίσιμες εφαρμογές ασφαλείας:
    - Ασφαλή Διακίνηση Δεδομένων μέσω SSL/TLS για την προστασία των συνδέσεων στο διαδίκτυο (π.χ. HTTPS).
    - Ψηφιακή Υπογραφή για την αυθεντικοποίηση των μηνυμάτων και την προστασία της ακεραιότητας.
    - Ανταλλαγή Κλειδιών για ασφαλή επικοινωνία, όπως στο πρωτόκολλο Diffie-Hellman.
    - Πιστοποιητικά SSL/TLS για την επιβεβαίωση της ταυτότητας ιστοσελίδων και υπηρεσιών.

- **Συντομογραφίες**

| | |
|---|---|
| **AES** | Advanced Encryption Standard |
| **ENISA** | European Union Agency for Cybersecurity |
| **RC6** | Rivest Cipher 6 |
| **RSA** | Rivest – Shamir – Adleman |

# 6. Έλεγχος πρόσβασης

## Σκοπός

Το παρόν έγγραφο περιγράφει την πολιτική της **«Π.Ε. ΚΑΣΙΝΑΚΗΣ Α.Ε.»** όσον αφορά τη χορήγηση και τον έλεγχο πρόσβασης στους πληροφοριακούς της πόρους.

## Εμπλεκόμενοι – Ευθύνες

Υποχρέωση εφαρμογής της παρούσας πολιτικής έχει το σύνολο του ανθρώπινου δυναμικού και των εξωτερικών συνεργατών της εταιρείας.

# Πολιτική Ελέγχου Πρόσβασης

## Εισαγωγή

Το παρόν έγγραφο περιγράφει την πολιτική της **«Π.Ε. ΚΑΣΙΝΑΚΗΣ Α.Ε.»** όσον αφορά τη χορήγηση και τον έλεγχο πρόσβασης στους πληροφοριακούς της πόρους που εμπίπτουν στο πεδίο εφαρμογής του Συστήματος Διαχείρισης.

## Γενικές Αρχές

Οι γενικές αρχές που διέπουν την πρόσβαση των χρηστών στους πληροφοριακούς πόρους της εταιρείας είναι οι ακόλουθοι:

- Τα δικαιώματα των χρηστών είναι ανάλογα του ρόλου τους και των ενεργειών που επιτελούν στους πληροφοριακούς πόρους.
- Τα δικαιώματα των χρηστών είναι ανάλογα με την κρισιμότητα και το επίπεδο διαβάθμισης των πληροφοριών στις οποίες αυτοί εξουσιοδοτούνται να έχουν πρόσβαση.
- Τα δικαιώματα των χρηστών επανεξετάζονται σε τακτά χρονικά διαστήματα, τουλάχιστον σε ετήσια βάση, κατά την Ανασκόπηση του Συστήματος Διαχείρισης, και προσαρμόζονται κατάλληλα, εφόσον απαιτείται.
- Τα δικαιώματα των χρηστών δύνανται να επανεξετάζονται και εκτάκτως, κατόπιν πρωτοβουλίας του **IT Admin.**
- Οι χρήστες έχουν τα ελάχιστα δυνατά δικαιώματα που χρειάζονται για να εκτελέσουν τις επιθυμητές λειτουργίες με βάση τα καθήκοντα που τους έχουν ανατεθεί.
- Οι ομάδες χρηστών έχουν τα ελάχιστα δυνατά δικαιώματα που χρειάζονται για να εκτελέσουν τις επιθυμητές λειτουργίες με βάση τα καθήκοντα που τους έχουν ανατεθεί.
- Η αναίρεση των δικαιωμάτων πρόσβασης του χρήστη σε περίπτωση διακοπής της ανάγκης πρόσβασης πρέπει να είναι άμεση.
- Η έγκριση των δικαιωμάτων πρόσβασης είναι υπευθυνότητα του **IT Admin.**

## Χορήγηση Πρόσβασης σε Πληροφοριακούς Πόρους

Η χορήγηση πρόσβασης σε πληροφοριακούς πόρους της **«Π.Ε. ΚΑΣΙΝΑΚΗΣ Α.Ε.»** ακολουθεί μια πολιτική περιορισμού διάχυσης πληροφορίας και αρμοδιοτήτων (Need to Know). Κάθε χρήστης θα πρέπει να έχει πρόσβαση σε όσους πληροφοριακούς πόρους είναι απαραίτητοι για την τέλεση των εργασιών του και μόνο σε αυτούς. Η πρόσβαση σε κρίσιμους πόρους θα πρέπει να εκχωρείται για το ελάχιστο απαιτητό διάστημα και σε κάθε περίπτωση να αίρεται αμέσως μετά την εκτέλεση της εργασίας. Το αίτημα μπορεί να αποσταλεί στον **IT Admin** και μέσω e-mail.

## Διαχείριση Προνομιακών Δικαιωμάτων

Ο καθορισμός και η χρήση προνομιακών δικαιωμάτων πρόσβασης (οποιοδήποτε σύνολο δικαιωμάτων ή χαρακτηριστικών σε ένα σύστημα, τα οποία επιτρέπουν την παράκαμψη των μηχανισμών ελέγχου του συστήματος) θα πρέπει να είναι ελεγχόμενα και περιορισμένα.

- Προνομιακά δικαιώματα πρόσβασης στα συστήματα της εταιρείας έχουν μόνο οι διαχειριστές που έχει ορίσει η εταιρεία. Τα προνομιακά αυτά δικαιώματα ισχύουν καθ' όλη τη διάρκεια απασχόλησης των στελεχών αυτών στην εταιρεία ή τουλάχιστον μέχρι την ανάκλησή τους εάν τροποποιηθεί το εύρος της εξουσιοδότησής τους. Για τους εξωτερικούς συνεργάτες ισχύει η ίδια διαδικασία έως ότου διακοπεί ή τροποποιηθεί το περιεχόμενο του συμφωνητικού / σύμβασης συνεργασίας τους με την εταιρεία.
- Τα προνομιακά δικαιώματα αποδίδονται σε λογαριασμούς διαφορετικούς από αυτούς που χρησιμοποιούν οι χρήστες για τις καθιερωμένες εργασίες τους στα συστήματα.
- Οι χρήστες των οποίων το αντικείμενο είναι η ανάπτυξη κώδικα επιτρέπεται να έχουν δικαιώματα εγκατάστασης λογισμικού στα τερματικά τους, καθώς η φύση της εργασίας τους απαιτεί συχνή εγκατάσταση και διαμόρφωση εργαλείων στα τερματικά τους.

## Πρόσβαση σε Πόρους – Διαπιστευτήρια Χρηστών

Η πρόσβαση στους σταθμούς εργασίας και τα πληροφοριακά συστήματα της εταιρείας επιτρέπεται κατόπιν κατάλληλης εξακρίβωσης της ταυτότητας του χρήστη. Αντίστοιχα, προτού επιτραπεί η πρόσβαση, είναι απαραίτητη η αυθεντικοποίηση των χρηστών από τα συστήματα.

Η ταυτοποίηση και αυθεντικοποίηση των χρηστών των πληροφοριακών συστημάτων της εταιρείας γίνεται με τη χρήση κατάλληλων μεθόδων ανά σύστημα, όπως:

- Έλεγχος μονού παράγοντα (Single-Factor)
- Έλεγχος ταυτότητας 2 παραγόντων (2FA)
- Τεχνολογία Single Sign-On (SSO)
- Έλεγχος ταυτότητας πολλαπλών παραγόντων (MFA)

# Διαχείριση Προσωπικού και Δικαιωμάτων Πρόσβασης

## Εισαγωγή

Το παρόν κεφάλαιο περιγράφει τη μεθοδολογία που ακολουθείται για τη διαχείριση του προσωπικού, και των δικαιωμάτων πρόσβασης, κατά την πρόσληψη, τη μετακίνηση ή την αποχώρηση από την εταιρεία. Επίσης αναφέρονται και οι μέθοδοι που εφαρμόζονται για την διαχείριση των δικαιωμάτων πρόσβασης στην εταιρεία.

## Επεξηγήσεις

### Επιλογή – Πρόσληψη Προσωπικού

Η διαδικασία επιλογής και πρόσληψης προσωπικού γίνεται σύμφωνα με τις περιγραφές της διαδικασίας Διαχείρισης Ανθρώπινου Δυναμικού.

### Μετακίνηση Προσωπικού

Στην περίπτωση που κάποιος εργαζόμενος χρειαστεί να αλλάξει σταθμό εργασίας ή να γίνει κάποια αλλαγή στα δικαιώματα πρόσβασής του, ο Υπεύθυνος του τμήματος ενημερώνει τον **IT Admin** για τις σχετικές αλλαγές.

### Αποχώρηση Προσωπικού

Στην περίπτωση αποχώρησης κάποιου εργαζομένου ο Υπεύθυνος του Τμήματος ενημερώνει τον **IT Admin**, ώστε να προχωρήσει στην απενεργοποίηση των δικαιωμάτων του χρήστη. Επίσης, ο εργαζόμενος που αποχωρεί ενημερώνεται σχετικά με Θέματα Εμπιστευτικότητας και Εχεμύθειας τα οποία ισχύουν και μετά την αποχώρηση του. Τέλος, ο εργαζόμενος υποχρεούται να παραδώσει οποιοδήποτε εξοπλισμό του είχε δοθεί κατά την πρόσληψή του.

## Δικαιώματα Ηλεκτρονικών Προσβάσεων

Ο **IT Admin** ανά τακτά χρονικά διαστήματα ελέγχει τα δικαιώματα πρόσβασης ανάλογα και με τις αλλαγές που μπορεί να προκύψουν στην Πολιτική Ασφάλειας της εταιρείας.

### Νέος Χρήστης

Η παρακάτω διαδικασία πρέπει να ακολουθείται πάντα για την δημιουργία όλων των λογαριασμών χρηστών.

| **Διαδικασία Νέου Χρήστη** | |
|---|---|
| **Βήμα 1** | Δημιουργία Λογαριασμού. |
| **Βήμα 2** | Δημιουργία Ονόματος Χρήστη (Username) και Κωδικού Πρόσβασης (Password). |
| **Βήμα 3** | Ανάθεση Δικαιωμάτων Πρόσβασης. |
| **Βήμα 4** | Ενημέρωση Χρήστη για Δημιουργία Λογαριασμού. |
| **Βήμα 5** | Τεκμηριωμένη Παραλαβή Κωδικών. |

## Τροποποίηση και Διαγραφή Δικαιωμάτων Πρόσβασης

Για κάθε αίτημα τροποποίησης/ διαγραφής δικαιωμάτων πρόσβασης, θα πρέπει να ακολουθείται η διαδικασία ενημέρωσης του **IT Admin** από τον προϊστάμενο του Τμήματος εγγράφως.

Επιπλέον σε περίπτωση διαγραφής χρήστη πραγματοποιούνται τα κάτωθι:

- Ο λογαριασμός του χρήστη απενεργοποιείται την ημέρα που ορίζεται η λύση σύμβασης. Σε περίπτωση που η λύση αναφέρεται σε προγενέστερο χρονικό σημείο η απενεργοποίηση γίνεται την ημέρα ενημέρωσης.
- Ο χρόνος διατήρησης των λογαριασμών που έχουν απενεργοποιηθεί ορίζεται σε δύο (2) μήνες, μετά το πέρας του οριζόμενου χρόνου γίνεται διαγραφεί του λογαριασμού. Σε περίπτωση όμως που κριθεί ότι ο λογαριασμός περιέχει κρίσιμα δεδομένα παραμένει και μετά το πέρας των δύο (2) μηνών, έως ότου κριθεί από τους διαχειριστές ότι μπορεί να διαγραφεί.

## Πρόσβαση στον File Server

Στον File Server της εταιρείας κάθε φάκελος έχει συγκεκριμένα δικαιώματα πρόσβασης, έτσι ώστε να διαχωρίζονται βάση του επιπέδου κρισιμότητας των αρχείων που περιέχουν. Επίσης διατίθεται ένας κοινόχρηστος φάκελος που διευκολύνει την ανταλλαγή αρχείων μεταξύ των χρηστών καθώς και αρχεία καθημερινής ενημέρωσης. Απαγορεύεται ρητά η αποθήκευση προσωπικών αρχείων με δεδομένα που δεν αφορούν την εταιρεία.

## Πρόσβαση E-mail

Η πρόσβαση και η διαχείριση εταιρικών λογαριασμών e-mail ελέγχεται από τον **IT Admin**. Λογαριασμούς e-mail και δυνατότητα πρόσβασης στο web mail διαθέτει όλο το προσωπικό βάσει της Πολιτικής.

## Διαχείριση Ταυτότητας

Η εταιρεία διαθέτει κατάλληλες πολιτικές με τις οποίες γίνεται πιο απλή η διαχείριση ταυτοποιήσεων, η διασφάλιση της ασφάλειας τους και η παρακολούθηση συμμόρφωσης των λογαριασμών με τις πολιτικές. Ο IT Admin διεξάγει δειγματοληπτικούς ελέγχους με την εποπτική ευθύνη του **IT Admin** για την εύρυθμη λειτουργία των πολιτικών. Σε περίπτωση εντοπισμού προβλήματος κατά τον δειγματοληπτικό έλεγχο γίνεται περαιτέρω ανάλυση ώστε να βρεθούν οι αιτίες. Επίσης όλα τα συστήματα που διατηρούν αρχείο με πληροφορίες όπως ημερομηνία και ώρα, συγχρονίζουν τα στοιχεία αυτά από τον Domain Controller (Clock synchronization).

# 7.Διαχειριση Επισκεπτών

## Σκοπός

Με την Πολιτική Διαχείρισης Επισκεπτών επιτυγχάνεται η ασφάλεια και η προστασία των δεδομένων, με σκοπό την αποφυγή της διακίνησης τους εκτός ορίων της εταιρείας. Η εταιρεία. προστατεύει τους ασφαλείς χώρους μέσω κατάλληλων ελέγχων εισόδου για να εξασφαλίσει ότι έχουν πρόσβαση μόνο εξουσιοδοτημένα άτομα.

## Εμπλεκόμενοι – Ευθύνες

Υποχρέωση εφαρμογής της παρούσας πολιτικής έχει το σύνολο του ανθρώπινου δυναμικού και των εξωτερικών συνεργατών της εταιρείας.

## Πολιτική Διαχείρισης Επισκεπτών

### Εισαγωγή

Η Πολιτική Διαχείρισης Επισκεπτών λειτουργεί ως κατευθυντήρια γραμμή για τη διαχείριση επισκεπτών από το αρμόδιο προσωπικό της εταιρείας, τις απαιτήσεις και τους κανόνες ασφαλείας κατά την είσοδο επισκεπτών στην εταιρεία, αλλά και τη διαδικασία που ακολουθείται για προγραμματισμένες και μη επισκέψεις. Αυτό επιτυγχάνεται μέσα από μία σειρά ενεργειών που απαιτούνται πριν και κατά την προσέλευση οποιουδήποτε ατόμου το οποίο δεν ανήκει στο ανθρώπινο δυναμικό της εταιρείας.

Με την Πολιτική Διαχείρισης Επισκεπτών επιτυγχάνεται η ασφάλεια και η προστασία των δεδομένων και λοιπών πληροφοριακών πόρων της εταιρείας, με σκοπό την αποφυγή της μη εξουσιοδοτημένης μετακίνησης τους εκτός ορίων των εταιρικών υποδομών. Η **«Π.Ε. ΚΑΣΙΝΑΚΗΣ Α.Ε.»** προστατεύει τους διαβαθμισμένους ανά επίπεδο ασφαλείας χώρους μέσω κατάλληλων ελέγχων και μέσων εισόδου για να εξασφαλίσει ότι η πρόσβαση σε αυτούς πραγματοποιείται μόνο από εξουσιοδοτημένα άτομα.

### Κεντρική Είσοδος

Η Διαχείριση Επισκεπτών περιλαμβάνει την υποδοχή και ταυτοποίηση των επισκεπτών, τακτικών - σε περίπτωση προκαθορισμένων συναντήσεων και εκτάκτων. Το προσωπικό της κεντρικής

εισόδου είναι πάντα ενημερωμένο για τις συναντήσεις, ενώ για τους υπόλοιπους επισκέπτες έρχεται σε συνεννόηση με τον εργαζόμενο τον οποίο ο επισκέπτης επιθυμεί να επισκεφθεί.

## Κατηγορίες Επισκέψεων

### Προγραμματισμένη Επίσκεψη

Με την άφιξη του επισκέπτη η γραμματεία θα πρέπει να:

- Ενημερώσει τον άμεσα ενδιαφερόμενο της επίσκεψης για την έγκριση εισόδου του επισκέπτη.
- Καταγράψει στο Έντυπο Επισκεπτών τα στοιχεία του.
- Παραδίδει την αναγνωριστική κάρτα με τίτλο "επισκέπτης" την οποία ο επισκέπτης πρέπει να φέρει σε εμφανές σημείο και να την παραδώσει κατά την έξοδο του.
- Διατηρήσει τον επισκέπτη κατά την αναμονή του στην είσοδο μέχρι να έρθει ο αρμόδιος να τον παραλάβει.
- Ενημερώσει τον εργαζόμενο ότι θα πρέπει να συνοδέψει τον επισκέπτη καθ' όλη την διάρκεια της επίσκεψης, τόσο στην είσοδο του στον χώρο όσο και στην έξοδό του από το χώρο της συνάντησης.

## Μη Προγραμματισμένη Επίσκεψη

Σε μη προγραμματισμένη επίσκεψη η γραμματεία πρέπει να:

- Παίρνει πληροφορίες από τον επισκέπτη για την ταυτότητα του και τον λόγο της επίσκεψης.
- Μην τον αφήσει χωρίς επίβλεψη στον χώρο.
- Επικοινωνήσει με τον άμεσα ενδιαφερόμενο της επίσκεψης για την έγκριση της εισόδου του επισκέπτη.
- Εφόσον εγκριθεί η είσοδος του επισκέπτη, να καταγράφονται στο Έντυπο Επισκεπτών τα στοιχεία του.
- Παραδίδει την αναγνωριστική κάρτα με τίτλο "επισκέπτης" την οποία ο επισκέπτης πρέπει να φέρει σε εμφανές σημείο και να την παραδώσει κατά την έξοδο του.
- Φροντίζει να έρθει ο αρμόδιος εργαζόμενος να τον συνοδεύσει στον χώρο της συνάντησης.
- Ενημερώσει τον εργαζόμενο ότι θα πρέπει να συνοδέψει τον επισκέπτη καθ' όλη την διάρκεια της επίσκεψης, τόσο στην είσοδο του στον χώρο όσο και στην έξοδό του από το χώρο της συνάντησης.

## Διατήρηση Αρχείου Επισκεπτών

Καταγράφεται η ημερομηνία, το ονοματεπώνυμο και η ώρα εισόδου και αναχώρησης των επισκεπτών, η εταιρεία / φορέας που εκπροσωπούν, ο σκοπός της επίσκεψης τους, καθώς και ο συνοδός / αποδέκτης της επίσκεψης. Τους παρέχεται πρόσβαση μόνο για ειδικούς, εγκεκριμένους σκοπούς και εκδίδονται οδηγίες εφόσον απαιτείται σχετικά με τις απαιτήσεις ασφαλείας της περιοχής και τις διαδικασίες έκτακτης ανάγκης. Η εταιρεία επικυρώνει την ταυτότητα των επισκεπτών και το έντυπο διατηρείται για ένα (1) μήνα.

# 8. Διαβάθμιση Πληροφοριών

## Σκοπός

Στόχος της Πολιτικής Διαβάθμισης Πληροφοριών είναι η προστασία των πληροφοριακών στοιχείων της εταιρείας και όλων των ευαίσθητων πληροφοριακών δεδομένων τρίτων, ενάντια σε όλες τις εσωτερικές, εξωτερικές, εκούσιες ή ακούσιες απειλές. Οι πληροφορίες ταξινομούνται βάσει των νομικών απαιτήσεων, της αξίας, της κρισιμότητας και της ευαισθησίας σε μη εξουσιοδοτημένη αποκάλυψη ή τροποποίηση.

## Εμπλεκόμενοι – Ευθύνες

Υποχρέωση εφαρμογής της παρούσας πολιτικής έχει το σύνολο του ανθρώπινου δυναμικού και των εξωτερικών συνεργατών της εταιρείας.

## Πολιτική Διαβάθμισης Πληροφοριών

### Εισαγωγή

Οι διαδικασίες της διαβάθμισης και της διαχείρισης είναι δύο διαφορετικά, αλλά αλληλένδετα μέρη, που έχουν να κάνουν με τις πληροφορίες της εταιρείας. Οι πληροφορίες πρέπει να προστατεύονται από οποιονδήποτε και κατά οποιασδήποτε μη εξουσιοδοτημένης πρόσβασης.

Η διαδικασία είναι υποχρεωτική για όλα τα εμπλεκόμενα μέρη, καθώς όλα τα αρμόδια τμήματα έχουν ευθύνη και υποχρέωση να διαφυλάττουν όλες τις πληροφορίες. Μέσα από αξιολόγηση που γίνεται από τους υπεύθυνους, κατανέμονται τα έγγραφα και τα αρχεία, και εν συνεχεία κάποια ακολουθούν τη διαδικασία της καταστροφής και άλλα της αρχειοθέτησης.

Τα περιουσιακά στοιχεία μπορούν να ταξινομηθούν σύμφωνα με την ταξινόμηση των πληροφοριών που αποθηκεύονται, υποβάλλονται σε επεξεργασία ή χειρίζονται με άλλο τρόπο ή προστατεύονται από το περιουσιακό στοιχείο.

## Εμπλεκόμενα Μέρη

### Υπεύθυνοι Τμημάτων

Οι Υπεύθυνοι όλων των Τμημάτων λαμβάνουν γνώση της Πολιτικής και μεριμνούν ώστε να αξιολογούνται οι πληροφορίες στις οποίες απέκτησαν πρόσβαση, είτε προς ανάγνωση είτε προς χρήση, όλοι οι εσωτερικοί ή / και εξωτερικοί συνεργάτες της εταιρείας και να τηρείται η διαδικασία της καταστροφής ή της αρχειοθέτησής τους όποτε απαιτείται η εφαρμογή της. Στόχο αποτελεί, μέσα από τακτικούς ελέγχους, η συμμόρφωση όλων των εμπλεκόμενων μερών στους κανόνες της Πολιτικής Διαβάθμισης Πληροφοριών και ο εντοπισμός πιθανών αποκλίσεων προς έγκαιρη και αποτελεσματική αντιμετώπισή τους, προκειμένου αυτές να μην ξεπερνούν το αποδεκτό επίπεδο επικινδυνότητας το οποίο έχει οριστεί για τη διασφάλιση της ασφάλειας πληροφοριών εντός της εταιρείας.

### Προσωπικό Εταιρείας

Οι εργαζόμενοι και οι εξωτερικοί συνεργάτες υποχρεούνται να προστατεύουν με τη σειρά τους όποια πληροφορία προέρχεται από έγγραφο ή αρχείο στα οποία αποκτούν πρόσβαση είτε για λόγους πληροφόρησής τους είτε για λόγους χρήσης και διεκπεραίωσης των καθηκόντων τους, καθώς επίσης και να μην την αναπαράγουν με οποιονδήποτε τρόπο ή τη γνωστοποιούν σε μη εξουσιοδοτημένα άτομα για προσωπικό τους όφελος και με σκοπό που αντιτίθεται στα έννομα συμφέροντα της εταιρείας. Οι προσωπικές σημειώσεις των υπαλλήλων θεωρούνται πληροφορίες, για αυτό φυλάσσονται στον χώρο της εταιρείας και δεν επιτρέπεται η διακίνησή τους εκτός αυτού.

## Κατηγοριοποίηση Πληροφοριών

Η κατηγοριοποίηση / διαβάθμιση των πληροφοριών της εταιρείας που εμπίπτουν στο πεδίο εφαρμογής της Πολιτικής Διαβάθμισης Πληροφοριών εφαρμόζεται σύμφωνα τα όσα ορίζονται στον ακόλουθο πίνακα:

| Α/Α | Διαβάθμιση | Εμπιστευτικότητα |
|---|---|---|
| 1 | Απόρρητο | Η διαβάθμιση με χαρακτηρισμό «Απόρρητο» αποδίδεται σε πληροφορίες που σύμφωνα με την Ελληνική νομοθεσία θεωρούνται άκρως εμπιστευτικές (π.χ. δεδομένα υγείας, η ιδιότητα ενός ατόμου ως άνεργου ή δικαιούχου κοινωνικού επιδόματος). Η μη εξουσιοδοτημένη αποκάλυψή τους θα είχε σοβαρές, ίσως και νομικές, συνέπειες για την εταιρεία. Ως απόρρητες πληροφορίες μπορούν επίσης να χαρακτηρισθούν πληροφορίες κρίσιμες για τη λειτουργία της εταιρείας οι οποίες αφορούν τα μέλη της Διοίκησης αυτής. Παράδειγμα: συμβάσεις, αρχεία μισθοδοσίας, ιατρικά αρχεία, αρχεία και έγγραφα Διοίκησης, βιογραφικά, στοιχεία χαρτοφυλακίου (βάσεις δεδομένων).<br>Η πρόσβαση σε πληροφορίες αυτής της κατηγορίας επιτρέπεται μόνο σε όσα στελέχη της εταιρείας έχουν άδεια επεξεργασίας τέτοιων στοιχείων. |
| 2 | Εμπιστευτικό | Η διαβάθμιση με χαρακτηρισμό «Εμπιστευτικό» αποδίδεται σε επιχειρησιακές πληροφορίες που χρησιμοποιούνται από το αρμόδιο προσωπικό της εταιρείας, κατά την εκτέλεση των εργασιών του, που δεν πρέπει να δημοσιοποιούνται και προορίζονται για χρήση αποκλειστικά στο εσωτερικό της εταιρείας. Η μη εξουσιοδοτημένη αποκάλυψή τους θα είχε και νομικές συνέπειες για την εταιρεία. Τα έγγραφα συστήματος διαχείρισης ανήκουν σε αυτή την κατηγορία.<br>Η πρόσβαση σε πληροφορίες αυτής της κατηγορίας επιτρέπεται μόνο στα στελέχη της εταιρείας, τα οποία χρησιμοποιούν τις πληροφορίες αυτές για την εκτέλεση των εργασιών τους. |
| 3 | Δημόσιο | Η διαβάθμιση με χαρακτηρισμό «Δημόσιο» αποδίδεται σε ευρέως γνωστές πληροφορίες που δεν χρήζουν ιδιαίτερης προστασίας. Παράδειγμα: πληροφορίες που δημοσιεύονται στο διαδικτυακό τόπο της εταιρείας, πληροφορίες που περιλαμβάνονται σε διαφημιστικό υλικό και υλικό προώθησης της εταιρείας.<br>Η πρόσβαση σε πληροφορίες αυτής της κατηγορίας επιτρέπεται σε όλους. |

Υπεύθυνος για το χαρακτηρισμό κάθε πληροφορίας σύμφωνα με τις οδηγίες διαβάθμισης που παρουσιάζονται στον προηγούμενο πίνακα είναι ο IT Admin σε συνεργασία με τους Υπεύθυνους των Τμημάτων.

Οι πληροφορίες μπορεί να πάψουν να είναι ευαίσθητες ή κρίσιμες μετά από ένα ορισμένο χρονικό διάστημα, για παράδειγμα, όταν οι πληροφορίες έχουν δημοσιοποιηθεί. Οι αλλαγές θα πρέπει να λαμβάνονται υπόψη, καθώς η υπερβολική ταξινόμηση μπορεί να οδηγήσει στην εφαρμογή περιττών ελέγχων με αποτέλεσμα πρόσθετες δαπάνες ή, αντίθετα, η αλόγιστη υποβάθμιση του βαθμού ασφαλείας των εγγράφων μπορεί να θέσει σε κίνδυνο την επίτευξη της επιχειρηματικής δραστηριότητας.

**Πληροφορίες σε φυσική μορφή**

- Αν απαιτηθεί σήμανση της πληροφορίας μπορεί να γίνει με κάθε πρόσφορο μέσο που διασφαλίζει την ακεραιότητα του χαρακτηρισμού, ενδεικτικά: σφραγίδα, κεφαλίδες εντύπων, χειρόγραφη αναγραφή του επιπέδου διαβάθμισης.
- Αν απαιτηθεί σήμανση αυτή τοποθετείται με τέτοιον τρόπο, ώστε να διασφαλίζεται ότι συνοδεύει διαρκώς την πληροφορία σε όλο τον κύκλο ζωής της, μέχρις ότου αλλάξει σκοπίμως ο χαρακτηρισμός της.

**Πληροφορίες σε ηλεκτρονική μορφή**

- Ηλεκτρονικές πληροφορίες που δημιουργούνται από την εταιρεία και περιέχουν πληροφορίες των επιπέδων «Εμπιστευτικό» ή «Απόρρητο» αποθηκεύονται σε συστήματα της εταιρείας με πρόσβαση που περιορίζεται μόνο σε εκείνα τα στελέχη της εταιρείας που έχουν την αντίστοιχη εξουσιοδότηση.
- Ηλεκτρονικές πληροφορίες που χαρακτηρίζονται από τον συντάκτη τους ως Εμπιστευτικά πρέπει πάντα να αποστέλλονται στον παραλήπτη τους «κλειδωμένα». Ο παραλήπτης θα ενημερώνεται σχετικά με τον κωδικό-κλειδί από τον αποστολέα με SMS, τηλεφωνική επικοινωνία ή 2ο e-mail.

## Διαδικασία Διαβάθμισης Πληροφοριών

Παρακάτω συνοψίζονται οι κυριότερες πρακτικές οι οποίες ακολουθούνται κατά την τήρηση της Πολιτικής Διαβάθμισης Πληροφοριών:

- Όλα τα έγγραφα αξιολογούνται βάσει του περιεχομένου τους για τη σημαντικότητα τους και το επίπεδο διαβάθμισής τους.
- Οι παρωχημένες ή όποιου άλλου είδους πληροφορίες κρίνουν απαραίτητο οι Υπεύθυνοι Τμημάτων αναλογικά με το πεδίο ευθύνης τους κατανέμονται κατάλληλα προς εφαρμογή της διαδικασίας καταστροφής ή της διαδικασίας αρχειοθέτησης.
- Εάν οι πληροφορίες προορίζονται για καταστροφή, ομαδοποιούνται και καταστρέφονται στο τέλος της ημέρας.

- Εάν οι πληροφορίες προορίζονται για αρχειοθέτηση, τακτοποιούνται στα ανάλογα κλασέρ ή καταχωρούνται στους κατάλληλους ηλεκτρονικούς φακέλους που έχουν υποδείξει οι Υπεύθυνοι των Τμημάτων στο τέλος της ημέρας.

## Διαχείριση Διαβαθμισμένων Πληροφοριών

Η Διαχείριση Διαβαθμισμένων Πληροφοριών αποτελεί τον πυρήνα της οργανωτικής δομής εντός της εταιρείας, προκειμένου να μη διασαλεύεται η ασφάλεια των πληροφοριών κατά την επιτέλεση των επιχειρησιακών λειτουργιών της. Για τον σκοπό αυτό, τηρούνται υποχρεωτικά από το σύνολο του προσωπικού οι ακόλουθοι κανόνες:

- Όλοι οι εργαζόμενοι και οι εξουσιοδοτημένοι εξωτερικοί συνεργάτες που χρησιμοποιούν οποιοδήποτε πληροφορία της εταιρείας για λόγους επιχειρησιακούς, λειτουργικούς ή πληροφοριακούς για τη διεκπεραίωση των καθηκόντων τους είναι υπεύθυνοι ώστε να μην αναπαραχθεί με οποιονδήποτε τρόπο το περιεχόμενο της. Σε κάθε αντίθετη περίπτωση, η πράξη τους αυτή δύναται να επιφέρει πειθαρχικές ή / και νομικές κυρώσεις.
- Καμία έντυπη πληροφορία δεν τοποθετείται σε κάδο απορριμμάτων.
- Αρμόδιος για την καταστροφή και την αρχειοθέτηση έντυπων πληροφοριών είναι ο Υπεύθυνος κάθε Τμήματος που ορίζεται από τη Διοίκηση με βάση το οργανόγραμμα της εταιρείας.

## Καταστροφή Πληροφοριών

Όλες οι πληροφορίες πρέπει να καταστρέφονται ή να απορρίπτονται, όταν δεν απαιτείται περαιτέρω η χρήση τους για την επιτέλεση των επιχειρησιακών λειτουργιών της εταιρείας. Η καταστροφή πληροφοριών δεν επιτρέπεται στις ακόλουθες περιπτώσεις:

- Εάν η διατήρησή τους απαιτείται από το κανονιστικό πλαίσιο.
- Σε περίπτωση που απαιτηθούν για μελλοντική διερεύνηση ή δίωξη που αφορά μη εξουσιοδοτημένες, παράνομες ή καταχρηστικές ενέργειες.
- Εάν υπάρχει πιθανότητα για μελλοντική χρήση.

Όλα τα έντυπα - έγγραφα που δεν χρησιμοποιούνται για την επιτέλεση των οργανωτικών ή λειτουργικών αναγκών της εταιρείας, ανεξάρτητα από το επίπεδο διαβάθμισης των πληροφοριών που εμπεριέχουν, πρέπει να καταστρέφονται με ασφαλή τρόπο μέσω εγκεκριμένου εξοπλισμού και διαδικασιών, έτσι ώστε τα δεδομένα αυτά να μην μπορούν να ανακτηθούν. Η καταστροφή των εγγράφων διεξάγεται με τη χρήση των παρακάτω μεθόδων:

- Τεμαχισμός από καταστροφέα.
- Ανακύκλωση (μετά από τεμαχισμό).

Όλα τα μέσα αποθήκευσης τα οποία περιέχουν πληροφορία σε ηλεκτρονική μορφή θα καταστρέφονται σύμφωνα με τον πλέον καταλληλότερο και ασφαλέστερο τρόπο.

# 9. Αντίγραφα Ασφαλείας

## Σκοπός

Σκοπός της παρούσας Πολιτικής είναι να περιγράψει τον τρόπο με τον οποίο η εταιρεία διατηρεί αντίγραφα ασφαλείας (back-up) για όλα τα συστήματα της, ώστε να διασφαλίζει τα δεδομένα καθώς και τη διαδικασία επαναφοράς δεδομένων από αυτά.

## Εμπλεκόμενοι – Ευθύνες

Υποχρέωση εφαρμογής της παρούσας πολιτικής έχει το σύνολο του ανθρώπινου δυναμικού και των εξωτερικών συνεργατών της εταιρείας.

## Πολιτική Αντιγράφων Ασφαλείας

### Εισαγωγή

Η παρούσα πολιτική περιέχει πληροφορίες και κανόνες για τη τήρηση αντιγράφων ασφαλείας των πληροφοριακών συστημάτων της εταιρείας.

### Γενικοί Κανόνες

- Οι πληροφορίες σε επίπεδο συστήματος περιλαμβάνουν, για παράδειγμα, πληροφορίες κατάστασης συστήματος (System - State), λειτουργικό σύστημα (Operating System), λογισμικό εφαρμογών (Application Software) και άδειες χρήσης. Οι πληροφορίες σε επίπεδο χρήστη περιλαμβάνουν οποιεσδήποτε άλλες πληροφορίες εκτός από τις πληροφορίες σε επίπεδο συστήματος.
- Σε επίπεδο σχεδιασμού των αντιγράφων ασφαλείας της εταιρείας, έχει ληφθεί υπόψη ο κανόνας δημιουργίας αντιγράφων σε δύο (2) διαφορετικά επίπεδα, τα οποία είναι φυσικά και τεχνικά ανεξάρτητα και ως εκ τούτου δεν υπόκειται στους ίδιους κινδύνους αναφορικά με την ασφάλεια πληροφοριών.
- Οι μηχανισμοί που χρησιμοποιούνται για την προστασία της ακεραιότητας των αντιγράφων ασφαλείας του συστήματος πληροφοριών περιλαμβάνουν, για παράδειγμα, ψηφιακές υπογραφές ή κρυπτογράφηση.
- Τα αντίγραφα ασφαλείας του συστήματος πληροφοριών αντικατοπτρίζουν τις απαιτήσεις σε σχέδια έκτακτης ανάγκης καθώς και άλλες οργανωτικές απαιτήσεις για τη δημιουργία αντιγράφων ασφαλείας πληροφοριών.

## Λήψη Αντιγράφων Ασφαλείας

Η εταιρεία εφαρμόζει τα κατάλληλα αντίγραφα ασφαλείας για να διασφαλίζεται ότι όλες οι βασικές πληροφορίες και το λογισμικό μπορεί να ανακτηθεί μετά από καταστροφή ή αποτυχία μέσων. Κατά το σχεδιασμό του εφεδρικού σχεδίου εφαρμόζονται τα εξής:

- Με ευθύνη του IT Admin τηρούνται ακριβή και πλήρη αρχεία των αντιγράφων ασφαλείας και τεκμηριωμένων διαδικασιών αποκατάστασης. Το σύστημα λήψης αντιγράφων ασφαλείας, λαμβάνει με αυτοματοποιημένο τρόπο, αντίγραφα ασφαλείας των σημαντικών συστημάτων και αρχείων σύμφωνα με τον προγραμματισμό που έχει πραγματοποιηθεί.
- Τηρούνται αντίγραφα ασφαλείας εντός των χώρων της εταιρείας αλλά και σε δευτερεύοντα χώρο για λόγους επιχειρησιακής συνέχειας.
- Τα αντίγραφα ασφαλείας αποθηκεύονται σε κρυπτογραφημένα αποθηκευτικά μέσα.
- Διασφάλιση ότι οι εφεδρικές πληροφορίες έχουν κατάλληλο επίπεδο φυσικής και περιβαλλοντικής ασφάλειας.
- Ο IT Admin μεριμνά για τη δοκιμή των διαδικασιών αποκατάστασης για να επιτύχει τον απαιτούμενου χρόνο αποκατάστασης. Έχουν ενεργοποιηθεί ειδοποιήσεις για την έκβαση της διαδικασίας του αντιγράφου ασφαλείας. Αποστέλλεται αυτόματη ειδοποίηση για την αποτυχημένη λήψη αντιγράφου ασφαλείας.
- Η εταιρεία εξετάζει τη διαγραφή πληροφοριών που τηρούνται σε αντίγραφα ασφαλείας μόλις λήξει η περίοδος διατήρησης των πληροφοριών. Λαμβάνεται υπόψιν η σχετική νομοθεσία και οι κανονισμοί τήρησης πληροφοριών.

### Έλεγχος και Διατήρηση Αντιγράφων Ασφαλείας

- Οι ρυθμίσεις δημιουργίας αντιγράφων ασφαλείας για μεμονωμένα συστήματα και υπηρεσίες ελέγχονται τακτικά για να διασφαλίζεται ότι πληρούν τις απαιτήσεις των σχεδίων επιχειρηματικής συνέχειας και της γενικότερης στρατηγικής της εταιρείας.

- Στην περίπτωση κρίσιμων συστημάτων και υπηρεσιών, οι ρυθμίσεις αντιγράφων ασφαλείας θα πρέπει να καλύπτουν όλες τις πληροφορίες συστημάτων, τις εφαρμογές και τα δεδομένα που είναι απαραίτητα για την ανάκτηση ολόκληρου του συστήματος σε περίπτωση καταστροφής.

## Διαδικασία Λήψης Αντιγράφων Ασφαλείας

Η διαδικασία λήψης και διαχείρισης αντιγράφων ασφάλειας ακολουθεί τα παρακάτω βήματα:

- Το σύστημα λήψης αντιγράφων ασφαλείας, λαμβάνει με αυτοματοποιημένο τρόπο πλήρη και καθημερινά αντίγραφα ασφαλείας των συστημάτων σύμφωνα με τον προγραμματισμό που έχει γίνει από τους διαχειριστές των συστημάτων. Το αντίγραφο ασφαλείας

αποθηκεύεται σε NAS Storage, το οποίο χρησιμοποιείται καθημερινά για Full/Incremental λήψη αντιγράφων.

- Εκτελούνται δειγματοληπτικά ενέργειες επιβεβαίωσης της ορθής λήψης των αντιγράφων, η οποία περιλαμβάνει τον έλεγχο των αρχείων που έχουν μεταφερθεί.
- Σε περίπτωση μη επιτυχούς ολοκλήρωσης της διαδικασίας, εξετάζεται το πρόβλημα.

### Ενημέρωση Αποτυχίας Αντιγράφων Ασφαλείας

Έχουν υλοποιηθεί προσαρμοσμένες εργασίες οι οποίες να πληροφορούν τον IT Admin για πιθανή βλάβη της διαδικασίας δημιουργίας αντιγράφων ασφαλείας, γράφοντας το κατάλληλο αρχείο καταγραφής, συμπεριλαμβανομένων πληροφοριών σχετικά με το σφάλμα, την ημερομηνία και την ώρα της δημιουργίας αντιγράφων ασφαλείας.

### Δοκιμή Αντιγράφων Ασφαλείας

Τα αντίγραφα ασφαλείας πρέπει να δοκιμάζονται ανά τακτά χρονικά διαστήματα μία φορά τον χρόνο ώστε να διασφαλίζεται η ακεραιότητα και η πληρότητα των περιεχόμενών τους. Έπειτα από κάθε δοκιμή των αντιγράφων ασφαλείας πρέπει να είναι σαφές αν:

- Η ολική επαναφορά των συστημάτων είναι εφικτή.
- Η διαδικασία επαναφοράς καλύπτει τους στόχους επαναφοράς.
- Τα δεδομένα μπορούν να εγκατασταθούν με επιτυχία σε εναλλακτικά συστήματα.
- Το προσωπικό το οποίο συμμετέχει στις διαδικασίες λήψης αντιγράφων ασφαλείας, δοκιμών και επαναφοράς έχουν πλήρη επίγνωση όλων των βημάτων που απαιτούνται στις διαδικασίες αυτές.

## Διαδικασία Επαναφοράς Δεδομένων από Αντίγραφα Ασφαλείας

Η διαδικασία επαναφοράς δεδομένων από αντίγραφα ασφάλειας ακολουθεί τα παρακάτω βήματα:

- Ο ιδιοκτήτης των δεδομένων που πρέπει να ανακτηθούν από τα αντίγραφα ασφαλείας αιτείται την ανάκτησή τους και δίνει όλα τα στοιχεία που μπορούν να οδηγήσουν στην ανεύρεση και ανάκτηση των δεδομένων, όπως περιγραφή των δεδομένων, ημερομηνία, ώρα κλπ.
    - Ανάλογα με τη φύση των δεδομένων προς ανάκτηση, το αίτημα γίνεται κατευθείαν από το χρήστη / ιδιοκτήτη των δεδομένων ή απαιτείται και η έγκριση του προϊσταμένου του.
    - Η αίτηση μπορεί να γίνει και μέσω ηλεκτρονικού ταχυδρομείου.
- Ο IT Admin αναζητά τα προς ανάκτηση δεδομένα στα αντίγραφα ασφαλείας.
- Επαναφέρουν τα δεδομένα από τα αντίγραφα ασφαλείας και βεβαιώνουν την επιτυχία της διαδικασίας επαναφοράς.

- Σε περίπτωση μη επιτυχούς ολοκλήρωσης της διαδικασίας, ο IT Admin εξετάζει το πρόβλημα. Αν το πρόβλημα δεν επιλυθεί ή δημιουργήθηκε από βλάβη του συστήματος λήψης αντιγράφων ασφάλειας λαμβάνονται διορθωτικά μέτρα.
- Ο IT Admin ενημερώνει τον ιδιοκτήτη των δεδομένων για την επαναφορά τους.

| **Διαδικασία Λήψης Αντιγράφων Ασφάλειας** | |
|---|---|
| **Βήμα 1** | Δημιουργία πλάνου λήψης αντιγράφων ασφαλείας. |
| **Βήμα 2** | Ενημέρωση αποτυχίας αντιγράφων ασφαλείας. |
| **Βήμα 3** | Δοκιμή αντιγράφων ασφαλείας. |
| **Βήμα 4** | Αξιολόγηση της επαναφοράς αντιγράφων ασφάλειας. |

# 10. Ασφάλεια Δικτύου

## Σκοπός

Η πολιτική αυτή θέτει οδηγίες σχετικά με τη διαχείριση και υποστήριξη των δικτύων δεδομένων και φωνής που σχετίζονται με τα συστήματα της Εταιρείας.

## Εμπλεκόμενοι – Ευθύνες

Η πολιτική εφαρμόζεται σε όλους τους τομείς και τις εγκαταστάσεις της εταιρείας, όπως επίσης και στο προσωπικό των εξωτερικών συνεργατών, εφόσον απαιτείται, στους οποίους παρέχεται πρόσβαση στο δίκτυο της εταιρείας για την άσκηση των εργασιών τους.

## Πολιτική Ασφάλειας Δικτύου

### Εισαγωγή

Το παρόν έγγραφο περιγράφει την Πολιτική Ασφάλειας Δικτύων της **«Π.Ε. ΚΑΣΙΝΑΚΗΣ Α.Ε.»** . Η εταιρεία εφαρμόζει ελέγχους για να διασφαλίσει την ασφάλεια των πληροφοριών στα δίκτυα και την προστασία των συνδεδεμένων υπηρεσιών από μη εξουσιοδοτημένη πρόσβαση.

## Κανόνες Ασφάλειας Δικτύου

Η **«Π.Ε. ΚΑΣΙΝΑΚΗΣ Α.Ε.»** εφαρμόζει ελέγχους για να διασφαλίσει την ασφάλεια των πληροφοριών στα δίκτυα και την προστασία των συνδεδεμένων υπηρεσιών από μη εξουσιοδοτημένη πρόσβαση. Συγκεκριμένα, λαμβάνονται υπόψη τα ακόλουθα στοιχεία:

- Ευθύνες και διαδικασίες για τη διαχείριση του εξοπλισμού δικτύωσης.
- Επιχειρησιακή ευθύνη για τα δίκτυα.
- Η ασφάλεια των δεδομένων που διαβιβάζονται μέσω δημόσιων δικτύων ή μέσω ασύρματων δικτύων (εμπιστευτικότητα και ακεραιότητα).
- Προστασία συνδεδεμένων συστημάτων και εγκατεστημένων εφαρμογών.
- Περιορισμοί σχετικά με την σύνδεση με το διαδίκτυο.

## Διαχείριση Ασφάλειας Δικτύου

### Λειτουργία Μηχανισμών Ασφάλειας Δικτύου

Η λειτουργία των μηχανισμών ασφάλειας του δικτύου της εταιρείας διέπεται από τις παρακάτω αρχές:

- Οι μηχανισμοί ασφάλειας του δικτύου είναι διαρκώς ενεργοποιημένοι ενώ γίνεται χρήση Συστημάτων Αδιάλειπτης Τάσης (UPS) για την παροχή ρεύματος.
- Τα αρχεία καταγραφής (log files) του δικτυακού εξοπλισμού και των εξυπηρετητών της εταιρείας είναι διαρκώς ενεργοποιημένα και ελέγχονται τακτικά από τους διαχειριστές της εταιρείας για τον εντοπισμό «μη προβλεπόμενων» ενεργειών.
- Κεντρική διαχείρισης και έλεγχος συσκευών δικτύου (Switches, Access Points κ. α.)

### Καταγραφή και Παρακολούθηση

Αρχεία καταγραφής όπως τα παρακάτω ελέγχονται σε τακτική βάση από τον IT Admin:

- Αρχεία καταγραφής Τείχους Προστασίας.
- Αρχεία καταγραφής του Domain Controller.
- Δεδομένα δικτυακής κίνησης από δικτυακές συσκευές.
- Δεδομένα καταγραφής από διαμεσολαβητές πρόσβασης σε δημόσιους δικτυακούς πόρους.

### Προστασία Υλικού Εξοπλισμού Εξυπηρετητών (Server) Μέσω Λογισμικού Επιτήρησης (Monitoring Software)

Για την σωστή και αδιάλειπτη λειτουργία των εξυπηρετητών της εταιρίας γίνεται χρήση εργαλείων επιτήρησης λειτουργιών (monitoring tools).

## Τείχη Προστασίας (Firewalls)

Η εταιρεία έχει εγκαταστημένα Τείχη Προστασίας (Firewalls) με κεντρική διαχείριση, που ελέγχουν σε μόνιμη βάση τη δικτυακή κίνηση και καλύπτουν όλο το παραγωγικό και το δίκτυο επισκεπτών (Guest) της εταιρείας.

- Έχουν οριστεί πολιτικές ελέγχου περιεχομένου (Web Filtering) και ελέγχου εφαρμογών (Application Control - Filtering).
- Τα αρχεία καταγραφών από το Τείχος Προστασίας συλλέγονται με χρήση κατάλληλου εργαλείου και παρακολουθούνται συνεχώς.
- Μετά από οποιαδήποτε αλλαγή στις ρυθμίσεις του Τείχους Προστασίας, λαμβάνεται αντίγραφο του αρχείου ρύθμισης παραμέτρων (Configuration File) και διατηρείται σε αρχείο με επαρκή ιστορικότητα.
- Πραγματοποιείται τακτικός και προγραμματισμένος έλεγχος για ενημερώσεις.
- Επιβάλλονται κανόνες πρόληψης εισβολής (IPS) για τον εντοπισμό και τον αποκλεισμό γνωστών και ύποπτων απειλών εφόσον αυτές είναι διαθέσιμες.
- Επιβάλλονται κανόνες σύνδεσης που καθορίζονται από τη γεωγραφική θέση.
- Παρακολούθηση των πορτών εισερχόμενης και εξερχόμενης κίνησης.

## Προστασία από κακόβουλο λογισμικό - EDR

Ο **IT Admin** ορίζει την πολιτική που θα εφαρμοστεί στην εταιρεία προκειμένου να διασφαλιστούν τα πληροφοριακά συστήματα από την απειλή κακόβουλου λογισμικού.
Η αντιμετώπιση των απειλών επιτυγχάνεται με τα κάτωθι:

- Εγκατάσταση λογισμικού EDR (Endpoint Detection and Response System) το οποίο προστατεύει σε πραγματικό χρόνο, όλους τους σταθμούς εργασίας και τους εξυπηρετητές της εταιρείας, ενώ η διαχείρισή του πραγματοποιείται μέσω Κεντρικής Κονσόλας. Τα αρχεία καταγραφών του λογισμικού EDR παρακολουθούνται σε μόνιμη βάση. Σε περίπτωση κρίσιμου συμβάντος ενημερώνεται άμεσα ο **IT Admin.**
- Το EDR έχει ρυθμιστεί ώστε να ελέγχει υποχρεωτικά τα αποσπώμενα μέσα, όταν εισάγονται στον σταθμό εργασίας για κακόβουλο λογισμικό. Ο χρήστης δεν μπορεί να παρακάμψει τον συγκεκριμένο έλεγχο.
- Αλλαγές στο λογισμικό EDR μπορεί να πραγματοποιήσει μόνο εξουσιοδοτημένο προσωπικό. Οι ρυθμίσεις είναι κλειδωμένες με κωδικό ασφαλείας για τον τελικό χρήστη.
- Τεχνικός περιορισμός που αποτρέπει την εγκατάσταση λογισμικού στους σταθμούς εργασίας από μη εξουσιοδοτημένο προσωπικό.
- Απαγόρευση εγκατάστασης και χρήσης λογισμικού που δεν έχει εγκριθεί ή για το οποίο η εταιρεία δε διαθέτει νόμιμη άδεια χρήσης.
- Οι αναβαθμίσεις των λειτουργικών συστημάτων των εξυπηρετητών της εταιρείας πραγματοποιούνται μετά την παρέλευση ενός καθορισμένου χρονικού διαστήματος από την κυκλοφορία τους, με ευθύνη του IT Admin, ώστε να λαμβάνονται εγκαίρως οι απαραίτητες ενημερώσεις ασφαλείας, ενώ ταυτόχρονα να διασφαλίζεται πως δεν θα

προκύψουν διακοπές στην εύρυθμη λειτουργία τους εξαιτίας προβληματικών ενημερώσεων.

- Στους χρήστες των σταθμών εργασίας είναι ενεργοποιημένες οι αυτόματες ενημερώσεις του λειτουργικού συστήματος και του EDR.
- Μέσω πολιτικής έχουν οριστεί πρότυπα με τις απαραίτητες εφαρμογές που θα πρέπει να είναι εγκατεστημένες στους σταθμούς εργασίας. Για την εγκατάσταση επιπλέον προγραμμάτων υποβάλλεται, μέσω αιτήματος στον IT Admin για την αξιολόγηση του προτεινόμενου προγράμματος και την εγκατάσταση αυτού εφ' όσον δεν παραβιάζονται οι πολιτικές ασφάλειας πληροφοριών.

## Απομακρυσμένη Πρόσβαση

Η απομακρυσμένη πρόσβαση σε πόρους του εσωτερικού δικτύου της εταιρείας θα χορηγείται μόνο όταν είναι απαραίτητη και όχι για όλους τους χρήστες από προεπιλογή. Για την ασφάλεια της απομακρυσμένης πρόσβασης τα συνθηματικά των χρηστών πρέπει να πληρούν την Πολιτική Προστασίας και Ορθής Χρήσης των Πόρων.

## Φυσική Ασφάλεια – Προστασία

Ο κύριος εξοπλισμός του δικτύου στεγάζεται σε ικριώματα (Racks), στο οποίο πρόσβαση υπάρχει μόνο από το εξουσιοδοτημένο προσωπικό υποστήριξης τον **IT Admin** και την Διοίκηση της εταιρείας.

## Διαχείριση Υπολογιστικής Ικανότητας (Capacity Management)

Οι διαχειριστές των συστημάτων της εταιρείας παρακολουθούν την απόδοση των συστημάτων, μέσω σχετικών διαγνωστικών εργαλείων που διαθέτουν, και προβαίνουν στις κατάλληλες ενέργειες, εφόσον απαιτείται. Οι απαιτήσεις απόδοσης έχουν προσδιοριστεί, λαμβάνοντας υπόψη την επιχειρησιακή κρισιμότητα του επιχειρησιακού περιβάλλοντος. Έχουν εφαρμοστεί ρυθμίσεις και παρακολούθηση του συστήματος για τη διασφάλιση και, όπου είναι απαραίτητο, τη βελτίωση της διαθεσιμότητας και αποτελεσματικότητας των συστημάτων.

Επιπλέον, η εκτίμηση της απαιτούμενης υπολογιστικής ισχύος για την εξυπηρέτηση νέων επιχειρησιακών απαιτήσεων / λειτουργιών περιλαμβάνεται στις παραμέτρους που εξετάζονται κατά την ανάπτυξη / αναβάθμιση πληροφοριακών συστημάτων.

Ειδικότερα, η διαχείριση της υπολογιστικής ικανότητας των υποδομών της εταιρείας ακολουθεί τους εξής κανόνες, ανά περίπτωση:

- Οι ανάγκες υπολογιστικής ικανότητας παρακολουθούνται μέσω εργαλείου κεντρικής διαχείρισης.

- Έχουν οριστεί ειδοποιήσεις σε περιπτώσεις που ξεπεραστούν τα αποδεκτά όρια λειτουργίας για ορισμένο χρόνο.

Εάν υπάρξει ανάγκη αναβάθμισης της υπολογιστικής ικανότητας ή του διαθέσιμου χώρου αποθήκευσης στους εξυπηρετητές της εταιρείας, ο **IT Admin** ενημερώνει την Διοίκηση για την αγορά του.

Ο Διευθύνων Σύμβουλος

Ανδρέας Κασινάκης