Όνομα Οργανισμού

Πολιτική Αποδεκτής Χρήσης

|  |  |
| --- | --- |
| **Περιεχόμενο:** | Πολιτική Αποδεκτής Χρήσης |
| **Δημιουργός:** |  |
| **Έκδοση:** | 1.0 |
| **Ημερομηνία Έκδοσης:** | ηη/μμ/χχχχ |
| **Εμπιστευτικότητα:** |  |
| **Ιδιοκτήτης:** |  |

Διανομή

| Ρόλος | Όνομα | Οργανισμός | Τοποθεσία | Αριθμός Αντιτύπων |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Καταγραφή Τροποποιήσεων

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Κατάσταση Έκδοσης | Έκδοση | Ημερομηνία | Ενέργειες από | Περιγραφή |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Αναφορές

|  |  |  |
| --- | --- | --- |
| **Αρ.** |  | **Αναφορά Εγγράφου** |
| 1 |  |  |
| 2 |  |  |
| 3 |  |  |

Υποστηρικτικό Υλικό

|  |  |
| --- | --- |
| **Αρ.** | **Αναφορά** |
| 1 |  |
| 2 |  |
| 3 |  |

Ειδικό Λεξιλόγιο

Οι όροι και συντμήσεις ορίζονται πιο κάτω:

| Όροι και συντμήσεις | Περιγραφή |
| --- | --- |
|  |  |
|  |  |
|  |  |

# Πίνακας Περιεχομένων

[Πίνακας Περιεχομένων 3](#_Toc184811104)

[1. Εισαγωγή 4](#_Toc184811105)

[1.1 Σκοπός 4](#_Toc184811106)

[1.2 Πεδίο Εφαρμογής 4](#_Toc184811107)

[2. Πολιτική Αποδεκτής Χρήσης 5](#_Toc184811108)

[2.1 Γενικές Απαιτήσεις -Υποχρεώσεις 5](#_Toc184811110)

[2.2 Ηλεκτρονικό Ταχυδρομείο 5](#_Toc184811111)

[2.3 Χρήση του διαδικτύου 6](#_Toc184811112)

[3. Κωδικοί Πρόσβασης 7](#_Toc184811113)

[4. Αποθήκευση Πληροφοριών 7](#_Toc184811114)

[5. Κινητές Συσκευές 8](#_Toc184811115)

[6. Εργασία εξ ’αποστάσεως 8](#_Toc184811116)

[7. Αποσπώμενα Μέσα Φύλαξης Δεδομένων 9](#_Toc184811117)

[8. Αναθεώρηση 10](#_Toc184811118)

[9. Αναφορές 11](#_Toc184811119)

# Εισαγωγή

## Σκοπός

Η παρούσα Πολιτική καθορίζει την Πολιτική Αποδεκτής Χρήσης του [Όνομα Οργανισμού] σε σχέση με την πρόσβαση και την ορθή χρήση των πληροφοριακών συστημάτων, των τεχνολογικών πόρων και των δεδομένων του. Στόχος είναι:

* Η προστασία της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των περιουσιακών στοιχείων πληροφοριών.
* Η αποτροπή της κακής χρήσης, της μη εξουσιοδοτημένης πρόσβασης ή ενέργειες που ενδέχεται να θέσουν σε κίνδυνο την ασφάλεια πληροφοριών.
* Η διασφάλιση της συμμόρφωσης με τις άλλες πολιτικές και κανονισμούς/νομοθεσίες.
* Η προώθηση της ασφαλούς και υπεύθυνης χρήσης των τεχνολογικών και άλλων πόρων για την υποστήριξη της αποστολής και των στόχων του οργανισμού.

## Πεδίο Εφαρμογής

Ο [Όνομα Οργανισμού] έχει ως στόχο τη διεξαγωγή δραστηριοτήτων με επαγγελματικότητα, εφαρμόζοντας υψηλές προδιαγραφές για την παροχή των υπηρεσιών. Συνεπώς, όλο το προσωπικό είναι απαραίτητο να λαμβάνει τα αναγκαία μέτρα για τη διασφάλιση της ακεραιότητας των πληροφοριών και των πληροφοριακών συστημάτων με τα δεδομένα τους, και να ακολουθήσει τις διαδικασίες και τις οδηγίες που περιγράφονται πιο κάτω, για τη διατήρηση της ασφάλειας και της νομιμότητας. Η Πολιτική Αποδεκτής Χρήσης εφαρμόζεται σε όλους τους εργαζομένους/χρήστες του [Όνομα Οργανισμού], συμπεριλαμβανομένων και των τρίτων μερών που ενδέχεται να έχουν πρόσβαση στους πόρους του [Όνομα Οργανισμού], ώστε να διατηρείται ένα ασφαλές, αποτελεσματικό και ηθικό περιβάλλον εργασίας. Αυτή η πολιτική ισχύει για όλες τις πληροφορίες και τα πληροφοριακά συστήματα του Οργανισμού, συμπεριλαμβανομένου του εξοπλισμού που χρησιμοποιείται για την εξ’ αποστάσεως εργασία καθώς και του υλικού που προέρχεται από τα διάφορα συστήματα πληροφορικής.

Η παρούσα πολιτική καθορίζει σαφείς προσδοκίες για όλους τους χρήστες όσο αφορά:

* Υπολογιστές, φορητοί υπολογιστές και φορητές συσκευές που ανήκουν στο [Όνομα Οργανισμού].
* Λογαριασμοί ηλεκτρονικού ταχυδρομείου που εκδίδονται από το [Όνομα Οργανισμού] και πρόσβαση σε εταιρική ηλεκτρονική αλληλογραφία.
* Το εσωτερικό δίκτυο του [Όνομα Οργανισμού].
* Πρόσβαση στο διαδίκτυο.
* Λογισμικό και εφαρμογές που παρέχονται από το [Όνομα Οργανισμού].

# Πολιτική Αποδεκτής Χρήσης



## Γενικές Απαιτήσεις -Υποχρεώσεις

Ο [Όνομα Οργανισμού] έχει θεσπίσει και εφαρμόζει βασικούς κανόνες ασφάλειας πληροφοριών, οι οποίοι να περιλαμβάνονται στις συμβάσεις των εργαζομένων. Πιο συγκεκριμένα:

Η Πολιτική Αποδεκτής Χρήσης κοινοποιείται σε όλο το προσωπικό και γίνεται αποδεκτή μέσω των συμβάσεων, καθώς και στην συνέχεια το προσωπικό να λαμβάνει σχετική εκπαίδευση για την αποδεκτή χρήση των πόρων ή/και των πληροφοριών του [Όνομα Οργανισμού], ώστε να εφαρμόζει μέτρα ανάλογα με την κρισιμότητα της πληροφορίας που διαχειρίζεται.

Οι υπολογιστές ή/και άλλοι πόροι που έχουν εκχωρηθεί στο προσωπικό πρέπει να χρησιμοποιούνται αποκλειστικά για εγκεκριμένους επιχειρησιακούς σκοπούς και απαγορεύεται οποιαδήποτε προσωπική χρήση.

Οι πόροι του [Όνομα Οργανισμού] πρέπει να χρησιμοποιούνται μόνο από εξουσιοδοτημένα άτομα και απαγορεύεται διάθεση τους σε συναδέλφους ή/και οποιαδήποτε τρίτα πρόσωπα.

Στους πόρους του [Όνομα Οργανισμού] πρέπει να γίνεται χρήση μόνο αδειοδοτημένου λογισμικού.

Κάθε υποψία περιστατικού ασφάλειας πρέπει να αναφέρεται από οποιονδήποτε εργαζόμενο γίνει αντιληπτό, σύμφωνα με την Πολιτική Διαχείρισης Συμβάντων και Περιστατικών.

Συστήνεται όπως η εναρμόνιση με την Πολιτική Αποδεκτής Χρήσης, να ελέγχεται μέσω ερωτηματολογίων που συμπληρώνονται από το προσωπικό σε ετήσια βάση. Πρέπει να υλοποιούνται τεχνικά μέτρα ώστε να ενημερώνεται το προσωπικό για τις οδηγίες αποδεκτής χρήσης κάθε φορά που πρόκειται να αποκτήσει πρόσβαση στα συστήματα του [Όνομα Οργανισμού].

## Ηλεκτρονικό Ταχυδρομείο

Η απρόσεκτη χρήση του ηλεκτρονικού ταχυδρομείου ή του διαδικτύου μπορεί να εκθέσει τα δίκτυα πληροφοριών του [Όνομα Οργανισμού] σε ένα ευρύ φάσμα κινδύνων που σχετίζονται με διάφορα ήδη ιών όπως spyware, Trojan, worms, spam και άλλες απειλές του κυβερνοχώρου, οι οποίες επιφέρουν αρνητικές συνέπειες στην εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των δεδομένων του [Όνομα Οργανισμού].

Κατά τη χρήση του ηλεκτρονικού ταχυδρομείου ή του διαδικτύου, το προσωπικό του [Όνομα Οργανισμού] φέρει την ευθύνη να δίνει συνεχώς τη δέουσα προσοχή στην ασφάλεια του δικτύου.

Οι κατευθυντήριες γραμμές/οδηγίες που περιέχονται στην παρούσα πολιτική ισχύουν τόσο για τα τυχόν προσωπικά ηλεκτρονικά μηνύματα όσο και για τα ηλεκτρονικά μηνύματα του Οργανισμού. Το ηλεκτρονικό ταχυδρομείο έχει εγκατασταθεί ως μέθοδος επικοινωνίας για τις δραστηριότητες του [Όνομα Οργανισμού]. Η προσωπική χρήση του εταιρικού ηλεκτρονικού ταχυδρομείου απαγορεύεται για αποφυγή και μείωση ανοίγματος ανεπιθύμητων μηνυμάτων.

Τα ηλεκτρονικά μηνύματα μπορούν να οδηγήσουν τον [Όνομα Οργανισμού] σε δεσμευτικές υποχρεώσεις και να τον εκθέσουν στον ίδιο βαθμό που μπορεί να τον εκθέσει η παραδοσιακή αλληλογραφία. Ακατάλληλες δηλώσεις σε μηνύματα ηλεκτρονικού ταχυδρομείου μπορεί να οδηγήσουν σε προσωπική ευθύνη του ατόμου που αποστέλλει το μήνυμα, καθώς οι δηλώσεις αυτές μπορεί να χρησιμοποιηθούν σε υποθέσεις δικαστηρίου. Χρειάζεται λοιπόν να δίδεται ιδιαίτερη προσοχή στη συγγραφή ηλεκτρονικών μηνυμάτων και να εφαρμόζονται τα ίδια πρότυπα και πρωτόκολλα όπως αυτά που εφαρμόζονται στη γραπτή αλληλογραφία.

Επιπρόσθετα, θα πρέπει να αποφεύγονται μηνύματα τα οποία αποστέλλονται μέσω ηλεκτρονικού ταχυδρομείου και που θα μπορούσε να θέσουν σε κίνδυνο την ακεραιότητα ή τη φήμη του [Όνομα Οργανισμού].

Δεν πρέπει να χρησιμοποιείτε το ηλεκτρονικό ταχυδρομείο του [Όνομα Οργανισμού] για αποθήκευση, αποστολή/προώθηση και γενικά μεταφορά περιεχομένου οποιασδήποτε από τις ακόλουθες κατηγορίες:

* Περιεχόμενο το οποίο παραβιάζει τις υποχρεώσεις του υπαλλήλου για τη διαφύλαξη των διαβαθμισμένων πληροφοριών του Οργανισμού, ή που παραβιάζει τις υποχρεώσεις του [Όνομα Οργανισμού] για τη διαφύλαξη των διαβαθμισμένων πληροφοριών των συνεργατών του, ή παραβιάζει το δικαίωμα ιδιοκτησίας (εμπορικό σήμα, εμπορικό μυστικό, πνευματικά δικαιώματα).
* Προσβλητικό ή άσεμνο περιεχόμενο (συμπεριλαμβανομένου κάθε είδους πορνογραφίας).
* Ρατσιστικού ή σεξιστικού περιεχομένου.
* Περιεχόμενο το οποίο είναι αναληθές ή κακόβουλο, είτε αυτό αφορά μέλος του προσωπικού, είτε αφορά οποιονδήποτε άτομο εκτός του [Όνομα Οργανισμού].
* Οποιοδήποτε περιεχόμενο που έχει να κάνει με εκφοβισμό ή παρενόχληση (όπως π.χ. για το φύλο, συμπεριλαμβανομένης της σεξουαλικής προτίμησης, τη φυλή ή αναπηρία).
* Οποιοδήποτε άλλο περιεχόμενο που θα μπορούσε αλλιώς να θεωρηθεί παράνομο.

Τέτοιες ενέργειες αποτελούν ανάρμοστη συμπεριφορά και θα μπορούσαν να ενεργοποιήσουν τις πειθαρχικές διαδικασίες του Οργανισμού.

## Χρήση του διαδικτύου

Οι διαδικασίες και οι απαιτήσεις για τη χρήση ηλεκτρονικού ταχυδρομείου του Οργανισμού, ισχύουν εξίσου και για τη χρήση του διαδικτύου, με τις ακόλουθες πρόσθετες οδηγίες:

* Οι εργαζόμενοι πρέπει να χρησιμοποιούν το διαδίκτυο αποκλειστικά για επαγγελματικούς σκοπούς και να αποφεύγουν την πρόσβαση σε ακατάλληλο ή μη εξουσιοδοτημένο περιεχόμενο.
* Η πρόσβαση σε ιστότοπους κοινωνικής δικτύωσης και προσωπικής ψυχαγωγίας πρέπει να περιορίζεται κατά τις ώρες εργασίας, εκτός αν υπάρχει σαφής επαγγελματικός λόγος.
* Οι εργαζόμενοι πρέπει να αποφεύγουν τη λήψη αρχείων από αναξιόπιστες πηγές
* και να μην εγκαθιστούν λογισμικό χωρίς την έγκριση του τμήματος πληροφορικής του [Όνομα Οργανισμού].
* Θα πρέπει να επιβεβαιώνεται ότι η λήψη πληροφοριών ή υλικού από ιστοσελίδες, δεν παραβιάζει τα δικαιώματα πνευματικής ιδιοκτησίας και ούτε επιφέρει μη εξουσιοδοτημένη δαπάνη στον [Όνομα Οργανισμού].
* Θα πρέπει να αποφεύγεται επίσκεψη σε ιστοσελίδες ή το αποστολή πληροφοριών μέσω αυτών που εμπίπτουν στις ακόλουθες κατηγορίες (ο κατάλογος δεν είναι εξαντλητικός):
  + δυσφημιστικό
  + προσβλητικό, άσεμνο (συμπεριλαμβανομένου κάθε είδους πορνογραφία)
  + ρατσιστικό ή σεξιστικό
  + θα μπορούσε να προκαλέσει εκφοβισμό ή παρενόχληση (σχετικά με το φύλο, συμπεριλαμβανομένου του σεξουαλικού προσανατολισμού, φυλής ή αναπηρίας)
  + με παράνομο λογισμικό ή άλλο πειρατικό οπτικοακουστικό υλικό
  + οτιδήποτε που θα μπορούσε να θεωρηθεί παράνομο

# Κωδικοί Πρόσβασης

Οι κωδικοί πρόσβασης αποτελούν κρίσιμο μέρος της ασφάλειας του Οργανισμού. Δεν επιτρέπεται η κοινή χρήση κωδικών πρόσβασης με άλλους εργαζόμενους ή τρίτα μέρη. Οι κωδικοί πρόσβασης πρέπει να αποθηκεύονται με ασφάλεια και να μην καταγράφονται σε ευανάγνωστες μορφές.

Οι εργαζόμενοι πρέπει να αλλάζουν τους κωδικούς πρόσβασης με κάποια περιοδικότητα σύμφωνα με τις καλές πρακτικές και να αποφεύγουν τη χρήση κοινών ή εύκολα προβλέψιμων κωδικών.

Οι εργαζόμενοι δεν πρέπει να τηρούν αρχείο φύλαξης κωδικών πρόσβασης εκτός εάν αυτοί μπορούν να αποθηκευτούν ασφάλεια, εφαρμόζοντας εγκεκριμένες μεθόδους αποθήκευσης και κρυπτογράφησης.

Για περισσότερες πληροφορίες βλέπε Πολιτική Ελέγχου Πρόσβασης.

# Αποθήκευση Πληροφοριών

Δεν επιτρέπεται η αποθήκευση επαγγελματικών πληροφοριών σε μη εγκεκριμένες εξωτερικές συσκευές αποθήκευσης ή προσωπικούς λογαριασμούς στο σύννεφο (cloud).

Οι εργαζόμενοι πρέπει να διατηρούν αντίγραφα ασφαλείας σημαντικών δεδομένων τακτικά και να εξασφαλίζουν ότι αυτά αποθηκεύονται σε ασφαλή μέσα.

Όλες οι ευαίσθητες και εμπιστευτικές πληροφορίες πρέπει να αποθηκεύονται σε ασφαλείς τοποθεσίες και να είναι κρυπτογραφημένες.

# Κινητές Συσκευές

Κατά τη χρήση κινητών συσκευών π.χ. φορητοί υπολογιστές, κινητά τηλέφωνα, κ.α. πρέπει να δίνεται ιδιαίτερη προσοχή ώστε να διασφαλιστεί ότι οι πληροφορίες του Οργανισμού δεν βρίσκονται σε κίνδυνο σε κίνδυνο. Ιδιαίτερη προσοχή πρέπει να δίδεται όταν ο εξοπλισμός αυτός χρησιμοποιείτε σε δημόσιους χώρους, αίθουσες συνεδριάσεων και άλλες μη προστατευόμενες περιοχές εκτός των εγκαταστάσεων του [Όνομα Οργανισμού].

κατά τη χρήση κινητών συστημάτων πληροφορικής σε

Όπου είναι δυνατό αυτές οι συσκευές θα πρέπει να είναι προστατεύονται μέσω κρυπτογράφησης για την αποφυγή της μη εξουσιοδοτημένης πρόσβασης ή αποκάλυψης των πληροφοριών που αποθηκεύονται σε αυτά (βλέπε Πολιτική Διαχείρισης Στοιχείων Ενεργητικού).

Απομακρυσμένη πρόσβαση σε πληροφορίες του Οργανισμού με τη χρήση του δημόσιου δικτύου και κινητών συστημάτων πληροφοριών, θα πρέπει να γίνεται μόνο κατόπιν παραχώρησης σχετικής άδειας και μετά την επιτυχή ταυτοποίηση και επαλήθευση της ταυτότητας του χρήστη καθώς και με τους κατάλληλους μηχανισμούς ελέγχου της πρόσβασης μόνο μέσω VPN.

Αν η μεταφορά φορητών υπολογιστών δεν είναι απαραίτητη, τότε oι φορητοί υπολογιστές του [Όνομα Οργανισμού] πρέπει να κλειδώνονται με την αποχώρηση από το γραφείο εκτός εάν υπάρχουν επαρκή μέτρα φυσικής ασφάλειας στο κτίριο. Εάν η μεταφορά είναι υποχρεωτική και αναγκαστική για την διεκπεραίωση των καθηκόντων ενός υπαλλήλου, τότε πρέπει να ακολουθούνται οι βέλτιστες πρακτικές ασφάλισης φορητών συσκευών όπως αναγράφονται στην ενότητα Ασφάλεια Πληροφοριακών Συστημάτων της παρούσας Πολιτικής.

# Εργασία εξ ’αποστάσεως

Στην περίπτωση εργασίας εξ’ αποστάσεως, χρειάζεται να λαμβάνονται κατάλληλα μέτρα για προστασία του χώρου πριν την έναρξη των εργασιών π.χ. κλοπή του εξοπλισμού και των πληροφοριών, μη εξουσιοδοτημένη αποκάλυψη πληροφοριών, μη εξουσιοδοτημένη εξ’ αποστάσεως πρόσβαση στα εσωτερικά συστήματα του [Όνομα Οργανισμού].

Οι εργασίες που πραγματοποιούνται εξ’ αποστάσεως χρειάζεται να εξουσιοδοτηθούν και να είναι ελεγμένες από τη Διεύθυνση του [Όνομα Οργανισμού]. Επιπρόσθετα, χρειάζεται να διασφαλιστεί ότι υπάρχει η υποδομή για τις αναγκαίες διευθετήσεις για υποστήριξη αυτού του τρόπου εργασίας.

Οποιοιδήποτε κωδικοί πρόσβασης που χρησιμοποιούνται για την εξ’ αποστάσεως πρόσβαση στα συστήματα του Οργανισμού, πρέπει να απομνημονεύονται και να μην καταγράφονται. Εάν ένας φορητός υπολογιστής κλαπεί, το αρμόδιο Τμήμα Πληροφορικής του [Όνομα Οργανισμού] θα πρέπει να ενημερωθεί το συντομότερο δυνατό.

# Αποσπώμενα Μέσα Φύλαξης Δεδομένων

Ο περιορισμός των αποσπώμενων μέσων αποθήκευσης δεδομένων(USB disks) αποτελεί ένα αποτελεσματικό μέτρο ασφαλείας σε εταιρικά περιβάλλοντα και θα πρέπει να τηρείται. Σε πολύ σπάνιες περιπτώσεις εάν υπάρχει τέτοια ανάγκη τότε θα πρέπει να λαμβάνονται τα πιο κάτω μέτρα:

* Μόνο εξουσιοδοτημένα αποσπώμενα μέσα φύλαξης δεδομένων μπορούν να χρησιμοποιούνται στα πληροφοριακά συστήματα και στις εγκαταστάσεις του [Όνομα Οργανισμού].
* Μόνο εξουσιοδοτημένο προσωπικό μπορεί να χρησιμοποιεί τα εξουσιοδοτημένα αποσπώμενα μέσα φύλαξης δεδομένων.
* Για την εξουσιοδότηση των φορητών μέσων φύλαξης, καταγράφεται και ακολουθείται διαδικασία. Όλες οι εξουσιοδοτήσεις πρέπει να είναι περιορισμένης χρονικής διάρκειας και πρέπει να αναθεωρούνται ανά τακτά χρονικά διαστήματα (τουλάχιστον ετησίως) και να τηρείται σχετικό μητρώο.
* Όλα τα αποσπόμενα μέσα φύλαξης που δίνονται στους εξουσιοδοτημένους χρήστες θα πρέπει να τηρούνται σε σχετικό μητρώο.
* Απαγορεύεται η χρήση προσωπικών αποσπώμενων μέσων φύλαξης δεδομένων στα πληροφοριακά συστήματα του[Όνομα Οργανισμού].
* Απαγορεύεται η χρήση εξουσιοδοτημένων αποσπώμενων μέσων φύλαξης δεδομένων για προσωπικό όφελος.
* Η αποθήκευση Εμπιστευτικών ή/και Εσωτερικής Χρήσης πληροφορίων δεν επιτρέπεται σε αποσπώμενα μέσα φύλαξης δεδομένων.
* Τα αποσπόμενα μέσα αποθήκευσης τύπου USB πρέπει να χρησιμοποιούν ισχυρούς μηχανισμούς κρυπτογράφησης (τουλάχιστον hardware-based 256-bit AES encryption) περιλαμβανομένης της διαδικασίας αποθήκευσης, on transit, της μετακίνησης κτλ.
* Περιττές αποθηκευμένες πληροφορίες, στα αποσπώμενα μέσα φύλαξης δεδομένων, πρέπει να διαγράφονται, σύμφωνα με την Πολιτική Διαχείρισης Στοιχείων Ενεργητικού.
* Τα αποσπώμενα μέσα φύλαξης δεδομένων δεν πρέπει να μένουν ποτέ αφύλακτα/ασυνόδευτα.
* Ο χρήστης των αποσπώμενων μέσων φύλαξης δεδομένων είναι υπεύθυνος για το αποσπώμενο μέσο φύλαξης καθώς και για την ακεραιότητα και διαθεσιμότητα της πληροφορίας που κατέχουν.
* Σε περίπτωση κλοπής ή απώλειας των αποσπώμενων μέσων φύλαξης δεδομένων, πρέπει να ενημερώνεται ο άμεσα προϊστάμενος του χρήστη, ο Υπεύθυνος Ασφάλειας Πληροφοριών του [Όνομα Οργανισμού], και ανάλογα με το περιεχόμενο του δύναται να ενεργοποιηθεί η Διαδικασία Συμβάντων και Περιστατικών (βλέπε Πολιτική Διαχείρισης Συμβάντων και Περιστατικών).

Η μη συμμόρφωση με την Πολιτική Αποδεκτής Χρήσης και τις οδηγίες που περιγράφονται στον παρόν έγγραφο, ή η κατάχρηση των συστημάτων του Οργανισμού αποτελεί σοβαρό πειθαρχικό παράπτωμα το οποίο μπορεί να επιφέρει απόλυση με ή χωρίς προειδοποίηση, ανάλογα με τη σοβαρότητα του γεγονότος.

# Αναθεώρηση

Τα έγγραφα σχετικά με την αποδεκτή χρήση πόρων θα πρέπει να επανεξετάζονται και να αναθεωρούνται τουλάχιστον ετησίως ή σε περίπτωση σημαντικών αλλαγών στο περιβάλλον του [Όνομα Οργανισμού] με στόχο να διασφαλίζεται ότι παραμένει επικαιροποιημένη, αποτελεσματική και ευθυγραμμισμένη με τις ανάγκες του οργανισμού, τυχόν νομικές/κανονιστικές απαιτήσεις και άλλες τεχνολογικές εξελίξεις όπως νέες αναδυόμενες απειλές κτλ.)

# Αναφορές

|  |  |  |  |
| --- | --- | --- | --- |
| **Κατηγορία** | **ID** | **Μέτρο** | **Στόχος Μέτρου** |
| Ασφάλεια Ανθρώπινων Πόρων | HRS6 | Συμφωνίες εργοδότησης και αποδεκτή χρήση | Να διασφαλιστεί ότι οι ευθύνες που αφορούν την ασφάλεια πληροφοριών και την αποδεκτή χρήση των στοιχείων ενεργητικού, ενσωματώνονται στις συμφωνίες εργοδότησης και στις διαδικασίες έναρξης απασχόλησης, για την επίτευξη υπευθυνότητας και ευαισθητοποίησης |
| Διαχείριση στοιχείων ενεργητικού | AM3 | Παρακολούθηση στοιχείων ενεργητικού | Να διασφαλιστεί ότι τα στοιχεία ενεργητικού είναι υπό παρακολούθηση για επιθέσεις, ανωμαλίες και απειλές κατά της ασφάλειας, προκειμένου να ενεργοποιηθούν οι διαδικασίες για την αντιμετώπιση συμβάντων και περιστατικών. |