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](#_Toc158630553)

[1. Σκοπός 4](#_Toc158630554)

[2. Ασφάλεια Πληροφοριακών Συστημάτων 4](#_Toc158630555)

[2.1. Γενικές Απαιτήσεις -Υποχρεώσεις 4](#_Toc158630556)

[2.2. Κωδικοί Πρόσβασης 5](#_Toc158630557)

[2.3. Ηλεκτρονικό Ταχυδρομείο 6](#_Toc158630558)

[2.4. Χρήση του διαδικτύου 7](#_Toc158630559)

[2.5. Προστασία από κακόβουλα λογισμικά 8](#_Toc158630560)

[2.6. Ασφάλεια Δικτύου 8](#_Toc158630561)

[2.7. Κινητά Συστήματα Πληροφορικής 8](#_Toc158630562)

[2.8. Εργασία εξ ’αποστάσεως 9](#_Toc158630563)

[3. Αποσπώμενα Μέσα Φύλαξης Δεδομένων 9](#_Toc158630564)

# Σκοπός

Το έγγραφο αυτό καθορίζει την Πολιτική Αποδεκτής Χρήσης του [Όνομα Οργανισμού] σε σχέση με την πρόσβαση στις πληροφορίες και στα συστήματα πληροφοριών του. Συγκεκριμένα:

Υπολογιστές, φορητοί υπολογιστές και φορητές συσκευές που ανήκουν στο [Όνομα Οργανισμού]

Λογαριασμοί ηλεκτρονικού ταχυδρομείου που εκδίδονται από το [Όνομα Οργανισμού] και πρόσβαση στην εταιρική ηλεκτρονική αλληλογραφία.

Το εσωτερικό δίκτυο του το [Όνομα Οργανισμού]

Πρόσβαση στο διαδίκτυο

Λογισμικό και εφαρμογές που παρέχονται από το [Όνομα Οργανισμού]

Ο [Όνομα Οργανισμού] έχει ως στόχο τη διεξαγωγή δραστηριοτήτων με επαγγελματικότητα, εφαρμόζοντας υψηλές προδιαγραφές για την παροχή 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.

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 συστήματα πληροφορικής.

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.

# Ασφάλεια Πληροφοριακών Συστημάτων

# Γενικές Απαιτήσεις -Υποχρεώσεις

Μη εξουσιοδοτημένη πρόσβαση: Απαγορεύεται σε χρήστες να έχουν πρόσβαση σε οποιαδήποτε συστήματα ή πόρους πληροφορικής στα οποία δεν έχουν δικαίωμα πρόσβασης.

Μη εξουσιοδοτημένη τροποποίηση: Απαγορεύεται σε χρήστες η τροποποίηση οποιουδήποτε συστήματος ή πόρους πληροφορικής του [Όνομα Οργανισμού] χωρίς τη ρητή άδεια του εκάστοτε ιδιοκτήτη.

Μη εξουσιοδοτημένη εγκατάσταση λογισμικού: Οι χρήστες απαγορεύεται να εγκαθιστούν οποιοδήποτε λογισμικό στα συστήματα ή τους πόρους πληροφορικής της [Όνομα Οργανισμού] χωρίς τη ρητή άδεια του τμήματος πληροφορικής του [Όνομα Οργανισμού].

Παράνομες δραστηριότητες: Απαγορεύεται στους χρήστες να χρησιμοποιούν τα συστήματα ή τους πόρους πληροφοριών για οποιαδήποτε παράνομη δραστηριότητα, όπως ενδεικτικά:

Πρόσβαση ή μετάδοση πορνογραφικού ή άλλου άσεμνου υλικού

Συμμετοχή σε παρενόχληση, εκφοβισμό ή εκφοβισμό στον κυβερνοχώρο

Απαγορεύεται η επίσκεψη σε ιστοσελίδες με παράνομο λογισμικό ή άλλο πειρατικό οπτικοακουστικό υλικό

Παραβίαση των νόμων περί πνευματικών δικαιωμάτων

Παραβίαση των νόμων περί προσωπικών δεδομένων

Συμμετοχή σε πειρατεία ή άλλη μη εξουσιοδοτημένη πρόσβαση σε συστήματα υπολογιστών

Απόπειρα διατάραξης ή ζημίας των συστημάτων ή πόρων πληροφορικής της [όνομα οργανισμού]

# Κωδικοί Πρόσβασης

Οι κωδικοί πρόσβασης αποτελούν κρίσιμο μέρος της ασφάλειας του Οργανισμού.

Θα πρέπει να :

* κρατούμε μυστικούς τους κωδικούς πρόσβασης
* αποφεύγουμε την τήρηση αρχείου (π.χ. εντύπων, αρχείων λογισμικού ή συσκευών χειρός) για τους κωδικούς πρόσβασης μας, εκτός αν μπορούμε να τους αποθηκεύσουμε με ασφάλεια, εφαρμόζοντας εγκριμένη μέθοδο αποθήκευσης
* αλλάζουμε τον κωδικό μας κάθε φορά που υπάρχει υπόνοια αυτός να γνωστοποιήθηκε
* αλλάζουμε τους κωδικούς πρόσβασης σε τακτικά χρονικά διαστήματα και να αποφύγουμε την επαναχρησιμοποίηση παλιών κωδικών πρόσβασης
* αλλάζουμε τους προσωρινούς κωδικούς πρόσβασης κατά την πρώτη σύνδεση
* μην περιλαμβάνουμε τους κωδικούς πρόσβασης μας σε οποιαδήποτε αυτοματοποιημένη διαδικασία σύνδεσης
* μην χρησιμοποιούμε τον ίδιο κωδικό πρόσβασης στα συστήματα του [Όνομα Οργανισμού], με αυτόν για πρόσβαση σε προσωπικούς μας λογαριασμούς π.χ. ηλεκτρονικό ταχυδρομείο, συνδρομές, τόπους κοινωνικής δικτύωσης
* μην αποστέλλονται κωδικοί πρόσβασης για τους νέους λογαριασμούς ηλεκτρονικά σε απομακρυσμένους χρήστες.
* μην μοιραζόμαστε τους προσωπικούς κωδικούς πρόσβασης μας με άλλα άτομα
* επιλέγουμε ποιοτικούς κωδικούς με επαρκές ελάχιστο μήκος, που να:
  + είναι εύκολο να θυμάστε
  + μην είναι βασισμένοι σε κάτι το οποίο κάποιος θα μπορούσε εύκολα να μαντέψει ή να αποκτήσει, χρησιμοποιώντας προσωπικές πληροφορίες, π.χ. ονόματα, αριθμούς τηλεφώνων, ημερομηνίες γέννησης
  + μην αποτελούνται από λέξεις οι οποίες περιλαμβάνονται σε λεξικά
  + μην αποτελούνται από πανομοιότυπους χαρακτήρες (δηλ. να είναι όλοι αριθμοί, ή όλα γράμματα)

# Ηλεκτρονικό Ταχυδρομείο

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

Οι κατευθυντήριες γραμμές/οδηγίες που περιέχονται στην παρούσα πολιτική ισχύουν τόσο για τα προσωπικά ηλεκτρονικά μηνύματα όσο και για τα ηλεκτρονικά μηνύματα του Οργανισμού. 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 δίνουμε ιδιαίτερη προσοχή στη συγγραφή ηλεκτρονικών μηνυμάτων και να εφαρμόζουμε τα ίδια πρότυπα και πρωτόκολλα όπως αυτά εφαρμόζονται στη γραπτή αλληλογραφία

Επιπρόσθετα, δεν πρέπει να γράφουμε οτιδήποτε στα μηνύματα μέσω ηλεκτρονικού ταχυδρομείου που θα μπορούσε να θέσει σε κίνδυνο την ακεραιότητα ή τη φήμη του [Όνομα Οργανισμού], ή τα οποία δεν μπορούμε ή δεν είμαστε έτοιμοι να δικαιολογήσουμε επαρκώς.

Ειδικότερα, να έχουμε υπόψη μας ότι τα μηνύματα ηλεκτρονικού ταχυδρομείου μπορούν εύκολα να οδηγήσουν σε παρεξηγήσεις και παραβάσεις. Ό,τι φαίνεται αθώο στον αποστολέα μπορεί να φαίνεται προσβλητικό στον αποδέκτη. Δεν πρέπει να γράφουμε οτιδήποτε σε ένα ηλεκτρονικό μήνυμα, το οποίο δεν θα είμασταν διατεθειμένοι να πούμε σε συνάντηση ή στο τηλέφωνο, ή να γράψουμε σε έγγραφο.

Δεν πρέπει να χρησιμοποιούμε το ηλεκτρονικό ταχυδρομείο του [Όνομα Οργανισμού] για να γράψουμε, να αποθηκεύσουμε, να αποστείλουμε, να προωθήσουμε και γενικά να μεταφέρουμε υλικό οποιασδήποτε από τις ακόλουθες κατηγορίες:

* Υλικό που 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 υλικό (συμπεριλαμβανομένου κάθε είδους πορνογραφίας)
* Υλικό το οποίο είναι αναληθές ή κακόβουλο, είτε αυτό αφορά μέλος του προσωπικού, είτε αφορά οποιονδήποτε εκτός του [Όνομα Οργανισμού]
* Ρατσιστικό ή σεξιστικό υλικό
* Οποιοδήποτε υλικό που έχει να κάνει με εκφοβισμό ή παρενόχληση (όπως π.χ. για το φύλο, συμπεριλαμβανομένης της σεξουαλικής προτίμησης, τη φυλή ή αναπηρία)
* Οποιοδήποτε υλικό θα μπορούσε αλλιώς να θεωρηθεί παράνομο.

Τέτοιες ενέργειες αποτελούν ανάρμοστη συμπεριφορά και θα μπορούσαν να οδηγήσουν σε απόλυση του υπαλλήλου σύμφωνα με τις πειθαρχικές διαδικασίες του Οργανισμού.

Επιπλέον, δεν πρέπει να:

* χρησιμοποιούμε τα συστήματα πληροφορικής του Οργανισμού για εμπορικούς σκοπούς οι οποίοι είτε δεν παρέχουν άμεσο όφελος στον [Όνομα Οργανισμού] είτε ανταγωνίζονται (άμεσα ή έμμεσα) τα συμφέροντα του, ενώ γενικά αποτελούν πραγματική ή φαινομενική σύγκρουση των συμφερόντων των υπαλλήλων και του [Όνομα Οργανισμού]
* διαβάζουμε, καταγράφουμε, αντιγράφουμε ή ακούμε μηνύματα και πληροφορίες που αποστέλλονται σε σύστημα πληροφορικής ενός άλλου ατόμου, χωρίς την προτέρα άδεια του.

Να θυμόμαστε ότι τα ηλεκτρονικά μηνύματα είναι μόνιμα και διαθέσιμα για μελλοντική αναφορά.

Τα ηλεκτρονικά μηνύματα μπορούν μελλοντικά να αποτελέσουν αντικείμενο μιας επίσημης διαδικασίας γνωστοποίησης. Δεν πρέπει να υποθέσουμε ότι αυτά έχουν εξαφανιστεί μόνο και μόνο επειδή έχουν διαγραφεί από το προσωπικό μας ηλεκτρονικό γραμματοκιβώτιο (inbox).

Με τη συνεχή αύξηση του όγκου των ηλεκτρονικών μηνυμάτων που λαμβάνονται θα πρέπει να τηρούνται κάποιες γενικές καλές πρακτικές:

* Να σκεφτόμαστε σε ποιους άλλους θα πρέπει να κοινοποιήσουμε την απάντησή μας σε κάποιο ηλεκτρονικό μήνυμα, ειδικά εάν έχει ήδη χρησιμοποιηθεί λίστα διανομής
* Να αποφεύγουμε το άνοιγμα μηνυμάτων junk/spam καθώς αυτά οδηγούν στην επιβεβαίωση της ταυτότητας μας και ενδεχομένως να προστεθούμε και σε άλλες λίστες τέτοιων μηνυμάτων.

# 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:

* Θα πρέπει να βεβαιωνόμαστε ότι η πηγή των δεδομένων είναι αξιόπιστη και αν είναι αναγκαίο να εξασφαλίσουμε επαλήθευση των πληροφοριών
* Θα πρέπει να βεβαιωνόμαστε ότι η λήψη πληροφοριών ή υλικού από ιστοσελίδες, δεν παραβιάζει τα δικαιώματα πνευματικής ιδιοκτησίας και ούτε επιφέρει μη εξουσιοδοτημένη δαπάνη στον [Όνομα Οργανισμού]
* Δεν πρέπει να επισκεπτόμαστε ιστοσελίδες, να κατεβάζουμε υλικό, ή να αποστέλλουμε πληροφορίες 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)
  + θα μπορούσε να θεωρηθεί παράνομο.

# Προστασία από κακόβουλα λογισμικά

Όλοι οι υπολογιστές και εξυπηρετητές με πρόσβαση στο δίκτυο του [Όνομα Οργανισμού] πρέπει να έχουν εγκατεστημένα τα κατάλληλα λογισμικά κατά των ιών και της υποκλοπής, τα οποία να είναι συνεχώς ενημερωμένα. Τα εν λόγω λογισμικά δεν πρέπει να απενεργοποιούνται.

Κάθε υπάλληλος ο οποίος επιχειρεί να απενεργοποιήσει, να ακυρώσει ή να παρακάμψει τα μέτρα ασφάλειας θα υπόκειται σε πιθανές πειθαρχικές κυρώσεις.

Κάθε συσκευή που πιστεύεται ότι έχει μολυνθεί από ιό, θα πρέπει να αποσυνδεθεί αμέσως από όλα τα δίκτυα του [Όνομα Οργανισμού]. Οι προσβεβλημένες από ιό συσκευές δεν πρέπει να επανασυνδεθούν στο δίκτυο έως ότου οι διαχειριστές από το [Αρμόδιο Τμήμα Πληροφορικής] επαληθεύσουν ότι ο ιός έχει αφαιρεθεί.

# Ασφάλεια Δικτύου

Η απρόσεκτη χρήση του διαδικτύου ή του ηλεκτρονικού ταχυδρομείου μπορεί να εκθέσει τα δίκτυα πληροφοριών του [Όνομα Οργανισμού] σε ένα ευρύ φάσμα κινδύνων που σχετίζονται με ιούς, spyware, 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 διαδικτύου και του ηλεκτρονικού ταχυδρομείου, το προσωπικό του [Όνομα Οργανισμού] φέρει την ευθύνη να δίνει συνεχώς τη δέουσα προσοχή στην ασφάλεια του δικτύου.

# Κινητά Συστήματα Πληροφορικής

Κατά τη χρήση κινητών συστημάτων πληροφορικής και συσκευών επικοινωνίας, π.χ. φορητοί υπολογιστές, κινητά τηλέφωνα, κ.α. πρέπει να δίνεται ιδιαίτερη προσοχή ώστε να διασφαλιστεί ότι οι πληροφορίες του Οργανισμού δεν είναι σε κίνδυνο.

Ιδιαίτερη προσοχή πρέπει να δίδεται κατά τη χρήση κινητών συστημάτων πληροφορικής σε δημόσιους χώρους, αίθουσες συνεδριάσεων και άλλες μη προστατευόμενες περιοχές εκτός των εγκαταστάσεων του Οργανισμού.

Τα υπο αναφορά συστήματα θα πρέπει να είναι κρυπτογραφημένα και να προστατεύονται για την αποφυγή της μη εξουσιοδοτημένης πρόσβασης ή αποκάλυψης των πληροφοριών που αποθηκεύονται σε αυτά (βλέπε Πολιτική Διαχείρισης Στοιχείων Ενεργητικού). Επίσης, θα πρέπει να προστατεύονται οι κινητές συσκευές, οι οποίες συνδέονται με τα δίκτυα του [Όνομα Οργανισμού].

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.

Αν η μεταφορά φορητών υπολογιστών δεν είναι απαραίτητη, τότε oι φορητοί υπολογιστές του [Όνομα Οργανισμού] πρέπει να κλειδώνονται με την αποχώρηση από το γραφείο. 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.

Οποιοιδήποτε κωδικοί πρόσβασης ή αριθμοί ΡΙΝ που χρησιμοποιούνται για την εξ’αποστάσεως πρόσβαση στα συστήματα του Οργανισμού, πρέπει να απομνημονεύονται και όχι να καταγράφονται. Κάθε εξοπλισμός ασφάλειας για απομακρυσμένη πρόσβαση πρέπει να φυλάσσεται χωριστά από τα συστήματα για την απομακρυσμένη πρόσβαση. Εάν ένας φορητός υπολογιστής κλαπεί, το [Αρμόδιο Τμήμα Πληροφορικής] θα πρέπει να ενημερωθούν το συντομότερο δυνατό.

# Εργασία εξ ’αποστάσεως

Στην περίπτωση που παρουσιαστεί μελλοντική απαίτηση για εργασία εξ’ αποστάσεως, χρειάζεται να παρθούν κατάλληλα μέτρα για προστασία του χώρου πρίν 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 Οργανισμού ή κατάχρηση των συστημάτων.

Οι εργασίες που πραγματοποιούνται εξ’ αποστάσεως χρειάζεται να εξουσιοδοτηθούν και να είναι ελεγμένες από τη Διεύθυνση. Επιπρόσθετα, χρειάζεται να διασφαλιστεί ότι υπάρχει η υποδομή για τις αναγκαίες διευθετήσεις για υποστήριξη αυτού του τρόπου εργασίας. Η εργασία από δημοσίους χώρους απαγορεύεται.

# Αποσπώμενα Μέσα Φύλαξης Δεδομένων

* Μόνο εξουσιοδοτημένα αποσπώμενα μέσα φύλαξης δεδομένων μπορούν να χρησιμοποιούνται στα πληροφοριακά συστήματα και στις εγκαταστάσεις του 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.
* Όλες οι εξουσιοδοτήσεις πρέπει να αναθεωρούνται ανά τακτά χρονικά διαστήματα (τουλάχιστον ετησίως)
* Όλες οι εξουσιοδοτήσεις πρέπει να τηρούνται σε 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 Οργανισμού.
* Απαγορεύεται η χρήση εξουσιοδοτημένων αποσπώμενων μέσων φύλαξης δεδομένων για προσωπικό όφελος.
* Η αποθήκευση Εμπιστευτικών ή/και Εσωτερικής Χρήσης πληροφορίων πρέπει να αποφεύγεται στα αποσπώμενα μέσα φύλαξης δεδομένων. Σε τέτοια περίπτωση πρέπει η πληροφορία να κρυπτογραφείται. (βλέπε Πολιτική Διαχείρισης Στοιχείων Ενεργητικού).
* Απαγορεύεται η αποθήκευση Εμπιστευτικών ή/και Εσωτερικής Χρήσης πληροφορίων σε μη κρυπτογραφημένα μέσα φύλαξης δεδομένων.
* Πρέπει να παρακολουθείται η χρήση αποσπώμενων μέσων και η μεταφορά πληροφοριών σε τέτοια μέσα.
* Τα αποσπόμενα μέσα αποθήκευσης τύπου USB πρέπει να χρησιμοποιούν ισχυρούς μηχανισμούς κρυπτογράφησης (τουλάχιστον hardware-based 256-bit AES encryption).
* 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.
* Τα αποσπώμενα μέσα φύλαξης δεδομένων πρέπει να τοποθετούνται σε ασφαλισμένα ντουλάπια (βλέπε Πολιτική Φυσικής Ασφάλειας).
* 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, και να ενεργοποιείται η Διαδικασία Περιστατικών Ασφάλειας (βλέπε Πολιτική Διαχείρισης Περιστατικών Ασφάλειας).