Όνομα Οργανισμού

Πολιτική Διαχείρισης Στοιχείων Ενεργητικού

|  |  |
| --- | --- |
| **Περιεχόμενο:** | Πολιτική Διαχείρισης Στοιχείων Ενεργητικού |
| **Δημιουργός:** |  |
| **Έκδοση:** | 1.0 |
| **Ημερομηνία Έκδοσης:** | ηη/μμ/χχχχ |
| **Εμπιστευτικότητα:** |  |
| **Ιδιοκτήτης:** |  |

Διανομή

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

Καταγραφή Τροποποιήσεων

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

Αναφορές

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

Υποστηρικτικό Υλικό

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

Ειδικό Λεξιλόγιο

Οι όροι και συντμήσεις ορίζονται πιο κάτω:

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

Πίνακας Περιεχομένων

[1. Σκοπός 5](#_Toc158623314)

[2. Απογραφή Στοιχείων Ενεργητικού 5](#_Toc158623315)

[3. Κατάλογος Καταγραφής Στοιχείων Ενεργητικού 6](#_Toc158623316)

[4. Ιδιοκτησία Στοιχείων Ενεργητικού 7](#_Toc158623317)

[5. Παρακολούθηση Στοιχείων Ενεργητικού 8](#_Toc158623318)

[5.1. Καθορισμός Παραμέτρων Παρακολούθησης 8](#_Toc158623319)

[6. Πρόληψη κινδύνου απώλειας δεδομένων και διαρροής δεδομένων 9](#_Toc158623320)

[7. Ασφάλεια εξοπλισμού εκτός εργασιακού περιβάλλοντος 9](#_Toc158623321)

[8. Ασφάλεια εξοπλισμού εντός εργασιακού περιβάλλοντος 10](#_Toc158623322)

[9. Ασφαλής απόσυρση ή επαναχρησιμοποίηση εξοπλισμού 10](#_Toc158623323)

[10. Αποδεκτή Χρήση Στοιχείων Ενεργητικού 10](#_Toc158623324)

[11. Διαβάθμιση Πληροφοριών 11](#_Toc158623325)

[11.1. Εντοπισμός και καταγραφή πληροφοριών 11](#_Toc158623326)

[11.2. Διαβάθμιση πληροφοριών 12](#_Toc158623327)

[12. Μεταφορές και ανταλλαγή πληροφοριών 13](#_Toc158623328)

[13. Ρόλοι και ευθύνες 13](#_Toc158623329)

[13.1. Ιδιοκτήτης Πληροφοριών 13](#_Toc158623330)

[13.2. Επιστάτης Δεδομένων 13](#_Toc158623331)

[14. Κύκλος Ζωής 14](#_Toc158623332)

[14.1. Διαγραφή ή Καταστροφή πληροφοριών 15](#_Toc158623333)

[14.2. Εφεδρικά Αντίγραφα Πληροφοριών 15](#_Toc158623334)

[15. Διευθέτηση Πληροφοριών 18](#_Toc158623335)

[16. Διαχείριση Διαθεσιμότητας 18](#_Toc158623336)

[17. Εφεδρεία και Ανάκτηση 20](#_Toc158623337)

[18. Κρυπτογράφηση 22](#_Toc158623338)

[18.1. Χρήση Κρυπτογράφησης 22](#_Toc158623339)

[18.2. Διαχείριση Δημοσίου Κλειδιού 22](#_Toc158623340)

[18.3. Ψηφιακές Υπογραφές 23](#_Toc158623341)

[18.4. Αποτροπή Αποποίησης Ευθύνης 24](#_Toc158623342)

[18.5. Υποδομή Δημόσιου Κλειδιού 24](#_Toc158623343)

[18.6. Κρίσιμα ή ευαίσθητα δεδομένα 24](#_Toc158623344)

[18.7. Εφαρμογή Κρυπτογράφησης 25](#_Toc158623345)

[19. Προβλέψεις σε Συμβάσεις με Τρίτα Μέρη: 25](#_Toc158623346)

# Σκοπός

Τα στοιχεία ενεργητικού θα πρέπει να προστατεύονται και να τυγχάνουν της κατάλληλης διαχείρισης. Τα στοιχεία ενεργητικού είναι περιουσιακά στοιχεία και πόροι ενός οργανισμού που έχουν δυνητική ή πραγματική αξία στον οργανισμό. Η αξία μπορεί να είναι χρηματοοικονομική ή μη χρηματοοικονομική και μπορεί να προέρχεται από τη δημιουργία εσόδων, τη μείωση του κόστους ή τον μετριασμό των κινδύνων. Ένας οργανισμός χρειάζεται να προστατεύσει τα στοιχεία αυτά από πιθανές απειλές και τρωτά σημεία καθώς είναι πολύτιμα - συχνά επειδή περιέχουν ευαίσθητα δεδομένα ή μπορεί να χρησιμοποιηθούν για την πρόσβαση σε τέτοιες πληροφορίες. Τα περιουσιακά στοιχεία μπορούν να ταξινομηθούν σε διάφορες κατηγορίες, όπως υλισμικό, λογισμικό, εγκαταστάσεις και προσωπικό, με βάση τα χαρακτηριστικά και την αξία τους.

Ο σκοπός της Πολιτική Διαχείρισης Στοιχείων Ενεργητικού είναι να καθορίσει τις κατευθυντήριες γραμμές για τη διατήρηση της κατάλληλης προστασίας των στοιχείων ενεργητικού του [Όνομα Οργανισμού].

Όλα τα πληροφοριακά στοιχεία ενεργητικού πρέπει να καταγράφονται σε σχετικό μητρώο και να έχουν ιδιοκτήτη. Ο ιδιοκτήτης είναι υπεύθυνος για τη διασφάλιση την προστασίας, εύρυθμης λειτουργίας, διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας των πληροφοριακών περιουσιακών αυτών στοιχείων.

Ο [Όνομα Οργανισμού] θα πρέπει να έχει θεσπίσει, εφαρμόζει και διατηρεί μέτρα ασφάλειας πληροφοριών για την προστασία πληροφοριών καθ’ όλη τη διάρκεια του κύκλου ζωής των πληροφοριών[βλέπε Πολιτική Ασφάλειας Πληροφοριών]. Κύκλος ζωής των πληροφοριών θεωρείται ως όλα τα στάδια που σχετίζονται με την επεξεργασία των πληροφοριών, ενώ η επεξεργασία αφορά κάθε πράξη, ή σειρά πράξεων, που πραγματοποιείται σε δεδομένα προσωπικού χαρακτήρα, ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, είτε με αυτοματοποιημένα μέσα είτε όχι, όπως η συλλογή, καταχώριση, οργάνωση, δομή, αποθήκευση, προσαρμογή ή μεταβολή, ανάκτηση, αναζήτηση, χρήση, κοινοποίηση με διαβίβαση, διάδοση ή κάθε άλλη μορφή διάθεσης, συσχέτιση ή συνδυασμός, περιορισμός, διαγραφή ή καταστροφή.

# Απογραφή Στοιχείων Ενεργητικού

* Όλα τα στοιχεία ενεργητικού πρέπει να ανιχνεύονται, να προσδιορίζονται και να απογράφονται.
* Αρχείο των στοιχείων ενεργητικού πρέπει να διατηρείται το οποίο πρέπει να περιλαμβάνει σχετικές πληροφορίες για το κάθε στοιχείο ενεργητικού. Επίσης πρέπει να περιλαμβάνει πληροφορίες σχετικές με την ανάκτηση του στοιχείου ενεργητικού σε περίπτωση της καταστροφής ή της αλλοίωσης ή και απώλειάς του.
* Όλα τα υλικά στοιχεία ενεργητικού πρέπει να έχουν τη δυνατότητα ταυτοποίησης με τα στοιχεία στο μητρώο όπου διατηρείται η απογραφή των πληροφοριακών στοιχείων ενεργητικού του [Όνομα Οργανισμού] (π.χ. το κάθε στοιχείο ενεργητικού πρέπει να περιλαμβάνει το Asset Code/Βarcode για γρήγορη ταυτοποίηση).
* Όλα τα υλικά στοιχεία ενεργητικού πρέπει να προσδιοριστούν με το επίπεδο κρισιμότητας.
* Όλα τα πληροφοριακά στοιχεία ενεργητικού πρέπει να διαβαθμιστούν ανάλογα
* Διατηρεί έναν κατάλογο καταγραφής των στοιχείων ενεργητικού, προκειμένου να διασφαλίσει ότι ο [Όνομα Οργανισμού] έχει σαφή, ακριβή και ενημερωμένη κατάσταση των στοιχείων.
* Ο κατάλογος προσδιορίζει τον ιδιοκτήτη των στοιχείων αυτών.
* Ο κατάλογος επίσης να επιτρέπει στον [Όνομα Οργανισμού] να παρακολουθεί όλα τα στοιχεία ενεργητικού για τα οποία θα πρέπει να εφαρμόζει και να διατηρεί μέτρα ασφάλειας πληροφοριών, τουλάχιστον με χειροκίνητο τρόπο.
* Ο [Όνομα Οργανισμού] πρέπει να συμπεριλαμβάνει την περιγραφή της αποδεκτής χρήσης, της λειτουργίας και της τοποθεσίας των στοιχείων στον κατάλογο των στοιχείων ενεργητικού, προκειμένου να υπάρχει πλήρης απογραφή των στοιχείων αυτών.
* Οι διαδικασίες θα πρέπει να καταγράφονται σχετικά με την απόκτηση και απομάκρυνση στοιχείων ενεργητικού να διενεργούνται με ad-hoc και σύμφωνα με τις γνώσεις του εμπλεκόμενου προσωπικού.
* Ο [Όνομα Οργανισμού] θα πρέπει να διατηρεί δυνατότητες παρακολούθησης των στοιχείων ενεργητικού, ώστε να είναι σε θέση να εντοπίζει ανωμαλίες σε σχέση με κανονικές συνθήκες(π.χ. τοποθεσία, χρήση) και/ή τη λειτουργία των στοιχείων αυτών. Όταν εντοπίζονται ανωμαλίες, θα πρέπει να ενεργοποιούνται διαδικασίες διαχείρισης συμβάντων και περιστατικών προκειμένου ο οργανισμός να είναι ανθεκτικός στην παρουσία ανωμαλιών. Τα αποτελέσματα της παρακολούθησης (logs) περιέχουν κατ’ ελάχιστο τις ακόλουθες πληροφορίες: ημερομηνία, ώρα, source address & destination address (όπου αυτό εφαρμόζεται), τύπος καταγραφής, και όποια άλλη πληροφορία μπορεί να δοθεί επιπλέον ως επεξήγηση.
* Ο [Όνομα Οργανισμού] θα πρέπει να προσδιορίσει το είδος της παρακολούθησης που είναι ενεργοποιημένο ανά στοιχείο ενεργητικού (π.χ. System, Security, Application κ.α.), την έκταση της παρακολούθησης σε επίπεδο γεγονότος (π.χ. types of events: audit success, audit failure, login success, object access success, warning, ….), το χρονικό διάστημα διατήρησης των σχετικών εγγραφών (π.χ. 3 μήνες) και την τοποθεσία αποθήκευσης (π.χ. στην συσκευή, σε syslog server, σε άλλο αποθηκευτικό μέσο κ.α.)

Η απογραφή στοιχείων ενεργητικού θα γίνεται μέσα στο Asset Based Risk Assessment Workbook.

# Κατάλογος Καταγραφής Στοιχείων Ενεργητικού

Ο [Όνομα Οργανισμού] καταρτίζει κατάλογο στοιχείων ενεργητικού, συστημάτων και διαδικασιών εντός του [Όνομα Οργανισμού] και καταγράφει τις εξαρτήσεις και αλληλεξαρτήσεις μεταξύ αυτών των στοιχείων ενεργητικού, των συστημάτων και των διαδικασιών με σκοπό τη σαφή αποτύπωση του πλαισίου / περιβάλλοντος στο οποίο θα πραγματοποιηθεί η εκτίμηση κινδύνου. Μια σαφής εικόνα του πλαισίου του [Όνομα Οργανισμού] θα επιτρέψει τον εντοπισμό των κινδύνων εντός του οργανισμού [RM2].

Η ύπαρξη ενός αναγνωρισμένου ιδιοκτήτη του καταλόγου διασφαλίζει την ορθή, συστηματική και ασφαλή διαχείριση των πληροφοριακών καταλόγων εντός του [Όνομα Οργανισμού]. Ένας ιδιοκτήτης καταλόγου πρέπει να :

* Να έχει καθορισμένες αρμοδιότητες και ευθύνες για την τήρηση, επικαιροποίηση και ασφάλεια των δεδομένων στον κατάλογο,
* Να ενημερώνεται για τις αλλαγές στις πολιτικές και διαδικασίες που αφορούν τη διαχείριση των πληροφοριακών καταλόγων,
* Να συνεργάζεται με άλλα τμήματα του οργανισμού, όπως το IT,
* Να εφαρμόζει μέτρα ασφαλείας για την προστασία του καταλόγου από ανεπιθύμητη πρόσβαση ή κακόβουλες ενέργειες,
* Να είναι καλά ενημερωμένος για τις βέλτιστες πρακτικές και τις εξελίξεις στον τομέα των πληροφοριακών καταλόγων.

Ο [Όνομα Οργανισμού] πρέπει να θεσπίσει, να εφαρμόζει και να διατηρεί έναν κατάλογο καταγραφής των στοιχείων ενεργητικού, προκειμένου να διασφαλίσει ότι ο οργανισμός έχει σαφή, ακριβή και ενημερωμένη κατάσταση των στοιχείων (π.χ. υλισμικό, λογισμικό, πληροφορίες) που διατηρεί. Ο κατάλογος προσδιορίζει τον ιδιοκτήτη των στοιχείων αυτών. Ο κατάλογος επίσης να επιτρέπει στον [Όνομα Οργανισμού] να παρακολουθεί όλα τα στοιχεία ενεργητικού για τα οποία θα πρέπει να εφαρμόζει και να διατηρεί μέτρα ασφάλειας πληροφοριών, τουλάχιστον με χειροκίνητο τρόπο [AM2]. Ο [Όνομα Οργανισμού] πρέπει να συμπεριλαμβάνει την περιγραφή της αποδεκτής χρήσης, της λειτουργίας και της τοποθεσίας των στοιχείων στον κατάλογο των στοιχείων ενεργητικού, προκειμένου να υπάρχει πλήρης απογραφή των στοιχείων αυτών [AM3].

# Ιδιοκτησία Στοιχείων Ενεργητικού

Οι πληροφορίες και τα συστήματα πληροφορικής του [Όνομα Οργανισμού] καταγράφονται σε κατάλογο και ορίζεται ιδιοκτήτης για το κάθε ένα. Ο εν λόγω κατάλογος επικαιροποιείται σε τακτά χρονικά διαστήματα και περιλαμβάνει

* την πληροφορία / σύστημα πληροφορικής,
* την ηλεκτρονική / φυσική τοποθεσία του
* τον ιδιοκτήτη
* το ενδεικνυόμενο επίπεδο ασφάλειας του,

διασφαλίζοντας με την εφαρμογή των προνοιών που αφορούν το κάθε επίπεδο, την αποτελεσματική προστασία της πληροφορίας / συστήματος.

Η καταγραφή της ιδιοκτησίας μίας πληροφορίας / ενός συστήματος συντείνει στη διατήρηση της κατάλληλης προστασίας της. Ο ιδιοκτήτης μπορεί να αναθέσει την παρακολούθηση του καταλόγου για επικαιροποίησή του, για την εφαρμογή των δικλείδων ασφαλείας καθώς και για την καταστροφή πληροφορίας / συστήματος αλλά παραμένει διοικητικά υπεύθυνος για την ορθή εφαρμογή των πιο πάνω καθ’ όλη τη διάρκεια της ζωής της πληροφορίας / του συστήματος.

# Παρακολούθηση Στοιχείων Ενεργητικού

Ο [Όνομα Οργανισμού] έχει θεσπίσει, εφαρμόζει και διατηρεί δυνατότητες παρακολούθησης των στοιχείων ενεργητικού (ορισμός του στόχου της παρακολούθησης και των στοιχείων που θα υπόκεινται σε παρακολούθηση), ώστε να είναι σε θέση να εντοπίζει ανωμαλίες σε σχέση με κανονικές συνθήκες (π.χ. τοποθεσία, χρήση) και/ή τη λειτουργία των στοιχείων αυτών (εφαρμογή αλγορίθμων και μηχανισμών παρακολούθησης για την ανίχνευση ανωμαλιών στα στοιχεία ενεργητικού). Όταν εντοπίζονται ανωμαλίες, θα πρέπει να ενεργοποιούνται διαδικασίες διαχείρισης συμβάντων και περιστατικών προκειμένου ο [Όνομα Οργανισμού] να είναι ανθεκτικός στην παρουσία ανωμαλιών (αυτοματοποιημένη ενεργοποίηση διαδικασίας διαχείρισης συμβάντων κατά τον εντοπισμό ανωμαλιών και δημιουργία ενός αποτελεσματικού συστήματος για την επεξεργασία και αντιμετώπιση τους). Τα αποτελέσματα της παρακολούθησης (logs) περιέχουν κατ’ ελάχιστο τις ακόλουθες πληροφορίες: ημερομηνία, ώρα, source address & destination address (όπου αυτό εφαρμόζεται), τύπος καταγραφής, καταγραφή πηγής (source) και προορισμού (destination) του συμβάντος και όποια άλλη πληροφορία μπορεί να δοθεί επιπλέον ως επεξήγηση.

# Καθορισμός Παραμέτρων Παρακολούθησης

Με αυτόν τον τρόπο, εξασφαλίζεται η αποτελεσματική παρακολούθηση, αντίδραση σε ανωμαλίες και την ασφάλεια των στοιχείων ενεργητικού του οργανισμού.

1. Είδος Παρακολούθησης:

Καθορισμός του είδους παρακολούθησης ανά στοιχείο ενεργητικού (π.χ., System, Security, Application).

Προσδιορισμός των συγκεκριμένων παραμέτρων παρακολούθησης για κάθε είδος (π.χ., συστημικά γεγονότα, ασφαλεία, εφαρμογές).

1. Έκταση Παρακολούθησης:

Καθορισμός της έκτασης της παρακολούθησης σε επίπεδο γεγονότος.

Καταγραφή διαφόρων τύπων γεγονότων (π.χ., audit success, audit failure, login success, object access success, warning).

1. Χρονικό Διάστημα Διατήρησης:

Καθορισμός του χρονικού διαστήματος διατήρησης των σχετικών εγγραφών.

Κατά προτίμηση, ορισμός συγκεκριμένου χρονικού διαστήματος (π.χ., 3 μήνες) για την αποθήκευση των logs.

1. Τοποθεσία Αποθήκευσης:

Καθορισμός της τοποθεσίας αποθήκευσης των logs.

Επιλογή ανάμεσα σε ενσωματωμένη αποθήκευση στη συσκευή, αποθήκευση σε syslog server, ή άλλο αποθηκευτικό μέσο.

1. Διαχείριση Παραμέτρων:

Υλοποίηση διασφαλίζοντας ότι οι παράμετροι παρακολούθησης είναι ενημερωμένοι και ανταποκρίνονται στις ανάγκες του οργανισμού.

Ευελιξία για προσαρμογή των παραμέτρων σύμφωνα με ενδεχόμενες αλλαγές στις απαιτήσεις ασφάλειας ή στην εκτίμηση του χρόνου διατήρησης.

# Πρόληψη κινδύνου απώλειας δεδομένων και διαρροής δεδομένων

Ο [Όνομα Οργανισμού] έχει θεσπίσει, εφαρμόζει και διατηρεί εύλογα μέτρα για τη μείωση του κινδύνου απώλειας δεδομένων και διαρροής δεδομένων, λαμβάνοντας τα κατάλληλα τεχνικά και οργανωτικά μέτρα για πρόληψη. Τα μέτρα πρόληψης, απώλειας ή διαρροής δεδομένων θα πρέπει να λαμβάνουν υπόψη εξωτερικούς και εσωτερικούς φορείς απειλής που θα μπορούσαν δυνητικά να αποκαλύψουν διαβαθμισμένες ή ευαίσθητες πληροφορίες. Θα πρέπει να εφαρμόζονται επαρκή μέτρα ελέγχου πρόσβασης για διεπαφή με τα μέτρα πρόληψης για την απώλεια δεδομένων και διαρροή δεδομένων. Οι πολιτικές για την ανταλλαγή και κοινοποίηση δεδομένων θα πρέπει να είναι βάσει του ρόλου του χρήστη, όπως ορίζεται στο [IAM1]. Να εφαρμοστούν μέτρα διαχείρισης ταυτότητας και πρόσβασης με βάση το **ρόλο**, με σκοπό να παρέχουν τεχνικά και οργανωτικά μέσα για την επιβολή της αρχής του ελάχιστου προνομίου και να διαχειρίζονται αντίστοιχα τους προνομιούχους χρήστες. Ο έλεγχος πρόσβασης βάσει ρόλου θα πρέπει να διασφαλίζει ότι χορηγούνται επαρκείς άδειες σε χρήστες με βάση τις αρμοδιότητες τους που συνδέονται με αντίστοιχους ρόλους. Κατά τον καθορισμό των μέτρων πρόληψης για την απώλεια και τη διαρροή δεδομένων, ο οργανισμός θα πρέπει να εξετάζει την ταξινόμηση, την προστασία και την παρακολούθηση των πληροφοριών. Τα μέτρα πρόληψης, απώλειας ή διαρροής δεδομένων θα πρέπει να λαμβάνουν υπόψη εξωτερικούς και εσωτερικούς φορείς απειλής που θα μπορούσαν δυνητικά να αποκαλύψουν διαβαθμισμένες ή ευαίσθητες πληροφορίες. Θα πρέπει να εφαρμόζονται επαρκή μέτρα ελέγχου πρόσβασης για διεπαφή με τα μέτρα πρόληψης για την απώλεια δεδομένων και διαρροή δεδομένων [DS5].

# Ασφάλεια εξοπλισμού εκτός εργασιακού περιβάλλοντος

Εξοπλισμός επεξεργασίας πληροφοριών μπορεί να είναι οποιασδήποτε μορφής υπολογιστής, κινητό τηλέφωνο ή οτιδήποτε άλλο χρησιμοποιείται για εργασία εκτός του συνήθους εργασιακού περιβάλλοντος του [Όνομα Οργανισμού]. Η χρήση τέτοιου εξοπλισμού είναι απαραίτητο να γίνεται κατόπιν συναίνεσης του αρμόδιου Προϊσταμένου. Για την σωστή χρήση εξοπλισμού εκτός εργασιακού περιβάλλοντος βλέπε Πολιτική Αποδεκτής Χρήσης.

Σε αυτές τις περιπτώσεις, καθορίζονται συγκεκριμένα μέτρα για ασφαλή εργασία π.χ. η ανάγκη χρήσης χαρτοκοπτικού μηχανήματος για καταστροφή εγγράφων, κρυπτογράφηση, των δεδομένων, εφαρμογή της πολιτικής καθαρού γραφείου ή οποιαδήποτε άλλα μέτρα συστήνονται.

Διενεργείται επίσης επαρκής ασφάλιση του εξοπλισμού για την προστασία του, όπου κρίνεται αναγκαίο.

Ο υπάλληλος είναι απαραίτητο να λάβει όλα τα εύλογα μέτρα για την προστασία του εξοπλισμού του Οργανισμού όταν αυτός βρίσκεται εκτός του [Όνομα Οργανισμού], εφόσον ο εξοπλισμός δύναται να είναι ψηλού κόστους και να περιέχει ευαίσθητες πληροφορίες και προσωπικά δεδομένα.

* Κατά τη διάρκεια ταξιδιού, ο εξοπλισμός δεν πρέπει να παραμένει αφύλακτος σε δημόσιους χώρους. Οι φορητοί υπολογιστές χρειάζεται να θεωρούνται χειραποσκευές ώστε να τις έχετε πάντοτε μαζί σας και να προστατεύονται με κρυπτογράφηση.
* Εξειδικευμένος εξοπλισμός χρειάζεται να μεταφέρεται με την κατάλληλη θήκη του καθώς και να λαμβάνεται υπόψη οποιαδήποτε υπόδειξη του κατασκευαστή.

# Ασφάλεια εξοπλισμού εντός εργασιακού περιβάλλοντος

Κατ΄ ελάχιστο ο εξοπλισμός που βρίσκεται στον [Όνομα Οργανισμού] διαθέτει εφεδρείες σε σχέση με την ενέργεια, την χωρητικότητα, το δίκτυο και τον τρόπο διασύνδεσης. Δεν υπάρχει κρίσιμος εξοπλισμός που δεν έχει εφεδρικό εντός του ίδιου χώρου σε ενεργή ή και ανενεργή λειτουργία. Υπάρχει εξοπλισμός σε δευτερεύον σημείο, ο οποίος έχει σχετικά μελετηθεί ώστε να μπορεί να χρησιμοποιηθεί για να ανακάμψουν οι βασικές δραστηριότητες του [Όνομα Οργανισμού] ενός συγκεκριμένου χρονικού διαστήματος και σε συγκεκριμένο επίπεδο.

# Ασφαλής απόσυρση ή επαναχρησιμοποίηση εξοπλισμού

Εξοπλισμός του [Όνομα Οργανισμού] ο οποίος περιέχει ευαίσθητες πληροφορίες, προσωπικά δεδομένα ή / και άδειες χρήσης λογισμικού είναι απαραίτητο να ελέγχεται πριν την απόσυρση του ότι αυτά έχουν αφαιρεθεί με ασφαλή τρόπο.

Η απόφαση για επιδιόρθωση ή απόσυρση κατεστραμμένου εξοπλισμού ο οποίος περιέχει διαβαθμισμένες πληροφορίες και ευαίσθητα δεδομένα είναι απαραίτητο να αξιολογείται ως προς τον κίνδυνο για την ασφάλεια των πληροφοριών.

# Αποδεκτή Χρήση Στοιχείων Ενεργητικού

Προσωπικό, προμηθευτές, και τρίτοι οι οποίοι είναι εξουσιοδοτημένοι να χρησιμοποιούν ή και να διαχειρίζονται το στοιχείο ενεργητικού, πρέπει να συμμορφώνονται με την Πολιτική Αποδεκτής Χρήσης, αλλά και γενικότερα με τις Πολιτικές του [Όνομα Οργανισμού] σχετικά με την Ασφάλεια Πληροφοριών*.*

Η μη εξουσιοδοτημένη ή/και παράνομη χρήση του οποιουδήποτε στοιχείου ενεργητικού του [Όνομα Οργανισμού] μπορεί να οδηγήσει σε λήψη νομικών μέτρων ενάντια στους μη εξουσιοδοτημένους χρήστες.

Ο [Όνομα Οργανισμού] δεν θα υπερασπίσει, ή/και δεν θα υποστηρίξει, οποιοδήποτε χρήστη χρησιμοποιήσει οποιοδήποτε στοιχείο ενεργητικού του [Όνομα Οργανισμού] για κακόβουλο ή/και παράνομο λόγο. Ο [Όνομα Οργανισμού] τηρεί αντίγραφα ασφαλείας που καλύπτουν το σύνολο του ενιαίου καταλόγου στοιχείων ενεργητικού, συστημάτων και διαδικασιών εντός του οργανισμού. Πρέπει να ορίζεται ένας αναγνωρισμένος υπεύθυνος για την λειτουργία και τήρηση των αντιγράφων ασφαλείας. Αυτός ο υπεύθυνος πρέπει να διασφαλίζει την τακτική εκτέλεση αντιγράφων ασφαλείας, την αποθήκευσή τους σε ασφαλή τοποθεσία, και τη δοκιμή των διαδικασιών ανάκτησης.

Οι διαδικασίες εφεδρικών αντιγράφων και ανάκτησης δεδομένων δοκιμάζονται επαρκώς και συχνά. Αυτό εξασφαλίζει ότι τα αντίγραφα ασφαλείας είναι προσβάσιμα και ότι οι διαδικασίες ανάκτησης λειτουργούν ορθά, ενισχύοντας την αξιοπιστία τους σε πραγματικές συνθήκες.

Προκειμένου να διασφαλίζεται η ορθή και αξιόπιστη λειτουργία όλων των υποστηρικτικών διαδικασιών και συστημάτων και τα αντίγραφα ασφαλείας πρέπει να λαμβάνουν το σύνολο της πληροφορίας ή τις αλλαγές της σε ημερήσια βάση τουλάχιστον. Αυτό εξασφαλίζει ότι οποιεσδήποτε αλλαγές στα δεδομένα καταγράφονται και αντιγράφονται αμέσως.

# Διαβάθμιση Πληροφοριών

Ο [Όνομα Οργανισμού] διαχειρίζεται όλα τα δεδομένα (ηλεκτρονικά η/και έντυπα) για τα οποία έχει ευθύνη με ασφάλεια, αξιοπιστία και ακρίβεια. Τα εν λόγω δεδομένα θα πρέπει να είναι πάντα διαθέσιμα σε εξουσιοδοτημένους χρήστες μόνο. Με βάση την κρισιμότητα τους, την ευαισθησία τους και την επικινδυνότητα τους, τα δεδομένα αυτά θα πρέπει να τυγχάνουν των κατάλληλων μέτρων ασφαλείας.

Για την αποτελεσματική διαχείριση των πληροφοριών ο [Όνομα Οργανισμού] έχει καθορίσει διαδικασία που να περιλαμβάνει στο ελάχιστο τα πιο κάτω στάδια:

1. Εντοπισμός και καταγραφή πληροφοριών
2. Διαβάθμιση πληροφοριών
3. Σήμανση πληροφορίας
4. Χειρισμός πληροφοριών

# Εντοπισμός και καταγραφή πληροφοριών

Το πρώτο στάδιο για την αποτελεσματική διαχείριση πληροφοριών είναι η αναγνώριση όλων των πληροφοριών. Συνεπώς, ο [Όνομα Οργανισμού] πρέπει να τηρεί ένα κεντροποιημένο αρχείο πληροφοριών (συστήνεται η χρήση εξειδικευμένου λογισμικού όπως odoo, NetSuite, Oracle ERP Cloud, SYSPRO, SAP Business One, ManageEngine κ.α.). Η κάθε επιχειρησιακή μονάδα (Ιδιοκτήτης Πληροφοριών) έχει την ευθύνη για την καταγραφή, διατήρηση και διαχείριση των δεδομένων του τομέα αρμοδιότητας και εμπειρογνωμοσύνης της. Ο κάθε ιδιοκτήτης πληροφοριών πρέπει να αναθεωρεί και να επικαιροποιεί το αρχείο πληροφοριών [ορίστε χρονικό διάστημα].

Το κεντροποιημένο αρχείο πληροφοριών, πρέπει να περιλαμβάνει σχετική περιγραφή για την κάθε πληροφορία. Επίσης πρέπει να περιλαμβάνει λεπτομέρειες σχετικές με την ανάκτηση του στοιχείου ενεργητικού σε περίπτωση της καταστροφής ή της αλλοίωσης ή/και απώλειάς του.

# Διαβάθμιση πληροφοριών

Η διαβάθμιση της πληροφορίας πρέπει να γίνει βάσει της αξίας της, το βαθμό ευαισθησίας της, την κρισιμότητά της για τον [Όνομα Οργανισμού] και τις νομικές απαιτήσεις που διέπουν την επεξεργασία της και την κατηγορία(εσωτερική και δημόσια).

1. Εσωτερικές Πληροφορίες:

Αυτές είναι πληροφορίες που περιορίζονται στον εσωτερικό κύκλο του οργανισμού.

Συνήθως πρόκειται για πληροφορίες που αφορούν τη λειτουργία, τη διαχείριση, τους εργαζομένους, τις οικονομικές δραστηριότητες και άλλες εσωτερικές λεπτομέρειες του οργανισμού.

Οι πληροφορίες αυτές είναι συχνά ευαίσθητες και απαιτούν προστασία από ανεπιθύμητη πρόσβαση.

1. Δημόσιες Πληροφορίες:

Αυτές είναι πληροφορίες που είναι διαθέσιμες για το κοινό.

Συμπεριλαμβάνουν πληροφορίες που ο οργανισμός είναι υποχρεωμένος να δημοσιοποιεί σύμφωνα με τους νόμους και τους κανονισμούς.

Μπορεί να περιλαμβάνουν δημόσιες ανακοινώσεις, δημόσια έγγραφα, πληροφορίες σχετικές με προϊόντα και υπηρεσίες κ.λπ.

Η διαβάθμιση και οι σχετιζόμενοι έλεγχοι προστασίας της πληροφορίας πρέπει να βασίζονται στις επιχειρησιακές ανάγκες για ανταλλαγή ή περιορισμό της πληροφορίας και τις επιπτώσεις που σχετίζονται με αυτές. Οι οδηγίες περιλαμβάνουν συμβάσεις για την αρχική διαβάθμιση καθώς και την τακτική αναθεώρηση αυτής, σύμφωνα με κάποια προκαθορισμένη πολιτική ελέγχου πρόσβασης. Είναι ευθύνη του «ιδιοκτήτη» να ορίζει το βαθμό διαβάθμισής και να το επαναξιολογεί τακτικά, για να διασφαλίζει ότι είναι ενημερωμένο και στο κατάλληλο επίπεδο.

Συνοπτικά, βλέπε πιο κάτω τις διαβαθμίσεις και τις σημάνσεις που πρέπει να χρησιμοποιούνται στον [Όνομα Οργανισμού]:

* Διαβάθμιση 1
* Διαβάθμιση 2
* Διαβάθμιση 3
* …

Όσον αφορά την ιδιωτικότητα της πληροφορίας, σε περίπτωση που οι πληροφορίες περιέχουν Δεδομένα Προσωπικού Χαρακτήρα, πρέπει να τυγχάνουν επιπρόσθετου διαχωρισμού (δηλαδή πρέπει να φέρουν επιπρόσθετη σήμανση).

Σημ.: Νοείται ότι για τα έγγραφα και πληροφορίες που διαβαθμίζονται βάσει τον περί Κανόνων Ασφαλείας Διαβαθμισμένων Πληροφοριών, Εγγράφων και Υλικού και για Συναφή Θέματα Νόμο του 2021 (84(I)/2021), θα ισχύουν οι πρόνοιες του εν λόγω Νόμου και Διαταγμάτων που εκδίδονται δυνάμει αυτού.

# Μεταφορές και ανταλλαγή πληροφοριών

Να εφαρμοστούν επαρκή μέτρα στο πλαίσιο της διαβίβασης και ανταλλαγής πληροφοριών εσωτερικά ή με τρίτα μέρη, προκειμένου να διασφαλιστεί η ασφαλής μεταφορά δεδομένων.

Ο [Όνομα Οργανισμού] πρέπει να θεσπίσει, να εφαρμόζει και να διατηρεί διαδικασίες μεταφοράς και ανταλλαγής πληροφοριών προκειμένου να διασφαλίζεται η προστασία των πληροφοριών κατά τη μεταφορά ή την ανταλλαγή τους εσωτερικά ή με τρίτα μέρη. Η μεταφορά και ανταλλαγή πληροφοριών θα πρέπει να λαμβάνει υπόψη τις κανονιστικές και νομοθετικές απαιτήσεις, όπως ορίζονται στο [GOV2], για παράδειγμα κατά την επεξεργασία πληροφοριών στο πλαίσιο διεθνών διαβιβάσεων δεδομένων. Ειδικά για τα κρίσιμα ή ευαίσθητα δεδομένα, υλοποιείται κρυπτογράφηση κατά την ανταλλαγή ή μεταφορά. Παραδείγματα τέτοιας υλοποίησης περιλαμβάνει (Transport Layer Security (TLS) and Open Secure Shell (OpenSSH) κα.). Βλέπε παράγραφο Προβλέψεις σε Συμβάσεις με Τρίτα Μέρη

# Ρόλοι και ευθύνες

Τα μέτρα ασφάλειας της κάθε κατηγορίας είναι διαφορετικά. Τα μέτρα αυτά πρέπει να καθορίζονται από τους «Ιδιοκτήτες της Πληροφορίας» σε συνεργασία με τους «Διαχειριστές Δεδομένων» και τους «Επιστάτες Πληροφορίας».

# Ιδιοκτήτης Πληροφοριών

Ο ιδιοκτήτης πληροφορίας είναι υπεύθυνος:

* Να ενημερώνει τακτικά το μητρώο ροών πληροφοριών για τις οποίες είναι υπεύθυνος.
* Να καθορίζει τη διαβάθμιση και την κλάση της πληροφορίας.
* Να αναθεωρεί τη διαβάθμιση των πληροφοριών του σε τακτά χρονικά διαστήματα.
* Να ενημερώνει και να ενημερώνεται από τον επιστάτη των δεδομένων για τα μέτρα ασφάλειας (φύλαξη, διακίνηση, μετάδοση, διάθεση και διαθεσιμότητα).
* Να αναλαμβάνει τη διαχείριση των όποιων έργων αφορούν σε διορθωτικά μέτρα που σχετίζονται με τη ασφάλεια των δεδομένων του

# Επιστάτης Δεδομένων

Ο επιστάτης δεδομένων είναι υπεύθυνος να:

* παρέχει μια ασφαλή υποδομή που να διασφαλίζει την ακεραιότητα, αξιοπιστία και εμπιστευτικότητα και διαθεσιμότητα της πληροφορίας.
* παρέχει τις κατάλληλες υπηρεσίες εφεδρείας και ανάκτησης των πληροφοριών ούτως ώστε οι πληροφορίες αυτές να είναι διαθέσιμες σε περίπτωση καταστροφής ή/και δυσλειτουργίας του συστήματος.
* παρέχει μια ασφαλή υποδομή για την ασφάλεια των πληροφοριών από μη εξουσιοδοτημένα πρόσωπα.

# Κύκλος Ζωής

Πρέπει να υπάρχει μια καταγεγραμμένη διαδικασία η οποία περιγράφει τον τρόπο με τον οποίο διαχειρίζονται τα στοιχεία ενεργητικού κατά τη διάρκεια του κύκλου ζωής τους. Η συγκεκριμένη διαδικασία περιλαμβάνει ενέργειες που διενεργούνται από σχετικά εξουσιοδοτημένους ρόλους για την: προμήθεια(ορίζονται οι κατηγορίες ενεργητικού και οι απαιτήσεις ασφάλειας πληροφοριών), την εγκατάσταση (καθορίζονται οι απαραίτητες προετοιμασίες για την εγκατάσταση και πραγματοποιείται η επαλήθευσή τους), τη συντήρηση (καθορίζεται το πρόγραμμα συντήρησης για το ενεργητικό, Περιλαμβάνονται περιοδικοί έλεγχοι και ενημερώσεις για την ασφάλεια, εφαρμόζονται τακτικές ενημερώσεις λογισμικού και αναβαθμίσεις εξοπλισμού, βεβαιώνεται η συμβατότητά τους με τις πολιτικές ασφαλείας, παρακολουθούνται συνεχώς οι ενδείξεις προβλημάτων και η άμεση επίλυσή τους) και τη διάθεση (πραγματοποιείται καταγραφή των δεδομένων και αποτελεσμάτων πριν από τη διάθεση). Στα πλαίσια της διαδικασίας περιλαμβάνονται και στοιχεία ασφάλειας πληροφοριών ώστε να διασφαλίζεται ότι η ασφάλεια των πληροφοριών είναι αναπόσπαστο κομμάτι αυτού του κύκλου ζωής, δηλαδή την προμήθεια, την εγκατάσταση, τη συντήρηση και τη διάθεση.

Η διαχείριση του κύκλου ζωής των πληροφοριών, όπως περιγράφεται στο μέτρο [DS1], αποτελεί μέρος του σχεδίου διαχείρισης του κύκλου ζωής των στοιχείων ενεργητικού. H διαδικασία διαχείρισης του κύκλου ζωής των στοιχείων ενεργητικού πρέπει να περιγράφει όλες τις επιμέρους διαδικασίες για τον χειρισμό των πληροφοριών σύμφωνα με την πολιτική ταξινόμησης και επισήμανσης των δεδομένων, όπως περιγράφεται στο μέτρο [DS2], σύμφωνα με την εμπιστευτικότητα και την ευαισθησία τους. Εξετάζεται το ενδεχόμενο εφαρμογής συστημάτων ταξινόμησης και επισήμανσης με βάση τις διεθνείς και βιομηχανικές βέλτιστες πρακτικές, όπως το πρωτόκολλο «Traffic Light Protocol -TLP». Τουλάχιστον, ο οργανισμός θα πρέπει να γίνεται διάκριση μεταξύ των δημόσιων, ιδιωτικών και διαβαθμισμένων πληροφοριών.

Αλλαγές στα στοιχεία ενεργητικού γίνονται σύμφωνα με την διαδικασία διαχείρισης αλλαγών [CM1], για τον έλεγχο και τη διαχείριση αλλαγών σε συστήματα, εφαρμογές και άλλα υποστηρικτικά στοιχεία ενεργητικού στο πλαίσιο της επεξεργασίας πληροφοριών. Κατά τον καθορισμό της διαδικασίας διαχείρισης αλλαγών, ο οργανισμός πρέπει να προνοεί αιτήσεις αλλαγής, προκειμένου να λαμβάνονται υπόψη οι αλλαγές που ζητούνται από τους συμμετέχοντες. Η διαδικασία διαχείρισης αλλαγών θα πρέπει να επιτρέπει στον οργανισμό να αξιολογεί τους κινδύνους στο πλαίσιο αιτημάτων αλλαγών και να σχεδιάζει αλλαγές λαμβάνοντας υπόψη κατάλληλα μέτρα ασφάλειας. Η διαδικασία διαχείρισης αλλαγών θα πρέπει να περιλαμβάνει την προετοιμασία και την επαλήθευση των αλλαγών.

Στα πλαίσια του σχεδίου περιγράφονται και τα κριτήρια που χρησιμοποιεί ο [Όνομα Οργανισμού] προκειμένου να κατανέμει τους πόρους σε κατηγορίες κρισιμότητας. Προδιαγραφές ασφαλείας, κατάλληλες για την επικείμενη χρήση του στοιχείου ενεργητικού προδιαγράφονται πριν την προμήθεια.

# Διαγραφή ή Καταστροφή πληροφοριών

1. Τα παρακάτω μέτρα που προτείνονται είναι συνήθως αποτελεσματικά για την ασφαλή καταστροφή πληροφοριών, είτε πρόκειται για ψηφιακά είτε φυσικά αντικείμενα.Multiple Passes of Software-Based Overwriting (Πολλαπλές Επαναγραφές Με Επικείμενο Λογισμικό):

Η διαδικασία αυτή περιλαμβάνει τον επαναγραφή επαναλαμβανόμενων προτύπων δεδομένων σε επαναχρησιμοποιούμενα μέσα αποθήκευσης.

Σκοπός είναι η εξασφάλιση ότι τα προηγούμενα δεδομένα δεν μπορούν να ανακτηθούν εύκολα με εργαλεία ανάκτησης δεδομένων.

1. Cross Cut Shredding (Ανακοπή με Διασταυρούμενα Κομμάτια):

Αναφέρεται στη διαδικασία κοπής των εγγράφων σε μικρά κομμάτια με διασταυρούμενες γραμμές.

Αυτό εμποδίζει την ανακατασκευή των εγγράφων και προσφέρει προστασία από την ανεπιθύμητη πρόσβαση σε ευαίσθητες πληροφορίες.

# Εφεδρικά Αντίγραφα Πληροφοριών

1. Σύμφωνα με τον Κανονισμό 389/2020, ο [Όνομα Οργανισμού] θεσπίζει, εφαρμόζει και διατηρεί διαδικασίες εφεδρικών αντιγράφων και ανάκτησης δεδομένων, προκειμένου να διασφαλίζεται η έγκαιρη και αποτελεσματική αποκατάσταση δεδομένων μετά την ύπαρξη ενός συμβάντος ή περιστατικού, ή κατόπιν αιτήματος. Οι διαδικασίες εφεδρικών αντιγράφων και ανάκτησης δεδομένων θα πρέπει να δοκιμάζονται επαρκώς και συχνά, προκειμένου να διασφαλίζεται η ορθή και αξιόπιστη λειτουργία όλων των υποστηρικτικών διαδικασιών και συστημάτων. Τα συστήματα και οι υποδομές υποστήριξης, που επιτρέπουν την εφεδρεία και την αποκατάσταση δεδομένων, θα πρέπει να είναι γεωγραφικά διεσπαρμένες (αποθήκευση σε άλλη τοποθεσία) προκειμένου να προστατεύονται από φυσικούς κινδύνους ασφάλειας
2. Καταγραφή Εξοπλισμού:

Καταγραφή όλου του εξοπλισμού που χρησιμοποιείται για την παροχή επιχειρησιακών υπηρεσιών.

Κατηγοριοποίηση του εξοπλισμού βάσει της κρισιμότητας του για την συνέχεια των επιχειρησιακών δραστηριοτήτων.

1. Εφεδρικά Αντίγραφα:

Δημιουργία εφεδρικών αντιγράφων για όλες τις κρίσιμες πληροφορίες και δεδομένα.

Αυτόματη εκτέλεση περιοδικών αντιγράφων για εξασφάλιση συνεχούς ενημέρωσης.

1. Εφεδρικός Εξοπλισμός:

Κάθε κρίσιμη συσκευή έχει εφεδρική συσκευή είτε εντός του ίδιου χώρου είτε σε δευτερεύοντα σημείο.

Η εφεδρική συσκευή είναι σχεδιασμένη να αναλαμβάνει τις λειτουργίες της πρωταρχικής σε περίπτωση αποτυχίας.

1. Παρακολούθηση και Συντήρηση:

Συστηματική παρακολούθηση της κατάστασης του εφεδρικού εξοπλισμού.

Καθορισμός συχνότητας επιθεωρήσεων και συντηρήσεων.

1. Συνεχής Βελτίωση:

Ανάλυση αποτυχιών και ανακαλύψεων κατά τις δοκιμές και την παρακολούθηση.

Εφαρμογή βελτιώσεων στη διαδικασία διαχείρισης διαθεσιμότητας

# Διευθέτηση Πληροφοριών

Ευαίσθητες και εμπιστευτικές πληροφορίες θα πρέπει να καταστρέφονται όταν δεν είναι πλέον απαραίτητες σύμφωνα με την παρούσα Πολιτικήόπως καθορίζεται από τον [Όνομα Οργανισμού]. Βάσει της διαβάθμισης της κάθε πληροφορίας οι μέθοδοι καταστροφής διαφοροποιούνται. Ο [Όνομα Οργανισμού] θα πρέπει να ορίσει μια περίοδο διατήρησης των δεδομένων για όλες τις κατηγορίες δεδομένων και εφαρμόζει τις σχετικές προβλέψεις.

* Όλες οι πληροφορίες πρέπει να είναι διαβαθμισμένες σύμφωνα με τη παρούσα Πολιτική
* Τα ηλεκτρονικά μέσα αποθήκευσης και το τυπωμένο ή χειρόγραφο υλικό πρέπει να καταστρέφονται όταν δεν είναι πλέον απαραίτητα.
* Τα μέσα αυτά πρέπει να διευθετούνται με ασφαλή και σίγουρο τρόπο όταν δεν είναι πλέον απαραίτητα.
* Όλες οι πληροφορίες πρέπει να καταστρέφονται ανεξαρτήτως του μέσου στο οποίο καταγράφηκαν.
* Όλες οι πληροφορίες πρέπει να καταστρέφονται ανεξαρτήτως της διαβάθμισης τους.
* Ο ιδιοκτήτης της πληροφορίας σε συνεργασία με τον επιστάτη και τον χρήστη της πληροφορίας πρέπει να διασφαλίσει ότι η επίσημη διαδικασία διευθέτησης πληροφοριών ακολουθείται πιστά. Επίσης o ιδιοκτήτης της Πληροφορίας (ή εντεταλμένο άτομο) πρέπει να είναι παρών κατά την διαδικασία διευθέτησης των πληροφοριών.

# Διαχείριση Διαθεσιμότητας

Η χρήση των υπολογιστικών πόρων (χωρητικότητα δίσκων, ποσοστό χρήσης επεξεργαστή, δυναμικότητα ταχύτητας συστημάτων κ.α.) πρέπει να παρακολουθείται, να συντονίζεται και να προγραμματίζεται κατάλληλα για να διασφαλίζεται η απαιτούμενη διαθεσιμότητα και απόδοση των συστημάτων, σύμφωνα με τις εξελισσόμενες απαιτήσεις του [Όνομα Οργανισμού] τόσο εσωτερικά και εξωτερικά (βλέπε Πολιτική Ασφάλειας Συστημάτων).

Οι Επιχειρησιακοί Ιδιοκτήτες είναι υποχρεωμένοι να καθορίσουν της απαιτούμενες διαδικασίες διαχείρισης της διαθεσιμότητας προκειμένου να διασφαλίζεται ότι παρέχεται το επιθυμητό επίπεδο και απόδοση των επιχειρησιακών αναγκών των συστημάτων πληροφοριών για την υποστήριξη των συναφών επιχειρησιακών διαδικασιών και φόρτων εργασίας. Το αρμόδιο τμήμα Τεχνολογίας είναι υποχρεωμένο να διασφαλίσει ότι οι απαιτήσεις αυτές πληρούνται με την κατανομή και διατήρηση των απαραίτητων πόρων, με το ελάχιστο κόστος.

Ο [Όνομα Οργανισμού] θα διατηρεί διαδικασία διαχείρισης της χωρητικότητας προκειμένου να διασφαλιστεί ότι η χωρητικότητα και οι επιδόσεις των συστημάτων πληροφορικής του οργανισμού δεν επηρεάζονται αρνητικά από αυξημένα επίπεδα ζήτησης υπηρεσιών. Η διαδικασία διαχείρισης χωρητικότητας θα πρέπει να περιλαμβάνει τη διαχείριση της επιχειρησιακής ικανότητας, (προκειμένου να διασφαλίζεται ότι οι επιχειρησιακές ανάγκες μετατρέπονται σε απαιτήσεις χωρητικότητας), διαχείριση της χωρητικότητας υπηρεσιών (ώστε να γίνεται σωστή διαχείριση της χωρητικότητας των υποσυστημάτων πληροφορικής) και ένα μηχανισμό υποβολής εκθέσεων διαχείρισης χωρητικότητας.

* Παρακολούθηση και καταγραφή των επιχειρησιακών δραστηριοτήτων και αναγκών
* Αξιολόγηση της τρέχουσας χωρητικότητας των συστημάτων πληροφορικής
* Πρόβλεψη των μελλοντικών αναγκών χωρητικότητας
* Ανάπτυξη σχεδίου για την επέκταση ή τη βελτίωση της χωρητικότητας
* Καθορισμός βέλτιστης χρήσης των υπαρχόντων πόρων και αποδοτικότητα των υπηρεσιών
* Αντιμετώπιση έκτακτων καταστάσεων αυξημένης ζήτηση
* Παρακολούθηση της χωρητικότητας κάθε υποσυστήματος
* Δημιουργία εκθέσεων που περιλαμβάνουν την κατάσταση της χωρητικότητας, προβλέψεις και προτεινόμενα μέτρα
* Ανάλυση των αποτελεσμάτων και της απόδοσης της διαχείρισης χωρητικότητας και η εφαρμογή βελτιώσεων

Το αρμόδιο τμήμα Τεχνολογίας πρέπει να αναπτύξει μια στρατηγική διαχείρισης διαθεσιμότητας και ένα σχέδιο διαθεσιμότητας. Το σχέδιο πρέπει να καλύπτει τόσο τα τρέχοντα προβλήματα διαθεσιμότητας και επιδόσεων, όσο και μελλοντικές απαιτήσεις. Το σχέδιο διαθεσιμότητας πρέπει να επανεξετάζεται σε τακτική βάση.

* Για κάθε νέα και τρέχουσα δραστηριότητα, προσδιορίζονται οι απαιτήσεις δυναμικότητας. Η ρύθμιση και η παρακολούθηση των συστημάτων εφαρμόζονται προκειμένου να διασφαλιστεί και, όπου είναι αναγκαίο, να βελτιωθεί η διαθεσιμότητα και η απόδοση τους.
  + Οι έλεγχοι ανίχνευσης και ειδοποίησης θα πρέπει να τεθούν σε εφαρμογή για να επισημάνουν τα προβλήματα σε εύθετο χρόνο.
  + Γραπτό μήνυμα θα πρέπει να αποστέλλεται αμέσως τόσο στους επιχειρησιακούς ιδιοκτήτες όσο και στους διαχειριστές συστημάτων σε περίπτωση μη διαθεσιμότητας ενός ή και πολλών συστημάτων ή αν το καθορισμένο κρίσιμο όριο έχει υπερβεί.
  + Οι μετρήσεις (Βασικοί Δείκτες Απόδοσης (KPI)) θα πρέπει να καθοριστούν προκειμένου να παρακολουθούνται οι διαθέσιμοι πόροι.
* Όλα τα συστήματα πληροφορικής που σχετίζονται με κρίσιμης σημασίας πόρο ή πόρους για τον Οργανισμό θα πρέπει να έχουν καθορισμένο όριο δυναμικότητας.
* Οι ιδιοκτήτες επιχειρήσεων υποχρεούνται να εντοπίζουν κρίσιμους πόρους του [Όνομα Οργανισμού]. Οι Επιχειρησιακοί Ιδιοκτήτες, σε συντονισμό με το αρμόδιο τμήμα Τεχνολογίας, συμφωνούν σχετικά με τις αποδεκτές μετρήσεις παρακολούθησης της δυναμικότητας που μεταφράζονται στα τρία επίπεδα κοινοποίησης και κλιμάκωσης, όπως σημειώνεται παρακάτω για τις κατηγορίες προειδοποίησης.
* Το αρμόδιο τμήμα Τεχνολογίας απαιτείται όπως καταγράφει όλα τα συμφωνημένα ενδεικτικά όρια και τις παραμετρικές αξίες τους και θα πρέπει να διενεργεί ετήσιες αναθεωρήσεις για να επιβεβαιώνει ότι υπάρχουν καθορισμένα όρια κοινοποίησης των συστημάτων .
* Πρέπει να οριστούν καθορισμένα όρια για το σύστημα για τις ακόλουθες τρεις κατηγορίες:
  + **Επίπεδο προειδοποίησης**: Είναι ένα ενδεικτικό όριο σε μια μονάδα λειτουργίας IT.
  + **Επίπεδο Συναγερμού**: Έχει επιτευχθεί ένα ενδεικτικό όριο σε μια μονάδα λειτουργίας ΙΤ που υποδεικνύει ένα κρίσιμο όριο για το οποίο θα πρέπει να αναληφθεί άμεση δράση από τον αρμόδιο μηχανικό και τον ιδιοκτήτη του συστήματος.
  + **Κρίσιμο Επίπεδο**: Η επίτευξη του κρίσιμου ορίου απαιτεί τη διαδικασία αντιμετώπισης περιστατικών ασφάλειας πληροφοριών
* Ιδιαίτερη προσοχή πρέπει να δοθεί σε όλους τους πόρους με μακρές προθεσμίες προμηθειών ή υψηλό κόστος. Επομένως οι διαχειριστές παρακολουθούν τη χρήση των βασικών πόρων του συστήματος. Προσδιορίζουν τις τάσεις στη χρήση, ιδίως σε σχέση με τις επιχειρηματικές εφαρμογές ή τα εργαλεία του συστήματος πληροφοριών διαχείρισης.

# Εφεδρεία και Ανάκτηση

Εφεδρικά αντίγραφα πρέπει να τηρούνται σε τακτά χρονικά διαστήματα (ημερήσια, εβδομαδιαία, μηνιαία, ετήσια)όπως αναγράφεται στο [DS3], ανάλογα με την κρισιμότητα της πληροφορίας. Πληροφορίες υψηλής, μεσαίας και χαμηλής κρισιμότητας πρέπει να αντιγράφονται σε πραγματικό χρόνο, ημερήσια και εβδομαδιαία, αντίστοιχα. Τα χρονικά διαστήματα μπορεί να τροποποιηθούν αναλόγως αναγκών και κρισιμότητας.

Ο **Επιχειρησιακός Ιδιοκτήτης** ενός συστήματος ή/ και δεδομένων, είναι υπεύθυνος να καθορίσει και να καταγράψει το πλάνο εφεδρείας και ανάκτησης για το συστήματα ή/ και των δεδομένων.

Οι χρήστες, οι επιστάτες δεδομένων και οι διαχειριστές των συστημάτων μπορούν να προτείνουν στον **Επιχειρησιακό Ιδιοκτήτη** τη συχνότητα της δημιουργίας εφεδρικών αντιγράφων.

* Τα εφεδρικά αντίγραφα μπορεί να φυλάσσονται σε:
  + Μαγνητικές ταινίες
  + Σκληρούς Δίσκους
  + Οπτικούς Δίσκους
  + Solid State Storage (Flash memory)
* Πρέπει να διατηρείται αρχείο που να περιέχει τουλάχιστον τις ακόλουθες πληροφορίες:
  + Όνομα του χρήστη που δημιούργησε το εφεδρικό αντίγραφο
  + Ημερομηνία λήψης του εφεδρικού αντιγράφου
  + Τύπος εφεδρικού αντιγράφου
  + Περιγραφή του περιεχόμενου
* Τα μέσα αποθήκευσης πρέπει να έχουν τις απαραίτητες ετικέτες (όπου είναι εφικτό) και να περιγράφονται με τις ακόλουθες πληροφορίες:
  + Τύπος εφεδρικού αντιγράφου
  + Όγκος δεδομένων
  + Ημερομηνία της πρώτης χρήσης
  + Περιγραφή του περιεχόμενου
* Πλήρη εφεδρικά αντίγραφα θα πρέπει να εξασφαλίζονται πριν από κάθε αναβάθμιση, αλλαγή ή τροποποίηση στις ρυθμίσεις των συστημάτων.
* Τα εφεδρικά αντίγραφα πρέπει να είναι κρυπτογραφημένα
* Για συστήματα ή/και πληροφορίες υψηλής κρισιμότητας πρέπει να δημιουργούνται και να τηρούνται δευτερεύων εφεδρικά αντίγραφα των εφεδρικών αντιγράφων.
* Για υψηλής και μεσαίας κρισιμότητας συστήματα ή/και πληροφορίες, πρέπει να δημιουργούνται εφεδρικά αντίγραφα αυτόματα με τη βοήθεια εξοπλισμού ή/και λογισμικού.
* Το λογισμικό πρέπει να επαληθεύει την ολοκλήρωση της διαδικασίας αντιγραφής των εφεδρικών αντιγράφων. Σε περίπτωση αποτυχίας το λογισμικό πρέπει να ενημερώνει τον επιστάτη της πληροφορίας ή τον Διαχειριστή του Συστήματος για την αστοχία εκτέλεσης της διαδικασίας, μέσω ηλεκτρονικού μηνύματος.
* Τα μέσα αποθήκευσης πρέπει να φυλάσσονται τόσο τοπικά όσο και σε απομακρυσμένη περιοχή. Οποιαδήποτε άλλη εναλλακτική προσέγγιση πρέπει να λαμβάνεται υπόψη και να αξιολογείται.
* Οι απομακρυσμένες εγκαταστάσεις όπου θα φυλάσσονται τα μέσα αποθήκευσης πρέπει πληρούν τις πρόνοιες της Πολιτικής Φυσικής Ασφάλειας.
* Τα μέσα αποθήκευσης πρέπει να διατηρούνται τουλάχιστο 3 (τρεις) κύκλους ζωής (grandfather, father and son) προτού ανακυκλωθεί το περιεχόμενο τους.
* Τα ηλεκτρονικά μέσα αποθήκευσης πρέπει να καταστρέφονται όταν δεν είναι πλέον απαραίτητα.
* Οι διαχειριστές της μηχανογραφικής υποδομής είναι αρμόδιοι να εξασφαλίσουν ότι οι ρυθμίσεις για τη λήψη αντιγράφων εφαρμόζονται στα εξής:
  + Συσκευές δικτύων.
  + Συσκευές ασφάλειας.
  + Κεντρικά ελεγχόμενους εξυπηρετητές.
  + Βάσεις δεδομένων.
  + Εξυπηρετητές αρχείων.
  + Εξυπηρετητές ηλεκτρονικού ταχυδρομείου.
  + Κύριους Φακέλους Χρηστών
  + Κοινούς προσβάσιμους αποθηκευτικούς χώρους.
* Το προσωπικό που συμμετέχει στη δημιουργία εφεδρικών δεδομένων πρέπει να τύχει κατάλληλης εκπαίδευσης.
* Το προσωπικό του [Όνομα Οργανισμού] είναι υπεύθυνο να διασφαλίσει ότι τα δεδομένα τα οποία φυλάσσονται σε συστήματα που βρίσκονται υπό τον έλεγχό του [Όνομα Οργανισμού], τυγχάνουν λήψης εφεδρικών αντιγράφων βάσει της παρούσας Πολιτικής.
* Τα εφεδρικά αντίγραφα πρέπει να ελέγχονται [ορίστε χρονικό διάστημα σε μήνες] προκειμένου να διασφαλιστεί ότι τα δεδομένα που περιέχουν μπορούν να ανακτηθούν πλήρως και επιτυχώς.
* Παρόλο που οι δοκιμές ανάκτησης από καταστροφή πρέπει να γίνονται τουλάχιστον σε ετήσια βάση, οι δοκιμές ανάκτησης από καταστροφή τουλάχιστον για τα κρίσιμα συστήματα πρέπει να γίνονται κάθε [ορίστε χρονικό διάστημα σε μήνες μικρότερο από το πάνω σημείο].

# Κρυπτογράφηση

# Χρήση Κρυπτογράφησης

Η χρήση κρυπτογράφησης είναι αναγκαία για την προστασία των πληροφοριών του [Όνομα Οργανισμού]. Συγκεκριμένα σημεία ελέγχου κρυπτογράφησης, πρέπει να εφαρμόζονται σε συστήματα, υπηρεσίες και εφαρμογές του [Όνομα Οργανισμού] που αποθηκεύουν ή επεξεργάζονται εσωτερική χρήσης ή εμπιστευτικής φύσεως πληροφορίες.

Διαδικασίες κρυπτογράφησης που να λαμβάνουν υπ’ όψη τα ακόλουθα έχουν καθοριστεί και ακολουθούνται:

* Την προσέγγιση σχετικά με τη χρήση των σημείων ελέγχου κρυπτογράφησης σε όλο το εύρος του [Όνομα Οργανισμού], συμπεριλαμβανομένων των γενικών κανόνων βάσει των οποίων (πρέπει να) προστατεύονται εμπιστευτικής φύσεως δεδομένα.
* Την προσέγγιση στη διαχείριση των «Κλειδιών Κρυπτογράφησης», συμπεριλαμβανομένων μεθόδων που περιγράφουν την ανάκτηση κρυπτογραφημένης πληροφορίας σε περιπτώσεις απώλειας, καταστροφής ή έκθεσης των «Κλειδιών» αυτών.
* Τους ρόλους και τα καθήκοντα, π.χ. ποιος είναι υπεύθυνος για:
  + Την υλοποίηση της πολιτικής κρυπτογράφησης.
  + Τη διαχείριση των «Κλειδιών Κρυπτογράφησης».
  + Τον καθορισμό του κατάλληλου επιπέδου κρυπτογραφικής προστασίας.
  + Τους κανόνες που πρέπει να υιοθετηθούν για την αποτελεσματική υλοποίηση της πολιτικής (ποια λύση χρησιμοποιείται σε ποια επιχειρηματική διαδικασία).

# Διαχείριση Δημοσίου Κλειδιού

Θα πρέπει να εφαρμόζονται ενέργειες διαχείρισης κρυπτογραφικών κλειδιών, εξασφαλίζοντας τουλάχιστον τα παρακάτω:

1) Θα πρέπει να υπάρχει διαδικασία διαχείρισης κλειδιού για το χειρισμό:

i. Δημιουργίας κλειδιού

ii. Χρήσης κλειδιού

iii. Ασφαλούς αποθήκευσης και αρχειοθέτησης κλειδιού (αντίγραφο ασφάλειας)

iv. Αλλαγής ή ενημέρωσης κλειδιού

v. Διανομής κλειδιού

vi. Ανάκτησης κρυπτογραφημένων δεδομένων εάν ένα κλειδί καταστραφεί κατά λάθος ή καταστεί μη διαθέσιμο

vii. Ανάκλησης κλειδιού

viii. Καταγραφής και ελέγχου βασικών δραστηριοτήτων που σχετίζονται με τη διαχείριση κλειδιού.

2) Κάθε κλειδί θα πρέπει να χρησιμοποιείται μόνο για έναν σκοπό.

3) Τα κλειδιά κρυπτογράφησης θα πρέπει να δημιουργούνται με μέσα, χειροκίνητα ή αυτοματοποιημένα, ώστε να είναι δύσκολο να αποκαλυφθούν.

4) Τα κλειδιά κρυπτογράφησης είναι εμπιστευτικά και η πρόσβαση στα κλειδιά αυτά θα πρέπει να περιορίζεται αυστηρά σε εκείνους που είναι εξουσιοδοτημένοι να γνωρίζουν.

5) Εάν χρησιμοποιηθεί λύση κρυπτογράφησης, τότε η λύση θα πρέπει να διανέμει τα κλειδιά με ασφάλεια, πράγμα που σημαίνει ότι τα κλειδιά δεν διανέμονται σε απλό κείμενο και είναι προσβάσιμα μόνο από τους βασικούς υπεύθυνους.

6) Η λύση κρυπτογράφησης θα πρέπει να αποθηκεύει τα κλειδιά με ασφάλεια, πράγμα που σημαίνει ότι τα κλειδιά δεν αποθηκεύονται απροστάτευτα (αλλά κρυπτογραφούνται με τη χρήση κρυπτογράφησης).

7) Οι τακτικές «χωρισμένης γνώσης» και «διπλού ελέγχου» των κλειδιών θα πρέπει να χρησιμοποιούνται όταν είναι τεχνικά εφικτό ώστε να αποφεύγεται η δυνατότητα ενός ατόμου να έχει πρόσβαση σε ολόκληρο το κλειδί.

8) Οι ημερομηνίες ενεργοποίησης και απενεργοποίησης των κλειδιών ορίζονται ώστε να επιτρέπουν τη χρήση του μόνο για καθορισμένο χρονικό διάστημα.

9) Τα παλαιά κλειδιά που δεν χρησιμοποιούνται ή δεν χρειάζονται πλέον θα πρέπει να αποσύρονται και να καταστρέφονται για να διασφαλιστεί ότι δεν μπορούν πλέον να χρησιμοποιηθούν. Εάν πρέπει να διατηρούνται παλιά κλειδιά (για την υποστήριξη αρχειοθετημένων, κρυπτογραφημένων δεδομένων, για παράδειγμα) θα πρέπει να προστατεύονται με ισχυρή κρυπτογράφηση.

10) Ένα κλειδί δεν πρέπει να χρησιμοποιείται εάν υπάρχει υποψία παραβίασης. Ο υπεύθυνος ασφάλειας πληροφοριών επανεξετάζει όλες τις αναφερόμενες περιπτώσεις παραβίασης για να προσδιορίσει τα μέτρα που πρέπει να ληφθούν.

11) Όλα τα κλειδιά κρυπτογράφησης πρέπει να αρχειοθετούνται και να είναι διαθέσιμα στο εξουσιοδοτημένο προσωπικό του Οργανισμού, όταν χρειάζεται.

# Ψηφιακές Υπογραφές

Οι ψηφιακές υπογραφές πρέπει να χρησιμοποιούνται για να ανιχνεύονται τυχόν μη εξουσιοδοτημένες μετατροπές σε δεδομένα και για να πιστοποιείται η ταυτότητα του υπογράφοντος.

Επιπρόσθετα, ένας οποιοσδήποτε παραλήπτης ψηφιακά υπογεγραμμένων δεδομένων δύναται να αποδείξει σε ένα τρίτο μέρος ότι η ψηφιακή αυτή υπογραφή παρήχθη από τον ίδιο τον υπογράφοντα και μόνο. Οι ψηφιακές υπογραφές βρίσκουν εφαρμογή σε οποιοδήποτε ηλεκτρονικό αρχείο και υλοποιούνται κάνοντας χρήση ενός ζεύγους «Κλειδιών»: Το «Ιδιωτικό Κλειδί», με το οποίο παράγεται η υπογραφή, και το «Δημόσιο Κλειδί», με το οποίο ελέγχεται η υπογραφή.

# Αποτροπή Αποποίησης Ευθύνης

Πρέπει να χρησιμοποιούνται μηχανισμοί προκυμμένου να επιτυγχάνεται η «Αποτροπή Αποποίησης Ευθύνης». Η «Αποτροπή Αποποίησης Ευθύνης» χρησιμοποιείται για να διασφαλιστεί ότι ένα ηλεκτρονικά μεταφερόμενο μήνυμα έχει πράγματι αποσταλεί και παραληφθεί από τα σωστά μέρη. Αυτό σημαίνει ότι κανείς εκ των δύο (αποστολέας και παραλήπτης) δεν μπορεί να αποποιηθεί την ευθύνη της πράξης του (αποστολή και παραλαβή μηνύματος αντίστοιχα). Η αποτροπή αποποίησης ευθύνης είναι ένα σύνολο μεθόδων και πρακτικών που βασίζονται στις τεχνικές της κρυπτογράφησης και της ψηφιακής υπογραφής, για να αποδείξουν, με αδιαμφισβήτητο τρόπο, ότι ένα γεγονός έλαβε πράγματι χώρα.

Η αποτροπή αποποίησης ευθύνης υλοποιείται με χρήση των ακόλουθων τεχνικών:

* Υπηρεσίες Επιβεβαίωσης, μέσω της δημιουργίας ψηφιακών αποδεικτικών, σε κάθε είδους αποστολή και παραλαβή μηνυμάτων.
* Με χρήση «Χρονοσήμανσης», προκειμένου να αποδειχτεί η ύπαρξη ενός μηνύματος ή κειμένου σε μια δεδομένη χρονική στιγμή.

# Υποδομή Δημόσιου Κλειδιού

Η Υποδομή Δημοσίου Κλειδιού είναι ένα μεθοδολογικό και τεχνολογικό πλαίσιο που ενοποιεί τις τεχνικές των ψηφιακών υπογραφών και πιστοποιητικών προκειμένου να παράσχει ακεραιότητα, έλεγχο πρόσβασης, εμπιστευτικότητα, πιστοποίηση και αποτροπή αποποίησης ευθύνης στις ηλεκτρονικές συναλλαγές.

Η τεχνολογία της ψηφιακής υπογραφής διασφαλίζει, με επαληθεύσιμο τρόπο, τη συσχέτιση μεταξύ του δημόσιου «συστατικού» ενός «Ασύμμετρου Δημοσίου Κλειδιού» με τον συγκεκριμένο κάτοχο ενός αντίστοιχου «Ιδιωτικού Κλειδιού». Η Υποδομή Δημοσίου Κλειδιού επιτρέπει σε χρήστες μη ασφαλών δημόσιων δικτύων, που χρησιμοποιούν ζεύγος Δημοσίων Κλειδιών, να ανταλλάσσουν ιδιωτικά και απόρρητα δεδομένα με ασφαλή τρόπο.

# Κρίσιμα ή ευαίσθητα δεδομένα

Θέσπιση, εφαρμογή και διατήρηση πολιτικής σχετικά με τη χρήση κρυπτογραφικών μέτρων, προκειμένου να διασφαλίζονται η εμπιστευτικότητα, η ακεραιότητα και η αυθεντικότητα των δεδομένων κατά την αποθήκευση, τη χρήση και τη μεταφορά. Η πολιτική κρυπτογράφησης θα πρέπει να λαμβάνει υπόψη την εφαρμογή κρυπτογραφικών μέτρων σε όλα τα στάδια του κύκλου ζωής των πληροφοριών και να εξετάζει εφαρμογές, συστήματα, εξοπλισμό δικτύου και διαύλους επικοινωνίας.

# Εφαρμογή Κρυπτογράφησης

Όλες οι εμπιστευτικής φύσεως πληροφορίες που δημιουργούνται, ανήκουν, λαμβάνονται, χρησιμοποιούνται, διακινούνται, διατηρούνται και αποθηκεύονται από/προς τον Οργανισμό θα πρέπει να τυγχάνουν κατάλληλης προστασίας. Σε τέτοιες περιπτώσεις η κρυπτογράφηση στον [Όνομα Οργανισμού]υ είναι υποχρεωτική.

Τα δεδομένα που πρόκειται να μεταφερθούν με φυσικά μέσα, πρώτα κρυπτογραφούνται κατάλληλα και μετά αποστέλλονται. Τα κλειδιά κρυπτογράφησης μεταφέρονται χωριστά, με άλλο μέσο (ή τρόπο) χωρίς επισήμανση της χρήσης τους. Για σύγχρονη μεταφορά χρησιμοποιούνται πρωτόκολλα όπως είναι οι πιο πρόσφατες σταθερές εκδόσεις πρωτοκόλλων όπως είναι το SFTP ή HTTPS.

Όλες οι φορητές ηλεκτρονικές συσκευές, που διαθέτουν χώρο αποθήκευσης δεδομένων, πρέπει να τυγχάνουν πλήρης κρυπτογράφησης. Οι ηλεκτρονικές συσκευές, μεταξύ άλλων περιλαμβάνουν τα ακόλουθα:

* Φορητοί ηλεκτρονικοί υπολογιστές
* Smartphones
* Tablets
* Αποσπόμενα μέσα φύλαξης δεδομένων (USB/CD)
* Back up tapes

Όλες οι ηλεκτρονικές συσκευές που διαθέτουν χώρο αποθήκευσης δεδομένων, και επεξεργάζονται ή/και αποθηκεύουν εμπιστευτικής φύσεως πληροφορίες πρέπει να τυγχάνουν πλήρης κρυπτογράφησης. Οι ηλεκτρονικές συσκευές, μεταξύ άλλων περιλαμβάνουν τα ακόλουθα.

* Ηλεκτρονικοί υπολογιστές
* Εξυπηρετητές
* Δικτυακές συσκευές
* Εκτυπωτές
* Φωτοτυπικές Μηχανές

# Προβλέψεις σε Συμβάσεις με Τρίτα Μέρη:

Είναι σημαντικό να περιλαμβάνονται ρητές προβλέψεις σχετικά με την ασφαλή διαχείριση και καταστροφή πληροφοριών σε συμβάσεις με τρίτα μέρη.

Αυτό εξασφαλίζει ότι οι προμηθευτές ή οι συνεργάτες ακολουθούν τις αναγκαίες διαδικασίες καταστροφής πληροφοριών για την προστασία των δεδομένων.

Είναι σημαντικό να σημειώσουμε ότι οι απαιτήσεις για την ασφαλή καταστροφή πληροφοριών μπορεί να διαφέρουν ανάλογα με τη νομοθεσία και τον τύπο πληροφοριών που πρέπει να καταστραφούν. Επιπλέον, η συνεχής παρακολούθηση και ενημέρωση σχετικά με τις βέλτιστες πρακτικές είναι ζωτικής σημασίας για τη διασφάλιση της αποτελεσματικής προστασίας των πληροφοριών.

Για τα δεδομένα που βρίσκονται σε μεταφορά ή ανταλλάσσονται τα μέτρα πρέπει να συμφωνούν αντίστοιχα με το [DS4] του Κανονισμού Κ.Δ.Π. 389/2020. Αυτό σημαίνει ότι ο [Όνομα Οργανισμού] πρέπει να θεσπίσει, εφαρμόσει και να διατηρεί διαδικασίες μεταφοράς και ανταλλαγής πληροφοριών προκειμένου να διασφαλίζεται η προστασία των πληροφοριών κατά τη μεταφορά ή την ανταλλαγή τους εσωτερικά ή με τρίτα μέρη. Για αυτό το σκοπό θα πρέπει να συμμορφωθεί με όλες τις σχετικές νομοθετικές, κανονιστικές και ρυθμιστικές απαιτήσεις, και συμβατικές απαιτήσεις όσον αφορά την ασφάλεια δικτύων και πληροφοριών.

Για τα κρίσιμα ή ευαίσθητα δεδομένα που βρίσκονται σε ηρεμία (data at rest), πρέπει να εφαρμόζεται κρυπτογραφία σε συμφωνία με την σχετική πολιτική του [ΑΜ5] του Κανονισμού Κ.Δ.Π. 389/2020. Ο [Όνομα Οργανισμού] πρέπει να θεσπίσει, εφαρμόσει και να διατηρεί πολιτική σχετικά με τη χρήση κρυπτογραφικών μέτρων, προκειμένου να διασφαλίζονται η εμπιστευτικότητα, η ακεραιότητα και η αυθεντικότητα των δεδομένων κατά την αποθήκευση, τη χρήση και τη μεταφορά. Η πολιτική κρυπτογράφησης θα πρέπει να λαμβάνει υπόψη την εφαρμογή κρυπτογραφικών μέτρων σε όλα τα στάδια του κύκλου ζωής των πληροφοριών και να εξετάζει εφαρμογές, συστήματα, εξοπλισμό δικτύου και διαύλους επικοινωνίας. Ο [Όνομα Οργανισμού] πρέπει να ορίσει μια περίοδο διατήρησης των δεδομένων για όλες τις κατηγορίες δεδομένων και εφαρμόζει τις σχετικές προβλέψεις.

Δύο παραδείγματα συχνά χρησιμοποιούμενων πρωτοκόλλων κρυπτογράφησης για την ασφάλεια της μεταφοράς δεδομένων είναι το Transport Layer Security (TLS) και το Open Secure Shell (OpenSSH).

1. Transport Layer Security (TLS):

Το TLS είναι ένα πρωτόκολλο κρυπτογράφησης που χρησιμοποιείται για την ασφαλή μεταφορά δεδομένων μέσω του Διαδικτύου.

Συνήθως χρησιμοποιείται στο πλαίσιο του HTTPS (HTTP Secure) για την ασφαλή μεταφορά δεδομένων μεταξύ πελάτη και εξυπηρετητή σε ιστοσελίδες.

1. Open Secure Shell (OpenSSH):

Το OpenSSH είναι ένα πρωτόκολλο ασφαλούς απομακρυσμένου συνδεδεμένου υπολογιστή, που χρησιμοποιείται για ασφαλή απομακρυσμένη διαχείριση.

Παρέχει κρυπτογραφημένη σύνδεση μεταξύ δύο συστημάτων, προστατεύοντας τη μεταφορά δεδομένων κατά τη διάρκεια απομακρυσμένων συνεδριών.

Η χρήση αυτών των πρωτοκόλλων εξασφαλίζει ότι οι επικοινωνίες μεταξύ συστημάτων είναι κρυπτογραφημένες, εμποδίζοντας έτσι την ανεπιθύμητη τροποποίηση των δεδομένων που μεταφέρονται. Είναι σημαντικό να υλοποιούνται αυτές οι πρακτικές, ιδίως όταν πρόκειται για ευαίσθητα ή κρίσιμα δεδομένα.

Η πρακτική του να κρυπτογραφούνται πρώτα τα δεδομένα και έπειτα να μεταφέρονται με φυσικά μέσα αποτελεί σημαντικό μέτρο ασφαλείας. Η χρήση ξεχωριστών μέσων για τη μεταφορά των κλειδιών κρυπτογράφησης επίσης αυξάνει την ασφάλεια του συστήματος, καθώς μειώνεται ο κίνδυνος επιθέσεων που στοχεύουν στα κλειδιά κατά τη διάρκεια της μεταφοράς τους.

Για τη σύγχρονη μεταφορά, η χρήση πρωτοκόλλων όπως το SFTP (Secure File Transfer Protocol) ή το HTTPS είναι πολύ συνηθισμένη και αποτελεί αξιόπιστη επιλογή:

1. SFTP (Secure File Transfer Protocol):

Το SFTP είναι ένα πρωτόκολλο μεταφοράς αρχείων πάνω από SSH (Secure Shell).

Χρησιμοποιεί κρυπτογράφηση για την ασφαλή μεταφορά αρχείων, προσφέροντας επίπεδο ασφαλείας στη μεταφορά δεδομένων.

1. HTTPS (Hypertext Transfer Protocol Secure):

Το HTTPS είναι μια ασφαλής εκδοχή του πρωτοκόλλου HTTP που χρησιμοποιείται για τη μεταφορά δεδομένων μέσω του πρωτοκόλλου TLS.

Χρησιμοποιείται κυρίως για ασφαλείς συναλλαγές στον κόσμο του διαδικτύου, όπως η μεταφορά ευαίσθητων πληροφοριών σε ιστοσελίδες.

Αυτά τα πρωτόκολλα προσφέρουν συνδυασμό αυθεντικοποίησης, εμπιστοσύνης και ασφάλειας κατά τη μεταφορά δεδομένων. Επιπλέον, η χρήση κρυπτογραφίας για τη μεταφορά κλειδιών προσθέτει επιπλέον στρώμα ασφαλείας στο σύστημα σας, προστατεύοντας τα κλειδιά από ανεπιθύμητη πρόσβαση κατά τη διάρκεια της μεταφοράς τους.