Όνομα Οργανισμού

Πολιτική Προστασίας Δεδομένων

|  |  |
| --- | --- |
| **Περιεχόμενο:** | Πολιτική Προστασίας Δεδομένων |
| **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](#_Toc190786649)

[1. Εισαγωγή 4](#_Toc190786650)

[1.1 Σκοπός 4](#_Toc190786651)

[1.2 Πεδίο Εφαρμογής 4](#_Toc190786652)

[2. Πολιτική Προστασίας Δεδομένων 5](#_Toc190786653)

[2.1 Διαχείριση κύκλου ζωής των δεδομένων 5](#_Toc190786655)

[2.2 Διαβάθμιση και επισήμανση πληροφοριών 5](#_Toc190786656)

[2.3 Μεταφορά και ανταλλαγή πληροφορίων 7](#_Toc190786657)

[2.4 Πρόληψη απώλειας δεδομένων και διαρροής δεδομένων 8](#_Toc190786658)

[2.5 Χρήση Κρυπτογραφίας 9](#_Toc190786659)

[2.6 Διαγραφή ή Καταστροφή πληροφοριών 10](#_Toc190786660)

[2.7 Ψηφιακές Υπογραφές 10](#_Toc190786661)

[3. Εφεδρικά Αντίγραφα Πληροφοριών 11](#_Toc190786662)

[4. Προβλέψεις σε Συμβάσεις με Τρίτα Μέρη 11](#_Toc190786663)

[5. Αναθεώρηση 12](#_Toc190786664)

[6. Αναφορές 13](#_Toc190786665)

# Εισαγωγή

## Σκοπός

Το παρόν έγγραφο περιλαμβάνει ενδεικτικούς Όρους Πολιτικής για την προστασία δεδομένων του [Όνομα Οργανισμού] για τη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας προσωπικών και ευαίσθητων δεδομένων σύμφωνα με την Απόφαση Κ.Δ.Π 389/2020 και με το Πλαίσιο Ωριμότητας Κυβερνοασφάλειας όπως δημοσιεύτηκε στην περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών (Έλεγχοι Ωριμότητας Κυβερνοασφάλειας) Απόφαση του 2024 (Κ.Δ.Π. 245/2024). Αυτή η πολιτική περιγράφει πώς συλλέγονται, αποθηκεύονται, επεξεργάζονται και προστατεύονται τα κρίσιμα δεδομένα του [Όνομα Οργανισμού].

Οι στόχοι της πολιτικής αυτής είναι οι ακόλουθοι:

* Η διασφάλιση της συμμόρφωσης για την ασφάλεια δεδομένων μέσω ευθυγράμμισης με κανονιστικές απαιτήσεις και σχετικές νομοθεσίες (π.χ. GDPR).
* Η προστασία Προσωπικών & Ευαίσθητων Δεδομένων μέσω αποτροπής μη εξουσιοδοτημένης πρόσβασης, επεξεργασίας, αποκάλυψης ή απώλειας.
* Η καθιέρωση διαφόρων ελέγχων ασφαλείας μέσω της εφαρμογής τεχνικών, οργανωτικών και μέτρων φυσικής ασφάλειας για την προστασία των δεδομένων.
* Ο μετριασμός των κινδύνων που σχετίζονται με παραβιάσεις δεδομένων, και από απειλές είτε στον κυβερνοχώρο είτε από εσωτερικές απειλές π.χ. διαρροές.

## Πεδίο Εφαρμογής

Το πεδίο εφαρμογής της Πολιτικής Προστασίας Δεδομένων καλύπτει όλες τις κρίσιμες πληροφορίες που διαχειρίζεται ο [Όνομα Οργανισμού]. Σε αυτά περιλαμβάνονται

* Όλα τα προσωπικά, ευαίσθητα και κρίσιμα δεδομένα του [Όνομα Οργανισμού] που αποθηκεύονται, υποβάλλονται σε επεξεργασία ή μεταδίδονται εντός του οργανισμού.
* Όλα τα συστήματα πληροφορικής, οι βάσεις δεδομένων, τα δίκτυα και οι υπηρεσίες cloud που αποθηκεύουν ή επεξεργάζονται ευαίσθητες πληροφορίες.
* Δεδομένα σε οποιαδήποτε άλλη μορφή π.χ. ηλεκτρονικά, έντυπα ή αποθηκευμένα στο cloud.

Επίσης, το πεδίο εφαρμογής περιλαμβάνει το προσωπικό του [Όνομα Οργανισμού], τους συνεργάτες, τους προμηθευτές και κάθε άλλο ενδιαφερόμενο μέρος που έχει πρόσβαση ή διαχειρίζεται πληροφορίες του [Όνομα Οργανισμού].

# Πολιτική Προστασίας Δεδομένων



## Διαχείριση κύκλου ζωής των δεδομένων

Ο [Όνομα Οργανισμού] ακολουθεί μια δομημένη διαδικασία Διαχείρισης Κύκλου Ζωής Δεδομένων (DLM) για να διασφαλίσει τον ασφαλή χειρισμό των δεδομένων από τη δημιουργία έως τη καταστροφή τους. Η πρόσβαση στα δεδομένα ελέγχεται αυστηρά με βάση τα επίπεδα ταξινόμησης και τις επιχειρηματικές απαιτήσεις, διασφαλίζοντας τη συμμόρφωση με την Απόφαση Κ.Δ.Π 389/2020. Τα δεδομένα διατηρούνται μόνο για όσο διάστημα είναι απαραίτητο και διαγράφονται με ασφάλεια ή ανωνυμοποιούνται όταν δεν χρειάζονται πλέον. Εφαρμόζονται τακτικοί έλεγχοι και αυτοματοποιημένα μέτρα πρόληψης απώλειας δεδομένων (DLP) για τη διαφύλαξη των δεδομένων καθ' όλη τη διάρκεια του κύκλου ζωής τους. Πιο συγκεκριμένα ο [Όνομα Οργανισμού] λαμβάνει τα ακόλουθα:

Καθορίζει κατάλληλα μέτρα, για την προστασία των δεδομένων καθ' όλη τη διάρκεια του κύκλου ζωής τους και ανάλογα με την διαβάθμιση τους, σε συμμόρφωση με τις ισχύουσες νομικές και κανονιστικές απαιτήσεις.

Καταγράφει σε μητρώο τις διαβαθμισμένες πληροφορίες, το οποίο πρέπει να διαθέτει έναν καθορισμένο υπεύθυνο, αρμόδιο για τη συντήρηση και την επικαιροποίηση των καταγεγραμμένων πληροφοριών.

Οι πληροφορίες πρέπει να προστατεύονται τόσο κατά την αποθήκευση όσο και κατά τη μεταφορά τους.

Για κρίσιμα ή ευαίσθητα δεδομένα του [Όνομα Οργανισμού] πρέπει να εφαρμόζεται κρυπτογράφηση κατά την αποθήκευσή τους (data at rest).

Ο [Όνομα Οργανισμού] έχει ορίσει συγκεκριμένες περιόδους διατήρησης για όλες τις κατηγορίες δεδομένων και να εφαρμόζει τις απαραίτητες ενέργειες διαγραφής.

## Διαβάθμιση και επισήμανση 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 μόνο σε εξουσιοδοτημένους χρήστες. 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

Περεταίρω, ώστε να διασφαλιστεί ο σωστός χειρισμός και η προστασία, όλα τα δεδομένα του Οργανισμού, ταξινομούνται (σήμανση) με βάση την ευαισθησία και το επίπεδο κινδύνου. Για σκοπούς σήμανσης ο [Όνομα Οργανισμού] έχει καθορίσει τις ακόλουθες κατηγορίες:

Δημόσιο (Public use),

Οι πληροφορίες δημόσιας χρήσης αναφέρονται σε δεδομένα που δεν υπόκεινται σε περιορισμούς πρόσβασης και μπορούν να κοινοποιηθούν ελεύθερα με το κοινό χωρίς να τίθεται σε κίνδυνο η ασφάλεια, η εμπιστευτικότητα ή οι νομικές υποχρεώσεις του οργανισμού.

Εσωτερικό (Internal Use),

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.

Περιορισμένη Χρήση (Limited Use),

Οι πληροφορίες περιορισμένης χρήσης αναφέρονται σε δεδομένα που προορίζονται μόνο για εσωτερική χρήση και δεν πρέπει να κοινοποιούνται εκτός του οργανισμού χωρίς την κατάλληλη εξουσιοδότηση. Αυτό μπορεί να περιλαμβάνει επιχειρησιακές στρατηγικές και διαδικασίες, εσωτερικά σημειώματα και άλλες μη δημόσιες πληροφορίες που είναι απαραίτητες για τις καθημερινές εργασίες, αλλά δεν απαιτούν το υψηλότερο επίπεδο προστασίας. Η πρόσβαση σε πληροφορίες περιορισμένης χρήσης περιορίζεται σε υπαλλήλους, συνεργάτες ή τρίτα μέρη που έχουν νόμιμη ανάγκη να γνωρίζουν και πρέπει να αντιμετωπίζονται σύμφωνα με καθιερωμένες πολιτικές ελέγχου πρόσβασης. Αν και αυτές οι πληροφορίες δεν απαιτούν το ίδιο επίπεδο ασφάλειας με τα Εμπιστευτικά δεδομένα, εξακολουθούν να απαιτούν την κατάλληλη προστασία, όπως κρυπτογράφηση κατά τη μετάδοση και περιορισμένη πρόσβαση αποθήκευσης.

Εμπιστευτικό(Confidential)

Οι εμπιστευτικές πληροφορίες αναφέρονται σε δεδομένα που είναι ευαίσθητα και θα πρέπει να έχουν πρόσβαση μόνο από εξουσιοδοτημένο προσωπικό με νόμιμη επιχειρησιακή ανάγκη. Η μη εξουσιοδοτημένη αποκάλυψη, πρόσβαση ή χρήση αυτών των πληροφοριών θα μπορούσε να προκαλέσει σημαντική βλάβη στον οργανισμό, και άλλους διασυνδεδεμένους φορείς. Ως εκ τούτου, πρέπει να εφαρμόζονται αυστηροί έλεγχοι πρόσβασης, κρυπτογράφηση και τεχνικές απόκρυψης δεδομένων (masking) για να διασφαλίζεται η προστασία του τόσο σε κατάσταση φύλαξης (Data at rest) όσο και κατά τη μεταφορά. Συστήνεται όπως εμπιστευτικές πληροφορίες υπόκεινται σε επίσημες διαδικασίες χειρισμού δεδομένων, συμπεριλαμβανομένων των συμφωνιών μη αποκάλυψης (NDA).

**Σημείωση: Ο κάθε Οργανισμός δύναται να καθορίσει της δικές του κατηγορίες ανάλογα με τις ανάγκες του.**

**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 και δεν σχετίζεται απαραίτητα με την πιο πάνω σήμανση**

Κάθε κατηγορία όπως καταγράφεται πιο πάνω, καθορίζει τα δικαιώματα πρόσβασης, την αποθήκευση και τους ελέγχους ασφαλείας, όπως ορίζεται στο [IAM1] της Απόφασης Κ.Δ.Π. 389/2020. Οι πληροφορίες πρέπει να επισημαίνονται κατάλληλα ώστε να αντικατοπτρίζουν την ταξινόμηση τους, χρησιμοποιώντας μεταδεδομένα, άλλες οπτικές σημάνσεις ή αυτοματοποιημένα συστήματα επισήμανσης π.χ. σύστημα TLP. Οι εργαζόμενοι πρέπει να συμμορφώνονται με τις οδηγίες επισήμανσης για να αποτρέψουν τη μη εξουσιοδοτημένη πρόσβαση και να υποστηρίζουν την αποτελεσματική προστασία δεδομένων και τη διαχείριση κινδύνου.

Πιο συγκεκριμένα θα πρέπει να εφαρμοστούν οι πιο κάτω κατευθυντήριες γραμμές:

Κάθε διαβαθμισμένη πληροφορία του [Όνομα Οργανισμού] πρέπει να επισημαίνεται με σαφήνεια για τους χρήστες της πληροφορίας.

Πρέπει να έχει θεσπιστεί, υιοθετηθεί και να διατηρείται μια διαδικασία διαβάθμισης και επισήμανσης που διασφαλίζει ότι οι πληροφορίες κατατάσσονται και επισημαίνονται σύμφωνα με την εμπιστευτικότητα και την ευαισθησία τους.

Οι πληροφορίες πρέπει να διαβαθμίζονται, τουλάχιστον, σε τρεις κατηγορίες: Δημόσιες, Εσωτερικές και Διαβαθμισμένες.

Οι αρμόδιοι ιδιοκτήτες πληροφοριών είναι υπεύθυνοι για την διαβάθμιση των πληροφοριών υπό την ευθύνη τους καθώς και για τη διαχείριση τους σύμφωνα με τις απαιτήσεις των διαδικασιών του [Όνομα Οργανισμού] .

Ο [Όνομα Οργανισμού] πρέπει να διασφαλίζει ότι διενεργούνται έλεγχοι για τη συμμόρφωση με τις απαιτήσεις ταξινόμησης και επισήμανσης.

Ο [Όνομα Οργανισμού] πρέπει να διαθέτει μια διαδικασία για την ασφαλή διαγραφή δεδομένων η οποία περιέχει ρόλους, αρμοδιότητες, μεθοδολογίες, κριτήρια και εργαλεία χρησιμοποιούνται για την διαγραφή των δεδομένων κάθε επιπέδου διαβάθμισης, συμπεριλαμβάνοντας μέτρα που εφαρμόζονται όταν μεταφέρονται στοιχεία (πόροι) σε εξωτερικά μέρη.

Σε περίπτωση χρησιμοποιείται τρίτο μέρος για την διαγραφή ή καταστροφή, ο [Όνομα Οργανισμού] πρέπει να συμπεριλαμβάνει σχετικές προβλέψεις και όρους που εξασφαλίζουν την ορθή και αποτελεσματική εφαρμογή των σχετικών κανόνων στο σχετικό συμβόλαιο. Σε περίπτωση που τα δεδομένα αποθηκεύονται σε τρίτα μέρη (π.χ. Cloud services) δίνονται συγκεκριμένες δεσμεύσεις και αποδείξεις από την μεριά του τρίτου μέρους για την υλοποίηση των συγκεκριμένων ρυθμίσεων. Σε διαφορετική περίπτωση λαμβάνονται άλλα αντισταθμιστικά μέτρα.

## Μεταφορά και ανταλλαγή πληροφορίων

Ο [Όνομα Οργανισμού] διασφαλίζει ότι όλες οι εσωτερικές και εξωτερικές μεταφορές δεδομένων πραγματοποιούνται με ασφάλεια για την αποτροπή μη εξουσιοδοτημένης πρόσβασης, υποκλοπής ή διαρροής δεδομένων. Πιο συγκεκριμένα:

Ο [Όνομα Οργανισμού] καθορίζει κατάλληλα μέτρα προστασίας μεταφοράς των δεδομένων, τόσο εσωτερικά όσο και με τρίτα μέρη, ανάλογα με το επίπεδο διαβάθμισής τους.

Τα μέτρα προστασίας πρέπει να κοινοποιούνται στα τρίτα μέρη με τα οποία γίνεται η ανταλλαγή δεδομένων και να εξασφαλίζεται η συμμόρφωση αυτών με τα μέτρα προστασίας.

Όλοι οι εργαζόμενοι του [Όνομα Οργανισμού] πρέπει να ακολουθούν εγκεκριμένες μεθόδους για την ανταλλαγή δεδομένων, διασφαλίζοντας την εμπιστευτικότητα και την ακεραιότητα σε όλη τη διαδικασία.

Κατά την μεταφορά και ανταλλαγή πληροφοριών πρέπει να λαμβάνονται υπόψη κανονιστικές και νομοθετικές απαιτήσεις, ειδικότερα σε περιπτώσεις διεθνών διαβιβάσεων δεδομένων όπως ορίζονται στο [GOV2] της Απόφασης Κ.Δ.Π 389/2020.

Ο [Όνομα Οργανισμού] πρέπει να υλοποιεί κατάλληλη κρυπτογράφηση κατά την ανταλλαγή ή μεταφορά κρίσιμων ή ευαίσθητων δεδομένων. Παραδείγματα τέτοιας υλοποίησης περιλαμβάνει (Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).

Τα κλειδιά κρυπτογράφησης πρέπει να μεταφέρονται χωριστά, με διαφορετικό μέσο (ή τρόπο), χωρίς ένδειξη της χρήσης τους.

O [Όνομα Οργανισμού] πρέπει να εφαρμόζει κατάλληλους μηχανισμούς για την διασφάλιση της ακεραιότητας και αυθεντικότητας της πληροφορίας που ανταλλάσσεται.

Εντός του [Όνομα Οργανισμού] πρέπει να τηρείται μητρώο με τις πληροφορίες που ανταλλάσσονται (κρίσιμες ή ευαίσθητες), καταγράφοντας τα μέτρα που εφαρμόστηκαν και τις σχετικές εγγυήσεις από τα εμπλεκόμενα μέρη.

Πρέπει να εφαρμόζονται μηχανισμοί data masking για αυξημένη προστασία ειδικά σε περιπτώσεις ευαίσθητων δεδομένων είναι απαραίτητη , όπου αυτό είναι δυνατό.

## Πρόληψη απώλειας δεδομένων και διαρροής δεδομένων

O [Όνομα Οργανισμού] εφαρμόζει ελέγχους πρόληψης απώλειας δεδομένων για την προστασία των ευαίσθητων πληροφοριών από μη εξουσιοδοτημένη πρόσβαση, τυχαία έκθεση ή κακόβουλη διείσδυση. Τα μέτρα ασφαλείας περιλαμβάνουν μεταξύ άλλων:

Ο [Όνομα Οργανισμού] πρέπει να καθορίσει μέτρα για την ελαχιστοποίηση του κινδύνου απώλειας και διαρροής δεδομένων, λαμβάνοντας τα κατάλληλα τεχνικά και οργανωτικά μέτρα για την πρόληψη σύμφωνα με το [DS5] της Απόφασης Κ.Δ.Π 389/2020.

Η μεταφορά δεδομένων σε χρήση USB **δεν** συστήνεται.

Η πρόσβαση σε μέσα για τη μεταφορά δεδομένων και σε μη εταιρικά συστήματα ανταλλαγής μηνυμάτων απαγορεύεται.

## Χρήση Κρυπτογραφίας

Ο [Όνομα Οργανισμού] χρησιμοποιεί τεχνικές κρυπτογράφησης για την προστασία ευαίσθητων δεδομένων κατά τη μετάδοση και την αποθήκευση. Συγκεκριμένα σημεία ελέγχου κρυπτογράφησης, εφαρμόζονται σε συστήματα, υπηρεσίες και εφαρμογές του [Όνομα Οργανισμού] που αποθηκεύουν ή επεξεργάζονται εσωτερική, περιορισμένης ή εμπιστευτικής φύσεως πληροφορίες. Αυτές οι πληροφορίες πρέπει να είναι κρυπτογραφημένες με χρήση αλγορίθμων κρυπτογράφησης (π.χ. AES, RSA) για να διασφαλιστεί η εμπιστευτικότητα και η ακεραιότητα των δεδομένων.

Πιο συγκεκριμένα:

Ο [Όνομα Οργανισμού] πρέπει να διασφαλίζει ότι τα δεδομένα που έχουν ταξινομηθεί ως κρίσιμα κρυπτογραφούνται κατά την αποθήκευση και μετάδοση τους.

Τα αφαιρούμενα μέσα αποθήκευσης καθώς και οι τερματικές συσκευές (endpoint devices) πρέπει να είναι κρυπτογραφημένα.

Ο [Όνομα Οργανισμού] πρέπει να έχει θεσπίσει διαδικασία για την διαχείριση των κρυπτογραφικών μέτρων που χρησιμοποιεί και η οποία να συμπεριλαμβάνει και την διαχείριση των κλειδιών κρυπτογράφησης (συμμετρικά και ασύμμετρα) σε όλο τον κύκλο ζωής τους (δημιουργία, αποθήκευση, έλεγχος, διανομή), χρησιμοποιώντας διεθνώς αποδεκτά πρότυπα και διαδικασίες, συμπεριλαμβανομένων αυστηρών κανόνων πρόσβασης στην πλατφόρμα διαχείρισης. Σε αυτή καταγράφονται ρόλοι και καθήκοντα σε σχέση με την υλοποίηση της πολιτικής κρυπτογράφησης, τη διαχείριση των κλειδιών και τους κανόνες που πρέπει να υιοθετηθούν για την αποτελεσματική υλοποίηση της πολιτικής.

Ο [Όνομα Οργανισμού] διασφαλίζει ότι κατά την κρυπτογράφηση χρησιμοποιούνται μόνο τελευταίες εκδόσεις εγκεκριμένων κρυπτογραφικών πρωτοκόλλων και λογισμικού, καθώς επίσης και το κατάλληλο μήκος κλειδιών.

Κατά την χρήση της κρυπτογράφησης, ο [Όνομα Οργανισμού] πρέπει να χρησιμοποιεί κατ’ ελάχιστον τους παρακάτω κρυπτογραφικούς αλγορίθμους:

Για την υλοποίηση συμμετρικής κρυπτογράφησης πρέπει να χρησιμοποιείται ο αλγόριθμος AES με μήκος κλειδιού τουλάχιστον 128 bits.

Για την υλοποίηση ψηφιακών υπογραφών πρέπει να χρησιμοποιείται ο αλγόριθμος RSA με μήκος κλειδιού τουλάχιστον 2048 bits.

Για την υλοποίηση αλγορίθμων κατακερματισμού πρέπει να χρησιμοποιούνται οι αλγόριθμοι SHA-256, SHA 512 ή SHA-341.

O [Όνομα Οργανισμού] πρέπει να χρησιμοποιεί λογισμικό και βιβλιοθήκες κρυπτογράφησης μόνο εφόσον έχουν ελεγχθεί από έγκυρα τρίτα μέρη.

Τα κλειδιά κρυπτογράφησης προστατεύονται ως δεδομένα του υψηλότερου βαθμού διαβάθμισης του [Όνομα Οργανισμού].

Η υποκλοπή ή διαρροή κλειδιών κρυπτογράφησης αντιμετωπίζεται σαν περιστατικό ασφάλειας πληροφοριών.

Ο [Όνομα Οργανισμού] ακολουθεί τις βέλτιστες πρακτικές κρυπτογράφησης για την cloud υποδομή του.

Σε περίπτωση που δεν είναι δυνατή η εφαρμογή κρυπτογράφησης, πρέπει να αναγνωρίζεται ως κίνδυνος και να γίνεται σχεδιασμός και υλοποίηση άλλων μέτρων για την εξασφάλιση του επιθυμητού επίπεδου ασφαλείας, σύμφωνα με την Πολιτική Διαχείρισης Κινδύνου.

## Διαγραφή ή Καταστροφή πληροφοριών

Τα παρακάτω μέτρα που προτείνονται είναι συνήθως αποτελεσματικά για την ασφαλή καταστροφή πληροφοριών, είτε πρόκειται για ψηφιακά είτε φυσικά αντικείμενα:

Οι πληροφορίες καταστρέφονται με ασφαλή τρόπο (π.χ. multiple passes of software-based overwriting), ώστε να αποφευχθεί οποιαδήποτε πιθανότητα ανάκτησης.

* Η διαδικασία αυτή περιλαμβάνει τον επανεγγραφή επαναλαμβανόμενων προτύπων δεδομένων σε επαναχρησιμοποιούμενα μέσα αποθήκευσης. Σκοπός είναι η εξασφάλιση ότι τα προηγούμενα δεδομένα δεν μπορούν να ανακτηθούν εύκολα με εργαλεία ανάκτησης δεδομένων.

Τα έγγραφα, πρέπει να καταστρέφονται με εγκεκριμένες μεθόδους (π.χ. cross cut shredding) που θα διασφαλίζουν την αδυναμία ανάκτησης.

## Ψηφιακές Υπογραφές

Συστήνεται όπως ξεκινήσει η ενσωμάτωση των ψηφιακών υπογραφών στα διάφορα συστήματα και διαδικασίες του [Όνομα Οργανισμού] με στόχο να ανιχνεύονται τυχόν μη εξουσιοδοτημένες μετατροπές δεδομένων και για να πιστοποιείται η ταυτότητα του υπογράφοντος. Οι ψηφιακές υπογραφές χρησιμεύουν ως ένα ισχυρό εργαλείο για τη διασφάλιση της ακεραιότητας των δεδομένων, τη διασφάλιση της νομικής συμμόρφωσης και τη διατήρηση της αξιοπιστίας των πληροφοριών σε όλη τη διάρκεια του κύκλου ζωής τους, από τη δημιουργία έως τη διαγραφή.

Κυρίως βοηθά στην:

* Λογοδοσία και ιχνηλασιμότητα (Accountability and Traceability) καθώς οι ψηφιακές υπογραφές δημιουργούν ένα μη μεταβλητό αρχείο σχετικά με το ποιος, πότε και πώς δημιουργήθηκαν, τροποποιήθηκαν, αποκτήθηκαν πρόσβαση ή διατέθηκαν τα δεδομένα. Αυτό ενισχύει τη λογοδοσία και διασφαλίζει την πλήρη ιχνηλασιμότητα σε ολόκληρο τον κύκλο ζωής των δεδομένων.
* Εμπιστοσύνη καθώς ο υπογραφών οικοδομεί εμπιστοσύνη με τους ενδιαφερόμενους, τους πελάτες και άλλους ρυθμιστικούς φορείς παρέχοντας εγγυήσεις ακεραιότητας και γνησιότητας δεδομένων, απαραίτητες για τη διατήρηση ενός ασφαλούς περιβάλλοντος δεδομένων και τη διασφάλιση της συμμόρφωσης.

# Εφεδρικά Αντίγραφα Πληροφοριών

Σύμφωνα με τον την Απόφαση Κ.Δ.Π 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.

# 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. Τέτοιες διατάξεις στα συμβόλαια συμβάλλουν στη διασφάλιση ευαίσθητων πληροφοριών και διασφαλίζουν ότι οι συνεργάτες του [Όνομα Οργανισμού] ακολουθούν τις αναγκαίες διαδικασίες και τηρούν τα ίδια πρότυπα ασφάλειας, εμπιστευτικότητας και συμμόρφωσης με τον οργανισμό.

Είναι σημαντικό να σημειωθεί 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.

Βασικές απαιτήσεις τέτοιας σύμβασης δύναται να περιλαμβάνουν πρόνοιες για τα ακόλουθα:

* Απαιτήσεις προστασίας δεδομένων και ασφάλειας
* Επεξεργασία και χειρισμός δεδομένων
* Εμπιστευτικότητα και μη αποκάλυψη (non-disclosure)
* Ειδοποίηση ανταπόκρισης περιστατικού και πιθανής παραβίασης δεδομένων
* Δικαίωμα ελέγχου και παρακολούθησης
* Χρήση υπεργολαβιών και άλλων τρίτων προμηθευτών
* Διατήρηση και Διάθεση Δεδομένων
* Ευθύνη και τυχόν επαγγελματική αποζημίωση
* Τερματισμός και Επιστροφή ή Καταστροφή Δεδομένων

# Αναθεώρηση

Τα έγγραφα σχετικά με την Προστασία Δεδομένων 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 π.χ. μετά από διδάγματα που αντλήθηκαν από συμβάντα που είχαν σαν αποτέλεσμα την απώλεια δεδομένων. Επιπρόσθετα η πολιτική πρέπει να αναθεωρηθεί ώστε να αντικατοπτρίζει αυτές τις αλλαγές σε περιπτώσεις που ο οργανισμός επεκτείνει τις υπηρεσίες του, αλλάξει τις δραστηριότητες επεξεργασίας δεδομένων ή αρχίσει να χειρίζεται νέους τύπους προσωπικών δεδομένων (π.χ. ευαίσθητα δεδομένα, βιομετρικά δεδομένα),

# Αναφορές

|  |  |  |  |
| --- | --- | --- | --- |
| **Κατηγορία** | **ID** | **Μέτρο** | **Στόχος Μέτρου** |
| Ασφάλεια Δεδομένων | DS1 | Διαχείριση του κύκλου ζωής των πληροφοριών | Να εξασφαλιστεί η προστασία δεδομένων καθ’ όλο τον κύκλο ζωής των πληροφοριών, συμπεριλαμβανομένης της συλλογής, καταχώρησης, οργάνωσης, δομής, αποθήκευσης, προσαρμογής ή μεταβολής, ανάκτησης, αναζήτησης, χρήσης, κοινοποίησης με διαβίβαση, διάδοσης ή κάθε άλλη μορφή διάθεσης, συσχέτισης ή συνδυασμού, περιορισμού, διαγραφής ή καταστροφής. |
| Ασφάλεια Δεδομένων | DS2 | Ταξινόμηση και επισήμανση πληροφοριών | Να εξασφαλιστεί ότι τα δεδομένα ταξινομούνται και επισημαίνονται κατά τρόπο ώστε να αντικατοπτρίζεται η ευαισθησία τους ώστε να εξασφαλίζεται η κατάλληλη επεξεργασία τους. |
| Ασφάλεια Δεδομένων | DS4 | 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. |
| Ασφάλεια Δεδομένων | DS5 | Πρόληψη απώλειας δεδομένων και διαρροής δεδομένων | Να εξασφαλιστεί η προστασία των δεδομένων από εκούσια ή ακούσια απώλεια και διαρροή δεδομένων. |
| Ασφάλεια Δικτύου | NS4 | Ασφαλή πρωτόκολλα επικοινωνίας | Να διασφαλιστούν κατάλληλα πρωτοκόλλα επικοινωνίας προκειμένου να επιτευχθεί ασφαλής επικοινωνία μεταξύ των πόρων του δικτύου. |
| Ασφάλεια Ανθρώπινων Πόρων | HRS4 | Εξωτερικοί συνεργάτες | Να εξασφαλιστεί ότι οι εξωτερικοί συνεργάτες που εργάζονται για λογαριασμό του Οργανισμού τηρούν την πολιτική ασφάλειας πληροφοριών και τους στόχους ασφάλειας του Οργανισμού. |