Όνομα Οργανισμού

Διαδικασία Ελέγχου Εγγράφων

|  |  |
| --- | --- |
| **Περιεχόμενο:** | Διαδικασία Ελέγχου Εγγράφων |
| **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. Εισαγωγή 4](#_Toc190345970)

[1.1. Σκοπός 4](#_Toc190345971)

[2. Πεδίο Εφαρμογής 4](#_Toc190345972)

[3. Χρόνος Ενεργοποίησης της Διαδικασίας 5](#_Toc190345973)

[4. Ρόλοι και Αρμοδιότητες 5](#_Toc190345974)

[4.1. Διευθύνουσα Επιτροπή Ασφάλειας Πληροφοριών (Information Security Steering Committee) 6](#_Toc190345975)

[4.2. Υπεύθυνος για την Ασφάλεια Δικτύων και Συστημάτων Πληροφοριών (ΥΑΠ) 6](#_Toc190345976)

[4.3. Ιδιοκτήτης Εγγράφου 7](#_Toc190345977)

[4.4. Συντάκτης του Εγγράφου 7](#_Toc190345978)

[4.5. Όλο το Προσωπικό 7](#_Toc190345979)

[5. Διεργασία Ελέγχου Εγγράφων 8](#_Toc190345980)

[5.1. Έκδοση & Έγκριση Εγγράφων 8](#_Toc190345981)

[5.2. Διανομή Εγγράφων 8](#_Toc190345982)

[5.3. Έλεγχος Αλλαγών 9](#_Toc190345983)

[5.4. Έλεγχος Αρχείων 9](#_Toc190345984)

[5.5. Έλεγχος Ηλεκτρονικών Αρχείων 10](#_Toc190345985)

[5.6. Περιοδικές Αναθεωρήσεις 10](#_Toc190345986)

[6. Ενέργειες 11](#_Toc190345987)

[7. Αναθεώρηση 16](#_Toc190345988)

[8. Αναφορές 16](#_Toc190345989)

# Εισαγωγή

# Σκοπός

Ο σκοπός της παρούσα διαδικασίας είναι η καθιέρωση μιας δομημένης προσέγγισης για τη δημιουργία, την σύνταξη, την αναθεώρηση, την έγκριση, τη διανομή, την ενημέρωση και την αρχειοθέτηση εγγράφων στο πλαίσιο ενός πλαισίου διαχείρισης ασφάλειας πληροφοριών, ώστε να υποβοηθάει τη συμμόρφωση με την Απόφαση Κ.Δ.Π 389/2020 και οποιονδήποτε άλλων νομοθετικών και κανονιστικών απαιτήσεων π.χ. συμμόρφωση με ISO 27001:2022.

Η διαδικασία αυτή διασφαλίζει ότι όλα τα έγγραφα είναι ακριβή, επικαιροποιημένα και προσβάσιμα από εξουσιοδοτημένο προσωπικό, αποτρέποντας παράλληλα μη εξουσιοδοτημένη πρόσβαση ή ακούσιες τροποποιήσεις που δύναται να γίνονται σε αυτά. Τυχόν τροποποιήσεις ή διαγραφές θα πραγματοποιούνται μόνο μέσω σχετικής τεκμηρίωσης.

Πιο συγκεκριμένα, στόχος αυτής της διαδικασίας είναι:

* Η διασφάλιση της ορθής διαχείρισης όλων των εγγράφων που σχετίζονται με ένα Πλαίσιο ασφάλειας πληροφοριών/κυβερνοασφάλειας καθ' όλη τη διάρκεια του κύκλου ζωής τους.
* Διατήρηση της συνέπειας, της ακεραιότητας και της ασφάλειας της τεκμηρίωσης του Πλαισίου.
* Συμμόρφωση με τις απαιτήσεις του Πλαισίου με την ύπαρξη των απαραίτητων τεκμηριωμένων πληροφοριών.
* Αποτροπή της χρήσης παρωχημένων, λανθασμένων ή μη εξουσιοδοτημένων εγγράφων εντός του [Όνομα Οργανισμού].
* Καθιέρωση ρόλων και αρμοδιοτήτων για τον έλεγχο των εγγράφων.

# Πεδίο Εφαρμογής

Η διαδικασία αυτή εφαρμόζεται για όλα τα έγγραφα που χρησιμοποιούνται σε ένα Πλαίσιο Ασφάλειας Πληροφοριών/κυβερνοασφάλειας που έχει υλοποιηθεί στον [Όνομα Οργανισμού].

Συγκεκριμένα, εφαρμόζεται για:

* Πολιτικές, διαδικασίες και άλλες κατευθυντήριες γραμμές.
* Αξιολογήσεις κινδύνων, σχέδια αντιμετώπισης καταστροφών και εκθέσεις ελέγχου.
* Αρχεία διαχείρισης περιστατικών και άλλα ημερολόγια ασφαλείας πληροφοριών
* Κάθε άλλο έγγραφο που απαιτείται για τη συμμόρφωση με την Απόφαση Κ.Δ.Π 389/2020 και οποιωνδήποτε άλλων νομοθετικών και κανονιστικών απαιτήσεων του Οργανισμού
* Ισχύει για όλους τους εργαζομένους, τους συνεργάτες και άλλα τρίτα μέρη που εμπλέκονται στο χειρισμό, τη διατήρηση ή τη τεκμηρίωση των αναγκών του Πλαισίου εντός του οργανισμού

προνοεί δραστηριότητες ώστε:

* να διασφαλίζεται ότι τα πιο πάνω είναι δομημένα, βελτιωμένα (όποτε υπάρχει ανάγκη) έγγραφα τα οποία ταυτίζονται με τις απαιτήσεις του εκάστοτε Πλαισίου ή και άλλων κανονιστικών απαιτήσεων συμμόρφωσης.
* να εγκρίνονται έγγραφα μόνο εφόσον έχει επιβεβαιωθεί η επάρκεια τους
* να καταγράφονται οι εκδόσεις των εγγράφων
* οι τελευταίες εκδόσεις των εγγράφων να είναι διαθέσιμες για χρήση

# Χρόνος Ενεργοποίησης της Διαδικασίας

Η υφιστάμενη διαδικασία ενεργοποιείται στην περίπτωση που σε νέα, ή τροποποίηση υφιστάμενης, επιχειρησιακής απαίτησης [Όνομα Οργανισμού] ή του προτύπου, διαπιστωθεί ανάγκη για:

* Δημιουργία νέου εγγράφου,
* Τροποποίηση υφιστάμενου εγγράφου
  + Περιοδικές ενημερώσεις ή αναθεωρήσεις
  + Ευρήματα ελέγχου που απαιτούν διορθωτικές ενέργειες.
  + Ρυθμιστικές ή άλλες οργανωτικές αλλαγές.
* Διαγραφή υφιστάμενου εγγράφου.

Για καλύτερη παρακολούθηση της συμμόρφωσης, συστήνεται όπως η ημερομηνία έναρξης ισχύος ενός εγγράφου και η υπογραφή έγκρισης να περιλαμβάνονται στην κεφαλίδα (header) ή στο υποσέλιδο (footer) του εγγράφου.

# Ρόλοι και Αρμοδιότητες

Ο αποτελεσματικός έλεγχος εγγράφων απαιτεί ξεκάθαρους ρόλους και αρμοδιότητες για τη διασφάλιση της συμμόρφωσης και την αποτελεσματικότητα της τεκμηρίωσης τους με το Πλαίσιο Διαχείρισης Ασφάλειας Πληροφοριών .

Ως ελάχιστοι ρόλοι καθορίζονται οι ακόλουθοι.

| **Ρόλος** | **Αρμοδιότητες** |
| --- | --- |
| **Διευθύνουσα Επιτροπή Ασφάλειας Πληροφοριών (IS Steering Committee)** | * Έγκριση βασικών εγγράφων του Πλαισίου * Κατανομή πόρων - Εξασφάλιση επαρκών εργαλείων, προσωπικού και προϋπολογισμού για τις διαδικασίες ελέγχου εγγράφων. * Παρακολούθηση & συνεχής βελτίωση * Διασφάλιση της συμμόρφωσης |
| **Υπεύθυνος για την Ασφάλεια Δικτύων και Συστημάτων Πληροφοριών (ΥΑΠ)** | * Επιβλέπει τη συμμόρφωση με τις απαιτήσεις τεκμηρίωσης του Πλαισίου Ασφάλειας Πληροφοριών /κυβερνοασφάλειας * Καθιερώνει μία συστηματική μέθοδο για τη μοναδική ταυτοποίηση και ονομασία των εγγράφων * Διατηρεί αποθετήριο εγγράφων και έλεγχο εκδόσεων. * Διασφαλίζει τη σωστή διανομή και τον έλεγχο πρόσβασης. |
| **Ιδιοκτήτης Εγγράφου** | * Διασφαλίζει ότι τα έγγραφα είναι ακριβή και ενημερωμένα. * Ελέγχει και εγκρίνει τις αλλαγές. * Διασφαλίζει τη σωστή διανομή και τον έλεγχο πρόσβασης. |
| **Συγγραφέας Εγγράφου** | * Υπεύθυνος για την σύνταξη, τη διάρθρωση του εγγράφου. * Επικύρωση περιεχομένου & διασφάλιση ακρίβεια του εγγράφου πριν αυτό προχωρήσει από τη διαδικασία αναθεώρησης και έγκρισης. * Έλεγχος εκδόσεων & διαχείριση αλλαγών |
| **Όλο το προσωπικό** | * Χρήση μόνο των τελευταίων εγκεκριμένων εκδόσεων των εγγράφων. * Αναφέρουν τυχόν ασυμφωνίες ή παρωχημένα έγγραφα. |

\*\* Ο κάθε οργανισμός δύναται να καθορίσει μόνο τους ρόλους οι οποίοι ευθυγραμμίζονται με τις ανάγκες και την δομή του και να απαλείψει τους ρόλους οι οποίοι δεν εφαρμόζονται σε κάθε περίπτωση.

# Διευθύνουσα Επιτροπή Ασφάλειας Πληροφοριών (Information Security Steering Committee)

Η Διευθύνουσα Επιτροπή Ασφάλειας Πληροφοριών έχει την ευθύνη για τον καθορισμό της στρατηγικής και της πολιτικής στα θέματα ασφάλειας πληροφοριών. Ως εκ τούτου, εγκρίνει τις πολιτικές του Πλαισίου και μέσω σχετικής ετήσιας διευθυντικής ενημέρωσης (Management Review) παρακολουθεί τη συμμόρφωση [Όνομα Οργανισμού] με την Απόφαση Κ.Δ.Π 389/2020 και άλλες σχετικές κανονιστικές απαιτήσεις καθώς και τις πολιτικές που απορρέουν από αυτές. Επιβεβαιώνει ότι οι πολιτικές του Πλαισίου είναι επικαιροποιημένες, ακριβείς, αποτελεσματικές και ότι σημειώνεται πρόοδος ως αποτέλεσμα των σχετικών διορθωτικών, προληπτικών, βελτιωτικών ενεργειών και παρέχει όλους τους απαραίτητους πόρους .

# Υπεύθυνος για την Ασφάλεια Δικτύων και Συστημάτων Πληροφοριών (ΥΑΠ)

Ο Υπεύθυνος για την Ασφάλεια Δικτύων και Συστημάτων Πληροφοριών (ΥΑΠ)διατηρεί το σύνολο των εγγράφων του Πλαισίου σύμφωνα με τη διαδικασία, διασφαλίζοντας ότι:

* Τα έγγραφα του Πλαισίου ταυτίζονται με τις πρόνοιες της Απόφασης Κ.Δ.Π 389/2020 και οποιονδήποτε άλλων νομοθετικών και κανονιστικών απαιτήσεων.
* Καθιερώνει μία συστηματική μέθοδο για τη μοναδική ταυτοποίηση και ονομασία των εγγράφων.
* Τα έγγραφα έχουν μοναδικό αριθμό αναφοράς και ελεγχόμενο αριθμό έκδοσης.
* Τα νέα έγγραφα καταγράφονται στα αρχεία του Πλαισίου και εγκρίνονται από το εκάστοτε αρμόδιο όργανο.
* Οι αναγκαίες τροποποιήσεις των εγγράφων ελέγχονται, καταγράφονται και εγκρίνονται από τα αρμόδια όργανα πριν τη δημοσίευση της νέας έκδοσης.
* Επιβεβαιώνει ότι δεν χρησιμοποιούνται έγγραφα τα οποία δεν είναι εγκριμένα.
* Δημιουργεί ένα σύστημα ελέγχου εκδόσεων(version control) για τη διαχείριση των διαφορετικών εκδόσεων των εγγράφων.

# Ιδιοκτήτης Εγγράφου

Ο Ιδιοκτήτης του εγγράφου είναι υπεύθυνος για την εφαρμογή των προνοιών των εγγράφων που αφορούν τις αρμοδιότητες του και τη συντήρηση των εγγράφων αυτών, σύμφωνα με την υφιστάμενη διαδικασία, κατά τη διάρκεια της ζωής τους, διασφαλίζοντας ότι:

* Το έγγραφο είναι ενημερωμένο, διατυπωμένο με ακρίβεια και είναι κατανοητό.
* Οποιαδήποτε ανάγκη για αλλαγή αντικατοπτρίζεται έγκαιρα στο έγγραφο.
* Αποσύρονται οι ανενεργές εκδόσεις.
* Δημιουργούνται νέα έγγραφα όπου απαιτείται.
* Το έγγραφο συνοδεύεται από ικανοποιητικά έντυπα προς υποστήριξη της ορθής εφαρμογής του.
* Τα έγγραφα εκδίδονται επίσημα και ενημερώνεται σχετικά το εμπλεκόμενο προσωπικό.
* Τα έγγραφα λειτουργούν αποτελεσματικά και προσφέρουν τον απαιτούμενο έλεγχο στις υπόλοιπες διαδικασίες [Όνομα Οργανισμού].

# Συντάκτης του Εγγράφου

Ο Συντάκτης του εγγράφου είναι υπεύθυνος να:

* συντάξει το έγγραφο τηρώντας την προδιαγραμμένη δομή των εγγράφων και εφαρμόζοντας την υφιστάμενη διαδικασία.
* βεβαιωθεί ότι οι πληροφορίες που περιέχονται στο έγγραφο είναι ακριβείς, επίκαιρες και δίνουν ξεκάθαρες επεξηγήσεις στα άτομα που χρησιμοποιούν το έγγραφο.
* καταγράψει τις αναφορές σε σχέση με την έκδοση και τις αλλαγές.
* ετοιμάσει, όπου υπάρχει ανάγκη, εκπαιδευτικό / ενημερωτικό υλικό για το προσωπικό (και/ή άλλους) των οποίων η εργασία επηρεάζεται από τις πρόνοιες του εγγράφου.

# Όλο το Προσωπικό

Το προσωπικό (ή άλλα υπεύθυνα άτομα) είναι υπεύθυνο να:

* γνωρίζει τις πρόνοιες των πολιτικών και των διαδικασιών που αφορούν την εργασία του και την αλληλεπίδραση που έχουν με την τελευταία εγκριμένη έκδοση.
* αναγνωρίζει τις επιχειρησιακές ανάγκες που οδηγούν στην ανάγκη για έναρξη της διαδικασίας αυτής.
* Αναφέρει τυχόν προβλήματα ή σφάλματα που εντόπισε στα έγγραφα.

# Διεργασία Ελέγχου Εγγράφων

# Έκδοση & Έγκριση Εγγράφων

* Μόλις εντοπιστεί η ανάγκη για νέο έγγραφο, ο **Υπεύθυνος για την Ασφάλεια Δικτύων και Συστημάτων Πληροφοριών (ΥΑΠ)**, σε συνεννόηση με την αρμόδια επιτροπή, ορίζει Ιδιοκτήτη και Συντάκτη του Εγγράφου.
* Στη συνέχεια, ο συντάκτης θα χρησιμοποιήσει ένα από τα Πρότυπα [Όνομα Οργανισμού] για να συντάξει το έγγραφο, ανάλογα με τον τύπο του εγγράφου (Διαδικασία, Μορφή, Διάγραμμα Ροής κ.λπ.).
* Όταν συντάσσεται έγγραφο τμήματος (δηλ. νέες διαδικασίες και/ή έντυπα που απαιτούνται για την επεξήγηση των δραστηριοτήτων που διεξάγονται), το έγγραφο επανεξετάζεται και εγκρίνεται από τον ενδιαφερόμενο [προϊστάμενο τμήματος] που συνήθως είναι και ο ιδιοκτήτης του Εγγράφου.
* Στη συνέχεια, το έγγραφο υποβάλλεται στον Υπεύθυνος για την Ασφάλεια Δικτύων και Συστημάτων Πληροφοριών (ΥΑΠ), ο οποίος προσθέτει στο έγγραφο τον Κωδικό Ονομασία (Τίτλος) με βάση το Σύστημα Κωδικοποίησης Εγγράφων που καθιερώθηκε εντός του [Όνομα Οργανισμού] .
* Τα Εγχειρίδια, οι Πολιτικές και οι Διαδικασίες που σχετίζονται με το Πλαίσιο Διαχείρισης Ασφάλειας Πληροφοριών συντάσσονται από τον ίδιο τον Υπεύθυνος για την Ασφάλεια Δικτύων και Συστημάτων Πληροφοριών (ΥΑΠ) και εξετάζονται από την Διευθύνουσα Επιτροπή Ασφάλειας Πληροφοριών (IS Steering Committee)ως προς τη συνάφεια και την ακρίβεια τους και, στη συνέχεια, εγκρίνονται από την Εκπρόσωπο της Ανώτατης Διοίκησης. Εάν το σχέδιο εγγράφου δεν εγκριθεί, επιστρέφεται στον συντάκτη του για διορθώσεις.
* Όλα τα έγγραφα του πλαισίου επανεξετάζονται από κάθε Ιδιοκτήτη Εγγράφου τουλάχιστον μία φορά ετησίως προκειμένου να διασφαλίζεται η καταλληλόλητα και η συμμόρφωση του ή όταν παρίσταται ανάγκη.

# Διανομή Εγγράφων

* Ο Υπεύθυνος για την Ασφάλεια Δικτύων και Συστημάτων Πληροφοριών (ΥΑΠ) είναι υπεύθυνος για τη διανομή ελεγχόμενων αντιγράφων όλων των εγγράφων του Πλαισίου, τα αντίγραφα μπορούν να διανεμηθούν είτε σε έντυπη είτε σε ψηφιακή μορφή.
* Διανομή Αντιγράφων σε Ψηφιακή Μορφή:
* Ο ΥΑΠ θα δημοσιεύει μέσω του ενδοδικτύου (intranet), όλα τα έγγραφα του Πλαισίου σε μορφή «μόνο για ανάγνωση», στην οποία μπορεί να έχει πρόσβαση όλο το προσωπικό που θα πρέπει να λάβει γνώση.
* Κατά την ανάπτυξη νέας διαδικασίας ή ακόμη και την αναθεώρηση υφιστάμενης διαδικασίας, ο ΥΑΠ κοινοποιεί τις λεπτομέρειες και τη θέση της διαδικασίας στον ενδοδίκτυο (intranet) αποστέλλοντας ηλεκτρονικό μήνυμα (email) σε όλα τα ενδιαφερόμενα μέρη.
* Διανομή Αντιγράφων σε Έντυπη Μορφή:
* Αντίγραφα σε εξωτερικά μέρη παρέχονται μόνο με τη συγκατάθεση ΥΑΠ ή εκπρόσωπο της Ανώτατης Διεύθυνσης.

# Έλεγχος Αλλαγών

* Αλλαγές στην τεκμηρίωση του Πλαισίου μπορούν να προταθούν ως αποτέλεσμα της ανασκόπησης της διοίκησης, των ελέγχων, της ανατροφοδότησης από τα ενδιαφερόμενα μέρη, των μελετών συγκριτικής αξιολόγησης και, σε περιπτώσεις προσωπικού που χειρίζονται τα εγχειρίδια, να προσδιοριστεί ένας τρόπος με τον οποίο μπορεί να βελτιωθεί.
* Τυχόν μικρές αλλαγές στα έγγραφα του συστήματος διαχείρισης εξετάζονται από τον αρχικό Συντάκτη του Εγγράφου, επαληθεύονται από τον Ιδιοκτήτη Εγγράφου και αποστέλλονται στον ΥΠΑ για έγκριση από εκπρόσωπο της Ανώτατης Διοίκησης.
* Σε περίπτωση αλλαγών που απαιτούν αναθεώρηση οποιουδήποτε εγγράφου του Πλαισίου, ολόκληρο το έγγραφο αναθεωρείται. Στην περίπτωση αυτή, ο δείκτης έκδοσης/αναθεώρησης είναι αυξητικός.
* Περιγραφή της αλλαγής, νέος αριθμός έκδοσης/αναθεώρησης και ημερομηνία αναθεώρησης σημειώνεται στον πίνακα ελέγχου εγγράφων του εγγράφου.
* Κατά κανόνα, όλα τα παρωχημένα έγγραφα απομακρύνονται από τον τόπο έκδοσης και από όλους τους τόπους χρήσης. Το πρωτότυπο αντίγραφο (κύριο αντίγραφο) των παρωχημένων εγγράφων φέρει τη σφραγίδα «ΠΑΡΩΧΗΜΕΝΟ» και κατατίθεται χωριστά στον εκπρόσωπο της Ανώτατης Διοίκησης για λόγους γνώσης και νομιμότητας και όλα τα άλλα αντίγραφα καταστρέφονται.

# Έλεγχος Αρχείων

Η περίοδος διατήρησης και ο τόπος αποθήκευσης οποιουδήποτε αρχείου καθορίζονται σε κάθε εγχειρίδιο ή διαδικασία και ανάλογα με τυχόν κανονιστικές απαιτήσεις του Οργανισμού Ενδεικτικά καταγράφονται πιο κάτω προτεινόμενοι περίοδοι διατήρησης και ενδεικτικός τρόπος απόρριψης των εγγράφων του Πλαισίου.

| **Είδος Εγγράφου** | **Περίοδος διατήρησης (Retention Period)** | **Μέθοδος απόρριψης** |
| --- | --- | --- |
| **Πολιτικές & Διαδικασίες Πλαισίου** | 3 έτη | Ασφαλής διαγραφή/καταστροφή (shredding) |
| **Αξιολογήσεις κινδύνων** | 5 έτη | Ασφαλής διαγραφή/καταστροφή (shredding) |
| **Αποτελέσματα Ελέγχων** | 5 έτη | Ασφαλής διαγραφή/καταστροφή (shredding) |
| **Αναφορές περιστατικών & αρχεία καταγραφής** | 2 έτη | Ασφαλής διαγραφή/καταστροφή (shredding) |
| **Αρχεία κατάρτισης & εκπαίδευσης** | 2 έτη | Ασφαλής διαγραφή/καταστροφή (shredding) |

* Κατά τη διάρκεια της περιόδου αποθήκευσης, όλα τα αρχεία πρέπει να προστατεύονται από τυχόν ζημιές, απώλειες και αλλοιώσεις λόγω περιβαλλοντικών συνθηκών ή άλλων παραγόντων.
* Στην αρχή κάθε έτους, όλα τα αρχεία και οι φάκελοι θα πρέπει να επανεξετάζονται για να διαπιστωθεί εάν έχουν υπερβεί την περίοδο διατήρησης, σφραγίζοντας τα ως «ΠΑΡΩΧΗΜΕΝΑ» ή/και αλλάζοντας την τοποθεσία τους ή καταστρέφοντας τα αφού λάβουν την έγκριση του Εκπροσώπου της Ανώτατης Διοίκησης.

# Έλεγχος Ηλεκτρονικών Αρχείων

* Όλα τα δεδομένα που αποθηκεύονται σε ηλεκτρονική μορφή προστατεύονται από καταστροφή, αλλοίωση και μη εξουσιοδοτημένη πρόσβαση.
* Όλα τα δεδομένα διατηρούνται σε έναν κεντρικό εξυπηρετητή αρχείων (fileserver) οργανωμένο σε υπηρεσιακή βάση. Κάθε τμήμα ή υπομονάδα έχει δικαιώματα πρόσβασης μόνο στα δικά του δεδομένα.
* Το Τμήμα Πληροφορικής του [Όνομα Οργανισμού] είναι υπεύθυνο για τη λήψη και διατήρηση αντιγράφων ασφαλείας όλων των δεδομένων σε ημερήσια, εβδομαδιαία και μηνιαία βάση (ακολουθώντας την αντίστοιχη πολιτική δημιουργίας αντιγράφων ασφαλείας).
* Όλα τα αντίγραφα ασφαλείας φυλάσσονται σε ασφαλές μέρος εντός [Όνομα Οργανισμού] και ένα σύνολο αντιγράφων ασφαλείας διατηρείται εκτός [Όνομα Οργανισμού] σε πυρίμαχα ασφαλή μέρη.

# Περιοδικές Αναθεωρήσεις

Η επίσημη επανεξέταση αυτής της διαδικασίας διεξάγεται τουλάχιστον ετησίως, ωστόσο ενδέχεται να διεξάγονται συχνότερες αναθεωρήσεις για να ληφθούν υπόψη οι μεταβαλλόμενες συνθήκες, η νομοθεσία, η τεχνολογία και οι κίνδυνοι ασφαλείας για την επιχείρηση ή λόγω σχετικής μη συμμόρφωσης.

Ο Εσωτερικός Έλεγχος που απαιτείται από τις πρόνοιες του Πλαισίου διεξάγει ανεξάρτητες αναθεωρήσεις με στόχο την αξιολόγηση της επάρκειας των εφαρμοζόμενων μέτρων όταν η έλλειψη τέτοιων μέτρων μπορεί να θέσει σε σημαντικό κίνδυνο τον [Όνομα Οργανισμού] . Οι επανεξετάσεις αυτές περιλαμβάνουν έλεγχο συμμόρφωσης με την παρούσα διαδικασία και μπορούν να οδηγήσουν σε τροποποιήσεις της διαδικασίας, ανάλογα με τις ανάγκες.

# Ενέργειες

| **Ενέργεια** | **Ιδιοκτήτης Ενέργειας** | **Λεπτομερής περιγραφή της ενέργειας της διαδικασίας** |
| --- | --- | --- |
| 1. Δημιουργία καταλόγου εγγράφων και αλλαγών στα έγγραφα του Πλαισίου | Υπεύθυνος για την Ασφάλεια Δικτύων και Συστημάτων Πληροφοριών (ΥΑΠ) | Δημιουργία Καταλόγου Εγγράφων και Καταλόγου Αλλαγών στα εγγραφα του Συστήματος, για να καταγράφονται οι ενέργειες που απορρέουν από την εν λόγω διαδικασία. |
| 2. Προληπτική θεώρηση εγγράφων | * Υπεύθυνος για την Ασφάλεια Δικτύων και Συστημάτων Πληροφοριών (ΥΑΠ)Ιδιοκτήτης Εγγράφου | Προληπτική θεώρηση όλων των εγγράφων του Οργανισμού. Κατα τη θεώρηση καθορίζεται πιθανή ανάγκη για τροποποίηση των πολιτικών, διαδικασιών, εγχειριδίων και εντύπων του Πλαισίου. |
| 3. Αναγνώριση απαίτησης για αλλαγή σε έγγραφο | Συγγραφέας Εγγράφου ή και Ιδιοκτήτη | Θεώρηση των απαιτήσεων της Απόφασης Κ.Δ.Π 389/2020 και άλλων καλών πρακτικών και αναγνώριση ανάγκης για δημιουργία νέου ή τροποποίηση υφιστάμενου εγγράφου του Πλαισίου. |
| 4. Αναγνώριση των αναγκών που θα καλύπτει το νέο έγγραφο / η νέα έκδοση του εγγράφου | Συγγραφέας Εγγράφου | Αναγνώριση των επιχειρησιακών αναγκών, συμπεριλαμβανομένης της χρήσης του εγγράφου και τα Τμήματα / Υπηρεσίες / Υπομονάδες που θα επηρεαστούν. |
| 5. Σύνταξη νέου / αναθεωρημένου εγγράφου | Συγγραφέας Εγγράφου | Σύνταξη / Αναθεώρηση εγγράφου στη βάση της προδιαγραμμένης δομής εγγράφων του Πλαισίου. |
| 6α. Υποβολή για θεώρηση / έγκριση | Συγγραφέας Εγγράφου | Υποβολή του εγγράφου στον Ιδιοκτήτη του για θεώρηση ως προς το τεχνικό περιεχόμενο του.  Εφόσον ολοκληρωθεί το έγγραφο και εγκριθεί από τον Ιδιοκτήτη, υποβάλλεται στον Υπεύθυνος για την Ασφάλεια Δικτύων και Συστημάτων Πληροφοριών (ΥΑΠ)για έλεγχο συμμόρφωσης με τις απαιτήσεις ασφάλειας πληροφοριών (προτύπων, καλών πρακτικών κ.α.).  Τα έγγραφα του Πλαισίου είναι απαραίτητο να λάβουν έγκριση του ΥΑΠ, προτού υποβληθούν για έγκριση στην Διευθύνουσα Επιτροπή Ασφάλειας Πληροφοριών)ή στον Επικεφαλής του Οργανισμού ή άλλο εκπρόσωπο της Ανώτατης Διεύθυνσης. |
| 6β. Θεώρηση νέου / αναθεωρημένου εγγράφου | Ιδιοκτήτης Εγγράφου & Υπεύθυνος για την Ασφάλεια Δικτύων και Συστημάτων Πληροφοριών (ΥΑΠ) | Ο Ιδιοκτήτης του εγγράφου και ο ΥΑΠ, ο καθένας στον τομέα του, πιθανώς να προβούν σε τροποποιήσεις στο έγγραφο, λαμβάνοντας υπόψη τουλάχιστον τα ακόλουθα:   * τον σκοπό και τον στόχο * την επάρκεια και την ακρίβεια των πληροφοριών σε αυτό * τη σαφήνεια και την ευκολία στην εφαρμογή * την ορθή κατηγοριοποίηση της εμπιστευτικότητας * την ορθή αναφορά αλλαγής, έκδοσης και εγγράφου * τη δομή και τον τρόπο σύνταξης.   Μέλη της Διευθύνουσας Επιτροπής Ασφάλειας Πληροφοριών μπορούν να υποβάλουν σχόλια εφ’ όλης της ύλης του εγγράφου, με ιδιαίτερη προσοχή σε θέματα πολιτικής και στρατηγικής. |
| 6γ. Έγκριση νέου εγγράφου / νέας έκδοσης εγγράφου | Ιδιοκτήτης Εγγράφου & Υπεύθυνος για την Ασφάλεια Δικτύων και Συστημάτων Πληροφοριών (ΥΑΠ) | Έγκριση εγγράφου με τη σειρά ως ακολούθως:   * Πολιτική: Ιδιοκτήτης Εγγράφου, ΥΑΠ, Διευθύνουσα Επιτροπή Ασφάλειας Πληροφοριών * Διαδικασία: Ιδιοκτήτης Εγγράφου, ΥΑΠ, Εκπρόσωπος της Ανώτατης Διοίκησης π.χ. Διευθυντής * Άλλα Έντυπα: Ιδιοκτήτης Εγγράφου * Κανένα έγγραφο δεν καταχωρείται επίσημα ως μέρος του Πλαισίου χωρίς να εξασφαλίσει τις πιο πάνω εγκρίσεις. |
| 7. Ετοιμασία Εκπαίδευσης / Ενημέρωσης | Ιδιοκτήτης Εγγράφου | Όπου κρίνεται αναγκαίο, διενεργείται εκπαίδευση / ενημέρωση στο επηρεαζόμενο προσωπικό (ή άλλα άτομα) για διασφάλιση της αποτελεσματικής εφαρμογής των νέων προνοιών του εγγράφου. |
| 8. Διαθεσιμότητα εκδόσεων των εγγράφων | Ιδιοκτήτης Εγγράφου | Ο ιδιοκτήτης του εγγράφου φροντίζει να ενημερώσει το προσωπικό με τη νέα έκδοση, ώστε η ανενεργή έκδοση να παύσει να είναι διαθέσιμη. |
| 9. Αξιολόγηση εφαρμογής νέων προνοιών | Ιδιοκτήτης Εγγράφου  Υπεύθυνος για την Ασφάλεια Δικτύων και Συστημάτων Πληροφοριών (ΥΑΠ) | Όπου κρίνεται αναγκαίο, π.χ. για νέο έγγραφο ή σημαντική τροποποίηση υφιστάμενου εγγράφου, προγραμματίζεται αξιολόγηση της εφαρμογής των νέων προνοιών ώστε να επιβεβαιωθεί η αποτελεσματικότητα τους.  Τα αποτελέσματα της αξιολόγησης υποβάλλονται στον Υπεύθυνος για την Ασφάλεια Δικτύων και Συστημάτων Πληροφοριών (ΥΑΠ)και εάν κριθεί απαραίτητο συμφωνείται η διενέργεια επιπρόσθετων ενεργειών. |
| 10. Σύνταξη Ετήσιας Έκθεσης Απόδοσης (όπου εφαρμοζεται) | Υπεύθυνος για την Ασφάλεια Δικτύων και Συστημάτων Πληροφοριών (ΥΑΠ) | Εφόσον μελετηθούν οι μετρήσεις απόδοσης της διαδικασίας καθώς και τυχόν εκθέσεις εσωτερικών και εξωτερικών ελεγκτών που αφορούν τα έγγραφα του Πλαισίου, καταγράφεται η ακρίβεια, η αποτελεσματικότητα και η ενημέρωση και συντάσσεται η ετήσια έκθεση απόδοσης του ελέγχου των εγγράφων του Πλαισίου Ασφάλειας πληροφοριών /κυβερνοασφάλειας σε περίπτωση που ζητηθεί από την Ανώτατη Διεύθυνσης ή της Διευθύνουσα Επιτροπή Ασφάλειας Πληροφοριών. |
| 11. Θεώρηση ετήσιας έκθεσης απόδοσης | Διευθύνουσα Επιτροπή Ασφάλειας Πληροφοριών | Θεώρηση της ετήσιας έκθεσης απόδοσης λαμβάνοντας υπόψη διορθωτικές / προληπτικές / βελτιωτικές ενέργειες. |
| 12. Συμφωνία και εφαρμογή δράσεων | Υπεύθυνος για την Ασφάλεια Δικτύων και Συστημάτων Πληροφοριών (ΥΑΠ) | Συμφωνούνται ενδεχόμενες διορθωτικές, προληπτικές και βελτιωτικές ενέργειες καθώς και οι ημερομηνίες ολοκλήρωσης τους.  Όπου κρίνεται αναγκαίο, αξιολογείται η αποτελεσματικότητα αυτών των ενεργειών. |

# Αναθεώρηση

Τα έγγραφα σχετικά με τη Διαδικασία Ελέγχου Εγγράφων επανεξετάζονται και να αναθεωρούνται τουλάχιστον ετησίως ή σε περίπτωση σημαντικών αλλαγών στο περιβάλλον του [Όνομα Οργανισμού] με στόχο να διασφαλίζεται ότι παραμένει επικαιροποιημένη, αποτελεσματική και ευθυγραμμισμένη με τις ανάγκες του οργανισμού, τυχόν νομικές/κανονιστικές απαιτήσεις και άλλες τεχνολογικές εξελίξεις όπως νέες αναδυόμενες απειλές κτλ.). Επιπρόσθετα, αυτή δύναται να αναθεωρείτε μετά τη διενέργεια εσωτερικών ελέγχων ή μετά από τυχόν σχόλια από τους ενδιαφερόμενους φορείς σε περίπτωση που εισηγηθούν βελτιώσεις ή εντοπίσουν λάθη ή προβλήματα αποτελεσματικότητας στην παρακολούθηση εγγράφων, τη διατήρηση ή τον έλεγχο μίας έκδοσης.

# Αναφορές

|  |  |  |  |
| --- | --- | --- | --- |
| **Κατηγορία** | **ID** | **Μέτρο** | **Στόχος Μέτρου** |
| Διακυβέρνηση | GOV3 | Πολιτικές, πρότυπα, κατευθυντήριες γραμμές και διαδικασίες ασφάλειας πληροφοριών. | Να θεσπιστούν πολιτικές, πρότυπα, κατευθυντήριες γραμμές και διαδικασίες για την ασφάλεια πληροφοριών που να αντικατοπτρίζουν τη στρατηγική ασφάλειας πληροφοριών. |