Όνομα Οργανισμού

Διαδικασία Ελέγχου Ασφάλειας Πληροφοριών

|  |  |
| --- | --- |
| **Περιεχόμενο:** | Διαδικασία Ελέγχου Ασφάλειας Πληροφοριών |
| **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](#_Toc155095256)

[2. Ρόλοι και Αρμοδιότητες 5](#_Toc155095257)

[3. Έλεγχοι Κ.Δ.Π. 389/2020 5](#_Toc155095258)

[3.1. Σκοπός 5](#_Toc155095259)

[3.2. Πεδίο Εφαρμογής 6](#_Toc155095260)

[3.3. Πόροι 6](#_Toc155095261)

[3.4. Κριτήρια 6](#_Toc155095262)

[3.5. Πρόγραμμα 6](#_Toc155095263)

[3.6. Μέθοδοι 6](#_Toc155095264)

[3.7. Πρόγραμμα Προ-Ελέγχου 7](#_Toc155095265)

[3.8. Προετοιμασία Εκθέσεων & Ανακοίνωση Ευρημάτων 7](#_Toc155095266)

# Εισαγωγή

Σκοπός του παρόντος εγγράφου είναι να καθορίσει τον τρόπο με τον οποίο ο [Όνομα Οργανισμού] θα ελέγχει την αποτελεσματικότητα των εφαρμοζόμενων μέτρων ασφαλείας που προβλέπει στο Σχέδιο Αντιμετώπισης Κινδύνων με βάση το Κ.Δ.Π. 389/2020.

Οι στόχοι αυτής της διαδικασίας ελέγχου είναι:

* Να διασφαλιστεί ότι οι διαδικασίες ασφάλειας των πληροφοριών διεξάγονται αποτελεσματικά, αποδοτικά και οικονομικά προς όφελος του [Όνομα Οργανισμού].
* Για τον προσδιορισμό της συμμόρφωσης ή τον εντοπισμό οποιωνδήποτε τομέων μη συμμόρφωσης με τον κανονισμό Κ.Δ.Π. 398/2020.
* Τον προσδιορισμό περαιτέρω ευκαιριών συνεχούς βελτίωσης, οι οποίες ενδέχεται να εκτείνονται πέραν των κριτηρίων που ορίζονται στον κανονισμό Κ.Δ.Π. 389/2020.
* Να παρέχει στον [Όνομα Οργανισμού] εσωτερική διαβεβαίωση ότι η διαχείριση της ασφάλειας των πληροφοριών γίνεται αποτελεσματικά και ότι ελαχιστοποιούνται οι κίνδυνοι για την επιχείρηση.

# Ρόλοι και Αρμοδιότητες

| Ρόλος | Αρμοδιότητα |
| --- | --- |
| Ελεγκτής | * Προετοιμασία και εκτέλεση του Προγράμματος Ελέγχου * Επιβολή των βέλτιστων αρχών και πρακτικών ελέγχου κατά τη συλλογή και ανταλλαγή ευρημάτων ως μέρος της ελεγκτικής δραστηριότητας * Σύνταξη έκθεσης εσωτερικού ελέγχου. |
| CISO (Chief Information Security Officer) | * Yπεύθυνος για τον σχεδιασμό, την υλοποίηση και τη διαχείριση των πολιτικών και των διαδικασιών ασφάλειας πληροφοριών * Παρακολούθηση απειλών και ευπαθειών * Ανάλυση των κινδύνων ασφάλειας πληροφοριών και ανάπτυξη στρατηγικών για τη μείωσή τους * Εφαρμογή ελέγχων ασφαλείας * Διαχείριση επιθέσεων και παραβιάσεων * Επικοινωνία με ενδιαφερόμενα μέρη * Διαχείριση αποκατάστασης και επαναφοράς * Παρακολούθηση υλοποίησης ευρημάτων ελέγχου |
| I.T. Manager | * Σχεδιασμός και εφαρμογή πολιτικών ασφαλείας (σε συνεργασία με CISO) * Διαχείριση συστημάτων ασφαλείας * Ανάπτυξη και εφαρμογή ελέγχων ασφαλείας * Διαχείριση καταστάσεων επείγουσας ανάγκης * Διαχείριση επιθέσεων * Eνημέρωση για νέες απειλές |
| ΚΕΑΠ (Καθοδηγητική Επιτροπή Ασφάλειας Πληροφοριών) | * Υπεύθυνη για την καθοδήγηση, την εποπτεία και την υποστήριξη των προσπαθειών ασφαλείας πληροφοριών * Έγκριση προγράμματος ελέγχου ασφαλείας πληροφοριών, συμπεριλαμβανομένων των ελέγχων, διαδικασιών και πολιτικών * Ενημέρωση σχετικά με τη μη συμμόρφωση με τις πολιτικές ασφαλείας * Προώθηση τυχόν αλλαγών στις πολιτικές * Συμβουλευτικό όργανο της διοίκησης για θέματα ασφάλειας * Ανάπτυξη και υλοποίηση εκπαιδευτικών προγραμμάτων ασφαλείας για το προσωπικό * Παρακολούθηση της αποτελεσματικότητας των μέτρων ασφαλείας πληροφοριών |

# Έλεγχοι Κ.Δ.Π. 389/2020

# Σκοπός

Κατά την διεκπεραίωση ενός ελέγχου, θα πρέπει να καθοριστεί ο λόγος για τον οποίο πρέπει να διενεργηθεί ο έλεγχος. Σκοπός ενός συγκεκριμένου ελέγχου θα μπορούσε να είναι ο προσδιορισμός του επιπέδου συμμόρφωσης με έναν συγκεκριμένο νόμο, κανονισμό, πρότυπο ή σύμβαση (π.χ. Κ.Δ.Π. 389/2020) . Επιπρόσθετα, ο σκοπός ενός ελέγχου θα μπορούσε να είναι να καθορίσει εάν έχουν αποκατασταθεί συγκεκριμένες ελλείψεις ελέγχου που εντοπίστηκαν σε προηγούμενους ελέγχους ή να καθοριστεί το επίπεδο συμμόρφωσης με έναν νέο νόμο ή πρότυπο στο οποίο μπορεί να υπόκειται ο οργανισμός στο μέλλον.

# Πεδίο Εφαρμογής

Οι έλεγχοι καλύπτουν όλα τα πληροφοριακά στοιχεία εντός του [Όνομα Οργανισμού]. Κατά περίπτωση, θα πραγματοποιούνται επίσης συζητήσεις με πρόσθετα εμπλεκόμενα μέρη. Οι πτυχές των υπηρεσιών που παρέχονται από τρίτους δεν θα ελέγχονται άμεσα, αλλά η διαχείριση των εν λόγω προμηθευτών θα ελέγχεται εξονυχιστικά.

Ενδέχεται επίσης να διενεργηθούν πιο συγκεκριμένοι έλεγχοι. Το πεδίο εφαρμογής των ελέγχων αυτών μπορεί να είναι πολυδιάστατο:

* Μια δεδομένη περίοδος – δηλαδή αρχεία που καλύπτουν ημερομηνία έναρξης και ημερομηνία λήξης μπορεί να περιλαμβάνουν το σώμα των αποδεικτικών στοιχείων
* Γεωγραφία – συστήματα σε μία συγκεκριμένη τοποθεσία
* Τεχνολογία – συστήματα που χρησιμοποιούν συγκεκριμένο λειτουργικό σύστημα, βάση δεδομένων, εφαρμογή ή άλλη πτυχή
* Επιχειρηματική διαδικασία – συστήματα που υποστηρίζουν συγκεκριμένες διαδικασίες, όπως λογιστική, καταχώρηση παραγγελιών ή υποστήριξη πελατών
* Τμήμα του οργανισμού

# Πόροι

Ο Υπεύθυνος Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών εκτελεί το πρόγραμμα ελέγχου με τη συμβολή της διοίκησης του [Όνομα Οργανισμού] και του προσωπικού.

Κατά περίπτωση, καθορίζονται και άλλοι τύποι πόρων, όπως ο αριθμός των ανθρωποωρών που θα απαιτηθούν, οι δεξιότητες που απαιτούνται από τον ελεγχόμενο, τα εξειδικευμένα εργαλεία κ.λπ.

# Κριτήρια

Η Απόφαση Κ.Δ.Π. 389/2020 χρησιμοποιείται ως βάση των κριτηρίων ελέγχου. Μπορούν να προστεθούν πρόσθετα κριτήρια, εάν χρειαστεί.

# Πρόγραμμα

Ένας αρχικός έλεγχος θα πραγματοποιηθεί στις [Ορίστε χρονικό διάστημα], ο οποίος θα καλύπτει όλα τα εφαρμοζόμενα μέτρα σχετικά με την ασφάλεια πληροφοριών. Στη συνέχεια, οι έλεγχοι θα πραγματοποιούνται κάθε 12 μήνες. Οι επιλεγμένες διαδικασίες επανεξετάζονται με την πρόθεση ότι όλες οι διαδικασίες θα καλύπτονται σε χρονικό πλαίσιο ενός έτους. Το λεπτομερές πρόγραμμα ελέγχων θα τηρείται από τον Υπεύθυνο Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών και θα διατίθεται κατόπιν αιτήματος.

# Μέθοδοι

Οι έλεγχοι θα συνίστανται σε συνδυασμό εργαστηρίων ανασκόπησης εγγράφων και ελέγχου για να συνομιλούν με τη διοίκηση και το προσωπικό. Τα κατάλληλα αρχεία θα εξεταστούν ως αποδεικτικά στοιχεία ότι ακολουθούνται οι τεκμηριωμένες διαδικασίες.

Θα αξιολογηθούν οι δράσεις που προέκυψαν από προηγούμενους ελέγχους.

# Πρόγραμμα Προ-Ελέγχου

Ο/Η Υπεύθυνος Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών λαμβάνει πληροφορίες σχετικά με τον έλεγχο που θα του επιτρέψουν να καταρτίσει το σχέδιο ελέγχου:

* Τοποθεσία ή τοποθεσίες που πρέπει να επισκεφθεί
* Κατάλογος των εφαρμογών που θα εξεταστούν
* Οι τεχνολογίες που υποστηρίζουν κάθε εφαρμογή
* Πολιτικές, πρότυπα και διαγράμματα που περιγράφουν το περιβάλλον

Χρησιμοποιώντας τις πληροφορίες που λαμβάνονται σχετικά με τους στόχους και το πεδίο εφαρμογής του ελέγχου, ο/η Υπεύθυνος Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών μπορεί πλέον να αναπτύξει διαδικασίες για τον ενάγων έλεγχο. Για κάθε στόχο και έλεγχο που πρέπει να εξεταστεί, ο ελεγκτής μπορεί να καθορίσει:

* Μια λίστα με τα άτομα προς συνέντευξη
* Ερωτήσεις που πρέπει να γίνουν κατά τη διάρκεια κάθε συνέντευξης
* Τεκμηρίωση που πρέπει να ζητηθεί κατά τη διάρκεια κάθε συνέντευξης
* Εργαλεία ελέγχου που θα χρησιμοποιηθούν
* Ποσοστά και μεθοδολογίες δειγματοληψίας
* Πώς και πού θα αρχειοθετηθούν τα αποδεικτικά στοιχεία
* Πώς θα αξιολογηθούν τα αποδεικτικά στοιχεία

# Προετοιμασία Εκθέσεων & Ανακοίνωση Ευρημάτων

Θα συνταχθεί προσχέδιο έκθεσης ελέγχου με τα πορίσματα και τις συστάσεις, και το περιεχόμενο θα κοινοποιηθεί αρχικά στους υπεύθυνους των εμπλεκόμενων τμημάτων, οι οποίοι θα έχουν την ευκαιρία να σχολιάσουν.

Θα συμφωνηθεί σχέδιο δράσης για την αντιμετώπιση τυχόν ελλείψεων και λήψη διορθωτικών μέτρων.

Η τελική έκθεση θα συνταχθεί και θα κοινοποιηθεί στους υπεύθυνους των εμπλεκόμενων τμημάτων και θα διατεθεί στην εκτελεστική ομάδα διαχείρισης, ανάλογα με την περίπτωση.

Οι έλεγχοι παρακολούθησης πραγματοποιούνται σύμφωνα με το σχέδιο δράσης για να διασφαλιστεί ότι έχουν αντιμετωπιστεί/εφαρμοστεί τυχόν ελλείψεις και διορθωτικά μέτρα.