Όνομα Οργανισμού

Οδηγός Συμπλήρωσης Εγγράφων

|  |  |
| --- | --- |
| **Περιεχόμενο:** | Οδηγός Συμπλήρωσης 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

[Πίνακας Περιεχομένων 3](#_Toc190346030)

[1. Βήμα 1 - Στρατηγική Ασφάλειας Πληροφοριών 5](#_Toc190346031)

[1.1. Βήμα 1.1 5](#_Toc190346032)

[2. Βήμα 2 - Πολιτική Διακυβέρνησης Ασφάλειας Πληροφοριών 5](#_Toc190346033)

[2.1. Βήμα 2.1 5](#_Toc190346034)

[3. Βήμα 3 - Πολιτική Ασφάλειας Πληροφοριών 6](#_Toc190346035)

[4. Βήμα 4 - Μεθοδολογία Διαχείρισης Κινδύνου 6](#_Toc190346036)

[5. Βήμα 5 - Asset Based Risk Assessment Workbook 6](#_Toc190346037)

[5.1. Βήμα 5.1 6](#_Toc190346038)

[5.2. Βήμα 5.2 7](#_Toc190346039)

[5.3. Βήμα 5.3 7](#_Toc190346040)

[5.4. Βήμα 5.4 8](#_Toc190346041)

[5.5. Βήμα 5.5 8](#_Toc190346042)

[5.6. Βήμα 5.6 8](#_Toc190346043)

[5.7. Βήμα 5.7 8](#_Toc190346044)

[5.8. Βήμα 5.8 8](#_Toc190346045)

[5.9. Βήμα 5.9 9](#_Toc190346046)

[5.10. Βήμα 5.10 9](#_Toc190346047)

[5.11. Βήμα 5.11 9](#_Toc190346048)

[5.12. Βήμα 5.12 9](#_Toc190346049)

[6. Βήμα 6 - Πολιτική Διαχείρισης Προμηθευτών 9](#_Toc190346050)

[7. Βήμα 7 - Πολιτική Διαχείρισης Στοιχείων Ενεργητικού 9](#_Toc190346051)

[8. Βήμα 8 - Πολιτική Διαχείρισης Αλλαγών και Διαμόρφωσης 10](#_Toc190346052)

[8.1. Βήμα 8.1 10](#_Toc190346053)

[8.2. Βήμα 8.2 11](#_Toc190346054)

[9. Βήμα 9 - Πολιτική Ελέγχου Πρόσβασης 11](#_Toc190346055)

[10. Βήμα 10 - Πολιτική Διαχείρισης Ευπαθειών 11](#_Toc190346056)

[10.1. Βήμα 10.1 12](#_Toc190346057)

[11. Βήμα 11 - Πολιτική Ασφάλειας Δικτύου 12](#_Toc190346058)

[11.1. Βήμα 11.1 12](#_Toc190346059)

[12. Βήμα 12 - Πολιτική Ασφάλειας Συστημάτων 12](#_Toc190346060)

[13. Βήμα 13 - Πολιτική Ανθρώπινου Δυναμικού 13](#_Toc190346061)

[14. Βήμα 14 - Πολιτική Αποδεκτής Χρήσης 13](#_Toc190346062)

[15. Βήμα 15 - Πολιτική Φυσικής Ασφάλειας 14](#_Toc190346063)

[16. Βήμα 16 - Πολιτική Διαχείρισης Συμβάντων και Περιστατικών 14](#_Toc190346064)

[17. Βήμα 17 - Σχέδιο Επιχειρησιακής Συνέχειας & Σχέδιο Αποκατάστασης από Καταστροφή 15](#_Toc190346065)

**Οδηγίες συμπλήρωσης εγγράφων**

**Τα έγγραφα που δημιουργήθηκαν είναι βασισμένα στις βέλτιστες πρακτικές σχετικά με την θεματολογία του κάθε εγγράφου και με βάση την νομοθεσία του ΚΔΠ 389/2020. Παρακαλείστε να αφαιρέσετε οτιδήποτε δεν αντιστοιχεί στον Οργανισμό σας όπως και επίσης να προσθέσετε οτιδήποτε δεν έχει συμπεριληφθεί.**

**Γενικό Σχόλιο 1**

Στις περιπτώσεις που αναγράφεται [Όνομα Οργανισμού] θα πρέπει να εισάγετε το όνομα του δικού σας Οργανισμού.

**Γενικό Σχόλιο 2**

Στις περιπτώσεις που αναγράφεται [Ορίστε χρονικό διάστημα] θα πρέπει να εισάγετε το χρονικό διάστημα όπως αναγράφεται στις οδηγίες μέσα στο έγγραφο.

# Βήμα 1 - Στρατηγική Ασφάλειας Πληροφοριών

Ξεκινώντας από το έγγραφο **Στρατηγική Ασφάλειας Πληροφοριών**, θα πρέπει να θεσπιστεί στρατηγική ασφάλειας πληροφοριών στην οποία να αναλύονται οι στόχοι και η προσέγγιση υψηλού επιπέδου με σκοπό τον μετριασμό των κινδύνων για την ασφάλεια πληροφοριών.

# Βήμα 1.1

Σε συνδυασμό με τα **Γενικά Σχόλια,** θα χρειαστεί να εισάγετε τις παρακάτω πληροφορίες:

* Στην υποενότητα ***Πλάνο Υλοποίησης Στρατηγικών Παρεμβάσεων Ασφάλειας Πληροφοριών/Κυβερνοασφάλειας*** θα πρέπει να καταγραφούν οι στρατηγικές δράσεις οι οποίες έτυχαν έγκρισης από την από την Ανώτατη Διεύθυνση του Οργανισμού.
* Στην υποενότητα ***Αιτιολογημένη Κατανομή Προϋπολογισμού και Πόρων για την υλοποίηση του πλάνου*** θα πρέπει να γίνει κατανομή του προϋπολογισμού και των πόρων για υλοποίηση των πρωτοβουλιών του Πλάνου Υλοποίησης Στρατηγικών Παρεμβάσεων Ασφάλειας Πληροφοριών/Κυβερνοασφάλειας.

# Βήμα 2 - Πολιτική Διακυβέρνησης Ασφάλειας Πληροφοριών

Στο έγγραφο **Πολιτική Διακυβέρνησης Ασφάλειας Πληροφοριών** θα πρέπει να καθοριστούν οι ρόλοι και οι αρμοδιότητες σχετικά με την ασφάλεια πληροφοριών εντός του οργανισμού και να εξασφαλιστεί η συμμόρφωση με όλες τις εφαρμοστέες νομικές και κανονιστικές υποχρεώσεις όσον αφορά την ασφάλεια δικτύων και πληροφοριών

# Βήμα 2.1

Σε συνδυασμό με τα **Γενικά Σχόλια,** θα χρειαστεί να εισάγετε τις παρακάτω πληροφορίες:

* Στην υποενότητα ***Οργανόγραμμα*** θα πρέπει να καταγράψετε το οργανόγραμμα του Οργανισμού σας όπως είναι την παρούσα φάση της συμπλήρωσης του εγγράφου. Αυτό θα πρέπει να αναθεωρείται κάθε φορά που υπάρχουν οργανωτικές αλλαγές στον Οργανισμό.
* Στην υποενότητα ***Ρόλοι και Αρμοδιότητες Ασφάλειας Πληροφοριών και Υπεύθυνοι επεξεργασίας πληροφοριών*** θα πρέπει να εισάγετε τα στοιχεία ατόμων συμπεριλαμβανομένου και τους ρόλους και αρμοδιότητες τους όπως αυτά εφαρμόζονται στον Οργανισμό σας.
* Στην υποενότητα ***Συμμόρφωση με Νομικές και Κανονιστικές Υποχρεώσεις***, θα πρέπει να συμπληρώσετε το πίνακα με τις νομοθεσίες που απαιτείται ο Οργανισμός σας να ακολουθεί.

# Βήμα 3 - Πολιτική Ασφάλειας Πληροφοριών

Στο έγγραφο **Πολιτική Ασφάλειας Πληροφοριών** θα πρέπει να θεσπιστούν πολιτικές, πρότυπα, κατευθυντήριες γραμμές και διαδικασίες για την ασφάλεια πληροφοριών που να αντικατοπτρίζουν τη στρατηγική ασφάλειας πληροφοριών.

# Βήμα 4 - Μεθοδολογία Διαχείρισης Κινδύνου

Στο έγγραφο **Πολιτική &** **Μεθοδολογία Διαχείρισης Κινδύνου** θα πρέπει να:

* θεσπιστεί μεθοδολογία διαχείρισης κινδύνων, η οποία αντικατοπτρίζει τη διαδικασία εκτίμησης κινδύνου του οργανισμού, τα κριτήρια ανάλυσης κινδύνου, τα κριτήρια αποδοχής κινδύνων και την πολιτική ανάληψης κινδύνων,
* καταρτιστεί κατάλογος στοιχείων ενεργητικού, συστημάτων και διαδικασιών εντός του οργανισμού,
* εντοπιστούν οι απειλές, ευπάθειες και κίνδυνοι στους οποίους εκτίθενται τα στοιχεία ενεργητικού, τα συστήματα και οι διαδικασίες του οργανισμού, και
* αναλυθούν οι κίνδυνοι για την ασφάλεια πληροφοριών στο πλαίσιο των στοιχείων ενεργητικού ανάλογα με τις διάφορες πιθανότητες και επιπτώσεις.

# Βήμα 5 - Asset Based Risk Assessment Workbook

Στο έγγραφο **Asset Based Risk Assessment Workbook** θα πρέπει να συμπεριλάβετε **ΟΛΑ** τα στοιχεία ενεργητικού του Οργανισμού σας στο φύλλο εργασίας «Κατάλογος Στοιχείων Ενεργητικού»

# Βήμα 5.1

Στο φύλλο εργασίας «**Κατάλογος Στοιχείων Ενεργητικού**» θα πρέπει να συμπεριλάβετε τα ακόλουθα:

* Επιχειρηματική Μονάδα που είναι υπεύθυνη για το συγκεκριμένο στοιχείο
* Το όνομα του στοιχείου ή σε ποια κατηγορία εμπίπτει (π.χ. Στοιχείο δικτύου, Έγγραφα κλπ.)
  + Στα πεδία Ομάδα Στοιχείων Ενεργητικού Τύπος 1 & 2 προσθέστε τις υπο-ομάδες του στοιχείου (π.χ. Πολιτικές, Συμβάσεις, Διανεμητές κλπ.)
* Τον τύπο του στοιχείου (Πληροφοριακό, Λογισμικό, Υλισμικό κλπ.)
* Περιγραφή του στοιχείου
* Τον σκοπό χρήσης του συγκεκριμένου στοιχείου
* Το αρμόδιο άτομο που είναι υπεύθυνο για τον στοιχείο
* Την αξία του στοιχείου προς τον οργανισμό (Ψηλή, Χαμηλή, Μέτρια)
* Τον προσδιορισμό εάν το συγκεκριμένο στοιχείο επεξεργάζεται ή αποθηκεύει προσωπικά δεδομένα (Ναι/Όχι)
* Την διαβάθμιση / ταξινόμηση του συγκεκριμένου στοιχείου
* Σε πια τοποθεσία αποθηκεύεται το στοιχείο (Φυσική και Ιδεατή τοποθεσία)
* Πιθανό αριθμό αναφοράς / ταυτοποίησης (serial number)
* Την περίοδο διατήρησης δεδομένων (στην περίπτωση που επεξεργάζεται ή αποθηκεύει προσωπικά δεδομένα)
* Πότε αποκτήθηκε από τον οργανισμό το συγκεκριμένο στοιχείο
* Τυχόν εξαρτήσεις από άλλα στοιχεία
* Την κατάσταση του στοιχείου (ενεργό, αποσυρμένο, διαγραμμένο)

*\*Για παραδείγματα σχετικά με τα Στοιχεία Ενεργητικού, ανατρέξτε στο φύλλο εργασίας «Παραδ. Στοιχείων Ενεργητικού»*

# Βήμα 5.2

Κάθε στοιχείο ενεργητικού που καταγράφηκε στο φύλλο εργασίας «Κατάλογος Στοιχείων Ενεργητικού» πρέπει να συμπεριληφθεί και στο φύλλο εργασίας «Επιχειρηματικός Αντίκτυπος».

# Βήμα 5.3

Μόλις συμπεριληφθούν όλα τα στοιχεία ενεργητικού στο φύλλο εργασίας «Επιχειρηματικός Αντίκτυπος», το/α υπεύθυνο/α άτομο/α θα πρέπει να αξιολογήσει τον αντίκτυπο στον Οργανισμό σε περίπτωση που το συγκεκριμένο στοιχείο δεν είναι διαθέσιμο. Οι κατηγορίες αντικτύπου είναι οι εξής:

* Εμπιστευτικότητα
* Ακεραιότητα
* Διαθεσιμότητα
* Αυθεντικότητα

Το/α υπεύθυνο/α άτομο/α θα πρέπει να αξιολογήσουν τον αντίκτυπο στην κάθε κατηγορία με κλίμακα 1 (ένα) ως 5 (πέντε) με το 1 (ένα) να είναι «πολύ χαμηλό» και το 5 (πέντε) να είναι «κρίσιμο». Όταν όλες οι κατηγορίες συμπληρωθούν με τον αντίστοιχο αντίκτυπο, η κρισιμότητα του κάθε στοιχείου θα αναγράφεται στην στήλη «G» με τον ανάλογο αριθμό. Αυτός ο αριθμός θα χρησιμοποιηθεί στο φύλλο εργασίας «Εκτίμηση Κινδύνου». Υπάρχει σχετικός υποβοηθητικός πίνακας με 5 παράγοντες οι οποίες μπορούν να ληφθούν υπόψη ως για την αξιολόγηση και βαθμολόγηση των 4 κατηγοριών πιο πάνω.

Αυτοί οι παράγοντες είναι :

* Επίδραση στη λειτουργία
* Οικονομικό κόστος
* Υγεία και ασφάλεια
* Βλάβη στη φήμη
* Νομική, συμβατική και οργανωτική Συμμόρφωση

# Βήμα 5.4

Τα στοιχεία ενεργητικού που αναγνωρίστηκαν στο βήμα 5.1, θα πρέπει συμπεριληφθούν στην στήλη «B» του φύλλου εργασίας «Εκτίμηση Κινδύνου». Η κρισιμότητα του κάθε στοιχείου που αναδείχθηκε στο βήμα 5.3, θα πρέπει να συμπεριληφθεί στην στήλη «I».

# Βήμα 5.5

Όταν διενεργείται η εκτίμηση κινδύνου του Οργανισμού, το κάθε στοιχείο έχει και τις αντίστοιχες Απειλές και Ευπάθειες. Αυτές θα συμπεριληφθούν στις στήλες «C» και «D» αντίστοιχα\*.

*\*Για παραδείγματα σχετικά με τις Απειλές και τις Ευπάθειες, ανατρέξτε στα φύλλα εργασίας «Κατάλογος Απειλών» και «Κατάλογος Ευπαθειών» αντίστοιχα. Οι κατάλογοι αυτοί δεν είναι εξαντλητικοί.*

# Βήμα 5.6

Στην στήλη «E» «Τύπος Κινδύνου» θα πρέπει να προσδιοριστεί τί θα επηρεαστεί σε περίπτωση που οι Απειλές και Ευπάθειες που αναγνωρίστηκαν στο βήμα 5.5 πραγματοποιηθούν (Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα, Αυθεντικότητα).

# Βήμα 5.7

Βάση της νομοθεσίας, ο κάθε κίνδυνος πρέπει να έχει και τον αντίστοιχο ιδιοκτήτη. Ο ιδιοκτήτης θα πρέπει να οριστεί από τον Οργανισμό βάση του ρόλου και αρμοδιοτήτων του στην στήλη «F».

# Βήμα 5.8

Βάση των Απειλών και Ευπαθειών που αναγνωρίστηκαν στο βήμα 5.5, πρέπει να αναγνωριστούν και οι Υφιστάμενες δικλείδες ασφαλείας που μπορούν να μετριάσουν τον κίνδυνο και να καταγραφούν στην στήλη «G». Οι υφιστάμενες δικλείδες ασφαλείας θα προσδιορίσουν και την ανάλογη πιθανότητα ο κίνδυνος να πραγματοποιηθεί χρησιμοποιώντας την κλίμακα 1 (ένα) ως 5 (πέντε) με το 1 (ένα) να είναι «πολύ απίθανο» και το 5 (πέντε) να είναι «σίγουρο». Η πιθανότητα θα πρέπει να καταγραφεί στην στήλη «H». Για κάθε υφιστάμενη δικλείδα ασφαλείας που αναγνωρίστηκε, θα ήταν υποβοηθητικό να υπάρχει και η αντίστοιχη αναφορά στο παράρτημα ΙΙΙ του ΚΔΠ 389/2020 μαζί με τις απαιτήσεις που αναγράφει το παράρτημα ΙΙΙ για τα συγκεκριμένα μέτρα ασφαλείας. Η αναφορά και οι απαιτήσεις θα πρέπει να καταγραφούν στις στήλες «N» και «O» αντίστοιχα. Επιπρόσθετα, συστήνεται να παρέχεται και η σχετική τεκμηρίωση της κάθε δικλείδας ασφαλείας που αναγράφεται στην στήλη «P».

# Βήμα 5.9

Πολλαπλασιάζοντας την πιθανότητα, που αναγνωρίστηκε στο βήμα 5.8, και την επίπτωση, που αναγνωρίστηκε στο βήμα 5.3, βγαίνει η βαθμολογία κινδύνου (Risk Score), που αναγράφεται στην στήλη «J», και συνάμα το επίπεδο κινδύνου (Risk Level) για το συγκεκριμένο στοιχείο ενεργητικού που αναγράφεται στην στήλη «K». Η μικρότερη βαθμολογία κινδύνου είναι ο συνδυασμός πιθανότητας «πολύ απίθανο» και «πολύ χαμηλό» που ισοδυναμεί με επίπεδο κινδύνου «Πολύ Χαμηλό». Η μεγαλύτερη βαθμολογία κινδύνου είναι ο συνδυασμός πιθανότητας «σίγουρο» και «κρίσιμο» που ισοδυναμεί με επίπεδο κινδύνου «Κρίσιμο».

# Βήμα 5.10

Όταν όλοι οι κίνδυνοι αναγνωριστούν με την μεθοδολογία που αναφέρθηκε πιο πάνω, ο Οργανισμός θα πρέπει να επιλέξει πώς θα αντιμετωπίσει το εκάστοτε κίνδυνο στην στήλη «L» σαν μέρος του Σχεδίου Αντιμετώπισης Κινδύνων. Οι επιλογές αντιμετώπισης είναι οι εξής:

* **Αποδοχή Κινδύνου** – Ο οργανισμός είναι ευχαριστημένος με τις υφιστάμενες δικλείδες ασφαλείας που αποδέχεται το επίπεδο κίνδυνου.
* **Αποφυγή Κινδύνου** – Ο Οργανισμός αποφασίζει πως δεν θα ασχοληθεί με τον συγκεκριμένο κίνδυνο και επιθυμεί να τον αποφύγει.
* **Μείωση** **Κινδύνου** – Ο Οργανισμός πιστεύει πως υπάρχει περιθώριο βελτίωσης στις υφιστάμενες δικλείδες ασφαλείας και αποφασίζει να τις βελτιώσει.
* **Μεταφορά** **Κινδύνου** – Λόγο μειωμένων πόρων, ο Οργανισμός αποφασίζει να μεταφέρει τον κίνδυνο σε έναν άλλο οργανισμό ή υπεργολάβο.

# Βήμα 5.11

Η στήλες από «Q» μέχρι «V» θα χρησιμοποιηθούν στην επανεκτίμηση κινδύνου με τις αναθεωρημένες δικλείδες ασφαλείας για να καταγραφεί τυχών βελτίωση στα επίπεδα κινδύνου.

# Βήμα 5.12

Τυχόν σχόλια που μπορεί να υπάρξουν, μπορούν να καταγραφούν στην στήλη «W»

# Βήμα 6 - Πολιτική Διαχείρισης Προμηθευτών

Στο έγγραφο **Πολιτική Διαχείρισης Προμηθευτών**, ο Οργανισμός θα πρέπει να επιδεικνύει τη δέουσα επιμέλεια σχετικά με τρίτα μέρη και προμηθευτές και διασφαλίζει την ενσωμάτωση συμβατικών ρητρών ασφάλειας πληροφοριών στις σχέσεις με τρίτα μέρη και προμηθευτές. Επίσης θα πρέπει να δημιουργήσει σχετικό Μητρώο Διαχείρισης Προμηθευτών.

# Βήμα 7 - Πολιτική Διαχείρισης Στοιχείων Ενεργητικού

Στο έγγραφο **Πολιτική Διαχείρισης Στοιχείων Ενεργητικού**, θα πρέπει 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,
* εξασφαλιστεί ότι τα δεδομένα ταξινομούνται και επισημαίνονται κατά τρόπο ώστε να αντικατοπτρίζεται η ευαισθησία τους ώστε να εξασφαλίζεται η κατάλληλη επεξεργασία τους,
* καταστεί δυνατή η αποκατάσταση των πληροφοριών στο πλαίσιο συμβάντων και περιστατικών ασφάλειας,
* εφαρμοστούν επαρκή μέτρα στο πλαίσιο της διαβίβασης και ανταλλαγής πληροφοριών εσωτερικά ή με τρίτα μέρη, προκειμένου να διασφαλιστεί η ασφαλής μεταφορά δεδομένων,
* εξασφαλιστεί η προστασία των δεδομένων από εκούσια ή ακούσια απώλεια και διαρροή δεδομένων,
* διασφαλιστεί ότι τα στοιχεία ενεργητικού είναι ασφαλή καθ’ όλη τη διάρκεια του κύκλου ζωής τους, συμπεριλαμβανομένης της προμήθειας, της ανάπτυξης, της συντήρησης και της διάθεσης τους,
* διασφαλιστεί ότι τα στοιχεία ενεργητικού καταγράφονται σε κατάλογο και ότι η ιδιοκτησία καθορίζεται με σκοπό την επίτευξη της ιχνηλασιμότητας και της ευθύνης για τα στοιχεία,
* διασφαλιστεί ότι τα στοιχεία ενεργητικού είναι υπό παρακολούθηση για επιθέσεις, ανωμαλίες και απειλές κατά της ασφάλειας, προκειμένου να ενεργοποιηθούν οι διαδικασίες για την αντιμετώπιση συμβάντων και περιστατικών,
* διασφαλιστεί η διαθεσιμότητα δικτύων και συστημάτων πληροφοριών με την επίτευξη επαρκούς διαθεσιμότητας πόρων, εφεδρείας και συστημάτων / διαδικασιών υψηλής διαθεσιμότητας,
* διασφαλιστεί η εμπιστευτικότητα, ακεραιότητα και αυθεντικότητα των πληροφοριών με την υιοθέτηση κατάλληλων κρυπτογραφικών λύσεων, και
* εξασφαλιστεί η κατάλληλη χωρητικότητα και επίδοση των υπηρεσιών των συστημάτων και διαδικασιών πληροφοριών.

# Βήμα 8 - Πολιτική Διαχείρισης Αλλαγών και Διαμόρφωσης

Στο έγγραφο **Πολιτική Διαχείρισης Αλλαγών και Διαμόρφωσης** θα πρέπει να διασφαλιστεί ότι οι αλλαγές στις διαδικασίες και τα συστήματα πληροφοριών εφαρμόζονται με ασφάλεια, χωρίς να θίγεται το απόρρητο, η ακεραιότητα, η διαθεσιμότητα ή η αυθεντικότητα των πληροφοριών. Επίσης, πρέπει να εντοπίζονται, να διατηρούνται και να επαληθεύονται οι πληροφορίες για τα στοιχεία ενεργητικού και τις διαμορφώσεις του οργανισμού.

# Βήμα 8.1

Σε συνδυασμό με τα **Γενικά Σχόλια,** θα χρειαστεί να εισάγετε τις παρακάτω πληροφορίες:

* Στην υποενότητα **Ρόλοι και αρμοδιότητες** 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. Επιπρόσθετα, ανάλογα με το μέγεθος του κάθε οργανισμού, θα υπάρχουν περιπτώσεις κατά τις οποίες δεν θα είναι εφικτός ο διορισμός ξεχωριστών ατόμων για τον κάθε ρόλο. Σε μια τέτοια περίπτωση ο οργανισμός δύναται να καθορίσει πέραν του ενός ρόλου σε ένα άτομο, νοουμένου ότι δεν θα προκύπτει σύγκρουση συμφέροντος μεταξύ των ρόλων αυτών.

# Βήμα 8.2

Σε συνδυασμό με τα **Γενικά Σχόλια,** θα χρειαστεί να εισάγετε τις παρακάτω πληροφορίες:

* Στην υποενότητα ***Διαδικασία ελέγχου αλλαγής και διαμόρφωσης*** *θ*α πρέπει να προσαρμοστεί ώστε να αντικατοπτρίζει την διαδικασία όπως αυτή εφαρμόζεται στον Οργανισμό.

# Βήμα 9 - Πολιτική Ελέγχου Πρόσβασης

Στο έγγραφο **Πολιτική Ελέγχου Πρόσβασης** θα πρέπει να

* επαληθευτεί η αυθεντικότητα και εξουσιοδότηση χρηστών, με βάση το ελάχιστο προνόμιο και τους οργανωτικούς ρόλους και αρμοδιότητες,
* εξασφαλιστούν επαρκή μέτρα στο πλαίσιο της εξωτερικής πρόσβασης σε οργανωτικούς πόρους,
* εξασφαλιστούν επαρκή μέτρα για τους χρήστες που έχουν προνομιακή πρόσβαση σε οργανωτικούς πόρους, συστήματα και δίκτυα,
* εξασφαλιστεί ότι γίνεται επαλήθευση της ταυτότητας των εξουσιοδοτημένων ατόμων με ασφάλεια και με τη χρήση μέτρων ισχυρής επαλήθευσης ταυτότητας,
* διασφαλιστεί ασφαλής διαχείριση διαπιστευτηρίων για πρόσβαση σε εταιρικούς πόρους, και ότι επαληθεύεται η ταυτότητα των χρηστών με ασφάλεια για χρήση υπηρεσιών του οργανισμού,
* διασφαλιστεί η μη-άρνηση ανιχνευσιμότητας των ενεργειών των χρηστών που εκτελούνται στο πλαίσιο των οργανωτικών πόρων, ώστε να είναι δυνατή η ανίχνευση και η διερεύνηση εκούσιων ή ακούσιων δραστηριοτήτων που έχουν αρνητικό αντίκτυπο, και
* διασφαλιστεί ότι οι ρόλοι και η έγκριση της ταυτότητας αντικατοπτρίζουν τον κύκλο ζωής της ταυτότητας του χρήστη.

# Βήμα 10 - Πολιτική Διαχείρισης Ευπαθειών

Στο έγγραφο **Πολιτική Διαχείρισης Ευπαθειών και Τρωτότητας** θα πρέπει να:

* διασφαλιστεί ότι οι ευπάθειες συστημάτων είναι γνωστές στον οργανισμό, προκειμένου να τύχουν κατάλληλου χειρισμού,
* διασφαλιστεί ότι οι ευπάθειες καταγράφονται και υποβάλλονται σε σχετικές εκθέσεις, ώστε να είναι δυνατή η λήψη τεκμηριωμένων αποφάσεων από τη διοίκηση όσον αφορά τον χειρισμό τους, και
* εξασφαλιστεί η αποκατάσταση των ευπαθειών συστημάτων και η εφαρμογή ενημερώσεων ασφάλειας, κατόπιν απόφασης της διοίκησης.

# Βήμα 10.1

Σε συνδυασμό με τα **Γενικά Σχόλια,** θα χρειαστεί να εισάγετε τις παρακάτω πληροφορίες:

* Στην υποενότητα ***Αξιολόγηση και Αποκατάσταση Ευπαθειών*** θα πρέπει να ορίσετε την συχνότητα αποστολής αξιολογήσεων ευπαθειών στους Επιχειρησιακούς Ιδιοκτήτες.
* Στην υποενότητα ***Δοκιμές Διείσδυσης*** θα πρέπει να καταγραφεί το τμήμα που είναι υπεύθυνο για τις δοκιμές διείσδυσης στα συστήματα / δίκτυο του Οργανισμού.

# Βήμα 11 - Πολιτική Ασφάλειας Δικτύου

Στο έγγραφο **Πολιτική Ασφάλειας Δικτύου** θα πρέπει να:

* διασφαλιστεί ότι η διεπαφή του τοπικού δικτύου με το εξωτερικό δίκτυο προστατεύεται από επιθέσεις, απειλές και άλλες εκούσιες ή ακούσιες ενέργειες με δυνητικά αρνητικές επιπτώσεις,
* εξασφαλιστεί ο διαχωρισμός του λογικού δικτύου, σύμφωνα με τις επιχειρηματικές λειτουργίες, και να αποφευχθεί η εξάπλωση κακόβουλων στοιχείων,
* διασφαλιστεί η προστασία των οργανωτικών πόρων από επιθέσεις άρνησης παροχής υπηρεσιών, και ότι δεν επηρεάζονται οι νόμιμες δραστηριότητες παροχής υπηρεσιών,
* διασφαλιστούν κατάλληλα πρωτοκόλλα επικοινωνίας προκειμένου να επιτευχθεί ασφαλής επικοινωνία μεταξύ των πόρων του δικτύου,
* εξασφαλιστεί ότι η πρόσβαση στο λογικό δίκτυο από εξωτερικά και εσωτερικά συστήματα ασφαλίζεται κατάλληλα, ώστε μόνο τα εξουσιοδοτημένα πρόσωπα να μπορούν να έχουν πρόσβαση σε οργανωτικούς πόρους,
* εξασφαλιστεί της η διαθεσιμότητα πληροφοριών και δικτύων πληροφοριών με την επίτευξη επαρκούς διαθεσιμότητας πόρων, εφεδρικού εξοπλισμού, συστημάτων και συνδέσεων υψηλής διαθεσιμότητας, και
* διασφαλιστεί η ανίχνευση και η πρόληψη από εξωτερικές απόπειρες εισβολής και επιθέσεις ασφάλειας.

# Βήμα 11.1

Σε συνδυασμό με τα **Γενικά Σχόλια,** θα χρειαστεί να εισάγετε τις παρακάτω πληροφορίες:

* στο ***Παράρτημα Α – Διάγραμμα Δικτύου [Όνομα Οργανισμού]*** θα πρέπει να αλλάξετε το παράδειγμα με ένα διάγραμμα που αντικατοπτρίζει τον Οργανισμό σας.

# Βήμα 12 - Πολιτική Ασφάλειας Συστημάτων

Στο έγγραφο **Πολιτική Ασφάλειας Συστημάτων** θα πρέπει να:

* διασφαλιστεί ότι δεν θα επηρεαστούν οργανωτικοί πόροι από κακόβουλο λογισμικό και κώδικα,
* ελαχιστοποιηθεί, στο μέτρο του δυνατού, η επιφάνεια επίθεσης των συστημάτων πληροφοριών, μέσω της μείωσης της λειτουργικότητας και των χαρακτηριστικών τους,
* εξασφαλιστεί η κατάλληλη ασφάλεια των κινητών συσκευών που έχουν πρόσβαση σε οργανωτικούς πόρους,
* διασφαλιστεί η κατάλληλη διαχείρισης των εφαρμογών που χρησιμοποιούνται για την πρόσβαση ή επεξεργασία οργανωτικών πόρων, και
* διασφαλιστούν επαρκή μέτρα ασφάλειας στο πλαίσιο των δραστηριοτήτων ανάπτυξης λογισμικού που αναπτύσσει ο οργανισμός.

# Βήμα 13 - Πολιτική Ανθρώπινου Δυναμικού

Στο έγγραφο **Πολιτική Ανθρώπινου Δυναμικού και Εκπαίδευσης** θα πρέπει να:

* υλοποιούνται επαρκή μέτρα για την εξασφάλιση ότι τα στελέχη που εργάζονται για λογαριασμό του οργανισμού, τα οποία έχουν πρόσβαση σε οργανωτικούς πόρους, υποστηρίζουν την πολιτική ασφάλειας πληροφοριών και τους στόχους του οργανισμού,
* εξασφαλιστεί ότι τα στελέχη που εργάζονται για λογαριασμό του οργανισμού συμμορφώνονται με την πολιτική ασφάλειας πληροφοριών και τηρούν τις ευθύνες ασφάλειας τους καθ’ όλη τη διάρκεια του κύκλου ζωής της απασχόλησης,
* εξασφαλιστεί ότι τα στελέχη που εργάζονται για λογαριασμό του οργανισμού, είναι υπεύθυνα για τις εκούσιες ή ακούσιες δραστηριότητες που επηρεάζουν τους στόχους ασφάλειας πληροφοριών του οργανισμού,
* εξασφαλιστεί ότι οι εξωτερικοί συνεργάτες που εργάζονται για λογαριασμό του οργανισμού τηρούν την πολιτική ασφάλειας πληροφοριών και τους στόχους ασφάλειας του οργανισμού,
* Να εξασφαλιστεί η προστασία από απειλές κατά της ασφάλειας δικτύων και πληροφοριών από το εσωτερικό του οργανισμού, και
* Να διασφαλιστεί ότι οι ευθύνες που αφορούν την ασφάλεια πληροφοριών και την αποδεκτή χρήση των στοιχείων ενεργητικού, ενσωματώνονται στις συμφωνίες εργοδότησης και στις διαδικασίες έναρξης απασχόλησης, για την επίτευξη υπευθυνότητας και ευαισθητοποίησης.
* Στην υποενότητα***Ετήσιο πρόγραμμα εκπαίδευσης*** θα πρέπει να θεσπιστεί πρόγραμμα ενημέρωσης σχετικά με την ασφάλεια πληροφοριών για όλα τα στελέχη εντός του οργανισμού, λαμβάνοντας υπόψη τα στοιχεία που περιγράφονται στις πολιτικές, τα πρότυπα, τις κατευθυντήριες γραμμές και τις διαδικασίες ασφάλειας πληροφοριών. Επίσης, ο Οργανισμός θα πρέπει να παρέχει εκπαίδευση προς όλα τα στελέχη του οργανισμού, όπως ορίζεται στο πρόγραμμα ασφάλειας πληροφοριών.

# Βήμα 14 - Πολιτική Αποδεκτής Χρήσης

Στο έγγραφο **Πολιτική Αποδεκτής Χρήσης** θα πρέπει να διασφαλιστεί ότι οι ευθύνες που αφορούν την ασφάλεια πληροφοριών και την αποδεκτή χρήση των στοιχείων ενεργητικού, ενσωματώνονται στις συμφωνίες εργοδότησης και στις διαδικασίες έναρξης απασχόλησης, για την επίτευξη υπευθυνότητας και ευαισθητοποίησης.

# Βήμα 15 - Πολιτική Φυσικής Ασφάλειας

Στο έγγραφο **Πολιτική Φυσικής Ασφάλειας** θα πρέπει να:

* εξασφαλιστούν επαρκή μέτρα για την προστασία του οργανισμού από τις επιπτώσεις φυσικών καταστροφών, όπως οι πλημμύρες, οι σεισμοί και οι πυρκαγιές,
* διασφαλιστεί η φυσική περίμετρος του οργανισμού, με την εξασφάλιση και αποτροπή της μη εξουσιοδοτημένης πρόσβασης,
* εξασφαλιστεί ο έλεγχος της πρόσβασης σε εσωτερικούς χώρους εργασίας και τις εγκαταστάσεις, ώστε να διασφαλίζεται ότι η φυσική πρόσβαση περιορίζεται κατόπιν ανάγκης,
* εξασφαλιστεί ότι για την καλωδίωση και τον εξοπλισμό που υποστηρίζουν την επεξεργασία των πληροφοριών, εξασφαλίζεται η φυσική προστασία από παρεμβολές, υποκλοπή ή ζημιά, και
* εξασφαλιστεί ότι οι εσωτερικοί χώροι και οι εγκαταστάσεις του οργανισμού προστατεύονται από φυσικές ζημιές.

# Βήμα 16 - Πολιτική Διαχείρισης Συμβάντων και Περιστατικών

Στο έγγραφο **Πολιτική Διαχείρισης Συμβάντων και Περιστατικών** θα πρέπει να:

* διασφαλίζει ότι ο οργανισμός είναι σε θέση να εντοπίζει συμβάντα και περιστατικά που ενδέχεται να συνιστούν απειλή για τους στόχους της ασφάλειας πληροφοριών του οργανισμού και να ενεργοποιεί τις αντίστοιχες διαδικασίες αντιμετώπισης περιστατικών,
* διασφαλιστεί ότι ο οργανισμός είναι σε θέση να αναλύει και να αξιολογεί συμβάντα και περιστατικά που αφορούν την ασφάλεια πληροφοριών, ούτως ώστε να ενεργοποιεί κατάλληλες διαδικασίες περιορισμού και ανάκτησης,
* εξασφαλιστεί επαρκής περιορισμός και αποκατάσταση από συμβάντα και περιστατικά ασφάλειας που επηρεάζουν αρνητικά τους στόχους ασφάλειας πληροφοριών του οργανισμού,
* διασφαλιστεί ότι ο οργανισμός μαθαίνει από συμβάντα και περιστατικά ασφάλειας, προκειμένου να αποτρέπονται παρόμοια συμβάντα και περιστατικά στο μέλλον,
* διασφαλίσει ότι ο οργανισμός ενημερώνει τα σχετικά ενδιαφερόμενα μέρη στην περίπτωση συμβάντων ή περιστατικών ασφάλειας, όπως περιγράφεται σε νομικές και ρυθμιστικές υποχρεώσεις, και
* εξασφαλίζει ότι ο οργανισμός κοινοποιεί πληροφορίες σχετικά με συμβάντα και περιστατικά ασφάλειας δικτύων και πληροφοριών σε εσωτερικούς και εξωτερικούς ενδιαφερόμενους φορείς.

# Βήμα 17 - Σχέδιο Επιχειρησιακής Συνέχειας & Σχέδιο Αποκατάστασης από Καταστροφή

Στο έγγραφο **Σχέδιο Επιχειρησιακής Συνέχειας** θα πρέπει να:

* εξασφαλιστεί ότι ο οργανισμός έχει αναλύσει και αξιολογήσει τις κρίσιμες επιχειρηματικές διαδικασίες που πρέπει να ληφθούν υπόψη στο σχέδιο επιχειρησιακής συνέχειας, ώστε να μπορέσει ο οργανισμός να αποκαταστήσει τις επιχειρηματικές διαδικασίες σε αποδεκτό επίπεδο, το συντομότερο δυνατόν, σε περίπτωση συμβάντος ή περιστατικού.
* εξασφαλιστεί ότι ο οργανισμός διαθέτει σχέδιο για τη διατήρηση της συνέχειας των κρίσιμων επιχειρηματικών διαδικασιών και την αποκατάσταση κατά τη διάρκεια συμβάντος ή περιστατικού και μετά από αυτό.
* διασφαλιστεί ότι ο οργανισμός και τα στελέχη του γνωρίζουν τις ευθύνες τους κατά τη διάρκεια ενός συμβάντος ή περιστατικού που ενεργοποιεί το σχέδιο επιχειρησιακής συνέχειας, και
* εξασφαλιστεί ότι ο οργανισμός διαθέτει σχέδιο για την αποκατάσταση των συστημάτων κρίσιμων πληροφοριών σε αποδεκτό επίπεδο κατά τη διάρκεια ή μετά από περιστατικό. Για το σκοπό αυτό θα πρέπει να συμπληρωθεί το **Σχέδιο Αποκατάστασης από Καταστροφή.**