| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου | | | | | | | |
| Αριθμός εγγράφου:<br>P02 | | | | | Τίτλος εγγράφου:<br>**Πολιτική P02 Ρόλων και Αρμοδιοτήτων Διακυβέρνησης** | | | | | | | |
| Έκδοση:<br>1.0 | | Ημερομηνία έναρξης ισχύος:<br>01.01.2025 | | | Ιδιοκτήτης εγγράφου: | | | | | | | |
| X | Πολιτική | | Πρότυπο | | Διαδικασία | | Έντυπο | | Μητρώο | | Άλλο | |

| **Ιστορικό αναθεωρήσεων** | | | | |
|---|---|---|---|---|
| **Αριθμός αναθεώρησης** | **Ημερομηνία αναθεώρησης** | **Αλλαγές** | **Ελέγχθηκε από** | **Ιδιοκτήτης διεργασίας** |
| | | | | |
| | | | | |

| **Εγκρίσεις** | | | |
|---|---|---|---|
| **Όνομα** | **Θέση** | **Ημερομηνία** | **Υπογραφή** |
| | | | |
| | | | |

Ευθυγραμμισμένη με πρότυπα και κανονιστικές απαιτήσεις

| Πρότυπο/Κανονισμός | Ρήτρα/Άρθρο | Σχόλιο |
|---|---|---|
| ISO/IEC 27001:2022 | Clause 5.3; Annex A Control 5 | |
| ISO/IEC 27002:2022 | Control 5 | |
| NIST SP 800-53 Rev.5 | PL-1 έως PL-4, PM-1 έως PM-13 | |
| ΓΚΠΔ της ΕΕ | Articles 5(1)(f), 24, 37 | |
| Οδηγία NIS2 της ΕΕ | Article 21(2)(a) | |
| Κανονισμός DORA της ΕΕ | Article 5 | |
| COBIT 2019 | EDM01, EDM02, APO01, APO12, MEA | |

**1. Σκοπός**

1.1 Η παρούσα πολιτική καθορίζει το μοντέλο διακυβέρνησης, τους οργανωτικούς ρόλους και τις αρμοδιότητες που απαιτούνται για τη λειτουργία ενός αποτελεσματικού Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ISMS).

1.2 Θεσπίζει σαφείς γραμμές λογοδοσίας, αρμοδιότητες λήψης αποφάσεων και διαδρομές κλιμάκωσης, ώστε η ασφάλεια πληροφοριών να ενσωματώνεται σε όλα τα επίπεδα του οργανισμού και να ευθυγραμμίζεται με τους στρατηγικούς επιχειρησιακούς στόχους.

1.3 Η πολιτική αυτή εφαρμόζει τις απαιτήσεις της ρήτρας 5.3 και του ελέγχου A.5.2 του ISO/IEC 27001:2022, διασφαλίζοντας ότι οι αρμοδιότητες για δραστηριότητες σχετικές με την ασφάλεια ανατίθενται με σαφήνεια, τεκμηριώνονται, κοινοποιούνται και υποβάλλονται σε περιοδική ανασκόπηση.

1.4 Η παρούσα πολιτική παρέχει επίσης τη βάση για ενοποιημένη διακυβέρνηση με άλλες λειτουργίες, όπως η διαχείριση κινδύνων, η συμμόρφωση, οι λειτουργίες ΤΠ και η νομική υπηρεσία.

**2. Πεδίο εφαρμογής**

**2.1 Η παρούσα πολιτική εφαρμόζεται σε όλα τα πρόσωπα και τις οντότητες που συμμετέχουν στη διακυβέρνηση, τη λειτουργία και την εποπτεία της ασφάλειας πληροφοριών εντός του πεδίου εφαρμογής του ISMS. Αυτό περιλαμβάνει:**

2.1.1 την εκτελεστική διοίκηση, τα ανώτατα διοικητικά στελέχη και τα μέλη του διοικητικού συμβουλίου

2.1.2 τους διαχειριστές ISMS, τους CISO και τους υπευθύνους ελέγχων

2.1.3 τους ιδιοκτήτες διεργασιών και περιουσιακών στοιχείων

2.1.4 αναδόχους και τρίτους παρόχους υπηρεσιών στους οποίους έχουν ανατεθεί αρμοδιότητες ασφάλειας

2.2 Καλύπτει τόσο εσωτερικές λειτουργίες όσο και εξωτερικά παρεχόμενες λειτουργίες (π.χ. εξωτερικά ανατεθειμένο SOC, διαχειριστές πλατφόρμας υπολογιστικού νέφους), όταν οι ρόλοι διακυβέρνησης έχουν ανατεθεί επίσημα ή προβλέπονται συμβατικά.

2.3 Η πολιτική εφαρμόζεται επίσης σε οργανωτικές μονάδες, τμήματα και ομάδες έργου που διαχειρίζονται ή επηρεάζουν περιουσιακά στοιχεία, συστήματα ή υπηρεσίες σχετικά με την ασφάλεια.

**3. Στόχοι**

3.1 Να διασφαλίζεται ότι οι ρόλοι και οι αρμοδιότητες ασφάλειας πληροφοριών ορίζονται, ανατίθενται, κοινοποιούνται και τεκμηριώνονται επίσημα.

3.2 Να διατηρείται ένα μοντέλο διακυβέρνησης που επιβάλλει τον διαχωρισμό καθηκόντων, αποτρέπει τις συγκρούσεις συμφερόντων και επιτρέπει την κλιμάκωση μη επιλυμένων ζητημάτων ασφάλειας.

3.3 Να διασφαλίζεται ότι η λογοδοσία και η αρμοδιότητα για αποφάσεις ασφάλειας κατανέμονται σύμφωνα με τον επιχειρησιακό αντίκτυπο και την οργανωτική δομή.

3.4 Να θεσπίζεται πλαίσιο για τη διαχείριση αναθέσεων, αλλαγών ρόλων και ανασκόπησης των ανατεθειμένων αρμοδιοτήτων.

3.5 Να παρέχεται διαβεβαίωση στα ενδιαφερόμενα μέρη — συμπεριλαμβανομένων των ρυθμιστικών αρχών, των ελεγκτών και των πελατών — ότι η ασφάλεια πληροφοριών διέπεται αποτελεσματικά και σε συμμόρφωση με τα ισχύοντα πρότυπα.

## 4. Ρόλοι και αρμοδιότητες

### 4.1 Εκτελεστική Διοίκηση (Ανώτατη Διοίκηση)

4.1.1 Παρέχει στρατηγική εποπτεία, διαθέτει πόρους και διασφαλίζει την ευθυγράμμιση μεταξύ των στόχων του ISMS και των επιχειρησιακών στόχων.

4.1.2 Εγκρίνει τη βασική τεκμηρίωση του ISMS, συμπεριλαμβανομένης της Πολιτικής Ασφάλειας Πληροφοριών, των σχεδίων αντιμετώπισης κινδύνων και των αποφάσεων αποκατάστασης ευρημάτων ελέγχου.

4.1.3 Συμμετέχει στις ανασκοπήσεις διοίκησης του ISMS και κλιμακώνει προς έγκριση σε επίπεδο διοικητικού συμβουλίου τις αποφάσεις που το απαιτούν.

4.1.4 Προάγει την κουλτούρα ασφάλειας και ενισχύει την τήρηση των αρχών διακυβέρνησης ασφάλειας σε όλο τον οργανισμό.

### 4.2 Επιτροπή Καθοδήγησης Ασφάλειας Πληροφοριών (ISSC)

4.2.1 Λειτουργεί ως διατμηματικό όργανο διακυβέρνησης για την εποπτεία του ISMS.

4.2.2 Ανασκοπεί τη θέση κινδύνου, την αποτελεσματικότητα των ελέγχων, τα ευρήματα ελέγχου και τις στρατηγικές πρωτοβουλίες ασφάλειας.

4.2.3 Διευκολύνει τον συντονισμό μεταξύ τμημάτων (π.χ. ΤΠ, Νομική Υπηρεσία, Ανθρώπινο Δυναμικό, Διαχείριση Κινδύνων, Συμμόρφωση, Λειτουργίες).

4.2.4 Εγκρίνει όρια κλιμάκωσης, κατανομές προϋπολογισμού και αλλαγές πολιτικών που απαιτούν εισήγηση της εκτελεστικής διοίκησης.

[ ... Οι ενότητες 4.3–8 δεν περιλαμβάνονται σε αυτή την προεπισκόπηση. Αγοράστε το πλήρες έγγραφο για πρόσβαση στο πλήρες περιεχόμενο. ... ]

## 9. Απαιτήσεις ανασκόπησης και επικαιροποίησης

### 9.1 Χρονοδιάγραμμα ανασκόπησης

**9.1.1 Η παρούσα πολιτική υποβάλλεται σε ανασκόπηση τουλάχιστον ετησίως ή με την επέλευση ενός από τα ακόλουθα:**

9.1.1.1 αλλαγές στην οργανωτική δομή ή στην εκτελεστική ομάδα

9.1.1.2 επέκταση ή επαναπροσδιορισμός του πεδίου εφαρμογής του ISMS

9.1.1.3 κανονιστικές αλλαγές που επηρεάζουν την ανάθεση ρόλων ή την εποπτεία

9.1.1.4 σημαντικά ευρήματα ελέγχου ή περιστατικά που αφορούν αστοχία διακυβέρνησης

### 9.2 Διαδικασία ανασκόπησης και έγκρισης

9.2.1 Ο Διαχειριστής ISMS οφείλει να εκκινεί και να καθοδηγεί τη διαδικασία ανασκόπησης, συμπεριλαμβανομένης της συλλογής εισροών από ενδιαφερόμενα μέρη και ανατροφοδότησης από ελέγχους.

9.2.2 Οι προτεινόμενες επικαιροποιήσεις υποβάλλονται σε ανασκόπηση από την ISSC και εγκρίνονται επίσημα από την Εκτελεστική Διοίκηση.

**9.2.3 Κάθε έκδοση πρέπει να παρακολουθείται στο Μητρώο Εγγράφων ISMS και να περιλαμβάνει τα ακόλουθα μεταδεδομένα:**

9.2.3.1 αναγνωριστικό πολιτικής και τίτλο

9.2.3.2 αριθμό έκδοσης και σύνοψη αλλαγών

9.2.3.3 ημερομηνία έναρξης ισχύος και ημερομηνία επόμενης ανασκόπησης

9.2.3.4 ιδιοκτήτη πολιτικής και εγκρίνοντα

9.2.3.5 επίπεδο ταξινόμησης εγγράφου

9.2.3.6 ιστορικό διατήρησης και αρχειοθέτησης

## 10. Συναφείς πολιτικές και διασυνδέσεις

**10.1 Η παρούσα πολιτική πρέπει να ερμηνεύεται σε συνδυασμό με τις ακόλουθες πολιτικές:**

10.1.1 P1 – Πολιτική Ασφάλειας Πληροφοριών: Καθορίζει το συνολικό πρόγραμμα ασφάλειας και περιγράφει τις αρμοδιότητες της διοίκησης για την έγκριση των πολιτικών και τη στρατηγική εποπτεία.

10.1.2 P5 – Πολιτική Διαχείρισης Αλλαγών: Διασφαλίζει ότι οι αλλαγές στις δομές διακυβέρνησης, στους ρόλους ή στις αρμοδιότητες υπόκεινται σε τεκμηριωμένη έγκριση και ανασκόπηση κινδύνου.

10.1.3 P6 – Πολιτική Διαχείρισης Κινδύνων: Εντοπίζει και αντιμετωπίζει κινδύνους διακυβέρνησης που προκύπτουν από συγκρούσεις ρόλων, μη ανατεθειμένα καθήκοντα ή έλλειψη κλιμάκωσης.

10.1.4 P7 – Πολιτική Ένταξης και Αποχώρησης Προσωπικού: Εφαρμόζει τις διαδικασίες ανάθεσης και ανάκλησης ελέγχων κατά τις μεταβολές του κύκλου ζωής προσωπικού.

10.1.5 P33 – Πολιτική Παρακολούθησης Ελέγχων και Συμμόρφωσης: Υποστηρίζει την ανεξάρτητη ανασκόπηση της αποτελεσματικότητας της διακυβέρνησης και επιβάλλει διορθωτικές ενέργειες για περιπτώσεις μη συμμόρφωσης.

10.2 Οι πολιτικές αυτές υποστηρίζουν συλλογικά ένα ενιαίο και εφαρμόσιμο πλαίσιο διακυβέρνησης ISMS.

## 11. Πρότυπα και πλαίσια αναφοράς

11.1 Η παρούσα πολιτική ευθυγραμμίζεται με διεθνώς αναγνωρισμένα πρότυπα και πλαίσια για τη διακυβέρνηση της ασφάλειας πληροφοριών και τη λογοδοσία ρόλων. Διασφαλίζει την ιχνηλασιμότητα προς κανονιστικές και πιστοποιητικές απαιτήσεις και υποστηρίζει μια τεκμηριώσιμη δομή ISMS.

**11.2 ISO/IEC 27001**

11.2.1 Ρήτρα 5.3 – Οργανωτικοί ρόλοι, αρμοδιότητες και εξουσιοδοτήσεις: Η παρούσα πολιτική καλύπτει την απαίτηση ώστε οι ρόλοι που σχετίζονται με την ασφάλεια πληροφοριών να ανατίθενται, να κοινοποιούνται και να τεκμηριώνονται με σαφήνεια.

11.2.2 Ρήτρα 9.3 – Ανασκόπηση από τη διοίκηση: Η παρούσα πολιτική επιβάλλει εποπτεία από την εκτελεστική διοίκηση επί των ρόλων και της διακυβέρνησης του ISMS μέσω τριμηνιαίων και ετήσιων ανασκοπήσεων.

11.2.3 Έλεγχος 5.2 του Παραρτήματος Α – Ρόλοι και αρμοδιότητες ασφάλειας πληροφοριών: Καθορίζει ρόλους σε τεχνικό, λειτουργικό και στρατηγικό επίπεδο ώστε να διασφαλίζονται ο διαχωρισμός καθηκόντων, η ιδιοκτησία κινδύνου και η ιχνηλάσιμη λογοδοσία.

**11.3 ISO/IEC 27002:2022 – Έλεγχος 5**

11.3.1 Παρέχει οδηγίες εφαρμογής για την ανάθεση αρμοδιοτήτων ασφάλειας πληροφοριών σε ολόκληρο τον οργανισμό. Η παρούσα πολιτική υιοθετεί τις οδηγίες αυτές καθορίζοντας τύπους ρόλων, κανόνες ανάθεσης, διαδικασίες κλιμάκωσης και μηχανισμούς ανασκόπησης.

**11.4 NIST SP 800-53 Rev.5**

11.4.1 PL-1 έως PL-4: Επιβάλλουν την ανάγκη για επίσημη τεκμηρίωση σχεδιασμού, συμπεριλαμβανομένων πολιτικών που καθορίζουν τη διακυβέρνηση και αναθέτουν αρμοδιότητες ασφάλειας.

11.4.2 PM-1 (Σχέδιο Προγράμματος Ασφάλειας Πληροφοριών) και PM-2 (Ανώτερος Υπεύθυνος Ασφάλειας Πληροφοριών): Αποτυπώνονται στην παρούσα πολιτική μέσω της ανάθεσης του ρόλου CISO/Διαχειριστή ISMS και των επίσημων ρόλων διακυβέρνησης.

11.4.3 PM-5 έως PM-13: Η παρούσα πολιτική καλύπτει απαιτήσεις για τεκμηρίωση ρόλων, ρόλους κινδύνου σε επίπεδο οργανισμού, εποπτεία διαχείρισης ρυθμίσεων και ενοποίηση με λειτουργίες αποστολής/επιχειρησιακές λειτουργίες.

**11.5 ΓΚΠΔ της ΕΕ (2016/679)**

11.5.1 Άρθρο 5(1)(f): Απαιτεί τα δεδομένα προσωπικού χαρακτήρα να προστατεύονται από μη εξουσιοδοτημένη ή παράνομη επεξεργασία. Η παρούσα πολιτική διασφαλίζει ότι τα άτομα που είναι υπεύθυνα για την προστασία δεδομένων ορίζονται με σαφήνεια και παρακολουθούνται.

11.5.2 Άρθρο 24: Απαιτεί κατάλληλα οργανωτικά μέτρα, συμπεριλαμβανομένων δομών διακυβέρνησης.

11.5.3 Άρθρο 37: Απαιτεί τον ορισμό Υπευθύνου Προστασίας Δεδομένων (DPO), ο οποίος πρέπει να αποτυπώνεται στο πλαίσιο διακυβέρνησης και στο μητρώο αρμοδιοτήτων του οργανισμού.

**11.6 Οδηγία NIS2 της ΕΕ (2022/2555)**

11.6.1 Άρθρο 21(2)(a): Επιβάλλει στις οντότητες να εφαρμόζουν πολιτικές για την ανάλυση κινδύνου και την ασφάλεια συστημάτων πληροφοριών, συμπεριλαμβανομένων αρμοδιοτήτων ανά ρόλο. Η παρούσα πολιτική καθορίζει τους ρόλους αυτούς και τους μηχανισμούς διακυβέρνησής τους.

**11.7 Κανονισμός DORA της ΕΕ (2022/2554)**

11.7.1 Άρθρο 5 – Πλαίσιο διακυβέρνησης και εσωτερικού ελέγχου: Απαιτεί την επίσημη ανάθεση αρμοδιοτήτων διαχείρισης κινδύνων ΤΠΕ, ρόλων λήψης αποφάσεων και διαύλων αναφοράς. Η παρούσα πολιτική παρέχει τη βάση για τη διακυβέρνηση ρόλων σχετικών με την ασφάλεια σε περιβάλλοντα ΤΠΕ.

**11.8 COBIT 2019**

11.8.1 EDM01 – Διασφαλισμένη θέσπιση πλαισίου διακυβέρνησης: Η παρούσα πολιτική διασφαλίζει ότι το ISMS διαθέτει σαφώς καθορισμένη δομή διακυβέρνησης ευθυγραμμισμένη με τις ανάγκες του οργανισμού.

11.8.2 EDM02 – Διασφαλισμένη παροχή οφελών: Ευθυγραμμίζει τις δραστηριότητες ασφάλειας βάσει ρόλων με στρατηγικούς και επιχειρησιακούς στόχους, διασφαλίζοντας λογοδοσία και μετρήσιμα αποτελέσματα.

11.8.3 APO01 – Διαχειριζόμενο πλαίσιο διοίκησης Πληροφορικής και Τεχνολογίας και APO12 – Διαχειριζόμενος κίνδυνος: Η παρούσα πολιτική υποστηρίζει τη δομημένη διαχείριση ρόλων ασφάλειας πληροφοριών στο πλαίσιο ευρύτερης διακυβέρνησης ΤΠ και διαχείρισης κινδύνων.

11.8.4 MEA01 – Παρακολούθηση, αξιολόγηση και εκτίμηση απόδοσης: Ενσωματώνει μηχανισμούς ανασκόπησης για την επαλήθευση ότι οι ρόλοι διακυβέρνησης είναι αποτελεσματικοί, επίκαιροι και εφαρμόζονται.