| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου | | | | | | | |
| Αριθμός εγγράφου:<br>P33 | | | | | Τίτλος εγγράφου:<br>**Πολιτική Ελέγχων και Παρακολούθησης Συμμόρφωσης** | | | | | | | |
| 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 | Ρήτρες 9.2, 9.3, 10 | |
| ISO/IEC 27002:2022 | Έλεγχοι 5.35–5.37 | |
| NIST SP 800-53 Rev.5 | CA-2, CA-5, CA-7 | |
| ΓΚΠΔ της ΕΕ | Άρθρα 24, 32, 33 | |
| Οδηγία NIS2 της ΕΕ | Άρθρο 21(2)(g), 27 | |
| Κανονισμός DORA της ΕΕ | Άρθρα 10(2)(e), 25 | |
| COBIT 2019 | MEA01, MEA03 | |

## 1. Σκοπός

**1.1 Σκοπός της παρούσας πολιτικής είναι να θεσπίσει και να διέπει το πρόγραμμα ελέγχων και παρακολούθησης συμμόρφωσης του οργανισμού, ώστε να:**

1.1.1 Επικυρώνει την αποτελεσματικότητα των ελέγχων ασφάλειας και προστασίας της ιδιωτικότητας

1.1.2 Διασφαλίζει την ευθυγράμμιση με τα εφαρμοστέα πρότυπα, τα νομικά και κανονιστικά πλαίσια και τις συμβατικές υποχρεώσεις

1.1.3 Εντοπίζει έγκαιρα μη συμμορφώσεις, αναποτελεσματικότητες και κινδύνους συμμόρφωσης

1.1.4 Υποστηρίζει τη συνεχή βελτίωση και την ετοιμότητα για πιστοποιήσεις, αξιολογήσεις και κανονιστικές ανασκοπήσεις

1.2 Η παρούσα πολιτική υποστηρίζει την ακεραιότητα και την ωριμότητα του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ISMS), ενσωματώνοντας δομημένες πρακτικές ελέγχου και παρακολούθησης, βάσει κινδύνου και τεκμηρίων.

## 2. Πεδίο εφαρμογής

**2.1 Η παρούσα πολιτική εφαρμόζεται σε όλα τα εξής:**

2.1.1 Εσωτερικές επιχειρησιακές μονάδες, λειτουργίες και τμήματα

2.1.2 Φυσικές εγκαταστάσεις, περιβάλλοντα νέφους, πλατφόρμες SaaS και υπηρεσίες εξωτερικής ανάθεσης

2.1.3 Πληροφοριακά συστήματα, εφαρμογές, υποδομές και στοιχεία δεδομένων που διέπονται από το ISMS

2.1.4 Εργαζομένους, αναδόχους και τρίτους παρόχους υπηρεσιών με υποχρεώσεις ελέγχου ή συμμόρφωσης

**2.2 Η πολιτική καλύπτει:**

2.2.1 Εσωτερικούς ελέγχους

2.2.2 Εξωτερικούς ελέγχους/ελέγχους πιστοποίησης

2.2.3 Τεχνική παρακολούθηση συμμόρφωσης

2.2.4 Ελέγχους προμηθευτών και τρίτων μερών

2.2.5 Διορθωτικές ενέργειες και προληπτικές ενέργειες (CAPA)

2.2.6 Μετρικές, πίνακες παρακολούθησης και διαδικασίες αναφοράς

2.3 Εφαρμόζεται σε όλα τα σχετικά πλαίσια στα οποία υπάγεται ο οργανισμός, συμπεριλαμβανομένων των ISO/IEC 27001, ΓΚΠΔ, NIS2, DORA και SOC 2, μεταξύ άλλων.

**3. Στόχοι**

3.1 Να επαληθεύει την επάρκεια και την αποτελεσματικότητα των εφαρμοζόμενων ελέγχων, πολιτικών και διαδικασιών σε όλο το ISMS και τα σχετικά περιβάλλοντα.

3.2 Να εντοπίζει και να αποκαθιστά αδυναμίες, μη συμμορφώσεις ή κενά συμμόρφωσης πριν αυτά εξελιχθούν σε περιστατικά ή παραβιάσεις.

3.3 Να διασφαλίζει διαρκή ετοιμότητα για εσωτερικές ανασκοπήσεις διακυβέρνησης, εξωτερικούς ελέγχους και ανεξάρτητες πιστοποιήσεις.

3.4 Να παράγει επαρκή και τεκμηριωμένα αποδεικτικά στοιχεία και ίχνη ελέγχου προς υποστήριξη κανονιστικών ερευνών, νομικών διαδικασιών ή αιτημάτων διασφάλισης πελατών.

3.5 Να ενσωματώνει τα αποτελέσματα των ελέγχων στην ευρύτερη διαχείριση κινδύνων, στις μετρικές ασφάλειας και στις δραστηριότητες συνεχούς βελτίωσης του οργανισμού.

**4. Ρόλοι και αρμοδιότητες**

**4.1 Επικεφαλής Εσωτερικού Ελέγχου / Διευθυντής Συμμόρφωσης**

4.1.1 Σχεδιάζει, προγραμματίζει και διενεργεί εσωτερικούς ελέγχους βάσει προτεραιότητας κινδύνου.

4.1.2 Τηρεί το Μητρώο Ελέγχων, συντονίζει τις δραστηριότητες ελέγχου και παρακολουθεί τις διορθωτικές ενέργειες.

**4.2 Επικεφαλής Ασφάλειας Πληροφοριών (CISO)**

4.2.1 Διασφαλίζει ότι το πεδίο ελέγχου καλύπτει όλα τα σχετικά στοιχεία του ISMS και τους ελέγχους του Παραρτήματος Α.

4.2.2 Ασκεί εποπτεία στην επαλήθευση των CAPA και ενσωματώνει τα αποτελέσματα των ελέγχων στο πρόγραμμα ασφάλειας.

[ ... 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 Η παρούσα πολιτική πρέπει να ανασκοπείται τουλάχιστον ετησίως από τον Διευθυντή Συμμόρφωσης και τον CISO, ή νωρίτερα σε απόκριση σε:**

9.1.1 Αλλαγές σε κανονιστικά, συμβατικά ή πιστοποιητικά πλαίσια

9.1.2 Σημαντικά ευρήματα ελέγχων ή επαναλαμβανόμενες αστοχίες ελέγχων

9.1.3 Αναδιοργάνωση του οργανισμού ή αλλαγές στο σύστημα GRC

9.1.4 Συστάσεις εξωτερικών ελεγκτών ή σχόλια ρυθμιστικών αρχών

**9.2 Η διαδικασία ανασκόπησης πρέπει να αξιολογεί:**

9.2.1 Τη μεθοδολογία και τη συχνότητα σχεδιασμού ελέγχων

9.2.2 Αλλαγές στο πεδίο εφαρμογής του ISMS ή στην υποδομή

9.2.3 Επικαιροποιήσεις στον κατάλογο ελέγχων ή στο νομικό μητρώο

9.2.4 Τη συνέπεια και την ποιότητα των τεκμηρίων ελέγχου και των διαδικασιών CAPA

**9.3 Όλες οι αλλαγές πολιτικής πρέπει να:**

9.3.1 Τεκμηριώνονται σε αποθετήριο υπό έλεγχο εκδόσεων

9.3.2 Εγκρίνονται από την Ανώτατη Διοίκηση

9.3.3 Γνωστοποιούνται σε όλο το επηρεαζόμενο προσωπικό και να ενσωματώνονται στις επικαιροποιημένες διαδικασίες και στα προγράμματα ευαισθητοποίησης

9.4 Η επικύρωση μετά την ανασκόπηση πρέπει να επιβεβαιώνει ότι οι επικαιροποιημένες απαιτήσεις αποτυπώνονται στο Μητρώο Ελέγχων, στα εργαλεία συμμόρφωσης και στους εσωτερικούς πίνακες παρακολούθησης.

**10. Συναφείς πολιτικές και διασυνδέσεις**

**10.1 Η παρούσα πολιτική ευθυγραμμίζεται με τις ακόλουθες συναφείς οργανωτικές πολιτικές:**

10.1.1 P1 – Πολιτική Ασφάλειας Πληροφοριών: Ορίζει το ISMS και καθορίζει τη λογοδοσία για τη συμμόρφωση και τη συνεχή βελτίωση

10.1.2 P5 – Πολιτική Διαχείρισης Αλλαγών: Διασφαλίζει την ορατότητα ελέγχου σε αλλαγές υποδομής και ρυθμίσεων παραμέτρων που επηρεάζουν τα περιβάλλοντα ελέγχου

10.1.3 P6 – Πολιτική Διαχείρισης Κινδύνων: Ενσωματώνει τα αποτελέσματα ελέγχων στην αξιολόγηση και στις δραστηριότητες αντιμετώπισης επιχειρησιακού κινδύνου

10.1.4 P14 – Πολιτική Διατήρησης και Διάθεσης Δεδομένων: Διέπει τη διατήρηση τεκμηρίων ελέγχου, αρχείων καταγραφής και αρχείων συμμόρφωσης

10.1.5 P18 – Πολιτική Κρυπτογραφικών Ελέγχων: Υποστηρίζει την ασφαλή αποθήκευση και μεταφορά ευαίσθητων δεδομένων ελέγχου

10.1.6 P26 – Πολιτική Ασφάλειας Τρίτων Μερών και Προμηθευτών: Καλύπτει τα δικαιώματα ελέγχου, την τεκμηρίωση διασφάλισης και την εποπτεία συμμόρφωσης προμηθευτών

10.1.7 P30 – Πολιτική Αντιμετώπισης Περιστατικών: Ευθυγραμμίζει τους ελέγχους των διαδικασιών χειρισμού περιστατικών με τους στόχους διασφάλισης του ISMS

10.1.8 P32 – Πολιτική Επιχειρησιακής Συνέχειας και Ανάκαμψης από Καταστροφή: Απαιτεί επαλήθευση των δοκιμών συνέχειας και της συμμόρφωσης του DRP κατά τους κύκλους ελέγχου

**11. Πρότυπα και πλαίσια αναφοράς**

11.1 Η παρούσα πολιτική ευθυγραμμίζεται με διεθνή πρότυπα και νομικές απαιτήσεις για τον έλεγχο και τη συνεχή επικύρωση της συμμόρφωσης.

**11.2 ISO/IEC 27001:**

11.2.1 Ρήτρα 9.2 – Εσωτερικός Έλεγχος: Απαιτεί τακτικούς ελέγχους του ISMS βάσει κινδύνου για την αξιολόγηση της αποτελεσματικότητας και της συμμόρφωσης.

11.2.2 Ρήτρα 9.3 – Ανασκόπηση από τη Διοίκηση: Τα αποτελέσματα των ελέγχων πρέπει να τροφοδοτούν τη στρατηγική ανασκόπηση και βελτίωση.

11.2.3 Ρήτρα 10.1 – Μη συμμόρφωση και διορθωτική ενέργεια: Τα ευρήματα ελέγχου πρέπει να αντιμετωπίζονται μέσω τεκμηριωμένων διαδικασιών CAPA.

**11.3 ISO/IEC 27002:2022 – Έλεγχοι 5.35–5.37:**

11.3.1 Οι έλεγχοι του Παραρτήματος Α 5.35–5.37 καλύπτουν την ανεξάρτητη ανασκόπηση, τη συμμόρφωση με νομικές/συμβατικές απαιτήσεις και την καταγραφή ελέγχου.

11.3.2 Παρέχουν οδηγίες εφαρμογής για τον σχεδιασμό, τη διενέργεια και τη βελτίωση προγραμμάτων ελέγχου και συμμόρφωσης.

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

11.4.1 CA-2 – Αξιολογήσεις ελέγχων: Απαιτεί τακτική ανασκόπηση των εφαρμοζόμενων ελέγχων ασφάλειας.

11.4.2 CA-5 – Plan of Action and Milestones (POA&M): Ευθυγραμμίζεται με την παρακολούθηση και αποκατάσταση ευρημάτων ελέγχου.

11.4.3 CA-7 – Continuous Monitoring: Υποστηρίζει προληπτικές, αυτοματοποιημένες αξιολογήσεις συμμόρφωσης.

**11.5 ΓΚΠΔ της ΕΕ (2016/679):**

11.5.1 Άρθρα 24 και 32: Επιβάλλουν την ύπαρξη τεκμηρίων εφαρμογής και αποτελεσματικότητας των ελέγχων ασφάλειας μέσω κατάλληλων δομών διακυβέρνησης.

11.5.2 Άρθρο 33: Υποστηρίζει την ανάγκη για επαληθευμένα ίχνη ελέγχου κατά την απόκριση και γνωστοποίηση παραβίασης.

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

11.6.1 Άρθρο 21(2)(g): Απαιτεί τον έλεγχο πολιτικών και διαδικασιών ως μέρος των ελάχιστων μέτρων διαχείρισης κινδύνων κυβερνοασφάλειας.

11.6.2 Άρθρο 27: Οι εθνικές αρχές δύνανται να διενεργούν ή να απαιτούν ελέγχους για ουσιώδεις και σημαντικές οντότητες.

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

11.7.1 Άρθρο 10(2)(e): Οι οντότητες πρέπει να διενεργούν εσωτερικούς και εξωτερικούς ελέγχους των πρακτικών διαχείρισης κινδύνων ΤΠΕ.

11.7.2 Άρθρο 25 – Απαιτήσεις ελέγχου: Επιβάλλει περιοδικούς ελέγχους από εσωτερικούς ή ανεξάρτητους εξωτερικούς ελεγκτές με κανονιστική ορατότητα.

**11.8 COBIT 2019:**

11.8.1 MEA01 – Παρακολούθηση, Αξιολόγηση και Εκτίμηση της απόδοσης και της συμμόρφωσης: Διασφαλίζει ότι η αποτελεσματικότητα των ελέγχων επαληθεύεται και αναφέρεται στα όργανα διακυβέρνησης.

11.8.2 MEA03 – Παρακολούθηση, Αξιολόγηση και Εκτίμηση της συμμόρφωσης: Απαιτεί ευθυγράμμιση των πρακτικών του οργανισμού με νομικές, συμβατικές και βασιζόμενες σε πρότυπα απαιτήσεις.