| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου | | | | | | | |
| Αριθμός εγγράφου:<br>P33S | | | | | Τίτλος εγγράφου:<br>**Πολιτική Ελέγχου και Παρακολούθησης της 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, 10 | Εσωτερικοί έλεγχοι, συνεχής βελτίωση και αποκατάσταση μη συμμορφώσεων |
| ISO/IEC 27002:2022 | Έλεγχοι 5.35, 5.37 | Προγραμματισμένες εσωτερικές ανασκοπήσεις, ανεξάρτητες ανασκοπήσεις για διαδικασίες εξωτερικής ανάθεσης |
| NIST SP 800-53 Rev.5 | CA-2, CA-7, AU-6 | Αξιολογήσεις ασφάλειας, συνεχής παρακολούθηση, ανασκόπηση/ανάλυση/αναφορά ελέγχου |
| ΓΚΠΔ της ΕΕ | Άρθρα 24 και 32 | Έλεγχος τεχνικών και οργανωτικών μέτρων, τεκμηρίωση της αποτελεσματικότητας των ελέγχων |
| Οδηγία NIS2 της ΕΕ | Άρθρο 21(2)(f) | Προληπτική ανασκόπηση και συμμόρφωση βάσει τεκμηρίων |
| Κανονισμός DORA της ΕΕ | Άρθρο 10 | Διαχείριση κινδύνων ΤΠΕ, παρακολούθηση και αναφορά |
| COBIT 2019 | MEA01, MEA03 | Παρακολούθηση/αξιολόγηση συμμόρφωσης, συμμόρφωση, ετοιμότητα για ελέγχους από τρίτα μέρη |

**1. Σκοπός**

1.1 Η παρούσα πολιτική καθορίζει την προσέγγιση του οργανισμού για τη διενέργεια εσωτερικών ελέγχων, επαληθεύσεων ελέγχων ασφάλειας και την παρακολούθηση της συμμόρφωσης με κανονιστικές απαιτήσεις. Διασφαλίζει ότι όλοι οι έλεγχοι, οι πολιτικές, τα συστήματα και οι πάροχοι υπηρεσιών υπόκεινται σε τακτική και δομημένη ανασκόπηση.

1.2 Σκοπός είναι ο εντοπισμός αστοχιών ελέγχου, η πρόληψη της μη συμμόρφωσης και η τεκμηρίωση της δέουσας επιμέλειας σύμφωνα με το ISO/IEC 27001, τον ΓΚΠΔ της ΕΕ και τα συναφή πλαίσια.

1.3 Επιτρέπει στις ΜΜΕ να διατηρούν επιχειρησιακό έλεγχο και ετοιμότητα για πιστοποίηση, ακόμη και χωρίς ειδικό τμήμα συμμόρφωσης, με τη χρήση απλών, επαναλαμβανόμενων καταλόγων ελέγχου και ευρημάτων ιεραρχημένων βάσει κινδύνου.

**2. Πεδίο εφαρμογής**

**2.1 Η παρούσα πολιτική εφαρμόζεται σε:**

2.1.1 Όλα τα εσωτερικά τμήματα και όλους τους εξωτερικούς παρόχους υπηρεσιών με αρμοδιότητες που σχετίζονται με συστήματα ΤΠ, δεδομένα προσωπικού χαρακτήρα και επιχειρησιακά κρίσιμες υπηρεσίες

2.1.2 Όλους τους ελέγχους και τα συστήματα που εμπίπτουν στο πεδίο εφαρμογής του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ)

2.1.3 Όλους τους εσωτερικούς ελέγχους, τις ανασκοπήσεις ελέγχων ασφάλειας και τους ελέγχους συμμόρφωσης, είτε διενεργούνται εσωτερικά είτε από εξωτερικό σύμβουλο, πελάτη ή ρυθμιστική αρχή

**2.2 Η παρούσα πολιτική εφαρμόζεται επίσης στη συλλογή τεκμηρίων και στην υποβολή αναφορών για:**

2.2.1 Ελέγχους πιστοποίησης και επαναπιστοποίησης ISO/IEC 27001

2.2.2 Ελέγχους προστασίας δεδομένων βάσει του ΓΚΠΔ της ΕΕ ή συμβατικών όρων

2.2.3 Ερωτηματολόγια ασφάλειας κατόπιν απαίτησης πελατών ή ανασκοπήσεις δέουσας επιμέλειας

2.2.4 Οποιεσδήποτε κανονιστικές ή ανεξάρτητες ανασκοπήσεις βάσει της Οδηγίας NIS2 της ΕΕ ή του Κανονισμού DORA της ΕΕ, όπου εφαρμόζεται

**3. Στόχοι**

3.1 Να διασφαλίζεται ότι όλοι οι βασικοί έλεγχοι και οι πολιτικές ανασκοπούνται τακτικά ως προς την αποτελεσματικότητα και τη συμμόρφωση.

3.2 Να τηρούνται ίχνος ελέγχου και αρχεία διορθωτικών ενεργειών, ώστε να τεκμηριώνονται η λογοδοσία και η βελτίωση.

3.3 Να υποστηρίζεται η προετοιμασία για πιστοποίηση, επαναπιστοποίηση και προγράμματα διασφάλισης πελατών (π.χ. ISO 27001, ένταξη προμηθευτή).

3.4 Να εντοπίζονται έγκαιρα τα κενά, ώστε να καθίσταται δυνατή η άμεση αποκατάσταση πριν τα ζητήματα κλιμακωθούν ή οδηγήσουν σε παραβίαση υποχρεώσεων.

3.5 Να υποστηρίζεται ο Γενικός Διευθυντής και ο εξωτερικός πάροχος υπηρεσιών πληροφορικής στον συντονισμό των ανασκοπήσεων με ελάχιστη πολυπλοκότητα, διασφαλίζοντας ταυτόχρονα τεκμηριώσιμα αποτελέσματα.

**4. Ρόλοι και αρμοδιότητες**

**4.1 Γενικός Διευθυντής (GM)**

4.1.1 Έχει την εποπτεία του προγράμματος ελέγχων

4.1.2 Εγκρίνει τα σχέδια εσωτερικής ανασκόπησης και τα ευρήματα

4.1.3 Αναθέτει και παρακολουθεί τις διορθωτικές ενέργειες

4.1.4 Εγκρίνει την ανάθεση σε εξωτερικούς ελεγκτές ή συμβούλους

**4.2 Εξωτερικός πάροχος υπηρεσιών πληροφορικής / Διαχειριστής**

4.2.1 Παρέχει τεκμήρια κατά τους εσωτερικούς και εξωτερικούς ελέγχους (π.χ. αρχεία καταγραφής, ρυθμίσεις παραμέτρων, αρχεία ελέγχου πρόσβασης)

4.2.2 Υποστηρίζει τους τεχνικούς ελέγχους (π.χ. κατάσταση αντιγράφων ασφαλείας, κατάσταση συμμόρφωσης διορθώσεων)

4.2.3 Τηρεί το κεντρικό αποθετήριο ελεγκτικών τεκμηρίων

[ ... 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 Ετήσια ανασκόπηση πολιτικής και σχεδίου ελέγχων**

9.1.1 Ο Γενικός Διευθυντής (GM) πρέπει να ανασκοπεί την παρούσα πολιτική και το πρόγραμμα ελέγχων τουλάχιστον μία φορά ετησίως.

**9.1.2 Η ανασκόπηση πρέπει να αξιολογεί:**

9.1.2.1 Την αποτελεσματικότητα των ελέγχων στον εντοπισμό κενών

9.1.2.2 Το ποσοστό ολοκλήρωσης των ελέγχων και των διορθωτικών ενεργειών

9.1.2.3 Τις αλλαγές στις εφαρμοστέες νομικές, κανονιστικές απαιτήσεις ή απαιτήσεις πιστοποίησης

**9.2 Επικαιροποιήσεις βάσει εναυσμάτων**

9.2.1 Η πολιτική πρέπει να ανασκοπείται και να επικαιροποιείται όταν:

9.2.2 Ένας έλεγχος πιστοποίησης ή επιτήρησης οδηγήσει σε σημαντική μη συμμόρφωση

9.2.3 Αλλάξουν τα νομικά ή κανονιστικά πλαίσια (π.χ. νέα καθοδήγηση για τον ΓΚΠΔ της ΕΕ, εθνική ενσωμάτωση της Οδηγίας NIS2 της ΕΕ)

9.2.4 Επιχειρησιακές αλλαγές επηρεάζουν συστήματα, διεργασίες ή προμηθευτές που περιλαμβάνονται στο πεδίο εφαρμογής του ελέγχου

9.2.5 Ένα κρίσιμο περιστατικό ή παραβίαση αποκαλύψει κενά ελέγχων που δεν είχαν προηγουμένως εντοπιστεί

**9.3 Τεκμηρίωση επικαιροποιήσεων**

9.3.1 Όλες οι αναθεωρήσεις πρέπει να παρακολουθούνται σε αρχείο ελέγχου εκδόσεων της πολιτικής

9.3.2 Οι επικαιροποιήσεις πρέπει να κοινοποιούνται σε όλα τα μέλη της ομάδας που συμμετέχουν στους ελέγχους

9.3.3 Μαζί με την επικαιροποιημένη πολιτική πρέπει να περιλαμβάνεται σύνοψη αλλαγών ώστε να διασφαλίζεται η κατανόηση

**10. Συναφείς πολιτικές και διασυνδέσεις**

**10.1 Η παρούσα πολιτική υποστηρίζεται από και ενισχύει αρκετές άλλες πολιτικές ΜΜΕ:**

10.1.1 P1S – Πολιτική Ασφάλειας Πληροφοριών: Καθορίζει τη βασική γραμμή για όλες τις προσδοκίες ελέγχου και απαιτεί την εφαρμογή της πολιτικής μέσω ελέγχων.

10.1.2 P2S – Πολιτική Ρόλων και Αρμοδιοτήτων Διακυβέρνησης: Καθορίζει τη λογοδοσία για τον σχεδιασμό ελέγχων, την εκτέλεση και την κυριότητα των διορθωτικών ενεργειών.

10.1.3 P6S – Πολιτική Διαχείρισης Κινδύνων: Εντοπίζει αδυναμίες ελέγχων που αναδεικνύονται κατά τους ελέγχους και διασφαλίζει ότι τα ευρήματα τεκμηριώνονται στο Μητρώο Κινδύνων.

10.1.4 P17S – Πολιτική Προστασίας Δεδομένων και Ιδιωτικότητας: Ορίζει τους ελέγχους του ΓΚΠΔ της ΕΕ που πρέπει να ελέγχονται, συμπεριλαμβανομένων της διαχείρισης δεδομένων, της απόκρισης σε παραβίαση και των ειδοποιήσεων ιδιωτικότητας.

10.1.5 P22S – Πολιτική Καταγραφής και Παρακολούθησης: Παρέχει τα αρχεία καταγραφής ελέγχου και τα ψηφιακά πειστήρια που χρησιμοποιούνται κατά τις ανασκοπήσεις συμμόρφωσης και ελέγχων.

10.1.6 P30S – Πολιτική Αντιμετώπισης Περιστατικών: Απαιτεί την περιοδική ανασκόπηση των αρχείων περιστατικών και των ανασκοπήσεων μετά από συμβάν για την επαλήθευση της αποτελεσματικότητας της απόκρισης.

10.1.7 P31S – Πολιτική Συλλογής Τεκμηρίων και Ψηφιακής Εγκληματολογίας: Παρέχει τις διαδικασίες για τη συλλογή επαληθεύσιμων τεκμηρίων με αλυσίδα επιμέλειας κατά τους ελέγχους.

10.2 Από κοινού, αυτές οι πολιτικές δημιουργούν ένα περιβάλλον ελέγχων κλειστού βρόχου που επιτρέπει την εσωτερική επαλήθευση, την εξωτερική διασφάλιση και τη διακυβέρνηση ευθυγραμμισμένη με πρότυπα.

**11. Πρότυπα και πλαίσια αναφοράς**

**11.1 ISO/IEC 27001:**

11.1.1 Ρήτρα 9.2 – Απαιτεί εσωτερικούς ελέγχους για την αξιολόγηση της απόδοσης του ΣΔΑΠ και της ευθυγράμμισής του με τις απαιτήσεις.

11.1.2 Ρήτρα 10.1 – Επιβάλλει συνεχή βελτίωση βάσει των αποτελεσμάτων ελέγχου και της αποκατάστασης μη συμμορφώσεων.

**11.2 ISO/IEC 27002:**

11.2.1 Έλεγχος 5.35 – Απαιτεί προγραμματισμένες εσωτερικές ανασκοπήσεις ελέγχων και διεργασιών.

11.2.2 Έλεγχος 5.37 – Δίνει έμφαση σε ανεξάρτητες ανασκοπήσεις, ιδίως για διαδικασίες εξωτερικής ανάθεσης.

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

11.3.1 CA-2 – Αξιολογήσεις ασφάλειας: Απαιτεί ελέγχους των εφαρμοσμένων ελέγχων για την επαλήθευση της αποτελεσματικότητάς τους.

11.3.2 CA-7 – Συνεχής παρακολούθηση: Δίνει έμφαση στην προληπτική ανίχνευση και ανασκόπηση αδυναμιών ελέγχων.

11.3.3 AU-6 – Ανασκόπηση, ανάλυση και αναφορά ελέγχου: Επιβάλλει την τακτική ανάλυση και επίλυση ζητημάτων που σχετίζονται με τα αρχεία καταγραφής ελέγχου και τα ευρήματα.

**11.4 ΓΚΠΔ της ΕΕ:**

11.4.1 Άρθρα 24 και 32 – Απαιτούν την εφαρμογή και τον έλεγχο τεχνικών και οργανωτικών μέτρων, συμπεριλαμβανομένης της τεκμηρίωσης της αποτελεσματικότητας των ελέγχων και της βελτίωσης με την πάροδο του χρόνου.

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

11.5.1 Άρθρα 20–21 – Επιβάλλουν προληπτική ανασκόπηση ελέγχων, συμμόρφωση βάσει τεκμηρίων και δυνατότητα ελέγχου για βασικές και σημαντικές οντότητες.

**11.6 COBIT 2019:**

11.6.1 MEA01 – Παρακολούθηση, Αξιολόγηση και Εκτίμηση Απόδοσης και Συμμόρφωσης: Απαιτεί περιοδική αξιολόγηση της απόδοσης διεργασιών και ελέγχων έναντι προτύπων και στόχων.

11.6.2 MEA03 – Διασφάλιση συμμόρφωσης με εξωτερικές απαιτήσεις: Εστιάζει στην εσωτερική παρακολούθηση και στην ετοιμότητα για ελέγχους από τρίτα μέρη και κανονιστικές ανασκοπήσεις.