					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P02S					Τίτλος εγγράφου: **Πολιτική ρόλων και αρμοδιοτήτων διακυβέρνησης P02S**							
Έκδοση: 1.0		Ημερομηνία έναρξης ισχύος: 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**

Ευθυγράμμιση με πρότυπα και κανονιστικές απαιτήσεις

Πρότυπο/Κανονισμός	Ρήτρα/Άρθρο	Σχόλιο
ISO/IEC 27001:2022	Ρήτρα 5	
ISO/IEC 27002:2022	Μέτρα ελέγχου: 5.2, 5.3, 5.4	
NIST SP 800-53 Rev.5	PM-1, PL-1, PL-4, CA-1, AC-1	
ΓΚΠΔ της ΕΕ	Άρθρα 5(2), 32	

1. Σκοπός

1.1 Η παρούσα πολιτική καθορίζει τον τρόπο με τον οποίο οι αρμοδιότητες διακυβέρνησης της ασφάλειας πληροφοριών ανατίθενται, εκχωρούνται και διαχειρίζονται στον οργανισμό, ώστε να διασφαλίζεται πλήρης συμμόρφωση με το ISO/IEC 27001:2022 και τις λοιπές κανονιστικές υποχρεώσεις.

1.2 Διασφαλίζει τη λογοδοσία σε κάθε επίπεδο και υποστηρίζει την επιχειρησιακή αποτελεσματικότητα, προσδιορίζοντας με σαφήνεια ποιος είναι υπεύθυνος για κάθε λειτουργία που σχετίζεται με την ασφάλεια.

1.3 Η παρούσα πολιτική ενισχύει την ετοιμότητα για έλεγχο και την εμπιστοσύνη των πελατών, τεκμηριώνοντας την ύπαρξη επίσημης διακυβέρνησης της ασφάλειας, ακόμη και σε οργανισμούς με περιορισμένο τεχνικό προσωπικό ή με εξωτερική ανάθεση υπηρεσιών πληροφορικής.

2. Πεδίο εφαρμογής

2.1 Η παρούσα πολιτική εφαρμόζεται σε όλα τα πρόσωπα που χειρίζονται συστήματα ή δεδομένα του οργανισμού, συμπεριλαμβανομένων των εξής:

2.1.1 Ιδιοκτήτες επιχειρησιακών λειτουργιών, γενικοί διευθυντές

2.1.2 Εργαζόμενοι και ανάδοχοι

2.1.3 Εξωτερικοί πάροχοι υπηρεσιών πληροφορικής ή σύμβουλοι

2.2 Καλύπτει όλα τα συστήματα, περιβάλλοντα και υπηρεσίες που χρησιμοποιούνται για την επεξεργασία, διαβίβαση ή αποθήκευση επιχειρησιακών πληροφοριών ή πληροφοριών πελατών, συμπεριλαμβανομένων των εξής:

2.2.1 Υποδομές πληροφορικής γραφείου και συσκευές απομακρυσμένης εργασίας

2.2.2 Πλατφόρμες υπολογιστικού νέφους και υπηρεσίες ηλεκτρονικού ταχυδρομείου

2.2.3 Φυσικά αρχεία και κοινόχρηστοι δίσκοι

2.3 Το πεδίο εφαρμογής περιλαμβάνει τόσο εσωτερικές δραστηριότητες όσο και δραστηριότητες με εξωτερική ανάθεση που αφορούν τη διακυβέρνηση της ασφάλειας πληροφοριών.

3. Στόχοι

3.1 Να καθιερωθεί σαφής λογοδοσία για όλα τα καθήκοντα που σχετίζονται με την ασφάλεια, συμπεριλαμβανομένης της διαχείρισης πολιτικών, του ελέγχου πρόσβασης, της διαχείρισης περιστατικών και της παρακολούθησης.

3.2 Να διασφαλιστεί αποτελεσματικός διαχωρισμός καθηκόντων για τη μείωση συγκρούσεων συμφερόντων ή κινδύνων απάτης.

3.3 Να διασφαλιστεί ότι τα καθήκοντα και οι ρόλοι ασφάλειας τεκμηριώνονται με σαφήνεια και υποβάλλονται σε τακτική ανασκόπηση.

3.4 Να υποστηρίζεται η τεκμηριωμένη λήψη αποφάσεων, η κλιμάκωση και η εποπτεία των κινδύνων πληροφορικής και ασφάλειας.

3.5 Να υποστηρίζεται η πιστοποίηση κατά ISO/IEC 27001:2022 και να ενισχύεται η εμπιστοσύνη πελατών, συνεργατών και ελεγκτών.

4. Ρόλοι και αρμοδιότητες

4.1 Γενικός Διευθυντής / Ιδιοκτήτης της επιχείρησης

4.1.1 Έχει τη συνολική ευθύνη για την εφαρμογή και την εποπτεία της παρούσας πολιτικής.

4.1.2 Εγκρίνει όλους τους ρόλους ασφάλειας, τις αρμοδιότητες και τις αποφάσεις εκχώρησης.

4.1.3 Παρακολουθεί τη συμμόρφωση και λαμβάνει τις τελικές αποφάσεις σχετικά με εξαιρέσεις από την πολιτική και κλιμακώσεις.

4.2 Ορισμένος Συντονιστής Ασφάλειας (εφόσον έχει οριστεί)

4.2.1 Μπορεί να είναι μέλος του προσωπικού ή έμπιστος σύμβουλος.

4.2.2 Ο ρόλος αυτός μπορεί να ασκείται από τον Γενικό Διευθυντή ή από εξωτερικό πάροχο σε περιβάλλον μικροεπιχείρησης.

4.2.3 Υποστηρίζει την καθημερινή εφαρμογή του ελέγχου πρόσβασης, της απόκρισης σε περιστατικά και βασικών τεχνικών καθηκόντων ασφάλειας.

4.2.4 Αναφέρεται απευθείας στον Γενικό Διευθυντή για οποιαδήποτε ζητήματα ή κινδύνους 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 Ετήσια ανασκόπηση

9.1.1 Η παρούσα πολιτική πρέπει να ανασκοπείται από τον Γενικό Διευθυντή κάθε 12 μήνες, ώστε να διασφαλίζεται ότι εξακολουθεί να αντανακλά τις νομικές υποχρεώσεις, τις επιχειρησιακές ανάγκες και τις απαιτήσεις πιστοποίησης κατά ISO/IEC 27001.

9.2 Έκτακτες ανασκοπήσεις

9.2.1 Ανασκοπήσεις πρέπει επίσης να διενεργούνται όταν:

9.2.1.1 Επέρχονται σημαντικές οργανωτικές αλλαγές

9.2.1.2 Εντάσσεται νέος πάροχος

9.2.1.3 Προκύπτει σοβαρό περιστατικό ασφάλειας

9.2.1.4 Επικαιροποιούνται κανονισμοί όπως ο ΓΚΠΔ της ΕΕ, η Οδηγία NIS2 της ΕΕ ή ο Κανονισμός DORA της ΕΕ

9.3 Έλεγχος εκδόσεων και τεκμηρίωση

9.3.1 Όλες οι ανασκοπήσεις πρέπει να περιλαμβάνουν:

9.3.1.1 Ημερομηνία ανασκόπησης

9.3.1.2 Σύνοψη τυχόν αλλαγών

9.3.1.3 Υπογραφή ή τεκμηριωμένη έγκριση από τον Γενικό Διευθυντή

9.3.1.4 Αρχειοθετημένες προηγούμενες εκδόσεις για αναφορά σε έλεγχο

9.4 Κοινοποίηση αλλαγών

9.4.1 Κάθε επικαιροποίηση της πολιτικής πρέπει να κοινοποιείται άμεσα στο προσωπικό και στους παρόχους μέσω ηλεκτρονικού ταχυδρομείου, εσωτερικών πυλών ή επίσημων υπηρεσιακών σημειωμάτων.

10. Σχετικές πολιτικές και διασυνδέσεις

10.1 Η παρούσα πολιτική πρέπει να εφαρμόζεται σε συνδυασμό με τις ακόλουθες πολιτικές SME, ώστε να διασφαλίζεται πλήρης αποτελεσματικότητα:

10.1.1 P4S – Πολιτική ελέγχου πρόσβασης: Καθορίζει τον τρόπο με τον οποίο η πρόσβαση χορηγείται, διαχειρίζεται και ανακαλείται, σε άμεση σύνδεση με τους ανατεθειμένους ρόλους και την εποπτεία.

10.1.2 P8S – Πολιτική ενημέρωσης, ευαισθητοποίησης και εκπαίδευσης για την ασφάλεια πληροφοριών: Ενισχύει τις αρμοδιότητες και τις προσδοκίες που συνδέονται με κάθε ρόλο.

10.1.3 P17S – Πολιτική προστασίας δεδομένων και ιδιωτικότητας: Περιγράφει τις νομικές υποχρεώσεις βάσει του ΓΚΠΔ, οι οποίες ανατίθενται στους ρόλους που ορίζονται στην παρούσα πολιτική διακυβέρνησης.

10.1.4 P30S – Πολιτική απόκρισης σε περιστατικά: Απαιτεί καθορισμένες αρμοδιότητες για την αναφορά, την κλιμάκωση και την επίλυση περιστατικών.

10.2 Από κοινού, οι πολιτικές αυτές επιτρέπουν συνεπή εφαρμογή, εσωτερική λογοδοσία και εξωτερική συμμόρφωση.

11. Πρότυπα και πλαίσια αναφοράς

11.1 ISO/IEC 27001

11.1.1 Ρήτρα 5.3 – Οργανωτικοί ρόλοι, αρμοδιότητες και εξουσιοδοτήσεις: Απαιτεί οι ρόλοι να ανατίθενται με σαφήνεια και να υποστηρίζονται από την ανώτατη διοίκηση.

11.2 ISO/IEC 27002

11.2.1 Μέτρα ελέγχου 5.2–5.4: Απαιτούν σαφή τεκμηρίωση των ρόλων ασφάλειας πληροφοριών, διαχωρισμό καθηκόντων και διοικητική εποπτεία.

11.3 NIST SP 800-53 Rev.5

11.3.1 PM-1: Καθιερώνει ένα συνολικό πρόγραμμα ασφάλειας πληροφοριών με καθορισμένες αρμοδιότητες.

11.3.2 PL-1 έως PL-4: Απαιτούν μέτρα ελέγχου σχεδιασμού, συμπεριλαμβανομένης της θέσπισης πολιτικών και των τεκμηριωμένων αναθέσεων ρόλων.

11.3.3 CA-1: Απαιτεί καθορισμένους ρόλους αξιολόγησης και εξουσιοδότησης.

11.3.4 AC-1: Συνδέει τον έλεγχο πρόσβασης βάσει ρόλων με τις ανατεθειμένες αρμοδιότητες διακυβέρνησης.

11.4 ΓΚΠΔ της ΕΕ

11.4.1 Άρθρο 5(2) – Λογοδοσία: Απαιτεί από τους οργανισμούς να αποδεικνύουν τη συμμόρφωση μέσω ρόλων και αρμοδιοτήτων.

11.4.2 Άρθρο 32 – Ασφάλεια της επεξεργασίας: Τονίζει τη σαφή ανάθεση καθηκόντων για την προστασία δεδομένων προσωπικού χαρακτήρα.

11.5 Οδηγία NIS της ΕΕ

11.5.1 Άρθρο 21(2)(a): Επιβάλλει δομές διακυβέρνησης που περιλαμβάνουν τυποποιημένους ρόλους για τη διαχείριση του κυβερνοκινδύνου και των περιστατικών.

11.6 Κανονισμός DORA της ΕΕ

11.6.1 Άρθρα 9 και 10: Απαιτούν από τις χρηματοοικονομικές οντότητες να αναθέτουν με σαφήνεια και να εποπτεύουν τις αρμοδιότητες που σχετίζονται με τις ΤΠΕ και την ασφάλεια.

11.7 COBIT 2019

11.7.1 EDM03 – Διασφάλιση βελτιστοποίησης κινδύνου: Απαιτεί σαφώς καθορισμένους ρόλους και διαδρομές κλιμάκωσης για τη διαχείριση του κινδύνου ασφάλειας.

11.7.2 APO13 – Διαχείριση ασφάλειας: Αναθέτει στρατηγικά και επιχειρησιακά καθήκοντα ασφάλειας σε πρόσωπα και ρόλους.

11.7.3 DSS05 – Διαχείριση υπηρεσιών ασφάλειας: Απαιτεί δομή και ιχνηλασιμότητα στις αρμοδιότητες για εξωτερικές και εσωτερικές υπηρεσίες ασφάλειας.