					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P37S					Τίτλος εγγράφου: **Πολιτική Νομικής και Κανονιστικής Συμμόρφωσης**							
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	Ρήτρες 5.1, 6.1, 6.2, 8	
ISO/IEC 27002:2022	Έλεγχος 5	
NIST SP 800-53 Rev.5	PL-1, PL-2, PM-1, CA-1, AU-1	
ΓΚΠΔ της ΕΕ	Άρθρα 5, 6, 32, 33	
Οδηγία NIS2 της ΕΕ	Άρθρα 21(2)(a), 21(2)(f), 23	
Κανονισμός DORA της ΕΕ	Άρθρα 5(2), 9(1), 17	
COBIT 2019	APO12, APO13, DSS01	

1. Σκοπός

1.1 Η παρούσα πολιτική καθορίζει την προσέγγιση του οργανισμού για την αναγνώριση, τη συμμόρφωση προς και την τεκμηρίωση της τήρησης των νομικών, κανονιστικών και συμβατικών υποχρεώσεων.

1.2 Παρέχει σαφείς αρμοδιότητες και πρακτικά βήματα, ώστε η επιχείρηση να εκπληρώνει τις υποχρεώσεις συμμόρφωσης που έχει αναλάβει, συμπεριλαμβανομένης της νομοθεσίας για την προστασία δεδομένων, των πλαισίων κυβερνοασφάλειας, των συμφωνιών με πελάτες και των απαιτήσεων πιστοποίησης.

1.3 Διασφαλίζει ότι, ακόμη και χωρίς ειδική λειτουργία συμμόρφωσης, η επιχείρηση μπορεί να λειτουργεί σύννομα, να ανταποκρίνεται κατάλληλα σε περιστατικά και να διατηρεί πλήρη ετοιμότητα για έλεγχο.

1.4 Η παρούσα πολιτική είναι ουσιώδης για την επίτευξη πιστοποίησης ISO/IEC 27001:2022 και για την ικανοποίηση εξωτερικών απαιτήσεων από πελάτες, ρυθμιστικές αρχές ή συνεργάτες.

2. Πεδίο εφαρμογής

2.1 Η παρούσα πολιτική εφαρμόζεται σε:

2.1.1 Όλους τους εργαζομένους, αναδόχους, ελεύθερους επαγγελματίες, προμηθευτές και λοιπά τρίτα μέρη.

2.1.2 Όλες τις υπηρεσίες, λειτουργίες, συστήματα και δραστηριότητες διαχείρισης δεδομένων για τις οποίες ο οργανισμός υποχρεούται να τηρεί νομικές ή συμβατικές απαιτήσεις.

2.1.3 Όλες τις τοποθεσίες και συσκευές που χρησιμοποιούνται για την επεξεργασία επιχειρησιακών πληροφοριών, είτε εντός γραφείου είτε εξ αποστάσεως είτε σε περιβάλλοντα νέφους.

2.2 Η πολιτική καλύπτει:

2.2.1 Τη νομοθεσία προστασίας δεδομένων, όπως ο ΓΚΠΔ της ΕΕ.

2.2.2 Τις κανονιστικές απαιτήσεις κυβερνοασφάλειας, όπως η Οδηγία NIS2 της ΕΕ.

2.2.3 Τις τομεακές υποχρεώσεις, όπου εφαρμόζονται.

2.2.4 Συμβάσεις πελατών, συμφωνίες εμπιστευτικότητας και ρήτρες ελέγχου.

2.2.5 Εθελοντικές πιστοποιήσεις (π.χ. ISO 27001) και εσωτερικές πολιτικές που πρέπει να τηρούνται για σκοπούς συμμόρφωσης.

3. Στόχοι

3.1 Καθιέρωση λογοδοσίας: Ανάθεση σαφούς ευθύνης για την παρακολούθηση, την επικαιροποίηση και την εφαρμογή των νομικών, κανονιστικών και συμβατικών υποχρεώσεων.

3.2 Προστασία της επιχείρησης: Ελαχιστοποίηση του κινδύνου νομικών παραβάσεων, προστίμων, παραβίασης δεδομένων και βλάβης της φήμης.

3.3 Υποστήριξη ελεγκτικής ετοιμότητας: Διατήρηση επαληθεύσιμων αρχείων που αποδεικνύουν πώς ο οργανισμός εκπληρώνει τις υποχρεώσεις συμμόρφωσής του.

3.4 Υποστήριξη ενσωμάτωσης πολιτικών: Διασφάλιση ότι οι νομικές και κανονιστικές υποχρεώσεις εφαρμόζονται με συνέπεια σε όλες τις πολιτικές και διαδικασίες.

3.5 Διαφανής διαχείριση εξαιρέσεων: Διασφάλιση ότι κάθε εξαίρεση συμμόρφωσης τεκμηριώνεται, αιτιολογείται και εγκρίνεται, ώστε να αποφεύγεται η έκθεση σε ευθύνη.

4. Ρόλοι και αρμοδιότητες

4.1 Γενικός Διευθυντής (GM)

4.1.1 Φέρει τη συνολική λογοδοσία για τη νομική και κανονιστική συμμόρφωση του οργανισμού.

4.1.2 Τηρεί το Μητρώο Συμμόρφωσης και διασφαλίζει ότι παραμένει επικαιροποιημένο.

4.1.3 Ανασκοπεί τις συμβάσεις πελατών και διασφαλίζει ότι οι ειδικές υποχρεώσεις παρακολουθούνται και εφαρμόζονται.

4.1.4 Εγκρίνει εξαιρέσεις από υποχρεώσεις συμμόρφωσης μόνο όταν αυτό δικαιολογείται νομικά και υφίστανται αντισταθμιστικοί έλεγχοι.

4.2 Εξωτερικοί Σύμβουλοι (π.χ. νομικοί, σύμβουλοι πληροφορικής ή συμμόρφωσης)

4.2.1 Υποστηρίζουν τον GM στον προσδιορισμό της εφαρμοστέας νομοθεσίας, των πιστοποιήσεων και των υποχρεώσεων (π.χ. ΓΚΠΔ, NIS2, ISO 27001).

4.2.2 Παρέχουν καθοδήγηση για την ερμηνεία νέων κανονιστικών απαιτήσεων ή μεταβολών της ισχύουσας νομοθεσίας.

4.2.3 Μπορούν να συνδράμουν στην επικαιροποίηση πολιτικών, στη διενέργεια ελέγχων ή στην απόκριση σε παραβιάσεις όταν υπάρχει νομική έκθεση.

[... 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 Προγραμματισμένη ετήσια ανασκόπηση

9.1.1 Η παρούσα πολιτική πρέπει να ανασκοπείται κάθε 12 μήνες από τον GM.

9.1.2 Η ανασκόπηση πρέπει να επιβεβαιώνει:

9.1.2.1 Τη συνάφεια με το ισχύον νομικό και συμβατικό πλαίσιο.

9.1.2.2 Την ορθή αποτύπωση των συμφωνιών με πελάτες και των υποχρεώσεων παροχής υπηρεσιών.

9.1.2.3 Την ευθυγράμμιση με το Μητρώο Συμμόρφωσης και τις λοιπές πολιτικές.

9.2 Επικαιροποιήσεις κατόπιν γεγονότος

9.2.1 Απαιτείται άμεση ανασκόπηση εάν:

9.2.1.1 Καταστεί εφαρμοστέος νέος νόμος ή νέα κανονιστική απαίτηση (π.χ. νέος κανόνας προστασίας δεδομένων).

9.2.1.2 Πελάτης προσθέσει σύνθετους όρους συμμόρφωσης στη συμφωνία του.

9.2.1.3 Σημειωθεί παραβίαση ή περιστατικό μη συμμόρφωσης.

9.2.1.4 Η εταιρεία επεκταθεί σε ρυθμιζόμενη αγορά ή κλάδο.

9.3 Έγκριση επικαιροποιήσεων και έλεγχος εκδόσεων

9.3.1 Όλες οι επικαιροποιήσεις πρέπει να τεκμηριώνονται, να λαμβάνουν έκδοση και να εγκρίνονται από τον GM.

9.3.2 Οι ιστορικές εκδόσεις πρέπει να διατηρούνται για ελεγκτικούς και νομικούς σκοπούς.

9.4 Επικοινωνία αλλαγών

9.4.1 Το προσωπικό και οι ανάδοχοι πρέπει να ενημερώνονται για τις αλλαγές πολιτικής εντός 5 εργάσιμων ημερών από την έγκριση.

9.4.2 Τυχόν επηρεαζόμενοι προμηθευτές πρέπει επίσης να επιβεβαιώνουν την αποδοχή των επικαιροποιημένων όρων πριν από τη συνέχιση της παροχής υπηρεσιών.

10. Συναφείς πολιτικές και διασυνδέσεις

10.1 Η παρούσα πολιτική υποστηρίζεται και εφαρμόζεται μέσω των ακόλουθων πολιτικών SME:

10.1.1 P3S – Πολιτική Αποδεκτής Χρήσης: Αποτρέπει συμπεριφορές που ενδέχεται να παραβιάζουν νομικούς ή συμβατικούς όρους (π.χ. μη εξουσιοδοτημένη κοινοποίηση αρχείων).

10.1.2 P8S – Πολιτική Εκπαίδευσης και Ευαισθητοποίησης για την Ασφάλεια Πληροφοριών: Εκπαιδεύει το προσωπικό σχετικά με τις υποχρεώσεις συμμόρφωσης και τον τρόπο αποφυγής παραβιάσεων.

10.1.3 P14S – Πολιτική Διατήρησης και Διάθεσης Δεδομένων: Διασφαλίζει νόμιμες πρακτικές διαχείρισης δεδομένων σε όλο τον κύκλο ζωής των δεδομένων.

10.1.4 P17S – Πολιτική Προστασίας Δεδομένων και Ιδιωτικότητας: Καλύπτει τις απαιτήσεις του ΓΚΠΔ και τις απαιτήσεις πελατών για τη διαχείριση δεδομένων.

10.1.5 P30S – Πολιτική Αντιμετώπισης Περιστατικών: Καθορίζει τον τρόπο απόκρισης σε παραβιάσεις δεδομένων ή αστοχίες συμμόρφωσης, συμπεριλαμβανομένων των χρονοδιαγραμμάτων γνωστοποίησης.

10.1.6 P36S – Πολιτική Μέσων Κοινωνικής Δικτύωσης και Εξωτερικών Επικοινωνιών: Διασφαλίζει ότι οι δημόσιες επικοινωνίες δεν παραβιάζουν νομικές ή κανονιστικές υποχρεώσεις.

10.2 Κάθε διασυνδεδεμένη πολιτική εφαρμόζει μέρος του πλαισίου νομικής συμμόρφωσης και πρέπει να εφαρμόζεται συνδυαστικά με τις υπόλοιπες.

11. Πρότυπα και πλαίσια αναφοράς

11.1 ISO/IEC 27001

11.1.1 Ρήτρα 6.1 – Ενέργειες για την αντιμετώπιση κινδύνων και ευκαιριών: Περιλαμβάνει κινδύνους συμμόρφωσης.

11.1.2 Ρήτρα 8.1 – Επιχειρησιακός σχεδιασμός και έλεγχος: Απαιτεί την εκτέλεση διαδικασιών που ικανοποιούν νομικές και συμβατικές απαιτήσεις.

11.2 ISO/IEC 27002

11.2.1 Έλεγχος 5.36 – Καθοδηγεί τον οργανισμό στη διατήρηση αρχείων υποχρεώσεων και στη διασφάλιση κατάλληλης απόκρισης σε νομικές και κανονιστικές απαιτήσεις.

11.3 NIST SP 800-53 Rev.5

11.3.1 PL-1 – Πολιτική και διαδικασίες: Επιβάλλει την ύπαρξη επίσημων πολιτικών συμμόρφωσης.

11.3.2 PM-1 – Σχέδιο προγράμματος ασφάλειας πληροφοριών: Απαιτεί την ενσωμάτωση της νομικής συμμόρφωσης στον σχεδιασμό της ασφάλειας.

11.3.3 CA-1 – Αξιολόγηση, εξουσιοδότηση και παρακολούθηση.

11.3.4 AU-1 – Πολιτική ελέγχου: Απαιτεί τη διατήρηση τεκμηρίων συμμόρφωσης.

11.4 ΓΚΠΔ της ΕΕ

11.4.1 Άρθρο 5 – Αρχές επεξεργασίας δεδομένων, συμπεριλαμβανομένης της λογοδοσίας.

11.4.2 Άρθρο 6 – Νομική βάση για την επεξεργασία.

11.4.3 Άρθρο 32 – Ασφάλεια της επεξεργασίας.

11.4.4 Άρθρο 33 – Γνωστοποίηση παραβίασης εντός 72 ωρών.

11.5 Οδηγία NIS2 της ΕΕ

11.5.1 Άρθρο 21(2)(a) και (f) – Εσωτερικές πολιτικές για τον έλεγχο κινδύνων και κανονιστικών απαιτήσεων.

11.5.2 Άρθρο 23 – Εφαρμογή και κυρώσεις για αστοχίες συμμόρφωσης.

11.6 Κανονισμός DORA της ΕΕ

11.6.1 Άρθρο 5(2) – Εποπτεία της διαχείρισης κινδύνων ΤΠΕ.

11.6.2 Άρθρο 9(1) – Εσωτερική διακυβέρνηση της συμμόρφωσης.

11.6.3 Άρθρο 17 – Συμβατικές ρυθμίσεις με παρόχους υπηρεσιών ΤΠΕ.

11.7 COBIT 2019

11.7.1 APO12 – Managed Risk: Διασφαλίζει ότι οι κίνδυνοι συμμόρφωσης παρακολουθούνται και αντιμετωπίζονται.

11.7.2 APO13 – Managed Security: Καλύπτει την εφαρμογή κανονιστικής και συμβατικής συμμόρφωσης βάσει κινδύνου.

11.7.3 DSS01 – Managed Operations: Επιβάλλει επιχειρησιακή ετοιμότητα για την εκπλήρωση νομικών υποχρεώσεων.