					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P37					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**

1. Σκοπός

1.1 Η παρούσα πολιτική θεσπίζει το υποχρεωτικό πλαίσιο για την αναγνώριση, διαχείριση και συμμόρφωση με όλες τις νομικές, κανονιστικές και συμβατικές υποχρεώσεις που σχετίζονται με την ασφάλεια πληροφοριών, την προστασία δεδομένων προσωπικού χαρακτήρα και τις επιχειρησιακές λειτουργίες του οργανισμού.

1.2 Στόχος είναι η αποτροπή περιπτώσεων μη συμμόρφωσης που θα μπορούσαν να οδηγήσουν σε πρόστιμα, νομική ευθύνη, διακοπή της επιχειρησιακής λειτουργίας, βλάβη της φήμης ή επιβολή κανονιστικών μέτρων.

1.3 Η παρούσα πολιτική υποστηρίζει την ενσωμάτωση των υποχρεώσεων συμμόρφωσης στη διακυβέρνηση, στις διαδικασίες διαχείρισης κινδύνων, στις επιχειρησιακές ροές εργασίας, στους κύκλους ζωής των έργων και στον σχεδιασμό συστημάτων.

1.4 Διασφαλίζει ότι όλες οι σχετικές υποχρεώσεις —σε διαφορετικές δικαιοδοσίες, κλάδους δραστηριότητας και πεδία κανονιστικής εφαρμογής— τεκμηριώνονται με σαφήνεια, αξιολογούνται, παρακολουθούνται και εφαρμόζονται εντός του οργανισμού.

2. Πεδίο εφαρμογής

2.1 Η παρούσα πολιτική εφαρμόζεται σε όλα τα τμήματα, τις λειτουργίες, τις επιχειρησιακές μονάδες και τα πρόσωπα που ενεργούν για λογαριασμό του οργανισμού, συμπεριλαμβανομένων των εξής:

2.1.1 Μόνιμοι και προσωρινοί εργαζόμενοι

2.1.2 Ανάδοχοι, σύμβουλοι και ασκούμενοι

2.1.3 Προμηθευτές ή άλλοι τρίτοι, εκτελούντες την επεξεργασία ή συνεργάτες που χειρίζονται δεδομένα, συστήματα ή κανονιστικές υποχρεώσεις του οργανισμού

2.1.4 Κάθε επιχειρησιακή διεργασία, έργο ή πρωτοβουλία που υπόκειται σε νομικές ή κανονιστικές απαιτήσεις

2.2 Οι τομείς συμμόρφωσης που διέπονται από την παρούσα πολιτική περιλαμβάνουν ενδεικτικά και όχι περιοριστικά:

2.2.1 Υποχρεώσεις ασφάλειας πληροφοριών και κυβερνοασφάλειας (π.χ. ISO/IEC 27001, NIS2, DORA)

2.2.2 Νομοθεσία προστασίας δεδομένων προσωπικού χαρακτήρα και ιδιωτικότητας (π.χ. ΓΚΠΔ, κλαδική νομοθεσία ιδιωτικότητας)

2.2.3 Τομεακές κανονιστικές απαιτήσεις (π.χ. χρηματοοικονομικός, ιατρικός, αυτοκινητοβιομηχανικός, αμυντικός τομέας)

2.2.4 Συμβατικές υποχρεώσεις που απορρέουν από συμφωνίες εμπιστευτικότητας, συμφωνίες επιπέδου υπηρεσιών (SLA) ή συμφωνίες επεξεργασίας με τρίτα μέρη

2.2.5 Νομικές απαιτήσεις που σχετίζονται με την αναφορά περιστατικών, την αλληλεπίδραση με διωκτικές αρχές και τις διεθνείς διαβιβάσεις δεδομένων

3. Στόχοι

3.1 Να διασφαλίζεται ότι όλοι οι εφαρμοστέοι νόμοι, κανονισμοί, πρότυπα και συμβατικές υποχρεώσεις αναγνωρίζονται, τεκμηριώνονται, ερμηνεύονται και εφαρμόζονται σε ολόκληρο τον οργανισμό.

3.2 Να ενσωματώνονται οι νομικές και κανονιστικές απαιτήσεις στο Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (ISMS), στις διαδικασίες διαχείρισης κινδύνων, στις συμφωνίες με προμηθευτές και στον σχεδιασμό προϊόντων και υπηρεσιών του οργανισμού.

3.3 Να παρέχεται μηχανισμός για την προληπτική παρακολούθηση κανονιστικών αλλαγών και την αντίστοιχη επικαιροποίηση των ελέγχων και της τεκμηρίωσης.

3.4 Να ορίζεται σαφής λογοδοσία για την εποπτεία της συμμόρφωσης, την κλιμάκωση περιπτώσεων μη συμμόρφωσης, τη διαχείριση εξαιρέσεων και την εξωτερική αναφορά.

3.5 Να διασφαλίζεται η ελεγκτική επάρκεια και η δυνατότητα τεκμηριωμένης υποστήριξης της νομικής και κανονιστικής θέσης του οργανισμού κατά τη διάρκεια επιθεωρήσεων, ερευνών ή ανασκοπήσεων πιστοποίησης.

4. Ρόλοι και αρμοδιότητες

4.1 Ανώτατη Διοίκηση

4.1.1 Έχει τη στρατηγική λογοδοσία για τη νομική και κανονιστική συμμόρφωση σε επίπεδο οργανισμού.

4.1.2 Ανασκοπεί και εγκρίνει αποφάσεις συμμόρφωσης υψηλού κινδύνου, συμπεριλαμβανομένης της αποδοχής κινδύνου και νομικών διαφορών.

4.2 Υπεύθυνος Συμμόρφωσης / Γενικός Νομικός Σύμβουλος / Νομικός Σύμβουλος

4.2.1 Τηρεί το Μητρώο Υποχρεώσεων Συμμόρφωσης, στο οποίο καταγράφονται όλοι οι εφαρμοστέοι νόμοι, τα πρότυπα, οι πιστοποιήσεις και οι συμβατικές ρήτρες.

4.2.2 Διενεργεί εκτιμήσεις νομικού αντικτύπου για νέες υπηρεσίες, αγορές ή ροές δεδομένων.

4.2.3 Παρέχει έγκυρη ερμηνεία νόμων και προτύπων.

[... 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 της πολιτικής

9.1.1 Η παρούσα πολιτική πρέπει να ανασκοπείται τουλάχιστον μία φορά ανά ημερολογιακό έτος, ώστε να:

9.1.1.1 διασφαλίζεται η διαρκής ευθυγράμμιση με επικαιροποιημένους νόμους, πρότυπα του κλάδου και κανονιστικά πλαίσια

9.1.1.2 επιβεβαιώνεται η επιχειρησιακή αποτελεσματικότητα βάσει ευρημάτων ελέγχου και ιστορικού περιστατικών

9.1.1.3 αποτυπώνονται οργανωτικές αλλαγές (π.χ. νέες δικαιοδοσίες, συστήματα ή γραμμές δραστηριότητας)

9.2 Ανασκοπήσεις βάσει εναυσμάτων

9.2.1 Πρέπει να διενεργούνται ενδιάμεσες ανασκοπήσεις όταν:

9.2.2 θεσπίζεται ή επικαιροποιείται νέα νομική ή κανονιστική απαίτηση

9.2.3 περιστατικό συμμόρφωσης ή έλεγχος αποκαλύπτει αδυναμίες της πολιτικής

9.2.4 ο οργανισμός εισέρχεται σε νέα αγορά ή γραμμή υπηρεσιών που διέπεται από διακριτά πλαίσια συμμόρφωσης

9.2.5 τάσεις κανονιστικής επιβολής ή κατευθυντήριες οδηγίες ρυθμιστικών αρχών υποδεικνύουν μεταβολές στη στάση κινδύνου

9.3 Ιδιοκτησία και έγκριση

9.3.1 Το Νομικό Τμήμα και ο Υπεύθυνος Συμμόρφωσης έχουν από κοινού τη λογοδοσία για τον συντονισμό της διαδικασίας ανασκόπησης.

9.3.2 Οι τελικές αναθεωρήσεις της πολιτικής πρέπει να εγκρίνονται από την Ανώτατη Διοίκηση και να καταγράφονται στο Μητρώο Αλλαγών Πολιτικών, με τις σχετικές παραπομπές ελέγχου αλλαγών και τα σχέδια επικοινωνίας.

9.4 Έλεγχος εκδόσεων και επικοινωνία

9.4.1 Κάθε επικαιροποιημένη έκδοση της παρούσας πολιτικής πρέπει:

9.4.1.1 να περιλαμβάνει σύνοψη των βασικών αλλαγών

9.4.1.2 να αναδιανέμεται μέσω επίσημων διαύλων (π.χ. πύλη πολιτικών, LMS, εσωτερικά ενημερωτικά δελτία)

9.4.1.3 να απαιτεί επιβεβαίωση λήψης και κατανόησης από το επηρεαζόμενο προσωπικό, ιδίως από όσους έχουν ρόλους στη νομική λειτουργία, στις επιχειρησιακές λειτουργίες, στην ασφάλεια και στη διαχείριση προμηθευτών

10. Συναφείς πολιτικές και διασυνδέσεις

10.1 Η παρούσα πολιτική λειτουργεί σε συνδυασμό με τις ακόλουθες πολιτικές του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ISMS) του οργανισμού και τις ενισχύει:

10.1.1 P1 – Πολιτική Ασφάλειας Πληροφοριών: Καθορίζει τις βασικές αρχές διακυβέρνησης που διασφαλίζουν ότι όλες οι πολιτικές ασφάλειας πληροφοριών —συμπεριλαμβανομένης της συμμόρφωσης— ευθυγραμμίζονται με τις στρατηγικές επιχειρησιακές και κανονιστικές απαιτήσεις.

10.1.2 P2 – Πολιτική Ρόλων και Αρμοδιοτήτων Διακυβέρνησης: Ορίζει τις αρμοδιότητες λήψης αποφάσεων, συμπεριλαμβανομένων των νομικών και κανονιστικών ρόλων που είναι υπεύθυνοι για την κανονιστική εποπτεία και τη λογοδοσία.

10.1.3 P6 – Πολιτική Διαχείρισης Κινδύνων: Υποστηρίζει την αξιολόγηση, την ιδιοκτησία και τον μετριασμό των κινδύνων νομικής και κανονιστικής συμμόρφωσης σε επίπεδο οργανισμού.

10.1.4 P8 – Πολιτική Ευαισθητοποίησης και Εκπαίδευσης για την Ασφάλεια Πληροφοριών: Διασφαλίζει ότι όλο το προσωπικό ενημερώνεται για τις αρμοδιότητες συμμόρφωσης και λαμβάνει κατάλληλη εκπαίδευση ανά ρόλο.

10.1.5 P12 – Πολιτική Διαχείρισης Περιουσιακών Στοιχείων: Ενισχύει τις νομικές υποχρεώσεις για τη διαχείριση και προστασία ρυθμιζόμενων ή συμβατικών περιουσιακών στοιχείων, συμπεριλαμβανομένων εκείνων που σχετίζονται με δεδομένα προσωπικού χαρακτήρα και κρίσιμες υποδομές.

10.1.6 P30 – Πολιτική Αντιμετώπισης Περιστατικών: Διέπει τις υποχρεωτικές νομικές γνωστοποιήσεις (π.χ. άρθρο 33 του ΓΚΠΔ) και τις διαδικασίες κλιμάκωσης σε περίπτωση παραβίασης συμμόρφωσης ή κανονιστικού συμβάντος.

10.1.7 P33 – Πολιτική Ελέγχου και Παρακολούθησης Συμμόρφωσης: Παρέχει δομημένες δραστηριότητες διασφάλισης —συμπεριλαμβανομένων των δοκιμών ελέγχων και της συλλογής τεκμηρίων— που απαιτούνται για την εσωτερική και εξωτερική επαλήθευση συμμόρφωσης.

11. Πρότυπα και πλαίσια αναφοράς

11.1 ISO/IEC 27001

11.1.1 Ρήτρα 4.2 – Κατανόηση των αναγκών και προσδοκιών των ενδιαφερόμενων μερών: Απαιτεί την αναγνώριση και ενσωμάτωση νομικών και κανονιστικών απαιτήσεων στο ISMS.

11.1.2 Ρήτρα 5.1 – Ηγεσία και δέσμευση: Καθιερώνει την εκτελεστική λογοδοσία για τη θέσπιση και διατήρηση της νομικής συμμόρφωσης σε ολόκληρο τον οργανισμό.

11.1.3 Ρήτρα 5.3 – Οργανωτικοί ρόλοι, αρμοδιότητες και εξουσίες: Διασφαλίζει σαφήνεια ρόλων για τη νομική εποπτεία και την κανονιστική συμμόρφωση.

11.1.4 Έλεγχος 5.36 του Παραρτήματος Α – Συμμόρφωση με νομικές και συμβατικές απαιτήσεις: Καθιερώνει την απαίτηση αναγνώρισης και εκπλήρωσης των υποχρεώσεων που απορρέουν από νόμους, κανονισμούς και συμβάσεις.

11.2 ISO/IEC 27002

11.2.1 Έλεγχος 5.36: Παρέχει οδηγίες εφαρμογής για τη διατήρηση μητρώου υποχρεώσεων συμμόρφωσης, την επικύρωση κανονιστικών απαιτήσεων και τη διασφάλιση δομημένης διατήρησης τεκμηρίων.

11.3 NIST SP 800-53 Rev.5

11.3.1 PL-1 – Πολιτική και διαδικασίες σχεδιασμού ασφάλειας: Απαιτεί οι υποχρεώσεις συμμόρφωσης να ενσωματώνονται στις δομές διακυβέρνησης και στην τεκμηρίωση.

11.3.2 PM-1 – Σχέδιο προγράμματος ασφάλειας πληροφοριών: Καθιερώνει τους κανονιστικούς ελέγχους ως στοιχείο του ευρύτερου προγράμματος ασφάλειας.

11.3.3 CA-7 – Συνεχής παρακολούθηση: Υποστηρίζει την εποπτεία της αποτελεσματικότητας των ελέγχων ως προς την κάλυψη νομικών απαιτήσεων και απαιτήσεων πολιτικής.

11.3.4 AU-9 – Προστασία πληροφοριών ελέγχου: Διασφαλίζει ότι τα αρχεία καταγραφής και τα αρχεία ελέγχου συμμόρφωσης προστατεύονται και είναι διαθέσιμα για επιθεώρηση.

11.4 ΓΚΠΔ της ΕΕ (2016/679)

11.4.1 Άρθρο 5 – Αρχές που διέπουν την επεξεργασία: Απαιτεί νόμιμη επεξεργασία, διαφάνεια και λογοδοσία.

11.4.2 Άρθρο 6 – Νομιμότητα της επεξεργασίας: Απαιτεί κατάλληλη νομική βάση για όλες τις δραστηριότητες επεξεργασίας δεδομένων.

11.4.3 Άρθρο 24 – Ευθύνη του υπευθύνου επεξεργασίας: Καθιερώνει άμεση λογοδοσία για τη διασφάλιση της κανονιστικής συμμόρφωσης.

11.4.4 Άρθρο 32 – Ασφάλεια της επεξεργασίας: Απαιτεί την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων.

11.4.5 Άρθρο 33 – Γνωστοποίηση παραβίασης: Απαιτεί οι παραβιάσεις δεδομένων προσωπικού χαρακτήρα να γνωστοποιούνται εντός 72 ωρών στις αρμόδιες αρχές.

11.5 Οδηγία NIS2 της ΕΕ (2022/2555)

11.5.1 Άρθρα 20–21: Απαιτούν από ουσιώδεις και σημαντικές οντότητες να εφαρμόζουν τεκμηριωμένη διακυβέρνηση, στρατηγικές νομικής συμμόρφωσης και συνεχή ανασκόπηση νομικών κινδύνων.

11.6 Κανονισμός DORA της ΕΕ (2022/2554)

11.6.1 Άρθρο 5(2) – Πλαίσιο διαχείρισης κινδύνων ΤΠΕ: Απαιτεί την ενσωμάτωση της νομικής συμμόρφωσης στις ευρύτερες λειτουργίες διαχείρισης κινδύνων και εποπτείας.

11.6.2 Άρθρο 19 – Κίνδυνος ΤΠΕ από τρίτα μέρη: Επιβάλλει ειδικές νομικές απαιτήσεις για τη διαχείριση συμβατικών και κανονιστικών υποχρεώσεων που αφορούν εξωτερικούς προμηθευτές και πλατφόρμες.

11.7 COBIT 2019

11.7.1 APO12 – Διαχείριση κινδύνων: Ενσωματώνει τη νομική και κανονιστική συμμόρφωση ως κρίσιμα στοιχεία της εταιρικής διακυβέρνησης κινδύνων.

11.7.2 MEA03 – Παρακολούθηση συμμόρφωσης με εξωτερικές απαιτήσεις: Ορίζει τη συνεχή παρακολούθηση, τη διαχείριση εξαιρέσεων και την ετοιμότητα για έλεγχο για όλες τις μορφές κανονιστικών υποχρεώσεων.