					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P01					Τίτλος εγγράφου: **Πολιτική Ασφάλειας Πληροφοριών**							
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 καθορίζει τη συνολική δέσμευση του οργανισμού για την ασφάλεια πληροφοριών μέσω της θέσπισης επίσημου Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ISMS).

1.2 Παρέχει τη στρατηγική κατεύθυνση και τις βασικές απαιτήσεις για την προστασία της εμπιστευτικότητας, της ακεραιότητας, της διαθεσιμότητας και της ανθεκτικότητας όλων των πληροφοριακών περιουσιακών στοιχείων σε φυσικά, ψηφιακά και νεφοϋπολογιστικά περιβάλλοντα.

1.3 Η πολιτική καλύπτει τις απαιτήσεις των Ρητρών 5.2 και 5.1 του ISO/IEC 27001:2022, αποτυπώνοντας την πρόθεση της ηγεσίας, τη δέσμευση της ανώτατης διοίκησης και την ευθυγράμμιση των δραστηριοτήτων ασφάλειας με τους οργανωτικούς στόχους.

1.4 Αποτελεί το δεσμευτικό σημείο αναφοράς για όλες τις επιμέρους πολιτικές, τα πρότυπα και τις διαδικασίες του ISMS και είναι ουσιώδης για τη διαμόρφωση ενός περιβάλλοντος ασφάλειας που βασίζεται στον κίνδυνο, στη συμμόρφωση και στη συνεχή βελτίωση.

2. Πεδίο εφαρμογής

2.1 Η παρούσα πολιτική εφαρμόζεται σε όλα τα πρόσωπα, τα περιουσιακά στοιχεία και τις διεργασίες που εμπίπτουν στο πεδίο εφαρμογής του ISMS, συμπεριλαμβανομένων των εξής:

2.1.1 Όλων των επιχειρησιακών μονάδων, τμημάτων, θυγατρικών και υποκαταστημάτων

2.1.2 Εργαζομένων, αναδόχων, προσωρινού προσωπικού, συμβούλων και τρίτων παρόχων υπηρεσιών

2.1.3 Όλων των δεδομένων, πληροφοριακών συστημάτων, εφαρμογών, υποδομών και διαύλων επικοινωνίας

2.1.4 Όλων των φυσικών, νεφοϋπολογιστικών, απομακρυσμένων και υβριδικών περιβαλλόντων στα οποία γίνεται επεξεργασία ή παρέχεται πρόσβαση σε εταιρικά δεδομένα

2.2 Η πολιτική είναι δεσμευτική για όλες τις οντότητες που χειρίζονται πληροφορίες του οργανισμού και εφαρμόζεται σε όλα τα στάδια του κύκλου ζωής της πληροφορίας, από τη δημιουργία και τη διαβίβαση έως την αποθήκευση και την απόρριψη.

2.3 Τυχόν εξαιρέσεις ή περιορισμοί από το παρόν πεδίο εφαρμογής πρέπει να τεκμηριώνονται στη Δήλωση Πεδίου Εφαρμογής του ISMS και να αιτιολογούνται με επίσημη έγκριση από την εκτελεστική διοίκηση.

3. Στόχοι

3.1 Η θέσπιση ενός ISMS που είναι ευθυγραμμισμένο με το ISO/IEC 27001:2022 και ικανό να υποστηρίζει τη λήψη αποφάσεων βάσει κινδύνου σε όλο τον οργανισμό.

3.2 Η διασφάλιση ότι οι αρχές της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας ενσωματώνονται σε όλες τις δραστηριότητες, τα συστήματα και τις συνεργασίες του οργανισμού.

3.3 Η υποστήριξη της κανονιστικής και συμβατικής συμμόρφωσης μέσω του καθορισμού μετρήσιμων στόχων ασφάλειας που απορρέουν από την πολιτική και της ενσωμάτωσής τους στις επιχειρησιακές λειτουργίες.

3.4 Η ελαχιστοποίηση της πιθανότητας εκδήλωσης και του αντικτύπου περιστατικών ασφάλειας πληροφοριών μέσω αποτελεσματικών προληπτικών, ανιχνευτικών και διορθωτικών ελέγχων.

3.5 Η προώθηση της συνεχούς βελτίωσης του επιπέδου ωριμότητας της ασφάλειας πληροφοριών μέσω καθορισμένων δεικτών απόδοσης, αποτελεσμάτων ελέγχων και ανασκοπήσεων της διοίκησης.

3.6 Η καλλιέργεια κουλτούρας λογοδοσίας, επίγνωσης και ανθεκτικότητας, στην οποία οι ευθύνες ασφάλειας γίνονται κατανοητές και ασκούνται από όλο το προσωπικό.

4. Ρόλοι και αρμοδιότητες

4.1 Εκτελεστική Διοίκηση

4.1.1 Εγκρίνει και επικυρώνει την Πολιτική Ασφάλειας Πληροφοριών και το πλαίσιο του ISMS.

4.1.2 Διασφαλίζει την ευθυγράμμιση μεταξύ των στόχων ασφάλειας και της επιχειρησιακής στρατηγικής.

4.1.3 Δείχνει έμπρακτα τη δέσμευσή της και προάγει ισχυρή κουλτούρα ασφάλειας πληροφοριών.

4.1.4 Ανασκοπεί και εγκρίνει σημαντικές αλλαγές στο πεδίο εφαρμογής του ISMS, στην αντιμετώπιση κινδύνων και στη δομή διακυβέρνησης.

4.2 Επικεφαλής Ασφάλειας Πληροφοριών (CISO) / Υπεύθυνος ISMS

4.2.1 Έχει τη συνολική ευθύνη για το ISMS και διασφαλίζει ότι η παρούσα πολιτική παραμένει σε συμμόρφωση με το ISO/IEC 27001.

4.2.2 Ηγείται της εκτίμησης κινδύνων, της εφαρμογής ελέγχων και των διεργασιών συνεχούς βελτίωσης.

4.2.3 Διασφαλίζει τον διαλειτουργικό συντονισμό των δράσεων ασφάλειας και ασκεί εποπτεία στις επιμέρους πολιτικές.

4.2.4 Αναφέρει στην εκτελεστική διοίκηση την κατάσταση του ISMS, τα περιστατικά, τα αποτελέσματα ελέγχων και τις μετρήσεις.

4.2.5 Διασφαλίζει ότι οι ανασκοπήσεις και οι επικαιροποιήσεις της πολιτικής πραγματοποιούνται σύμφωνα με την Ενότητα 9 του παρόντος εγγράφου.

[... 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 Συχνότητα ανασκόπησης

9.1.1 Η παρούσα πολιτική πρέπει να ανασκοπείται τουλάχιστον ετησίως ή όταν συντρέχει οποιοδήποτε από τα ακόλουθα γεγονότα ενεργοποίησης:

9.1.1.1 Σημαντικές αλλαγές σε νομικές, κανονιστικές ή συμβατικές υποχρεώσεις

9.1.1.2 Ουσιώδεις μεταβολές στο προφίλ κινδύνου του οργανισμού

9.1.1.3 Αποτελέσματα από εσωτερικούς ή εξωτερικούς ελέγχους

9.1.1.4 Σημαντικά περιστατικά ή αστοχίες ελέγχων

9.2 Αρμόδια αρχή και διαδικασία ανασκόπησης

9.2.1 Ο CISO ή ο ορισμένος Υπεύθυνος ISMS πρέπει να ηγείται της διαδικασίας ανασκόπησης.

9.2.2 Οι εισροές της ανασκόπησης πρέπει να περιλαμβάνουν:

9.2.2.1 Αποτελέσματα εσωτερικού ελέγχου

9.2.2.2 Τάσεις εκτίμησης κινδύνων

9.2.2.3 Αλλαγές σε επιχειρησιακές διεργασίες και τεχνολογία

9.2.2.4 Απόδοση έναντι δεικτών KPI και ορίων κινδύνου

9.2.3 Όλες οι επικαιροποιήσεις πρέπει:

9.2.3.1 Να υπόκεινται σε έλεγχο εκδόσεων και να τεκμηριώνονται

9.2.3.2 Να εγκρίνονται από την Εκτελεστική Διοίκηση

9.2.3.3 Να κοινοποιούνται σε όλα τα επηρεαζόμενα μέρη μέσω επίσημων διαύλων επικοινωνίας

9.2.3.4 Να ενεργοποιούν τις αναγκαίες επικαιροποιήσεις της επιμέρους τεκμηρίωσης και της εκπαίδευσης

10. Σχετικές πολιτικές και διασυνδέσεις

10.1 Η παρούσα θεμελιώδης πολιτική συνδέεται άμεσα με τις ακόλουθες οργανωτικές πολιτικές και τα αντίστοιχα πλαίσια ασφάλειας:

10.1.1 P2 – Πολιτική Ρόλων και Αρμοδιοτήτων Διακυβέρνησης: Καθορίζει τη δομή διακυβέρνησης και την ιεραρχία αρμοδιοτήτων στην οποία παραπέμπει το παρόν έγγραφο.

10.1.2 P3 – Πολιτική Αποδεκτής Χρήσης: Καθορίζει τη συμμόρφωση ως προς τη συμπεριφορά και τον αποδεκτό χειρισμό των πληροφοριακών περιουσιακών στοιχείων.

10.1.3 P4 – Πολιτική Ελέγχου Πρόσβασης: Εξειδικεύει στην πράξη τους ελέγχους πρόσβασης που απορρέουν από την παρούσα υπερκείμενη πολιτική.

10.1.4 P6 – Πολιτική Διαχείρισης Κινδύνων: Παρέχει το πλαίσιο βάσει κινδύνου για την επιλογή ελέγχων και την αποδοχή υπολειπόμενων κινδύνων.

10.1.5 P33 – Πολιτική Ελέγχου και Παρακολούθησης Συμμόρφωσης: Περιγράφει τον τρόπο με τον οποίο οι εσωτερικοί μηχανισμοί διασφάλισης επικυρώνουν την εφαρμογή της πολιτικής.

10.2 Οι εν λόγω αλληλεξαρτήσεις διασφαλίζουν ολοκληρωμένη ευθυγράμμιση και ιχνηλασιμότητα σε όλο το ISMS και υποστηρίζουν ενιαία διακυβέρνηση κινδύνων και συμμόρφωσης.

11. Πρότυπα και πλαίσια αναφοράς

11.1 Η παρούσα Πολιτική Ασφάλειας Πληροφοριών είναι επίσημα ευθυγραμμισμένη με τα ακόλουθα πρότυπα και πλαίσια, ώστε να διασφαλίζεται πλήρης συμμόρφωση, ετοιμότητα για έλεγχο και δυνατότητα τεκμηρίωσης έναντι κανονιστικών απαιτήσεων:

11.2 ISO/IEC 27001

11.2.1 Ρήτρα 5.1 – Ηγεσία και Δέσμευση: Η παρούσα πολιτική αποδεικνύει τη δέσμευση της ανώτατης διοίκησης για την ασφάλεια πληροφοριών και καθορίζει αρμοδιότητες και κατανομή πόρων για το ISMS.

11.2.2 Ρήτρα 5.2 – Πολιτική Ασφάλειας Πληροφοριών: Το παρόν έγγραφο αποτελεί την επίσημη πολιτική ασφάλειας του οργανισμού, ευθυγραμμισμένη με τους δηλωμένους στόχους ασφάλειας, την επιχειρησιακή στρατηγική και τη συμμόρφωση με το ISO/IEC 27001.

11.2.3 Ρήτρα 6.1 – Ενέργειες για την αντιμετώπιση κινδύνων και ευκαιριών: Η προσέγγιση βάσει κινδύνου που αποτυπώνεται στην παρούσα πολιτική διασφαλίζει ότι οι πόροι ασφάλειας εφαρμόζονται αναλογικά προς τις απειλές.

11.2.4 Ρήτρα 9.2 – Εσωτερικός Έλεγχος και Ρήτρα 10 – Βελτίωση: Η παρούσα πολιτική ενσωματώνεται στον κύκλο συνεχούς βελτίωσης του οργανισμού και υπόκειται σε επικύρωση μέσω εσωτερικού ελέγχου.

11.2.5 ISO/IEC 27002:2022 – Έλεγχος 5.1: Παρέχει κατευθύνσεις για τη θέσπιση και τη διατήρηση πολιτικών ασφάλειας. Η παρούσα πολιτική αντανακλά τις συστάσεις του ISO 27002 ως προς την ιεραρχική τεκμηρίωση, τους κύκλους ανασκόπησης και τη δεσμευτική εφαρμογή.

11.3 NIST SP 800-53 Rev.5

11.3.1 PL-1 (Πολιτική και Διαδικασίες Σχεδιασμού Ασφάλειας): Η παρούσα πολιτική καλύπτει την απαίτηση για ανάπτυξη, κοινοποίηση και ανασκόπηση επίσημης πολιτικής ασφάλειας πληροφοριών σε επίπεδο οργανισμού.

11.3.2 PM-1 έως PM-5: Καλύπτει τη διακυβέρνηση σε επίπεδο προγράμματος, συμπεριλαμβανομένων των ρόλων ασφάλειας πληροφοριών, της κατανομής πόρων, της στρατηγικής κινδύνου και της ενσωμάτωσης του σχεδιασμού ασφάλειας στις επιχειρησιακές λειτουργίες.

11.4 ΓΚΠΔ της ΕΕ (2016/679)

11.4.1 Άρθρο 5(2): Ενισχύει την αρχή της λογοδοσίας. Η παρούσα πολιτική καθορίζει υπεύθυνα μέρη και ιχνηλάσιμες ενέργειες εφαρμογής.

11.4.2 Άρθρο 24: Απαιτεί την εφαρμογή τεχνικών και οργανωτικών μέτρων, συμπεριλαμβανομένων πολιτικών ευθυγραμμισμένων με τον κίνδυνο.

11.4.3 Άρθρο 32: Υποστηρίζει την εφαρμογή κατάλληλων μέτρων για τη διασφάλιση της ασφάλειας των δεδομένων προσωπικού χαρακτήρα καθ' όλο τον κύκλο ζωής τους.

11.5 Οδηγία NIS2 της ΕΕ (2022/2555)

11.5.1 Άρθρο 21(2)(a): Υποχρεώνει τις οντότητες να εφαρμόζουν τεκμηριωμένη πολιτική ασφάλειας που καλύπτει τη διαχείριση κινδύνων και τη διακυβέρνηση. Η παρούσα πολιτική καλύπτει την απαίτηση αυτή και υποστηρίζει ευρύτερα την ετοιμότητα κυβερνοασφάλειας και την προστασία κρίσιμων υποδομών.

11.6 Κανονισμός DORA της ΕΕ (2022/2554)

11.6.1 Άρθρο 5(2): Απαιτεί τεκμηριωμένο πλαίσιο εσωτερικών ελέγχων για τη διαχείριση κινδύνων ΤΠΕ. Η παρούσα πολιτική υποστηρίζει τη συμμόρφωση του χρηματοοικονομικού τομέα μέσω της ανάθεσης ρόλων, ελέγχων και λειτουργιών εποπτείας που ευθυγραμμίζονται με τις απαιτήσεις διακυβέρνησης του DORA.

11.7 COBIT 2019

11.7.1 EDM01 – Θέσπιση Πλαισίου Διακυβέρνησης: Η παρούσα πολιτική υποστηρίζει την εταιρική διακυβέρνηση με τον καθορισμό ρόλων ISMS, δεσμεύσεων της ηγεσίας και στρατηγικών στόχων.

11.7.2 APO01 – Πλαίσιο Διοίκησης: Υποστηρίζει τη θέσπιση και λειτουργία ενός δομημένου ISMS.

11.7.3 APO12 – Διαχείριση Κινδύνων: Παρέχει τη βάση για τη διακυβέρνηση κινδύνων ασφάλειας πληροφοριών.

11.7.4 MEA01/MEA03 – Παρακολούθηση, Αξιολόγηση και Αποτίμηση: Ενισχύει τη συνεχή αξιολόγηση της απόδοσης και την παρακολούθηση εσωτερικών ελέγχων μέσω της εφαρμογής της συμμόρφωσης με την πολιτική.