					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P06S					Τίτλος εγγράφου: **Πολιτική Διαχείρισης Κινδύνων**							
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 κανονισμούς

Πρότυπο/Κανονισμός	Ρήτρα/Άρθρο	Σχόλιο
ISO/IEC 27001:2022	Ρήτρες 6.1, 6.1.3	
ISO/IEC 27002:2022	5.4, 5.25	
NIST SP 800-53 Rev. 5	RA-1 έως RA-7, PM-9	
Οδηγία NIS2 της ΕΕ	Άρθρο 21(2)(a–d)	
Κανονισμός DORA της ΕΕ	Άρθρο 5	
COBIT 2019	APO12, MEA01 Παρακολούθηση, Αξιολόγηση και Εκτίμηση	

1. Σκοπός

1.1 Η παρούσα πολιτική καθορίζει τον τρόπο με τον οποίο ο οργανισμός εντοπίζει, αξιολογεί και διαχειρίζεται κινδύνους που σχετίζονται με την ασφάλεια πληροφοριών, τις λειτουργίες, την τεχνολογία και τις υπηρεσίες τρίτων.

1.2 Διασφαλίζει ότι η διαχείριση κινδύνων αποτελεί ενεργό μέρος του σχεδιασμού, της υλοποίησης έργων, της επιλογής προμηθευτών και της απόκρισης σε περιστατικά, σε ευθυγράμμιση με το ISO 27001, το ISO 31000 και τις κανονιστικές υποχρεώσεις.

1.3 Η πολιτική υποστηρίζει τη λήψη τεκμηριωμένων αποφάσεων, την προστασία των πληροφοριακών περιουσιακών στοιχείων και την ανθεκτικότητα των κρίσιμων επιχειρησιακών λειτουργιών.

2. Πεδίο εφαρμογής

2.1 Η παρούσα πολιτική εφαρμόζεται σε:

2.1.1 Όλα τα τμήματα, τα συστήματα και τους χρήστες εντός του οργανισμού

2.1.2 Όλες τις πληροφορίες, τις υπηρεσίες και τα περιουσιακά στοιχεία που διαχειρίζονται εσωτερικά ή μέσω τρίτων

2.1.3 Όλες τις δραστηριότητες που σχετίζονται με κινδύνους, συμπεριλαμβανομένων των ανασκοπήσεων έργων, των αναβαθμίσεων συστημάτων, της εξωτερικής ανάθεσης και της κανονιστικής συμμόρφωσης

2.2 Περιλαμβάνει όλους τους τύπους κινδύνων, όπως:

2.2.1 Απειλές κυβερνοασφάλειας και ευπάθειες συστημάτων

2.2.2 Λειτουργικές διαταραχές και διακοπές υπηρεσιών

2.2.3 Νομική, κανονιστική ή σχετιζόμενη με τη φήμη έκθεση σε κίνδυνο

2.2.4 Κινδύνους τρίτων και της εφοδιαστικής αλυσίδας

2.3 Όλοι οι εργαζόμενοι, οι ανάδοχοι και οι πάροχοι υπηρεσιών οφείλουν να τηρούν την παρούσα πολιτική κατά τον εντοπισμό ή την αναφορά κινδύνων.

3. Στόχοι

3.1 Ενσωμάτωση απλών και επαναλαμβανόμενων διαδικασιών αξιολόγησης κινδύνου στις συνήθεις επιχειρησιακές λειτουργίες.

3.2 Αναγνώριση και ιεράρχηση κινδύνων που θα μπορούσαν να επηρεάσουν την εμπιστευτικότητα, την ακεραιότητα, τη διαθεσιμότητα ή τη νομική συμμόρφωση.

3.3 Ανάθεση ιδιοκτησίας και καθορισμός ενεργειών αντιμετώπισης για όλους τους σημαντικούς κινδύνους.

3.4 Διατήρηση ακριβούς και επικαιροποιημένου Μητρώου Κινδύνων προς υποστήριξη της ετοιμότητας για έλεγχο και της παρακολούθησης κινδύνων.

3.5 Διασφάλιση της συμμετοχής της διοίκησης στην έγκριση της ανοχής κινδύνου και των σημαντικών σχεδίων αντιμετώπισης κινδύνων.

4. Ρόλοι και αρμοδιότητες

4.1 Γενικός Διευθυντής

4.1.1 Καθορίζει τη διάθεση ανάληψης κινδύνου του οργανισμού και εγκρίνει το πλαίσιο διαχείρισης κινδύνων.

4.1.2 Εγκρίνει σημαντικές αποφάσεις διαχείρισης κινδύνων και τους σχετικούς πόρους.

4.1.3 Ανασκοπεί τους κυριότερους κινδύνους σε τριμηνιαία βάση με τον Συντονιστή Κινδύνων.

4.2 Συντονιστής Κινδύνων (ή Ιδιοκτήτης ISMS)

4.2.1 Διευκολύνει τις αξιολογήσεις κινδύνου και τηρεί το Μητρώο Κινδύνων.

4.2.2 Διασφαλίζει ότι η βαθμολόγηση κινδύνου, η ιδιοκτησία κινδύνου και οι ενέργειες αντιμετώπισης τεκμηριώνονται.

4.2.3 Οργανώνει τουλάχιστον μία επίσημη ανασκόπηση κινδύνων ετησίως.

[... 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

9.1.1 Η παρούσα πολιτική πρέπει να ανασκοπείται τουλάχιστον μία φορά ετησίως από τον Γενικό Διευθυντή και τον Συντονιστή Κινδύνων, ώστε να διασφαλίζεται η συνάφεια και η πληρότητά της.

9.2 Μηχανισμοί ενεργοποίησης επικαιροποίησης

9.2.1 Πρέπει να διενεργείται έκτακτη ανασκόπηση και επικαιροποίηση εάν:

9.2.1.1 Σημαντικό περιστατικό ή εύρημα ελέγχου αναδείξει κενά στη διαχείριση κινδύνων

9.2.1.2 Εισαχθούν νέες επιχειρησιακές μονάδες, τεχνολογίες ή συνεργασίες

9.2.1.3 Μεταβληθεί κανονιστική ή συμβατική απαίτηση

9.3 Έλεγχος εκδόσεων

9.3.1 Όλες οι επικαιροποιήσεις της παρούσας πολιτικής πρέπει να υπόκεινται σε έλεγχο εκδόσεων με τα ακόλουθα μεταδεδομένα:

9.3.1.1 Αριθμό έκδοσης και ημερομηνία έναρξης ισχύος

9.3.1.2 Σύνοψη αλλαγών

9.3.1.3 Εγκρίνων (Γενικός Διευθυντής)

9.3.1.4 Αρχειοθετημένες προηγούμενες εκδόσεις για σκοπούς ελέγχου

9.4 Επικοινωνία και ευαισθητοποίηση

9.4.1 Οι επικαιροποιημένες εκδόσεις της πολιτικής και τα σημαντικά σχέδια αντιμετώπισης κινδύνων πρέπει να κοινοποιούνται στο επηρεαζόμενο προσωπικό. Η ετήσια επαναληπτική εκπαίδευση πρέπει να περιλαμβάνει βασικές αρχές ευαισθητοποίησης ως προς τους κινδύνους.

10. Σχετικές πολιτικές και διασυνδέσεις

10.1 Η παρούσα πολιτική λειτουργεί σε συντονισμό με άλλες πολιτικές, ώστε να διασφαλίζεται ολοκληρωμένη διακυβέρνηση ασφάλειας:

10.1.1 P2S – Πολιτική ρόλων και αρμοδιοτήτων διακυβέρνησης: Καθορίζει ποιος λογοδοτεί για την ιδιοκτησία κινδύνου και τη λήψη αποφάσεων.

10.1.2 P5S – Πολιτική Διαχείρισης Αλλαγών: Απαιτεί αξιολόγηση κινδύνου πριν από την εφαρμογή τεχνικών ή διαδικαστικών αλλαγών.

10.1.3 P17S – Πολιτική προστασίας δεδομένων και ιδιωτικότητας: Αντιμετωπίζει τον κανονιστικό κίνδυνο που συνδέεται με τον χειρισμό δεδομένων προσωπικού χαρακτήρα.

10.1.4 P30S – Πολιτική αντιμετώπισης περιστατικών: Διασφαλίζει ότι η διαχείριση κινδύνων συνεχίζεται κατά τη διάρκεια και μετά από περιστατικά ασφάλειας.

10.1.5 P33S – Πολιτική επιχειρησιακής συνέχειας: Προσδιορίζει υπολειπόμενους κινδύνους και μέτρα ανάκαμψης για κρίσιμες υπηρεσίες.

11. Πρότυπα και πλαίσια αναφοράς

11.1 ISO/IEC 27001:

11.1.1 Η Ρήτρα 6.1 καθιερώνει επίσημη διαδικασία διαχείρισης κινδύνων και σχεδιασμό αντιμετώπισης κινδύνων.

11.1.2 Η Ρήτρα 6.1.3 απαιτεί από τους οργανισμούς να διατηρούν τεκμηριωμένα σχέδια αντιμετώπισης και εγκρίσεις.

11.2 ISO/IEC 27002:

11.2.1 Οι έλεγχοι 5.4 και 5.25 παρέχουν οδηγίες εφαρμογής για την ιδιοκτησία κινδύνου, την ιεράρχηση και τη διαχείριση του κύκλου ζωής.

11.3 NIST SP 800-53 Rev. 5:

11.3.1 Τα RA-1 έως RA-7 καθορίζουν την αξιολόγηση κινδύνου, τις στρατηγικές απόκρισης, την τεκμηρίωση και τους μηχανισμούς ανασκόπησης.

11.4 PM-9

11.4.1 Απαιτεί συνεπή εποπτεία σε επίπεδο διοίκησης για τους κινδύνους του οργανισμού.

11.5 Οδηγία NIS2 της ΕΕ

11.5.1 Το Άρθρο 21(2)(a–d) επιβάλλει υποχρεωτικούς ελέγχους αξιολόγησης κινδύνου, μετριασμού και διακυβέρνησης σε ουσιώδεις και σημαντικές οντότητες.

11.6 Κανονισμός DORA της ΕΕ

11.6.1 Το Άρθρο 5 απαιτεί από τις εποπτευόμενες οντότητες να ορίζουν και να διαχειρίζονται πλαίσια διαχείρισης κινδύνου ΤΠΕ, συμπεριλαμβανομένων του εντοπισμού, της ταξινόμησης και της απόκρισης.

11.7 COBIT 2019

11.7.1 APO12 – Διαχείριση κινδύνων: Ενσωματώνει τον κίνδυνο στον στρατηγικό και επιχειρησιακό σχεδιασμό.

11.7.2 MEA01 – Παρακολούθηση, Αξιολόγηση και Εκτίμηση: Διασφαλίζει την αποτελεσματικότητα και τη συμμόρφωση των διαδικασιών και ενεργειών διαχείρισης κινδύνων.