					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P06					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, 8.32, 10	Βασικός πυρήνας για την αναγνώριση και διαχείριση κινδύνων, ενσωμάτωση στη διαχείριση αλλαγών, συνεχής βελτίωση
ISO/IEC 27005:2024	Πλήρης μεθοδολογία κύκλου ζωής κινδύνου	Πλήρης διαδικασία διαχείρισης κινδύνων σε ευθυγράμμιση με το πρότυπο
ISO 31000:2018	Αρχές και πλαίσιο διαχείρισης κινδύνων	Αρχές διαχείρισης κινδύνων που έχουν υιοθετηθεί στο πλαίσιο
NIST SP 800-30 Rev.1	SP 800-30, SP 800-39	Καθοδήγηση και δομή για αξιολογήσεις κινδύνου, πολυεπίπεδη διακυβέρνηση κινδύνων
ΓΚΠΔ της ΕΕ	Άρθρα 24, 25, 32	Διαδικασίες και έλεγχοι κινδύνου για την προστασία δεδομένων
Οδηγία NIS2 της ΕΕ	Άρθρο 21(2)(a–d)	Υποχρεώσεις αξιολόγησης κινδύνου και ασφάλειας
Κανονισμός DORA της ΕΕ	Άρθρα 5, 6	Διαχείριση κινδύνων ΤΠΕ και επιχειρησιακή ανθεκτικότητα
COBIT 2019	APO12, MEA	Δομή διαχείρισης κινδύνων και εποπτεία

1. Σκοπός

1.1 Η παρούσα πολιτική θεσπίζει ένα ενιαίο και τυποποιημένο πλαίσιο για την αναγνώριση, ανάλυση, αξιολόγηση, αντιμετώπιση, παρακολούθηση και ανασκόπηση κινδύνων ασφάλειας πληροφοριών σε όλο τον οργανισμό.

1.2 Διασφαλίζει τη συνεπή εφαρμογή αρχών βάσει κινδύνου για την προστασία της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητας των πληροφοριακών περιουσιακών στοιχείων, σε ευθυγράμμιση με τη Ρήτρα 6.1 του ISO/IEC 27001:2022 και το ISO 31000:2018.

1.3 Η πολιτική ενσωματώνει τη διαχείριση κινδύνων ασφάλειας πληροφοριών στις διαδικασίες λήψης αποφάσεων του οργανισμού, ώστε να ικανοποιούνται οι εσωτερικοί στρατηγικοί στόχοι και οι εξωτερικές κανονιστικές απαιτήσεις.

2. Πεδίο εφαρμογής

2.1 Η παρούσα πολιτική εφαρμόζεται σε όλες τις οργανωτικές μονάδες, τις επιχειρησιακές διεργασίες, τα συστήματα, το προσωπικό και τις συνεργασίες με τρίτα μέρη που εμπλέκονται στον χειρισμό, την ανάπτυξη, την αποθήκευση ή τη διαχείριση πληροφοριακών περιουσιακών στοιχείων.

2.2 Το πεδίο εφαρμογής εκτείνεται σε φυσικά, ψηφιακά και φιλοξενούμενα σε περιβάλλον νέφους στοιχεία, συμπεριλαμβανομένων δομημένων και αδόμητων δεδομένων, εφαρμογών, υποδομών, δικτύων και υπηρεσιών.

2.3 Καλύπτει κινδύνους ασφάλειας πληροφοριών σε στρατηγικό, επιχειρησιακό, τεχνικό επίπεδο και σε επίπεδο έργου και είναι υποχρεωτική για όλους τους εργαζομένους, τους αναδόχους και τους παρόχους υπηρεσιών που συμμετέχουν σε δραστηριότητες του ΣΔΑΠ.

2.4 Η διαχείριση κινδύνων πρέπει να εφαρμόζεται στα ακόλουθα σενάρια:

2.4.1 Υλοποίηση νέου έργου ή συστήματος

2.4.1.1 Σημαντικές αλλαγές (π.χ. αρχιτεκτονική, ιδιοκτησία, διεργασίες)

2.4.1.2 Ένταξη προμηθευτή και συμφωνίες με τρίτα μέρη

2.4.1.3 Απόκριση σε περιστατικά και ανασκοπήσεις μετά το περιστατικό

2.4.1.4 Περιοδικές οργανωτικές ανασκοπήσεις κινδύνων ή έλεγχοι

3. Στόχοι

3.1 Να θεσπιστεί και να εφαρμόζεται στην πράξη μια επαναλήψιμη, ενιαία σε όλο τον οργανισμό διαδικασία διαχείρισης κινδύνων, βασισμένη στις μεθοδολογίες ISO/IEC 27005 και ISO 31000.

3.2 Να διασφαλίζεται ότι οι κίνδυνοι αναγνωρίζονται, αναλύονται, αξιολογούνται και αντιμετωπίζονται με δομημένες και ιχνηλάσιμες μεθόδους, συμπεριλαμβανομένης της ανάθεσης ιδιοκτησίας κινδύνου και της σύνδεσης με ελέγχους.

3.3 Να τηρείται ένα κεντρικό Μητρώο Κινδύνων με έλεγχο εκδόσεων και ένα σχέδιο αντιμετώπισης κινδύνων, που αποτυπώνουν την τρέχουσα κατάσταση κινδύνου, την κάλυψη ελέγχων και την πρόοδο του μετριασμού.

3.4 Να ευθυγραμμίζονται οι αποφάσεις για τους κινδύνους με τεκμηριωμένα επίπεδα διάθεσης ανάληψης κινδύνου και ανοχής κινδύνου και να υποστηρίζονται τεκμηριωμένες αποφάσεις διακυβέρνησης σχετικά με την αποδοχή, τη μείωση, τη μεταφορά ή την αποφυγή κινδύνου.

3.5 Να παρακολουθούνται συνεχώς οι τάσεις κινδύνου και να διασφαλίζεται η αποτελεσματικότητα των δραστηριοτήτων αντιμετώπισης κινδύνων, με δυνατότητα έγκαιρων προσαρμογών βάσει της εξέλιξης του τοπίου απειλών ή επιχειρησιακών αλλαγών.

4. Ρόλοι και αρμοδιότητες

4.1 Εκτελεστική Διοίκηση / Διοικητικό Συμβούλιο

4.1.1 Εγκρίνει το πλαίσιο διαχείρισης κινδύνων και καθορίζει αποδεκτά επίπεδα διάθεσης ανάληψης κινδύνου και όρια ανοχής κινδύνου.

4.1.2 Εγκρίνει στρατηγικές διαχείρισης κινδύνων για υπολειπόμενους κινδύνους που υπερβαίνουν την ανοχή.

4.1.3 Διαθέτει πόρους και ασκεί εποπτεία για την αποτελεσματική λειτουργία του προγράμματος διαχείρισης κινδύνων.

4.2 Υπεύθυνος ΣΔΑΠ / Υπεύθυνος Διαχείρισης Κινδύνων

4.2.1 Έχει την ευθύνη της παρούσας πολιτικής και διασφαλίζει την ευθυγράμμισή της με τα πρότυπα ISO/IEC 27001 και ISO/IEC 27005.

4.2.2 Ηγείται της διαδικασίας αξιολόγησης κινδύνων σε επίπεδο οργανισμού και τηρεί το Μητρώο Κινδύνων και το σχέδιο αντιμετώπισης κινδύνων.

4.2.3 Διασφαλίζει τις περιοδικές ανασκοπήσεις και την κλιμάκωση βασικών κινδύνων προς την Εκτελεστική Διοίκηση ή την Επιτροπή Καθοδήγησης ΣΔΑΠ.

[... 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 Η παρούσα πολιτική και το σχετικό πλαίσιο πρέπει να ανασκοπούνται ετησίως ή:

9.1.1 Μετά από σημαντικό συμβάν κινδύνου ή περιστατικό ασφάλειας

9.1.2 Μετά από σημαντική οργανωτική ή τεχνική αλλαγή

9.1.3 Σε απόκριση σε ευρήματα ελέγχου ή νέες κανονιστικές απαιτήσεις

9.2 Ο Υπεύθυνος ΣΔΑΠ, ο Υπεύθυνος Διαχείρισης Κινδύνων και η ομάδα Συμμόρφωσης είναι από κοινού υπεύθυνοι για:

9.2.1 Την έναρξη του κύκλου ανασκόπησης

9.2.2 Τη συλλογή εισροών από τις επιχειρησιακές μονάδες

9.2.3 Την αναθεώρηση διαδικασιών και ορίων, όπου απαιτείται

9.3 Όλες οι αναθεωρήσεις πρέπει:

9.3.1 Να τελούν υπό έλεγχο εκδόσεων και να καταγράφονται

9.3.2 Να εγκρίνονται από την Εκτελεστική Διοίκηση

9.3.3 Να κοινοποιούνται στα ενδιαφερόμενα μέρη

9.3.4 Να τηρούνται στο ελεγκτικό αποθετήριο για ελάχιστο διάστημα 5 ετών

10. Σχετικές πολιτικές και διασυνδέσεις

10.1 Η παρούσα πολιτική έχει αλληλεξάρτηση με τις ακόλουθες πολιτικές ασφάλειας πληροφοριών:

10.1.1 P1 – Πολιτική Ασφάλειας Πληροφοριών: Καθορίζει το συνολικό μοντέλο διακυβέρνησης ασφάλειας στο πλαίσιο του οποίου εφαρμόζεται η παρούσα πολιτική κινδύνων.

10.1.2 P2 – Πολιτική ρόλων και αρμοδιοτήτων διακυβέρνησης: Καθορίζει τους υπόλογους ιδιοκτήτες και τα επίπεδα διακυβέρνησης στα οποία γίνεται αναφορά στη μήτρα κλιμάκωσης κινδύνων.

10.1.3 P5 – P05 Πολιτική Διαχείρισης Αλλαγών: Ενεργοποιεί επαναξιολόγηση κινδύνου για αλλαγές στην υποδομή και στον οργανισμό.

10.1.4 P13 – Πολιτική ταξινόμησης και επισήμανσης δεδομένων: Υποστηρίζει την εκτίμηση επιπτώσεων κατά την αναγνώριση κινδύνων.

10.1.5 P33 – Πολιτική ελέγχου και παρακολούθησης συμμόρφωσης: Επικυρώνει την τήρηση της πολιτικής, συμπεριλαμβανομένης της πληρότητας του Μητρώου Κινδύνων και των τεκμηρίων αντιμετώπισης κινδύνων.

11. Πρότυπα και πλαίσια αναφοράς

11.1 Η παρούσα πολιτική ευθυγραμμίζεται ρητά με τα ακόλουθα πρότυπα και πλαίσια, ώστε να διασφαλίζεται ότι καλύπτει τις διεθνείς βέλτιστες πρακτικές και τις κανονιστικές προσδοκίες για τη διαχείριση κινδύνων ασφάλειας πληροφοριών:

11.2 ISO/IEC 27001:

11.2.1 Ρήτρα 6.1: Καθορίζει τις απαιτήσεις για την αναγνώριση κινδύνων και ευκαιριών, συμπεριλαμβανομένου του πλήρους κύκλου ζωής των αξιολογήσεων και των ενεργειών αντιμετώπισης κινδύνων ασφάλειας πληροφοριών. Η παρούσα πολιτική θέτει σε επιχειρησιακή εφαρμογή τις Ρήτρες 6.1.2 και 6.1 μέσω ενός δομημένου πλαισίου που επιβάλλει τεκμηριωμένα πρωτόκολλα αναγνώρισης, ανάλυσης, αξιολόγησης, αντιμετώπισης κινδύνων και αποδοχής υπολειπόμενου κινδύνου.

11.2.2 Ρήτρα 8.32: Η ενσωμάτωση σκέψης βάσει κινδύνου στις διαδικασίες διαχείρισης αλλαγών διασφαλίζει ότι όλες οι σημαντικές οργανωτικές αλλαγές ενεργοποιούν επίσημες επαναξιολογήσεις κινδύνου.

11.2.3 Ρήτρα 10: Η συνεχής βελτίωση ενσωματώνεται μέσω τακτικών ανασκοπήσεων της πολιτικής, ανάλυσης τάσεων κινδύνων και επικαιροποιήσεων της Δήλωσης Εφαρμοσιμότητας (SoA) βάσει στοιχείων κινδύνου.

11.3 ISO/IEC 27005:

11.3.1 Παρέχει εξειδικευμένη και λεπτομερή καθοδήγηση για τη διαχείριση κινδύνων ασφάλειας πληροφοριών. Η παρούσα πολιτική εφαρμόζει το πλήρες μοντέλο διαδικασίας κινδύνου του ISO/IEC 27005: καθορισμός πλαισίου, αναγνώριση κινδύνων, ανάλυση κινδύνων, αξιολόγηση κινδύνων, αντιμετώπιση κινδύνων, αποδοχή κινδύνου, επικοινωνία κινδύνου, παρακολούθηση κινδύνων και ανασκόπηση.

11.4 ISO 31000:

11.4.1 Η παρούσα πολιτική ενσωματώνει τις αρχές του ISO 31000, όπως η δέσμευση της ηγεσίας, η ενσωμάτωση στη λήψη αποφάσεων και η συνεχής βελτίωση. Διασφαλίζει ότι η διαχείριση κινδύνων ενσωματώνεται στην κουλτούρα και στη λειτουργία του οργανισμού.

11.5 NIST SP 800-30 Rev.1:

11.5.1 Ευθυγραμμίζεται με τον οδηγό του NIST για τη διενέργεια αξιολογήσεων κινδύνου, συμπεριλαμβανομένων της αναγνώρισης απειλών, της ανάλυσης ευπαθειών, της εκτίμησης πιθανότητας και του προσδιορισμού επιπτώσεων. Η δομή της παρούσας πολιτικής αντικατοπτρίζει τα καθορισμένα βήματα αξιολόγησης κινδύνου του NIST και τα προσαρμόζει τόσο σε τεχνικές όσο και σε επιχειρησιακές διεργασίες.

11.6 NIST SP 800-39:

11.6.1 Υποστηρίζει τη διακυβέρνηση κινδύνων σε επίπεδο οργανισμού, δίνοντας έμφαση στην πολυεπίπεδη διαχείριση κινδύνων σε επίπεδο οργανισμού, αποστολής/επιχειρησιακής διεργασίας και πληροφοριακού συστήματος. Η πολιτική διασφαλίζει ότι η ιδιοκτησία κινδύνου ορίζεται με σαφήνεια σε όλα τα επίπεδα και περιλαμβάνει στρατηγικές αντιμετώπισης κινδύνων σε επίπεδο οργανισμού.

11.7 ΓΚΠΔ της ΕΕ:

11.7.1 Άρθρο 24: Απαιτεί την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων ώστε οι κίνδυνοι προστασίας δεδομένων να διαχειρίζονται ορθά — απαίτηση που καλύπτεται μέσω της δομημένης διαδικασίας κινδύνου της παρούσας πολιτικής.

11.7.2 Άρθρο 25: Η «προστασία δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού» ευθυγραμμίζεται με την ενσωμάτωση της διαχείρισης κινδύνων στον σχεδιασμό συστημάτων και διεργασιών.

11.7.3 Άρθρο 32: Επιβάλλει προσέγγιση βάσει κινδύνου για τα μέτρα ασφάλειας — απαίτηση που ικανοποιείται μέσω αξιολογήσεων κινδύνου βάσει επιπτώσεων και επιλογής ελέγχων.

11.8 Οδηγία NIS2 της ΕΕ:

11.8.1 Άρθρο 21(2)(a–d): Απαιτεί από τους φορείς να διενεργούν αξιολογήσεις κινδύνου, να εφαρμόζουν πολιτικές για την ανάλυση κινδύνου και να διασφαλίζουν αναλογικά μέτρα ασφάλειας. Η παρούσα πολιτική καλύπτει τις υποχρεώσεις αυτές μέσω της συνεχούς εφαρμογής του κύκλου ζωής κινδύνου και της τεκμηριωμένης διακυβέρνησης.

11.9 Κανονισμός DORA της ΕΕ:

11.9.1 Άρθρο 5: Απαιτεί τεκμηριωμένο πλαίσιο διαχείρισης κινδύνων ΤΠΕ — απαίτηση που καλύπτεται πλήρως από την αρχιτεκτονική της παρούσας πολιτικής, συμπεριλαμβανομένης της αντιστοίχισης στη Δήλωση Εφαρμοσιμότητας (SoA) και των KRIs.

11.9.2 Άρθρο 6: Απαιτεί την ενσωμάτωση της διαχείρισης κινδύνων στις στρατηγικές επιχειρησιακής ανθεκτικότητας, κάτι που αντιμετωπίζεται μέσω μητρών κλιμάκωσης και παρακολούθησης κρίσιμων περιουσιακών στοιχείων.

11.10 COBIT 2019:

11.10.1 APO12 – Manage Risk: Αντιστοιχίζεται άμεσα με τη θέσπιση από τον οργανισμό μιας δομημένης προσέγγισης διαχείρισης κινδύνων, με ανάθεση ρόλων, παρακολούθηση ενεργειών αντιμετώπισης κινδύνων και διασφάλιση λογοδοσίας σε επίπεδο Διοικητικού Συμβουλίου.

11.10.2 MEA01 – Monitor, Evaluate and Assess Performance and Conformance: Αντικατοπτρίζεται στην έμφαση της παρούσας πολιτικής στην ανάλυση τάσεων, στην παρακολούθηση των KRIs και στην ενσωμάτωση ανατροφοδότησης από ελέγχους στους κύκλους συνεχούς βελτίωσης.