					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P13S					Τίτλος εγγράφου: **Πολιτική Ταξινόμησης και Επισήμανσης Δεδομένων**							
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**

Ευθυγραμμισμένη με πρότυπα και κανονιστικές απαιτήσεις

Πρότυπο/Κανονισμός	Ρήτρα/Άρθρο	Σχόλιο
ISO/IEC 27001:2022	Ρήτρες 5.3, 8	
ISO/IEC 27002:2022	Έλεγχοι 5.12, 5.13	
NIST SP 800-53 Rev.5	AC-16, MP-3, MP-5	
Οδηγία NIS2 της ΕΕ	Άρθρο 21(2)(a)	
Κανονισμός DORA της ΕΕ	Άρθρο 5(8)	
COBIT 2019	BAI03.05, DSS05	
ΓΚΠΔ της ΕΕ	Άρθρα 5, 32	

1. Σκοπός

1.1 Η παρούσα πολιτική καθορίζει τον τρόπο με τον οποίο όλες οι πληροφορίες που χειρίζεται ο οργανισμός πρέπει να ταξινομούνται και να επισημαίνονται, ώστε να διασφαλίζονται η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητά τους σε όλο τον κύκλο ζωής τους.

1.2 Αποσκοπεί στη συνεπή διαχείριση των δεδομένων μέσω της απόδοσης κατάλληλων επιπέδων προστασίας στις πληροφορίες, με βάση την ευαισθησία, τον επιχειρησιακό αντίκτυπο ή τις νομικές υποχρεώσεις.

1.3 Η ταξινόμηση και η επισήμανση συμβάλλουν στη μείωση του κινδύνου τυχαίας γνωστοποίησης, μη εξουσιοδοτημένης πρόσβασης ή ακατάλληλου χειρισμού ευαίσθητων δεδομένων, ιδίως σε ΜΜΕ που ενδέχεται να βασίζονται σε απλούστερα συστήματα και λιγότερο τυποποιημένους ελέγχους ασφάλειας.

1.4 Η παρούσα πολιτική είναι κρίσιμη για την πιστοποίηση κατά ISO/IEC 27001 και τη συμμόρφωση, ιδίως με νομοθετήματα προστασίας δεδομένων όπως ο ΓΚΠΔ της ΕΕ και πλαίσια κυβερνοασφάλειας όπως η Οδηγία NIS2 της ΕΕ και ο Κανονισμός DORA της ΕΕ.

2. Πεδίο εφαρμογής

2.1 Η παρούσα πολιτική εφαρμόζεται σε όλα τα δεδομένα του οργανισμού, ανεξαρτήτως μορφής ή τοποθεσίας, συμπεριλαμβανομένων των εξής:

2.1.1 Ηλεκτρονικά έγγραφα, υπολογιστικά φύλλα, μηνύματα ηλεκτρονικού ταχυδρομείου, φόρμες, εικόνες και σαρωμένα αρχεία

2.1.2 Φυσικά έγγραφα όπως έντυπα αρχεία, αναφορές, τιμολόγια και σημειώσεις

2.1.3 Δεδομένα που αποθηκεύονται ή υποβάλλονται σε επεξεργασία σε υπηρεσίες υπολογιστικού νέφους, σε τοπικούς διακομιστές, σε αφαιρούμενα μέσα ή σε προσωπικές συσκευές που χρησιμοποιούνται για επαγγελματικούς σκοπούς

2.1.4 Προσωρινά ή παροδικά δεδομένα που παράγονται κατά τις επιχειρησιακές λειτουργίες (π.χ. αρχεία καταγραφής, προσωρινή μνήμη cache, μηνύματα ηλεκτρονικού ταχυδρομείου)

2.2 Όλο το προσωπικό, οι ανάδοχοι, οι προσωρινοί εργαζόμενοι και οι εξωτερικοί πάροχοι με πρόσβαση στα δεδομένα του οργανισμού υποχρεούνται να συμμορφώνονται με την παρούσα πολιτική.

2.3 Η παρούσα πολιτική εφαρμόζεται σε όλο τον κύκλο ζωής των δεδομένων, από τη δημιουργία και την αποθήκευση έως την πρόσβαση και τη μεταφορά, και μέχρι την αρχειοθέτηση ή τη διαγραφή.

3. Στόχοι

3.1 Να καθιερωθεί ένα απλό και εφαρμόσιμο σχήμα ταξινόμησης, το οποίο μπορεί να γίνεται εύκολα κατανοητό και να εφαρμόζεται σε όλο τον οργανισμό.

3.2 Να απαιτείται κάθε στοιχείο δεδομένων να ταξινομείται σύμφωνα με την ευαισθησία του και να επισημαίνεται αναλόγως, ώστε να καθοδηγείται ο ορθός χειρισμός, η αποθήκευση και η πρόσβαση.

3.3 Να διασφαλίζεται ότι οι πρακτικές επισήμανσης δεδομένων ενσωματώνονται στις επιχειρησιακές ροές εργασίας, όπως κατά την ένταξη προσωπικού, την έναρξη έργων και την παραμετροποίηση συστημάτων.

3.4 Να μειώνεται ο κίνδυνος παραβίασης δεδομένων μέσω της εφαρμογής ελέγχων χειρισμού (π.χ. κρυπτογράφηση, περιορισμός πρόσβασης) ανάλογα με το επίπεδο ταξινόμησης.

3.5 Να διασφαλίζεται η συμμόρφωση με τη νομοθεσία περί ιδιωτικότητας και ασφάλειας πληροφοριών, αποδεικνύοντας ότι τα ευαίσθητα δεδομένα (π.χ. προσωπικά, οικονομικά ή ιδιόκτητα) επισημαίνονται και διαχειρίζονται ορθά.

3.6 Να θεσπιστεί λογοδοσία για τις αποφάσεις ταξινόμησης και να διασφαλίζονται περιοδικές ανασκοπήσεις και επικαιροποιήσεις με βάση τις εξελισσόμενες επιχειρησιακές και νομικές ανάγκες.

4. Ρόλοι και αρμοδιότητες

4.1 Γενικός Διευθυντής (GM)

4.1.1 Έχει τη συνολική ευθύνη για την παρούσα πολιτική και εγκρίνει το σχήμα ταξινόμησης.

4.1.2 Παρέχει εποπτεία ώστε οι αρμοδιότητες ταξινόμησης να ανατίθενται και να ασκούνται.

4.1.3 Ανασκοπεί και εγκρίνει τυχόν εξαιρέσεις από τις απαιτήσεις ταξινόμησης ή επισήμανσης.

4.1.4 Διασφαλίζει ότι οι πρακτικές διαχείρισης δεδομένων πληρούν τις απαιτήσεις συμμόρφωσης βάσει νομοθετημάτων όπως ο ΓΚΠΔ της ΕΕ και ο Κανονισμός DORA της ΕΕ.

4.2 Ιδιοκτήτης Πληροφοριών / Υπεύθυνος Δεδομένων

4.2.1 Αποδίδει αρχική ταξινόμηση σε κάθε νέο σύνολο δεδομένων ή πληροφοριακό περιουσιακό στοιχείο κατά τη δημιουργία ή την απόκτησή του.

4.2.2 Διασφαλίζει ότι εφαρμόζονται, όπου είναι εφικτό, ευδιάκριτες επισημάνσεις (π.χ. κεφαλίδες αρχείων, υποσέλιδα, υδατογραφήματα, ονομασίες φακέλων).

4.2.3 Ανασκοπεί περιοδικά τις ταξινομήσεις, ώστε να επαληθεύεται η συνάφεια, η ακρίβεια και τυχόν απαιτούμενες αλλαγές (π.χ. μετά από αποχαρακτηρισμό ή δημοσίευση).

4.2.4 Συνεργάζεται με τον Υπεύθυνο Πληροφορικής για την εφαρμογή τεχνικών μέτρων προστασίας βάσει της ταξινόμησης (π.χ. δικαιώματα πρόσβασης, κρυπτογράφηση).

[... 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 πρέπει να ανασκοπείται ετησίως από τον GM και τον Υπεύθυνο Δεδομένων, ώστε να διασφαλίζεται ότι αντανακλά:

9.1.1 Αλλαγές στις επιχειρησιακές λειτουργίες ή στους τύπους δεδομένων

9.1.2 Νέες κανονιστικές απαιτήσεις (π.χ. ιδιωτικότητα δεδομένων ή χρηματοοικονομική εποπτεία)

9.1.3 Τεχνολογικές μεταβολές που επηρεάζουν τις δυνατότητες επισήμανσης ή ταξινόμησης

9.2 Η ανασκόπηση πρέπει να περιλαμβάνει επικαιροποιήσεις στις κατηγορίες ταξινόμησης, στα εργαλεία ή στις πρακτικές επισήμανσης, καθώς και στο περιεχόμενο ευαισθητοποίησης και εκπαίδευσης.

9.3 Οι αναθεωρήσεις της πολιτικής πρέπει να εγκρίνονται από τον GM και να γνωστοποιούνται σε όλο το προσωπικό. Πρέπει να τηρείται αρχείο μεταβολών έκδοσης για σκοπούς ελέγχου.

10. Συναφείς πολιτικές και διασυνδέσεις

10.1 P2S – Πολιτική Ρόλων και Αρμοδιοτήτων Διακυβέρνησης: Αναθέτει λογοδοσία για την κυριότητα και την εφαρμογή της πολιτικής.

10.2 P4S – Πολιτική Ελέγχου Πρόσβασης: Ευθυγραμμίζει την πρόσβαση στα συστήματα με τα επίπεδα ταξινόμησης δεδομένων.

10.3 P12S – Πολιτική Διαχείρισης Περιουσιακών Στοιχείων: Παρακολουθεί τα φυσικά και ψηφιακά περιουσιακά στοιχεία που αποθηκεύουν ταξινομημένα δεδομένα.

10.4 P17S – Πολιτική Προστασίας Δεδομένων και Ιδιωτικότητας: Διέπει την προστασία προσωπικών δεδομένων, μεγάλο μέρος των οποίων ταξινομείται ως Εμπιστευτικό.

10.5 P30S – Πολιτική Αντιμετώπισης Περιστατικών: Καθορίζει τις διαδρομές κλιμάκωσης και τις διαδικασίες απόκρισης σε περίπτωση παραβιάσεων ταξινόμησης ή έκθεσης δεδομένων.

11. Πρότυπα και πλαίσια αναφοράς

11.1 ISO/IEC 27001

11.1.1 Ρήτρα 5.3: Απαιτεί σαφώς καθορισμένες αρμοδιότητες για τη διαχείριση και την προστασία δεδομένων.

11.1.2 Ρήτρα 8.1: Επιβάλλει επιχειρησιακό σχεδιασμό και ελέγχους, συμπεριλαμβανομένων εκείνων που συνδέονται με την κατηγοριοποίηση δεδομένων.

11.2 ISO/IEC 27002

11.2.1 Έλεγχος 5.12: Παρέχει καθοδήγηση για την ταξινόμηση πληροφοριών βάσει κινδύνου και κανονιστικών απαιτήσεων.

11.2.2 Έλεγχος 5.13: Περιγράφει πρακτικούς μηχανισμούς επισήμανσης και τους σχετικούς κανόνες χειρισμού.

11.3 NIST SP 800-53 Rev.5

11.3.1 AC-16: Απαιτεί επισήμανση πληροφοριών ώστε τα μέτρα προστασίας να ευθυγραμμίζονται με την ταξινόμηση.

11.3.2 MP-3 / MP-5: Παρέχουν καθοδήγηση για την επισήμανση και τον έλεγχο μέσων και εκροών.

11.4 ΓΚΠΔ της ΕΕ

11.4.1 Άρθρα 5 και 32: Επιβάλλουν ελαχιστοποίηση δεδομένων και ακεραιότητα μέσω κατάλληλων δικλίδων ταξινόμησης και χειρισμού.

11.5 Οδηγία NIS2 της ΕΕ

11.5.1 Άρθρο 21(2)(a): Επιβάλλει τεχνικά και οργανωτικά μέτρα για την προστασία δεδομένων βάσει κινδύνου.

11.6 Κανονισμός DORA της ΕΕ

11.6.1 Άρθρο 5(8): Απαιτεί από τις επιχειρήσεις να ταξινομούν τα στοιχεία δεδομένων ως μέρος του προγράμματος διαχείρισης κινδύνων ΤΠΕ.

11.7 COBIT 2019

11.7.1 BAI03.05: Απαιτεί ταξινόμηση πληροφοριών και προστασία προσαρμοσμένη στον κίνδυνο.

11.7.2 DSS05.02: Καλύπτει την εφαρμογή ελέγχων βάσει ταξινόμησης και την παρακολούθηση.