					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P13					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**

1. Σκοπός

1.1 Η παρούσα πολιτική καθορίζει το επίσημο πλαίσιο για την ταξινόμηση και επισήμανση των πληροφοριακών περιουσιακών στοιχείων του οργανισμού με βάση την ευαισθησία, την έκθεση σε κίνδυνο και τις κανονιστικές υποχρεώσεις.

1.2 Διασφαλίζει ότι όλες οι πληροφορίες — είτε αποθηκεύονται, είτε διαβιβάζονται, είτε υποβάλλονται σε επεξεργασία — ταξινομούνται και επισημαίνονται με σαφή τρόπο, ώστε να αποτυπώνεται το απαιτούμενο επίπεδο προστασίας και χειρισμού τους.

1.3 Η πολιτική επιβάλλει δομημένη ταξινόμηση, ευθυγραμμισμένη με τις πρακτικές διαχείρισης κινδύνων του οργανισμού, υποστηρίζοντας τους στόχους εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας τόσο για ψηφιακά όσο και για φυσικά δεδομένα.

1.4 Η παρούσα δικλίδα είναι ουσιώδης για την υποστήριξη της πρόσβασης βάσει ρόλων, της ετοιμότητας για έλεγχο, της ορθής κοινοποίησης δεδομένων και της αποτελεσματικής εφαρμογής τεχνικών δικλίδων ασφαλείας, όπως η κρυπτογράφηση, τα αντίγραφα ασφαλείας και η παρακολούθηση.

2. Πεδίο εφαρμογής

2.1 Η παρούσα πολιτική εφαρμόζεται σε:

2.1.1 Όλα τα πληροφοριακά περιουσιακά στοιχεία του οργανισμού, συμπεριλαμβανομένων εγγράφων, βάσεων δεδομένων, αρχείων και επικοινωνιών

2.1.2 Όλες τις μορφές δεδομένων, συμπεριλαμβανομένων ψηφιακών, έντυπων, γραπτών ή προφορικών

2.1.3 Όλα τα περιβάλλοντα: εντός εγκαταστάσεων, απομακρυσμένα, κινητά και νεφοϋπολογιστικά

2.1.4 Όλους τους εργαζομένους, αναδόχους, παρόχους υπηρεσιών και εκτελούντες την επεξεργασία τρίτων μερών που δημιουργούν, χειρίζονται ή αποθηκεύουν πληροφορίες του οργανισμού

2.2 Το πεδίο εφαρμογής καλύπτει περιεχόμενο που αναπτύσσεται εσωτερικά, δεδομένα από εξωτερικές πηγές, δεδομένα προσωπικού χαρακτήρα που υπάγονται σε υποχρεώσεις της νομοθεσίας περί ιδιωτικότητας (π.χ. ΓΚΠΔ της ΕΕ), καθώς και πληροφορίες που ανταλλάσσονται με πελάτες, συνεργάτες και ρυθμιστικές αρχές.

2.3 Εφαρμόζεται σε όλα τα συστήματα που χρησιμοποιούνται για αποθήκευση ή διαβίβαση δεδομένων, συμπεριλαμβανομένων επιχειρησιακών εφαρμογών, διακομιστών αρχείων, συστημάτων ηλεκτρονικού ταχυδρομείου, νεφοϋπολογιστικών πλατφορμών και αποθετηρίων αντιγράφων ασφαλείας.

3. Στόχοι

3.1 Η καθιέρωση ενός τυποποιημένου, ενιαίου για όλο τον οργανισμό σχήματος ταξινόμησης με βάση τον αντίκτυπο από την έκθεση ή την παραβίαση δεδομένων.

3.2 Η διασφάλιση ότι όλες οι πληροφορίες επισημαίνονται με ορατό και μόνιμο τρόπο, ώστε να αποτυπώνεται το επίπεδο ταξινόμησης και οι απαιτήσεις χειρισμού τους.

3.3 Η εφαρμογή ελέγχων διαχείρισης δεδομένων και ελέγχου πρόσβασης, ευθυγραμμισμένων με την ταξινόμηση, συμπεριλαμβανομένων της κρυπτογράφησης, της καταγραφής, της προστασίας κατά τη διαβίβαση και του προγραμματισμού διατήρησης.

3.4 Η υποστήριξη της συμμόρφωσης με διεθνή πρότυπα (ISO/IEC 27001, 27002), νομικά πλαίσια (ΓΚΠΔ της ΕΕ, Οδηγία NIS2 της ΕΕ, Κανονισμός DORA της ΕΕ) και εσωτερικές πολιτικές διαχείρισης κινδύνων.

3.5 Η διασφάλιση ότι όλοι οι χρήστες κατανοούν τις αρμοδιότητές τους για την προστασία δεδομένων, την εφαρμογή επισημάνσεων και τον ορθό χειρισμό διαβαθμισμένων πληροφοριών.

3.6 Η διατήρηση ιχνηλασιμότητας μεταξύ της κατάστασης ταξινόμησης, των συναφών ελέγχων και του αποθετηρίου περιουσιακών στοιχείων του οργανισμού για σκοπούς ελέγχου και συμμόρφωσης.

4. Ρόλοι και αρμοδιότητες

4.1 Επικεφαλής Ασφάλειας Πληροφοριών (CISO)

4.1.1 Έχει την ευθύνη της πολιτικής ταξινόμησης και επισήμανσης πληροφοριών και διασφαλίζει την ευθυγράμμισή της με κανονιστικές, συμβατικές και επιχειρησιακές απαιτήσεις.

4.1.2 Εγκρίνει τα επίπεδα ταξινόμησης, τα πρότυπα επισήμανσης και τις αναθεωρήσεις της πολιτικής.

4.1.3 Ασκεί εποπτεία της συμμόρφωσης με την πολιτική μέσω ελέγχων, μετρήσεων και ανασκοπήσεων εξαιρέσεων.

4.1.4 Συντονίζει τη διατμηματική διακυβέρνηση με τις ομάδες Νομικής, προστασίας προσωπικών δεδομένων και διαχείρισης κινδύνων.

4.2 Ιδιοκτήτες Πληροφοριακών Περιουσιακών Στοιχείων

4.2.1 Είναι υπεύθυνοι για την ταξινόμηση των πληροφοριακών περιουσιακών στοιχείων που τελούν υπό τον έλεγχό τους, χρησιμοποιώντας το σχήμα ταξινόμησης του οργανισμού.

4.2.2 Εφαρμόζουν επισημάνσεις ταξινόμησης κατά τη δημιουργία, επικαιροποίηση ή παραλαβή των πληροφοριών.

4.2.3 Ανασκοπούν περιοδικά την ταξινόμηση των περιουσιακών στοιχείων, ιδίως σε απόκριση σε μεταβολές της ευαισθησίας, του κανονιστικού πεδίου ή της επιχειρησιακής αξίας.

4.2.4 Διασφαλίζουν ότι τα ευαίσθητα δεδομένα χειρίζονται και επισημαίνονται κατάλληλα σε όλο τον κύκλο ζωής τους.

[... 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 τουλάχιστον ετησίως, ώστε να διασφαλίζεται η ευθυγράμμισή της με:

9.1.1 Εξελισσόμενες κανονιστικές απαιτήσεις (π.χ. ΓΚΠΔ της ΕΕ, Οδηγία NIS2 της ΕΕ, Κανονισμός DORA της ΕΕ)

9.1.2 Επικαιροποιήσεις της καθοδήγησης ταξινόμησης των ISO/IEC 27001 ή 27002

9.1.3 Οργανωτικές μεταβολές που επηρεάζουν την ευαισθησία των δεδομένων ή την ιδιοκτησία τους

9.1.4 Τεχνολογικές μεταβολές, συμπεριλαμβανομένων νέων πλατφορμών διαχείρισης εγγράφων ή δεδομένων

9.2 Ο Επικεφαλής Ασφάλειας Πληροφοριών (CISO) πρέπει να εκκινεί την ανασκόπηση σε συνεργασία με την Επιτροπή Ασφάλειας Πληροφοριών, τον νομικό σύμβουλο και τις επηρεαζόμενες επιχειρησιακές μονάδες.

9.3 Οι ανασκοπήσεις πρέπει να περιλαμβάνουν:

9.3.1 Την αποτελεσματικότητα της εφαρμογής της ταξινόμησης και την τήρηση από τους χρήστες

9.3.2 Ανάλυση περιστατικών ή εξαιρέσεων που συνδέονται με εσφαλμένη ταξινόμηση

9.3.3 Ανατροφοδότηση χρηστών σχετικά με εργαλεία επισήμανσης ή υλικό καθοδήγησης

9.3.4 Συγκριτική αξιολόγηση με πρότυπα ταξινόμησης του κλάδου

9.4 Οι επικαιροποιήσεις της πολιτικής πρέπει να υπόκεινται σε έλεγχο έκδοσης, να τεκμηριώνονται στο αποθετήριο ISMS και να κοινοποιούνται σε όλο το σχετικό προσωπικό, με έμφαση σε νέες αρμοδιότητες ή αλλαγές εργαλείων.

9.5 Οι νεοπροσλαμβανόμενοι πρέπει να ενημερώνονται για την τρέχουσα έκδοση της πολιτικής κατά τη διαδικασία ένταξης. Όλοι οι εργαζόμενοι πρέπει να ολοκληρώνουν επαναληπτική εκπαίδευση μετά από σημαντικές αλλαγές της πολιτικής.

10. Συναφείς πολιτικές και διασυνδέσεις

10.1 Η παρούσα πολιτική υποστηρίζεται άμεσα από και εφαρμόζει ελέγχους που περιγράφονται στις ακόλουθες συναφείς πολιτικές:

10.1.1 P4 - Πολιτική Ελέγχου Πρόσβασης: Η πρόσβαση στις πληροφορίες διέπεται από τα επίπεδα ταξινόμησης· τα πλέον ευαίσθητα δεδομένα απαιτούν αυστηρότερο έλεγχο πρόσβασης και μηχανισμούς εξουσιοδότησης.

10.1.2 P11 - Πολιτική Διαχείρισης Λογαριασμών Χρηστών και Προνομίων: Ενισχύει την κατανομή προνομίων βάσει της αρχής της ανάγκης γνώσης, η οποία επηρεάζεται από τις βαθμίδες ταξινόμησης.

10.1.3 P12 - Πολιτική Διαχείρισης Περιουσιακών Στοιχείων: Διασφαλίζει ότι κάθε περιουσιακό στοιχείο στο αποθετήριο περιλαμβάνει την ταξινόμηση και την επισήμανσή του, υποστηρίζοντας την ιχνηλασιμότητα και τη λογοδοσία.

10.1.4 P14 - Πολιτική Διατήρησης και Διάθεσης Δεδομένων: Οι κανόνες διάθεσης και διατήρησης καθορίζονται από το επίπεδο ταξινόμησης των δεδομένων και από κανονιστικές υποχρεώσεις διατήρησης.

10.1.5 P18 - Πολιτική Κρυπτογραφικών Ελέγχων: Εφαρμόζει κατάλληλα πρότυπα κρυπτογράφησης βάσει της ταξινόμησης του πληροφοριακού περιουσιακού στοιχείου.

10.1.6 P22 - Πολιτική Καταγραφής και Παρακολούθησης: Επιτρέπει την παρακολούθηση της πρόσβασης και της διακίνησης διαβαθμισμένων πληροφοριών, διασφαλίζοντας τη δυνατότητα ελέγχου και την ανίχνευση εσφαλμένης επισήμανσης ή κακής χρήσης.

10.2 Κάθε διασύνδεση διασφαλίζει συνεπή προστασία των πληροφοριών σε όλο τον κύκλο ζωής τους, από τη δημιουργία και την ταξινόμηση έως τον ασφαλή χειρισμό, την αποθήκευση, τη διαβίβαση και την τελική καταστροφή.

11. Πρότυπα και πλαίσια αναφοράς

11.1 Η παρούσα πολιτική είναι ευθυγραμμισμένη με διεθνώς αναγνωρισμένα πρότυπα και κανονιστικά πλαίσια που διέπουν την ταξινόμηση και επισήμανση ευαίσθητων πληροφοριών.

11.2 ISO/IEC 27001

11.2.1 Ρήτρα 4.2 - Κατανόηση των αναγκών και των προσδοκιών των ενδιαφερόμενων μερών. Οι απαιτήσεις ταξινόμησης συχνά απορρέουν από νομικές, κανονιστικές ή συμβατικές υποχρεώσεις που επιβάλλονται από ενδιαφερόμενα μέρη (π.χ. ΓΚΠΔ της ΕΕ, συμφωνίες εμπιστευτικότητας πελατών), οι οποίες πρέπει να αποτυπώνονται στην πολιτική.

11.2.2 Ρήτρα 6.1.3 - Αντιμετώπιση κινδύνων ασφάλειας πληροφοριών. Η ταξινόμηση επηρεάζει άμεσα την επιλογή ελέγχων αντιμετώπισης κινδύνων, συμπεριλαμβανομένων του ελέγχου πρόσβασης, της κρυπτογράφησης και της διατήρησης, βάσει της ευαισθησίας των δεδομένων.

11.2.3 Ρήτρα 7.2 - Επάρκεια. Η πολιτική επιβάλλει ότι το προσωπικό που είναι υπεύθυνο για την ταξινόμηση και την επισήμανση πρέπει να εκπαιδεύεται, κάτι που εντάσσεται στις απαιτήσεις επάρκειας.

11.2.4 Ρήτρα 7.3 - Ευαισθητοποίηση. Η πολιτική απαιτεί όλοι οι χρήστες να γνωρίζουν τις βαθμίδες ταξινόμησης και τις αρμοδιότητές τους κατά τον χειρισμό πληροφοριών, σε ευθυγράμμιση με τις σχετικές υποχρεώσεις ευαισθητοποίησης.

11.2.5 Ρήτρα 7.5 - Τεκμηριωμένες πληροφορίες. Η ίδια η πολιτική ταξινόμησης αποτελεί ελεγχόμενο έγγραφο, ενώ οι διαδικασίες, τα αρχεία εκπαίδευσης και οι επισημάνσεις ταξινόμησης αποτελούν μέρος των τεκμηριωμένων πληροφοριών.

11.2.6 Ρήτρα 8.1 - Επιχειρησιακός σχεδιασμός και έλεγχος. Η ταξινόμηση και η επισήμανση είναι επιχειρησιακές διαδικασίες ενσωματωμένες στη διαχείριση του κύκλου ζωής των δεδομένων και η παρούσα ρήτρα διασφαλίζει ότι αυτές οι δραστηριότητες σχεδιάζονται, υλοποιούνται και ελέγχονται.

11.2.7 Ρήτρα 9.1 - Παρακολούθηση, μέτρηση, ανάλυση και αξιολόγηση. Η πολιτική περιλαμβάνει προβλέψεις για την παρακολούθηση της συμμόρφωσης ως προς την ταξινόμηση, των τάσεων περιστατικών και της αποτελεσματικότητας του σχήματος επισήμανσης.

11.2.8 Ρήτρα 10.1 - Μη συμμόρφωση και διορθωτική ενέργεια. Η πολιτική ορίζει αποκρίσεις σε εσφαλμένη ταξινόμηση, συμπεριλαμβανομένων διορθωτικών ενεργειών όπως επανεκπαίδευση, επικαιροποιήσεις και διαχείριση εξαιρέσεων.

11.3 ISO/IEC 27002:2022

11.3.1 Έλεγχος 5.12 - Ταξινόμηση πληροφοριών. Ο παρών έλεγχος διασφαλίζει ότι οι πληροφορίες ταξινομούνται βάσει της ευαισθησίας, της αξίας και της κρισιμότητάς τους — ακριβώς αυτό που τυποποιεί η παρούσα πολιτική.

11.3.2 Έλεγχος 5.13 - Επισήμανση πληροφοριών. Ο παρών έλεγχος απαιτεί κατάλληλη επισήμανση των πληροφοριών σύμφωνα με το επίπεδο ταξινόμησής τους, κάτι που καλύπτεται πλήρως από την πολιτική.

11.3.3 Έλεγχος 5.10 - Αποδεκτή χρήση πληροφοριών και άλλων συναφών περιουσιακών στοιχείων. Η πολιτική επιβάλλει τον τρόπο με τον οποίο οι χρήστες πρέπει να χειρίζονται διαβαθμισμένα δεδομένα, υποστηρίζοντας άμεσα την αποδεκτή χρήση και αποτρέποντας την κακή χρήση.

11.3.4 Έλεγχος 5.11 - Επιστροφή περιουσιακών στοιχείων. Η ταξινόμηση συμβάλλει στη διασφάλιση ότι τα ευαίσθητα δεδομένα αναγνωρίζονται και επιστρέφονται ή εξυγιαίνονται με ασφάλεια όταν αποχωρεί εργαζόμενος ή προμηθευτής.

11.3.5 Έλεγχος 5.9 - Απογραφή πληροφοριών και άλλων συναφών περιουσιακών στοιχείων. Η ταξινόμηση συχνά συνδέεται με το αποθετήριο περιουσιακών στοιχείων, το οποίο πρέπει να αποτυπώνει το επίπεδο ταξινόμησης κάθε στοιχείου ώστε να υποστηρίζεται η ορθή κατανομή ελέγχων.

11.3.6 Έλεγχος 5.14 - Μεταφορά πληροφοριών. Τα επίπεδα ταξινόμησης επηρεάζουν τους ελέγχους στις εσωτερικές και εξωτερικές μεταφορές δεδομένων (π.χ. κρυπτογράφηση, έγκριση, περιορισμοί πρόσβασης).

11.3.7 Έλεγχος 8.12 - Πρόληψη διαρροής δεδομένων. Η εφαρμογή ταξινόμησης και επισήμανσης υποστηρίζει την πρόληψη μη εξουσιοδοτημένης γνωστοποίησης και απώλειας δεδομένων.

11.3.8 Έλεγχος 8.11 - Απόκρυψη δεδομένων. Ορισμένα επίπεδα ταξινόμησης (π.χ. Εμπιστευτικό, Περιορισμένο) μπορεί να απαιτούν απόκρυψη όταν τα δεδομένα χρησιμοποιούνται σε περιβάλλοντα δοκιμών/ανάπτυξης ή αναλύσεων.

11.4 NIST SP 800-53 Rev.5

11.4.1 PL-2 - Πολιτική και διαδικασίες προστασίας συστημάτων και επικοινωνιών: Υποστηρίζει πολιτικές ταξινόμησης ως μέρος της συνολικής προστασίας δεδομένων.

11.4.2 AC-16 - Χαρακτηριστικά ασφάλειας: Υλοποιεί την επιβολή πρόσβασης βάσει μεταδεδομένων ταξινόμησης και δικαιωμάτων χρηστών.

11.4.3 MP-3 / MP-5 - Επισήμανση μέσων και προστασία κατά τη μεταφορά: Εφαρμόζει επισήμανση και προστασία δεδομένων κατά την αποθήκευση και κατά τη μεταφορά βάσει ταξινόμησης.

11.5 ΓΚΠΔ της ΕΕ (2016/679)

11.5.1 Άρθρο 5 - Αρχές προστασίας δεδομένων: Απαιτεί τα δεδομένα προσωπικού χαρακτήρα να υποβάλλονται σε ασφαλή επεξεργασία, ανάλογη με την ευαισθησία τους.

11.5.2 Άρθρο 32 - Ασφάλεια της επεξεργασίας: Ενισχύει την ταξινόμηση ως μηχανισμό προστασίας δεδομένων βάσει κινδύνου και εφαρμογής κατάλληλων τεχνικών μέτρων.

11.6 Οδηγία NIS2 της ΕΕ (2022/2555)

11.6.1 Άρθρο 21(2)(a): Απαιτεί πολιτικές για τη διαχείριση κινδύνων ασφάλειας πληροφοριών, συμπεριλαμβανομένων ελέγχων ταξινόμησης περιουσιακών στοιχείων και δεδομένων.

11.6.2 Άρθρο 21(3): Ενθαρρύνει την υιοθέτηση μέτρων για την εφαρμογή κατάλληλου χειρισμού δεδομένων — κάτι που υποστηρίζεται μέσω επισήμανσης βάσει ταξινόμησης.

11.7 Κανονισμός DORA της ΕΕ (2022/2554)

11.7.1 Άρθρο 5 - Διακυβέρνηση και έλεγχος: Απαιτεί πλαίσια διακυβέρνησης που ταξινομούν στοιχεία δεδομένων για τον έλεγχο του κινδύνου ΤΠΕ.

11.7.2 Άρθρο 9 - Διαχείριση κινδύνων ΤΠΕ: Επιβάλλει τεχνικά και οργανωτικά μέτρα για κρίσιμα στοιχεία ΤΠΕ, συμπεριλαμβανομένης της ταξινόμησης και της επισήμανσης.

11.8 COBIT 2019

11.8.1 DSS05.02 - Διαχείριση υπηρεσιών ασφάλειας: Επιβάλλει ταξινομήσεις ασφάλειας πληροφοριών για τη διασφάλιση της προστασίας των επιχειρησιακών δεδομένων.

11.8.2 MEA03 - Παρακολούθηση, αξιολόγηση και εκτίμηση της συμμόρφωσης: Υποστηρίζει τακτικό έλεγχο και ανασκόπηση των πρακτικών ταξινόμησης ώστε να διασφαλίζεται η τήρηση της πολιτικής και η ωριμότητα.