					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P14					Τίτλος εγγράφου: **Πολιτική Διατήρησης και Διάθεσης 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 6.1.3, 8.1	
ISO/IEC 27002:2022	Έλεγχοι 5.10, 5.12, 5.30, 5	
NIST SP 800-53 Rev. 5	AU-11, MP-6, SI-12, PL-2	
ΓΚΠΔ της ΕΕ	Άρθρα 5(1)(e), 17, 32	
Οδηγία NIS2 της ΕΕ	Άρθρο 21(2)(a-e)	
Κανονισμός DORA της ΕΕ	Άρθρα 5, 9	
COBIT 2019	DSS01, DSS05, MEA	

1. Σκοπός

1.1 Σκοπός της παρούσας πολιτικής είναι ο καθορισμός των οργανωτικών απαιτήσεων για τη διατήρηση δεδομένων και την ασφαλή διάθεσή τους σε όλα τα στάδια του κύκλου ζωής της πληροφορίας. Εξασφαλίζει τη συμμόρφωση με τις εφαρμοστέες νομικές, κανονιστικές και συμβατικές υποχρεώσεις και αποτρέπει την περιττή ή επικίνδυνη συσσώρευση δεδομένων.

1.2 Η παρούσα πολιτική υποστηρίζει την εφαρμογή του ISO/IEC 27001:2022, επιβάλλοντας έλεγχο επί της διάρκειας αποθήκευσης των δεδομένων και των πρακτικών μη αναστρέψιμης διάθεσης. Παρέχει τη δυνατότητα ιχνηλάσιμης τεκμηρίωσης αρχείων, επιβάλλει διατήρηση ευθυγραμμισμένη με την ευαισθησία της ταξινόμησης και διασφαλίζει ετοιμότητα για ελέγχους, επιθεωρήσεις από ρυθμιστικές αρχές και νομική γνωστοποίηση στοιχείων.

1.3 Περαιτέρω, αποσκοπεί στη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των δεδομένων, με παράλληλη ελαχιστοποίηση του επιχειρησιακού κινδύνου, των λειτουργικών αναποτελεσματικοτήτων και της έκθεσης σε παραβιάσεις ιδιωτικότητας που προκύπτουν από ακατάλληλη διατήρηση ή καταστροφή δεδομένων.

2. Πεδίο εφαρμογής

2.1 Η παρούσα πολιτική εφαρμόζεται σε όλα τα φυσικά και ψηφιακά πληροφοριακά περιουσιακά στοιχεία που ανήκουν στον οργανισμό, υποβάλλονται σε επεξεργασία ή διατηρούνται από αυτόν, συμπεριλαμβανομένων όσων τελούν υπό τον έλεγχο τρίτων μερών, θυγατρικών ή εξωτερικών συνεργατών.

2.2 Το πεδίο εφαρμογής περιλαμβάνει, ενδεικτικά και όχι περιοριστικά:

2.2.1 Έγγραφα, αρχεία και καταχωρίσεις (ψηφιακά και έντυπα)

2.2.2 Βάσεις δεδομένων και αρχεία αρχειοθέτησης

2.2.3 Μηνύματα ηλεκτρονικού ταχυδρομείου και αρχεία καταγραφής άμεσων μηνυμάτων

2.2.4 Αντίγραφα ασφαλείας, αρχεία καταγραφής συστημάτων και ίχνη ελέγχου

2.2.5 Πηγαίος κώδικας, δεδομένα εφαρμογών και στοιχεία που φιλοξενούνται σε περιβάλλοντα νέφους

2.2.6 Αφαιρούμενα μέσα και παρωχημένος εξοπλισμός που περιέχει δεδομένα

2.3 Η πολιτική διέπει τόσο τα λειτουργικά αρχεία όσο και τα ρυθμιζόμενα σύνολα δεδομένων (π.χ. οικονομικά, νομικά, ανθρώπινου δυναμικού, περιεχόμενο σχετικό με πελάτες και περιεχόμενο σχετικό με ελέγχους), ανεξάρτητα από τη θέση αποθήκευσης ή το σύστημα.

2.4 Εφαρμόζεται σε όλα τα τμήματα του οργανισμού και σε κάθε εργαζόμενο, ανάδοχο και προμηθευτή που συμμετέχει στη δημιουργία, αποθήκευση, διαχείριση ή διάθεση δεδομένων.

3. Στόχοι

3.1 Να διασφαλίζεται ότι τα δεδομένα διατηρούνται μόνο για όσο χρονικό διάστημα είναι νομικά, συμβατικά ή λειτουργικά αναγκαίο και ότι διατίθενται με ασφαλή τρόπο όταν δεν απαιτούνται πλέον.

3.2 Να αποτρέπεται η πρόωρη, μη εξουσιοδοτημένη ή ακούσια διαγραφή αρχείων που απαιτούνται για συνεχιζόμενες λειτουργίες, συμμόρφωση, δικαστική διαδικασία ή σκοπούς ελέγχου.

3.3 Να καθορίζονται και να εφαρμόζονται συνεπή χρονοδιαγράμματα διατήρησης βάσει της ταξινόμησης πληροφοριών, του τύπου περιουσιακού στοιχείου, των εφαρμοστέων νόμων και της έκθεσης σε κίνδυνο.

3.4 Να προστατεύονται η ιδιωτικότητα και η εμπιστευτικότητα των δεδομένων κατά τη διάρκεια της περιόδου διατήρησής τους και κατά τη διάθεσή τους, συμπεριλαμβανομένης της ικανοποίησης των δικαιωμάτων των υποκειμένων των δεδομένων (π.χ. διαγραφή σύμφωνα με το Άρθρο 17 του ΓΚΠΔ της ΕΕ).

3.5 Να διασφαλίζεται ότι όλες οι μέθοδοι διάθεσης δεδομένων είναι μη αναστρέψιμες, τεκμηριώνονται κατάλληλα και συμμορφώνονται με αναγνωρισμένα πρότυπα όπως το NIST SP 800-88.

3.6 Να ελαχιστοποιούνται οι λειτουργικές αναποτελεσματικότητες, το πρόσθετο κόστος και η νομική έκθεση που προκαλούνται από υπερβολική διατήρηση ή από παλαιά δεδομένα χωρίς παρακολούθηση.

3.7 Να υποστηρίζονται οι στόχοι επιχειρησιακής συνέχειας και ανάκαμψης από καταστροφή μέσω ολοκληρωμένης διακυβέρνησης της διατήρησης αντιγράφων ασφαλείας και τεκμηριωμένων πρακτικών αρχειοθέτησης δεδομένων.

4. Ρόλοι και αρμοδιότητες

4.1 Ανώτατη Διοίκηση

4.1.1 Εγκρίνει την παρούσα πολιτική και διασφαλίζει την κατάλληλη χρηματοδότηση, στελέχωση και ενσωμάτωσή της στα προγράμματα διαχείρισης επιχειρησιακών κινδύνων και συμμόρφωσης.

4.1.2 Φέρει τη συνολική λογοδοσία για τη νομική και κανονιστική συμμόρφωση που σχετίζεται με τη διατήρηση δεδομένων και την ασφαλή διάθεση.

4.2 Επικεφαλής Ασφάλειας Πληροφοριών (CISO)

4.2.1 Είναι ο ιδιοκτήτης της παρούσας πολιτικής και υπεύθυνος για τον καθορισμό και την ανασκόπηση της διακυβέρνησης διατήρησης και διάθεσης σε ευθυγράμμιση με το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (ISMS).

4.2.2 Διασφαλίζει ότι οι απαιτήσεις διατήρησης και διάθεσης βάσει ταξινόμησης εφαρμόζονται στις επιχειρησιακές μονάδες και στα τεχνικά συστήματα.

4.2.3 Παρακολουθεί τη συμμόρφωση με την πολιτική και επιβάλλει διορθωτικές ενέργειες όπου απαιτείται.

[... 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 ή όταν πληρούται οποιαδήποτε από τις ακόλουθες προϋποθέσεις:

9.1.1 Αλλαγές σε εφαρμοστέους νόμους ή κανονισμούς που επηρεάζουν τη διατήρηση δεδομένων (π.χ. επικαιροποιήσεις του ΓΚΠΔ της ΕΕ, φορολογικών κωδίκων, του Κανονισμού DORA της ΕΕ)

9.1.2 Αναθεωρήσεις του πλαισίου ταξινόμησης ή των επιχειρησιακών διεργασιών που επηρεάζουν τα στάδια του κύκλου ζωής δεδομένων

9.1.3 Εισαγωγή νέων συστημάτων ΤΠ, πλατφορμών αρχειοθέτησης ή τεχνολογιών διάθεσης μέσων

9.1.4 Ευρήματα Εσωτερικού Ελέγχου ή συστάσεις ρυθμιστικών αρχών που αναδεικνύουν κενά στις πρακτικές διατήρησης ή διάθεσης

9.2 Η ανασκόπηση πρέπει να καθοδηγείται από τον Επικεφαλής Ασφάλειας Πληροφοριών (CISO) και τον Υπεύθυνο Προστασίας Δεδομένων (DPO), με συνεισφορά από τη Νομική και τη Συμμόρφωση, την Πληροφορική και τις επιχειρησιακές μονάδες.

9.3 Το Κύριο Χρονοδιάγραμμα Διατήρησης Δεδομένων (MDRS) και το Μητρώο Διάθεσης πρέπει να ανασκοπούνται παράλληλα ώστε να διασφαλίζεται ότι:

9.3.1 Τα χρονοδιαγράμματα παραμένουν ακριβή και αντανακλούν τις λειτουργικές, νομικές και κανονιστικές ανάγκες

9.3.2 Η τεκμηρίωση διάθεσης είναι πλήρης και ελέγξιμη

9.3.3 Τα αρχεία νομικής δέσμευσης διατήρησης επικυρώνονται και αποδεσμεύονται όταν είναι σκόπιμο

9.4 Τυχόν επικαιροποιήσεις της πολιτικής πρέπει:

9.4.1 Να λαμβάνουν επίσημη έκδοση και να διατηρούνται στο αποθετήριο εγγράφων του ISMS

9.4.2 Να περιλαμβάνουν ιστορικό αναθεωρήσεων και αιτιολόγηση μεταβολών

9.4.3 Να εγκρίνονται από την Ανώτατη Διοίκηση

9.4.4 Να κοινοποιούνται στο σχετικό προσωπικό μαζί με επικαιροποιημένο εκπαιδευτικό υλικό ή οδηγίες

9.5 Όταν επέρχονται σημαντικές αλλαγές πολιτικής, οι επηρεαζόμενοι εργαζόμενοι πρέπει να ολοκληρώνουν στοχευμένη εκπαίδευση εντός 30 ημερών από την έκδοση, ώστε να διασφαλίζεται η συνεχής συμμόρφωση.

9.6 Συναφείς πολιτικές και διασυνδέσεις

10. Συναφείς πολιτικές και διασυνδέσεις

10.1.1 P4 - Πολιτική Ελέγχου Πρόσβασης: Διασφαλίζει ότι μόνο εξουσιοδοτημένα άτομα αποκτούν πρόσβαση σε δεδομένα κατά τη διάρκεια της περιόδου διατήρησής τους και ότι τα ληγμένα δεδομένα περιορίζονται ενόψει διάθεσης.

10.1.2 P12 - Πολιτική Διαχείρισης Περιουσιακών Στοιχείων: Προσδιορίζει ποια περιουσιακά στοιχεία περιέχουν δεδομένα που απαιτούν προγραμματισμένη διάθεση και παρακολουθεί τον κύκλο ζωής τους από την απόκτηση έως την καταστροφή.

10.1.3 P13 - Πολιτική Ταξινόμησης και Επισήμανσης Δεδομένων: Καθοδηγεί τις αποφάσεις ταξινόμησης που επηρεάζουν άμεσα τη διάρκεια διατήρησης των δεδομένων και τη μέθοδο διάθεσης που απαιτείται.

10.1.4 P15 - Πολιτική Αντιγράφων Ασφαλείας και Επαναφοράς: Καθορίζει περιόδους διατήρησης και διαδικασίες διάθεσης για μέσα αντιγράφων ασφαλείας και αναπαραγόμενα στοιχεία δεδομένων.

10.1.5 P18 - Πολιτική Κρυπτογραφικών Ελέγχων: Υποστηρίζει την κρυπτογραφική διαγραφή για σκοπούς διάθεσης και επιβάλλει κρυπτογράφηση κατά την αποθήκευση δεδομένων έως την καταστροφή.

10.1.6 P30 - Πολιτική Αντιμετώπισης Περιστατικών: Ενεργοποιείται σε περιπτώσεις όπου η ακατάλληλη διάθεση οδηγεί σε πιθανή απώλεια δεδομένων, παραβίαση ή κανονιστική παράβαση.

10.2 Κάθε συνδεδεμένη πολιτική διαδραματίζει ρόλο στην εφαρμογή συνεκτικού μοντέλου διακυβέρνησης δεδομένων ως προς την ταξινόμηση, τον έλεγχο του κύκλου ζωής, την πρόσβαση και την ετοιμότητα για έλεγχο.

11. Πρότυπα και πλαίσια αναφοράς

11.1 Η παρούσα πολιτική ευθυγραμμίζεται με διεθνώς αναγνωρισμένα πρότυπα και κανονιστικά πλαίσια που καθορίζουν ασφαλείς, συμμορφούμενες και αποδοτικές πρακτικές για τον κύκλο ζωής των δεδομένων.

11.2 ISO/IEC 27001:

11.2.1 Ρήτρα 6.1.3 - Σχέδιο Αντιμετώπισης Κινδύνων: Υποστηρίζει τον μετριασμό των κινδύνων που συνδέονται με υπερβολική διατήρηση, παραβιάσεις δεδομένων ή αστοχίες διάθεσης.

11.2.2 Ρήτρα 8.1 - Επιχειρησιακός σχεδιασμός και έλεγχος: Καθιερώνει ελέγχους κύκλου ζωής που διέπουν την αποθήκευση, την αρχειοθέτηση και την καταστροφή.

11.3 ISO/IEC 27002:2022 - Έλεγχοι 5.10, 5.12, 5.30, 5: Παρέχουν πρακτική καθοδήγηση για αποδεκτή χρήση δεδομένων, αιτιολόγηση διατήρησης, ελεγχόμενη διαγραφή και τεκμηριώσιμη τήρηση αρχείων σε ευθυγράμμιση με τα όρια ανοχής κινδύνου του οργανισμού.

11.4 NIST SP 800-53 Rev. 5:

11.4.1 AU-11 - Διατήρηση αρχείων ελέγχου: Διασφαλίζει επαρκή αποθήκευση αρχείων καταγραφής ελέγχου και αποδεικτικών συμμόρφωσης.

11.4.2 MP-6 - Εξυγίανση μέσων: Απαιτεί ασφαλείς και τεκμηριωμένες μεθόδους καταστροφής για φυσικά και ηλεκτρονικά μέσα.

11.4.3 SI-12 - Χειρισμός πληροφοριών: Επιβάλλει κατάλληλο χειρισμό δεδομένων σε ευθυγράμμιση με ελέγχους διατήρησης και διάθεσης.

11.4.4 PL-2 - Σχέδιο ασφάλειας και ιδιωτικότητας συστήματος: Απαιτεί τεκμηρίωση ειδική για κάθε σύστημα σχετικά με τον χειρισμό του κύκλου ζωής δεδομένων και τις προβλέψεις ασφαλούς διάθεσης.

11.5 ΓΚΠΔ της ΕΕ (2016/679):

11.5.1 Άρθρο 5(1)(e) - Ελαχιστοποίηση δεδομένων και περιορισμός αποθήκευσης: Απαιτεί τα δεδομένα να μη διατηρούνται περισσότερο από όσο είναι αναγκαίο.

11.5.2 Άρθρο 17 - Δικαίωμα διαγραφής («δικαίωμα στη λήθη»): Απαιτεί άμεση και μόνιμη διαγραφή δεδομένων προσωπικού χαρακτήρα κατόπιν έγκυρου αιτήματος.

11.5.3 Άρθρο 32 - Ασφάλεια της επεξεργασίας: Ενισχύει την προστασία δεδομένων κατά τη διατήρηση και επιβάλλει ασφαλή καταστροφή ληγμένων αρχείων.

11.6 Οδηγία NIS2 της ΕΕ (2022/2555):

11.6.1 Άρθρο 21(2)(a-e): Απαιτεί από τις οντότητες να υιοθετούν πολιτικές και τεχνικά και οργανωτικά μέτρα για ασφαλή διαχείριση δεδομένων, συμπεριλαμβανομένων περιορισμών αποθήκευσης και μεθόδων διάθεσης.

11.7 Κανονισμός DORA της ΕΕ (2022/2554):

11.7.1 Άρθρο 5 - Διακυβέρνηση και έλεγχος: Επιβάλλει δομημένη διαχείριση κινδύνων ΤΠΕ, συμπεριλαμβανομένου του ασφαλούς χειρισμού του κύκλου ζωής της πληροφορίας.

11.7.2 Άρθρο 9 - Πλαίσιο διαχείρισης κινδύνων ΤΠΕ: Απαιτεί πολιτικές για τη διατήρηση δεδομένων, την καταστροφή και τη νομική/κανονιστική συμμόρφωση των ψηφιακών λειτουργιών.

11.8 COBIT 2019:

11.8.1 DSS01 - Διαχειριζόμενες λειτουργίες: Υποστηρίζει την παρακολούθηση της διατήρησης και τη συνέπεια στα συστήματα δεδομένων.

11.8.2 DSS05 - Διαχειριζόμενες υπηρεσίες ασφάλειας: Διασφαλίζει την προστασία αποθηκευμένων και αρχειοθετημένων δεδομένων έως την ασφαλή διάθεσή τους.

11.8.3 MEA03 - Παρακολούθηση, Αξιολόγηση και Εκτίμηση της Συμμόρφωσης: Επιτρέπει τον έλεγχο της εφαρμογής της διατήρησης, των διαδικασιών διαγραφής και της εκπλήρωσης κανονιστικών υποχρεώσεων.