					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P14S					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	Καλύπτει την αντιμετώπιση κινδύνων, τους λειτουργικούς ελέγχους και τις απαιτήσεις διατήρησης
ISO/IEC 27002:2022	Έλεγχος 5	Παρέχει καθοδήγηση για τις περιόδους διατήρησης και τις ασφαλείς μεθόδους καταστροφής
NIST SP 800-53 Rev.5	AU-11, MP-6, SI-12	Διατήρηση αρχείων ελέγχου, εξυγίανση μέσων, όρια διατήρησης δεδομένων και επιβολή τους
Οδηγία NIS2 της ΕΕ	Άρθρο 21(2)(a)	Απαιτεί πολιτική διαχείρισης κύκλου ζωής ανάλογη του κινδύνου
Κανονισμός DORA της ΕΕ	Άρθρο 5(1)	Διαχείριση κινδύνων ΤΠΕ: διαθεσιμότητα και αφαίρεση δεδομένων
COBIT 2019	BAI03.04, DSS01	Έλεγχοι κύκλου ζωής πληροφοριών, ασφαλής διάθεση
ΓΚΠΔ της ΕΕ	Άρθρο 5(1)(e), 17	Τα δεδομένα δεν διατηρούνται περισσότερο από όσο είναι αναγκαίο· δικαίωμα διαγραφής

1. Σκοπός

1.1 Σκοπός της παρούσας πολιτικής είναι ο καθορισμός δεσμευτικών κανόνων για τη διατήρηση και την ασφαλή διάθεση πληροφοριών σε περιβάλλον ΜΜΕ. Διασφαλίζει ότι τα αρχεία τηρούνται μόνο για το χρονικό διάστημα που απαιτείται από τη νομοθεσία, συμβατική υποχρέωση ή επιχειρησιακή ανάγκη και στη συνέχεια καταστρέφονται με ασφαλή τρόπο.

1.2 Η παρούσα πολιτική αποσκοπεί στη μείωση του κινδύνου που συνδέεται με την πληροφορία, στη διαχείριση της νομικής έκθεσης και στον περιορισμό της αποθήκευσης πλεοναζόντων ή παρωχημένων δεδομένων. Συμβάλλει στη συμμόρφωση με το ISO/IEC 27001 και με πλαίσια προστασίας ιδιωτικότητας, όπως ο ΓΚΠΔ της ΕΕ, ελαχιστοποιώντας τη μη εξουσιοδοτημένη διατήρηση προσωπικών ή ευαίσθητων πληροφοριών.

1.3 Ένα καλά δομημένο πλαίσιο διατήρησης και διάθεσης μειώνει το λειτουργικό κόστος, βελτιώνει την απόδοση των συστημάτων και ενισχύει την ετοιμότητα για έλεγχο. Για ΜΜΕ με περιορισμένη δυναμικότητα ΤΠ, παρέχει έναν πρακτικό τρόπο υπεύθυνης διαχείρισης ψηφιακών και φυσικών πληροφοριακών περιουσιακών στοιχείων.

2. Πεδίο εφαρμογής

2.1 Η παρούσα πολιτική εφαρμόζεται σε:

2.1.1 Όλα τα αρχεία, έγγραφα, αρχεία καταγραφής, επικοινωνίες και σύνολα δεδομένων που δημιουργούνται, συλλέγονται, υποβάλλονται σε επεξεργασία ή αποθηκεύονται από τον οργανισμό

2.1.2 Όλους τους εργαζομένους, τους αναδόχους και τους εξωτερικούς παρόχους που χειρίζονται δεδομένα του οργανισμού

2.1.3 Όλες τις μορφές δεδομένων (π.χ. έντυπα, ηλεκτρονικά, εικόνας, ήχου ή αρχεία καταγραφής) και όλα τα μέσα αποθήκευσης (π.χ. τοπικοί δίσκοι, υπηρεσίες νέφους, διακομιστές ηλεκτρονικού ταχυδρομείου, αντίγραφα ασφαλείας)

2.2 Το πεδίο εφαρμογής περιλαμβάνει:

2.2.1 Επιχειρησιακά έγγραφα (π.χ. τιμολόγια, συμβάσεις, αναφορές έργων)

2.2.2 Λειτουργικά αρχεία (π.χ. αρχεία καταγραφής, ιστορικό πρόσβασης, στιγμιότυπα αντιγράφων ασφαλείας)

2.2.3 Προσωπικά δεδομένα (π.χ. αρχεία ανθρώπινου δυναμικού, επικοινωνίες πελατών, αρχεία υποστήριξης)

2.2.4 Δεδομένα που φιλοξενούνται εσωτερικά, εξωτερικά ή σε υβριδικά συστήματα

2.2.5 Αρχειοθετημένα δεδομένα και δεδομένα αντιγράφων ασφαλείας, είτε ενεργά είτε ανενεργά

2.3 Όλα τα στάδια του κύκλου ζωής των δεδομένων εμπίπτουν στο πεδίο εφαρμογής, από τη δημιουργία έως την εξουσιοδοτημένη διάθεση.

3. Στόχοι

3.1 Να καθοριστούν συνεπείς κανόνες διατήρησης βάσει νομικών, λειτουργικών και κανονιστικών κριτηρίων.

3.2 Να αποτρέπεται η πρόωρη διαγραφή κρίσιμων αρχείων και να εξαλείφεται η άσκοπη συσσώρευση δεδομένων.

3.3 Να διασφαλίζεται η ασφαλής και μη αναστρέψιμη διάθεση δεδομένων όταν η διατήρησή τους δεν απαιτείται πλέον.

3.4 Να ορίζεται σαφής υπευθυνότητα για την εφαρμογή αποφάσεων διατήρησης και διαγραφής, λαμβάνοντας υπόψη τους περιορισμούς στελέχωσης σε επίπεδο ΜΜΕ.

3.5 Να παρέχεται τεκμηρίωση κατάλληλη για έλεγχο, ώστε να αποδεικνύεται η δέουσα επιμέλεια βάσει ISO 27001, ΓΚΠΔ της ΕΕ, Οδηγίας NIS2 της ΕΕ και άλλων πλαισίων.

3.6 Να προάγεται ο ασφαλής χειρισμός δεδομένων σε όλο τον κύκλο ζωής τους, χωρίς να επιβάλλεται περιττό τεχνικό βάρος σε προσωπικό χωρίς εξειδίκευση.

4. Ρόλοι και αρμοδιότητες

4.1 Γενικός Διευθυντής (GM)

4.1.1 Εγκρίνει την παρούσα πολιτική και έχει τη συνολική ευθύνη για αυτήν.

4.1.2 Διασφαλίζει ότι οι διαδικασίες διατήρησης και διάθεσης εφαρμόζονται κατά τρόπο συνεπή με τον νομικό και επιχειρησιακό κίνδυνο.

4.1.3 Εγκρίνει εξαιρέσεις και νομικές δεσμεύσεις διατήρησης όταν απαιτείται.

4.1.4 Κινεί τη διαδικασία ανασκόπησης της πολιτικής και εγκρίνει επικαιροποιήσεις βάσει επιχειρησιακών ή κανονιστικών αλλαγών.

4.2 Ορισμένος Ιδιοκτήτης Δεδομένων

4.2.1 Ορίζεται ανά κατηγορία δεδομένων (π.χ. οικονομικά, ανθρώπινο δυναμικό, αρχεία πελατών).

4.2.2 Ταξινομεί τα αρχεία και καθορίζει την κατάλληλη περίοδο διατήρησης βάσει της πολιτικής και της νομικής καθοδήγησης.

4.2.3 Εγκρίνει τη διαγραφή όταν έχουν εκπληρωθεί οι απαιτήσεις διατήρησης.

4.2.4 Υποστηρίζει τους εσωτερικούς ελέγχους παρέχοντας τεκμηρίωση σχετικά με τη λογική διατήρησης και τα συμβάντα διάθεσης.

[... 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 μία φορά ετησίως ή σε περίπτωση:

9.1.1 Αλλαγών στην εφαρμοστέα νομοθεσία (π.χ. προστασία ιδιωτικότητας δεδομένων, χρηματοοικονομική αναφορά)

9.1.2 Υιοθέτησης νέων συστημάτων ή διαδικασιών που επηρεάζουν τον κύκλο ζωής των δεδομένων

9.1.3 Ευρημάτων ελέγχου ή περιστατικών που αποκαλύπτουν κενά στις πρακτικές διατήρησης

9.2 Οι ανασκοπήσεις πρέπει να διασφαλίζουν ότι το Μητρώο Διατήρησης παραμένει πλήρες και αποτυπώνει όλες τις βασικές κατηγορίες αρχείων.

9.3 Οι επικαιροποιήσεις της πολιτικής πρέπει να εγκρίνονται από τον GM και να κοινοποιούνται στο επηρεαζόμενο προσωπικό. Η πλέον πρόσφατη έκδοση πρέπει να είναι προσβάσιμη και να υπόκειται σε έλεγχο εκδόσεων.

10. Συναφείς πολιτικές και διασυνδέσεις

10.1 P2S – Πολιτική Ρόλων και Αρμοδιοτήτων Διακυβέρνησης: Καθορίζει την ευθύνη για την πολιτική και την αρμοδιότητα για εξαιρέσεις.

10.2 P13S – Πολιτική Ταξινόμησης και Επισήμανσης Δεδομένων: Καθορίζει πώς οι κανόνες διατήρησης ευθυγραμμίζονται με την ταξινόμηση δεδομένων.

10.3 P12S – Πολιτική Διαχείρισης Περιουσιακών Στοιχείων: Διέπει τα μέσα αποθήκευσης που περιέχουν δεδομένα τα οποία υπόκεινται σε διατήρηση ή διάθεση.

10.4 P17S – Πολιτική Προστασίας Δεδομένων και Ιδιωτικότητας: Διασφαλίζει την ελαχιστοποίηση δεδομένων και υποστηρίζει τη νόμιμη επεξεργασία βάσει του ΓΚΠΔ της ΕΕ.

10.5 P30S – Πολιτική Αντιμετώπισης Περιστατικών: Ενεργοποιείται όταν αστοχίες διάθεσης ή διατήρησης οδηγούν σε πιθανή έκθεση δεδομένων.

11. Πρότυπα και πλαίσια αναφοράς

11.1 ISO/IEC 27001

11.1.1 Ρήτρα 6.1.3: Απαιτεί την αντιμετώπιση κινδύνων που σχετίζονται με την πληροφορία, συμπεριλαμβανομένων των κινδύνων διατήρησης.

11.1.2 Ρήτρα 8.1: Ορίζει λειτουργικούς ελέγχους του κύκλου ζωής.

11.2 ISO/IEC 27002

11.2.1 Έλεγχος 5.33: Παρέχει καθοδήγηση για τον καθορισμό περιόδων διατήρησης και ασφαλών μεθόδων καταστροφής.

11.3 NIST SP 800-53 Rev. 5

11.3.1 AU-11: Απαιτείται διατήρηση αρχείων ελέγχου.

11.3.2 MP-6: Ορίζει διαδικασίες εξυγίανσης μέσων.

11.3.3 SI-12: Καλύπτει τα όρια διατήρησης δεδομένων και την επιβολή τους.

11.4 ΓΚΠΔ της ΕΕ

11.4.1 Άρθρο 5(1)(e): Τα δεδομένα πρέπει να τηρούνται όχι περισσότερο από όσο είναι αναγκαίο.

11.4.2 Άρθρο 17: Το δικαίωμα διαγραφής εφαρμόζεται όταν τα δεδομένα δεν διατηρούνται πλέον νομίμως.

11.5 Οδηγία NIS2 της ΕΕ

11.5.1 Άρθρο 21(2)(a): Απαιτεί οργανωτικές πολιτικές ανάλογες του κινδύνου, συμπεριλαμβανομένης της διαχείρισης κύκλου ζωής.

11.6 Κανονισμός DORA της ΕΕ

11.6.1 Άρθρο 5(1): Η διαχείριση κινδύνων ΤΠΕ περιλαμβάνει τη διαθεσιμότητα και την αφαίρεση δεδομένων.

11.7 COBIT 2019

11.7.1 BAI03.04: Απαιτούνται έλεγχοι κύκλου ζωής πληροφοριών.

11.7.2 DSS01.06: Διαδικασίες ασφαλούς διάθεσης ως μέρος της προστασίας των πληροφοριακών περιουσιακών στοιχείων.