

				Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P12S				Τίτλος εγγράφου: <b>Πολιτική Διαχείρισης Περιουσιακών Στοιχείων</b>							
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

<p><b>Νομική σημείωση (πνευματικά δικαιώματα και περιορισμοί χρήσης)</b> (C) 2025 Clarysec LLC. All rights reserved.</p> <p>Το παρόν έγγραφο αποτελεί πνευματική ιδιοκτησία της Clarysec LLC. Απαγορεύεται η αντιγραφή, επαναχρησιμοποίηση, διανομή ή τροποποίησή του, εν όλω ή εν μέρει, για εμπορικούς ή σκοπούς υλοποίησης χωρίς προηγούμενη ρητή έγγραφη άδεια. Η μη εξουσιοδοτημένη χρήση απαγορεύεται αυστηρά και ενδέχεται να επιφέρει νομικές ενέργειες. Για θέματα αδειοδότησης, επικοινωνήστε με: <a href="mailto:info@clarysec.com">info@clarysec.com</a></p>
--

Ευθυγραμμισμένη με πρότυπα και κανονιστικές απαιτήσεις

Πρότυπο/Κανονισμός	Ρήτρα/Άρθρο	Σχόλιο
ISO/IEC 27001:2022	Clause 8	Απαιτήσεις διαχείρισης περιουσιακών στοιχείων
ISO/IEC 27002:2022	Control 5	Έλεγχοι διαχείρισης περιουσιακών στοιχείων
NIST SP 800-53 Rev.5	CM-8	Απογραφή στοιχείων συστήματος
Οδηγία NIS2 της ΕΕ	Article 21(2)(a)	Παρακολούθηση περιουσιακών στοιχείων για την προστασία δικτυακών και πληροφοριακών συστημάτων
Κανονισμός DORA της ΕΕ	Article 5(8)	Απαιτήσεις απογραφής περιουσιακών στοιχείων ΤΠΕ
COBIT 2019	BAI	Διαχείριση του κύκλου ζωής περιουσιακών στοιχείων πληροφορικής
ΓΚΠΔ της ΕΕ	Article 30	Απογραφή δραστηριοτήτων επεξεργασίας δεδομένων

## 1. Σκοπός

1.1 Η παρούσα πολιτική καθορίζει τον τρόπο με τον οποίο ο οργανισμός αναγνωρίζει, παρακολουθεί, προστατεύει και αποσύρει τα πληροφοριακά περιουσιακά στοιχεία του, συμπεριλαμβανομένων τόσο των φυσικών όσο και των ψηφιακών στοιχείων.

1.2 Στόχος είναι η μείωση των λειτουργικών κινδύνων και των κινδύνων ασφάλειας μέσω της διατήρησης ορατότητας, λογοδοσίας και ασφαλούς χειρισμού όλων των επιχειρησιακών περιουσιακών στοιχείων σε όλο τον κύκλο ζωής τους.

1.3 Ένα αξιόπιστο Αποθετήριο Περιουσιακών Στοιχείων υποστηρίζει τη συμμόρφωση με κανονιστικές απαιτήσεις, την αντιμετώπιση περιστατικών, τον σχεδιασμό επιχειρησιακής συνέχειας και τη διαχείριση κινδύνων.

1.4 Η παρούσα πολιτική υποστηρίζει επίσης την πιστοποίηση κατά ISO/IEC 27001 και αποδεικνύει ευθυγράμμιση με νομικές, χρηματοοικονομικές και σχετικές με την κυβερνοασφάλεια υποχρεώσεις βάσει πλαισίων όπως ο ΓΚΠΔ της ΕΕ, η Οδηγία NIS2 της ΕΕ και ο Κανονισμός DORA της ΕΕ.

1.5 Για τις μικρές και μεσαίες επιχειρήσεις (SMEs), μια απλή αλλά συστηματική προσέγγιση στη διαχείριση περιουσιακών στοιχείων είναι ουσιώδης, ώστε να αποφεύγονται μη διαχειριζόμενες συσκευές, διαρροές δεδομένων ή αστοχίες ελέγχου, ιδίως όταν οι διαθέσιμοι τεχνικοί και στελεχιακοί πόροι είναι περιορισμένοι.

## 2. Πεδίο εφαρμογής

**2.1 Η παρούσα πολιτική εφαρμόζεται σε όλα τα περιουσιακά στοιχεία που ανήκουν, μισθώνονται ή με οποιονδήποτε άλλο τρόπο διαχειρίζεται ο οργανισμός, συμπεριλαμβανομένων όσων χρησιμοποιούνται σε:**

2.1.1 εργασία εντός γραφείου

2.1.2 ρυθμίσεις απομακρυσμένης ή υβριδικής εργασίας

2.1.3 επιτόπιες ή κινητές λειτουργίες

2.1.4 περιβάλλοντα νέφους και περιβάλλοντα εξωτερικής ανάθεσης

## **2.2 Οι καλυπτόμενοι τύποι περιουσιακών στοιχείων περιλαμβάνουν ενδεικτικά και όχι περιοριστικά:**

2.2.1 Υλισμικό: φορητούς υπολογιστές, επιτραπέζιους υπολογιστές, οθόνες, τηλέφωνα, tablets, μονάδες USB, δρομολογητές, εκτυπωτές, μέσα αντιγράφων ασφαλείας

2.2.2 Λογισμικό: εγκατεστημένες εφαρμογές, εργαλεία SaaS, λειτουργικά συστήματα, εργαλεία προστασίας από ιούς, άδειες χρήσης

2.2.3 Στοιχεία δεδομένων: αποθετήρια επιχειρησιακών δεδομένων, υπολογιστικά φύλλα, αρχεία πελατών, πηγαίο κώδικα

2.2.4 Ψηφιακά διαπιστευτήρια και υπηρεσίες: ονόματα τομέα, ψηφιακά πιστοποιητικά, κλειδιά API, λογαριασμούς ηλεκτρονικού ταχυδρομείου, συνδέσεις σε υπηρεσίες νέφους

2.2.5 Μέσα πρόσβασης: κλειδιά, έξυπνες κάρτες, μπρελόκ πρόσβασης, βιομετρικά διακριτικά

2.3 Όλοι οι εργαζόμενοι και οι ανάδοχοι, καθώς και οι τρίτοι πάροχοι που χειρίζονται περιουσιακά στοιχεία του οργανισμού, εμπíπτουν στο πεδίο εφαρμογής της παρούσας πολιτικής.

2.4 Η πολιτική διέπει επίσης τόσο βραχυπρόθεσμα περιουσιακά στοιχεία (π.χ. φορητούς υπολογιστές ειδικού έργου) όσο και μακροπρόθεσμα περιουσιακά στοιχεία, καθώς και κοινόχρηστα περιουσιακά στοιχεία που χρησιμοποιούνται από περισσότερα του ενός μέλη του προσωπικού.

## **3. Στόχοι**

3.1 Να θεσπιστεί και να διατηρείται ένα πλήρες και ακριβές αποθετήριο όλων των σχετικών περιουσιακών στοιχείων, το οποίο επικαιροποιείται σε συνεχή βάση.

3.2 Να διασφαλίζεται ότι κάθε περιουσιακό στοιχείο έχει ορισμένο κάτοχο, υπεύθυνο για τη χρήση, τη φύλαξη και την επιστροφή του.

3.3 Να ταξινομούνται τα περιουσιακά στοιχεία βάσει ευαισθησίας, επιχειρησιακού αντικτύπου ή κανονιστικής σημασίας, ώστε να εφαρμόζονται διαφοροποιημένα επίπεδα προστασίας.

3.4 Να ορίζονται σαφείς διαδικασίες για τη διάθεση, την επανανάθεση, τη συντήρηση, την αναφορά απώλειας και την απόσυρση περιουσιακών στοιχείων.

3.5 Να διασφαλίζεται ότι τα περιουσιακά στοιχεία χειρίζονται με ασφάλεια σε όλο τον κύκλο ζωής τους και ότι οι πληροφορίες που αποθηκεύουν είτε προστατεύονται είτε διαγράφονται με ασφαλή τρόπο κατά τη διάθεσή τους.

3.6 Να μειώνεται η πιθανότητα περιστατικών ασφάλειας που προκαλούνται από μη παρακολουθούμενους, μη επιστραφέντες ή κακώς χρησιμοποιούμενους πόρους του οργανισμού.

3.7 Να υποστηρίζεται η συμμόρφωση με τη σχετική νομοθεσία (π.χ. την αρχή λογοδοσίας του ΓΚΠΔ) και με πρότυπα πιστοποίησης κυβερνοασφάλειας.

## **4. Ρόλοι και αρμοδιότητες**

### **4.1 Γενικός Διευθυντής (GM)**

4.1.1 Είναι ο ιδιοκτήτης της παρούσας πολιτικής και υπεύθυνος για τη διασφάλιση ότι οι πρακτικές διαχείρισης περιουσιακών στοιχείων εφαρμόζονται και τηρούνται σε όλο τον οργανισμό.

4.1.2 Ανασκοπεί και εγκρίνει επικαιροποιήσεις του αποθετηρίου περιουσιακών στοιχείων και εξουσιοδοτεί τον παροπλισμό ή τη μεταφορά περιουσιακών στοιχείων, όπου απαιτείται.

4.1.3 Πρέπει να ενημερώνεται για κάθε σημαντική απώλεια, κλοπή ή κακή χρήση περιουσιακών στοιχείων.

### **4.2 Υπεύθυνος Πληροφορικής ή Ορισμένος Συντονιστής Ασφάλειας Περιουσιακών Στοιχείων**

4.2.1 Τηρεί το αποθετήριο περιουσιακών στοιχείων (π.χ. σε υπολογιστικό φύλλο, σύστημα διαχείρισης αιτημάτων helpdesk ή ελαφρύ εργαλείο παρακολούθησης περιουσιακών στοιχείων).

4.2.2 Αναθέτει την ιδιοκτησία των περιουσιακών στοιχείων και παρακολουθεί μεταβολές στην κατάστασή τους (π.χ. νέο, σε χρήση, υπό επισκευή, αποσυρμένο).

4.2.3 Επαληθεύει ότι όλα τα διατεθέντα περιουσιακά στοιχεία είναι τεκμηριωμένα και συνδεδεμένα με συγκεκριμένο άτομο ή επιχειρησιακή μονάδα.

4.2.4 Διασφαλίζει ότι οι ετικέτες ταξινόμησης εφαρμόζονται και τηρούνται (π.χ. Internal, Confidential).

4.2.5 Συντονίζει την ανάκτηση, την εξυγίανση και την απενεργοποίηση περιουσιακών στοιχείων κατά την αποχώρηση ή την απόσυρση.

4.2.6 Αναφέρει στον GM κάθε ανεπίλυτη απόκλιση που σχετίζεται με περιουσιακά στοιχεία.

[ ... 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 και κάθε φορά που:**

9.1.1 εισάγονται νέοι τύποι τεχνολογίας ή περιουσιακών στοιχείων

9.1.2 μεταβάλλονται οι διαδικασίες παρακολούθησης περιουσιακών στοιχείων (π.χ. με την υιοθέτηση νέων εργαλείων ή πλατφορμών)

9.1.3 νέες κανονιστικές υποχρεώσεις επηρεάζουν την ιχνηλασιμότητα ή τη διάθεση περιουσιακών στοιχείων

9.1.4 περιστατικό ή έλεγχος εντοπίζει κενό στις τρέχουσες πρακτικές διαχείρισης περιουσιακών στοιχείων

9.2 Οι ανασκοπήσεις πρέπει να περιλαμβάνουν τον GM και τον Υπεύθυνο Πληροφορικής και να καλύπτουν επικαιροποιήσεις στις διαδικασίες χειρισμού περιουσιακών στοιχείων, στα πρότυπα αποθετηρίου και στις οδηγίες ταξινόμησης.

9.3 Όλες οι επικαιροποιήσεις πρέπει να τεκμηριώνονται και να γνωστοποιούνται στο επηρεαζόμενο προσωπικό. Πρέπει να τηρείται αρχείο μεταβολών με έλεγχο έκδοσης.

## **10. Συναφείς πολιτικές και διασυνδέσεις**

10.1 P2S – Πολιτική Ρόλων και Αρμοδιοτήτων Διακυβέρνησης: Αναθέτει λογοδοσία για την ιδιοκτησία πολιτικών και τις λειτουργίες πληροφορικής.

10.2 P4S – Πολιτική Ελέγχου Πρόσβασης: Συνδέει τη χρήση περιουσιακών στοιχείων (π.χ. φορητών υπολογιστών, φορητών συσκευών) με τα δικαιώματα πρόσβασης χρηστών και τη διαχείριση ταυτοτήτων.

10.3 P7S – Πολιτική Ένταξης και Αποχώρησης: Διασφαλίζει ότι η διάθεση και η ανάκτηση περιουσιακών στοιχείων ενσωματώνονται στις διαδικασίες του κύκλου ζωής του προσωπικού.

10.4 P13S – Πολιτική Ταξινόμησης και Επισήμανσης Δεδομένων: Παρέχει κανόνες για τον προσδιορισμό του κατά πόσον ένα περιουσιακό στοιχείο πρέπει να ταξινομείται ως Internal ή Confidential.

10.5 P30S – Πολιτική Αντιμετώπισης Περιστατικών: Καθοδηγεί τις διαδικασίες απόκρισης εάν συμβάν που σχετίζεται με περιουσιακό στοιχείο καταλήξει σε παραβίαση ασφάλειας ή ιδιωτικότητας.

## **11. Πρότυπα και πλαίσια αναφοράς**

### **11.1 ISO/IEC 27001**

11.1.1 Clause 8.1: Απαιτεί λειτουργικούς ελέγχους για τη διαχείριση περιουσιακών στοιχείων και την προστασία τους καθ' όλη τη διάρκεια της χρήσης τους.

### **11.2 ISO/IEC 27002**

11.2.1 Control 5.9: Περιγράφει τον τρόπο αναγνώρισης, ανάθεσης ιδιοκτησίας, ταξινόμησης και ασφαλούς διαχείρισης περιουσιακών στοιχείων.

### **11.3 NIST SP 800-53 Rev**

11.3.1 CM-8: Απαιτεί από τους οργανισμούς να αναπτύσσουν και να διατηρούν απογραφή στοιχείων συστήματος, συμπεριλαμβανομένων υλισμικού, λογισμικού και εικονικών περιουσιακών στοιχείων.

#### **11.4 ΓΚΠΔ της ΕΕ**

11.4.1 Article 30: Απαιτεί την τεκμηρίωση δραστηριοτήτων επεξεργασίας δεδομένων, η οποία εξαρτάται από τη γνώση του πού αποθηκεύονται τα δεδομένα και σε ποια περιουσιακά στοιχεία.

#### **11.5 Οδηγία NIS2 της ΕΕ**

11.5.1 Article 21(2)(a): Προβλέπει τεχνικά και οργανωτικά μέτρα, συμπεριλαμβανομένης της παρακολούθησης περιουσιακών στοιχείων, για την προστασία δικτυακών και πληροφοριακών συστημάτων.

#### **11.6 Κανονισμός DORA της ΕΕ**

11.6.1 Article 5(8): Οι χρηματοοικονομικές οντότητες πρέπει να διατηρούν λεπτομερείς απογραφές περιουσιακών στοιχείων ΤΠΕ ως μέρος των αρμοδιοτήτων διαχείρισης κινδύνων ΤΠΕ.

#### **11.7 COBIT 2019**

11.7.1 BAI09: Προσδιορίζει ότι τα περιουσιακά στοιχεία πληροφορικής πρέπει να διαχειρίζονται σε όλο τον κύκλο ζωής τους — από την απόκτηση έως την απόσυρση — με σαφή ιδιοκτησία και ελέγχους.