					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P34					Τίτλος εγγράφου: **Πολιτική Κινητών Συσκευών και Χρήσης Προσωπικών Συσκευών (BYOD)**							
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**

Νομική σημείωση (πνευματικά δικαιώματα και περιορισμοί χρήσης)

(C) 2025 Clarysec LLC. All rights reserved.

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: info@clarysec.com

Ευθυγραμμισμένη με πρότυπα και κανονιστικές απαιτήσεις

Πρότυπο/Κανονισμός	Ρήτρα/Άρθρο	Σχόλιο
ISO/IEC 27001:2022	5.2, 6.1, 7.5, 8	Εφαρμόζει ελέγχους ασφάλειας και απαιτήσεις συμμόρφωσης
ISO/IEC 27002:2022	5.10, 8.1, 8.5, 8	Παρέχει αναλυτικούς ελέγχους για τη διαχείριση κινητών συσκευών
NIST SP 800-53 Rev.5	AC-19, AC-17, CM-7, MP-5, SC-12	Έλεγχος πρόσβασης, απομακρυσμένη πρόσβαση, διαχείριση ρυθμίσεων και απαιτήσεις ασφάλειας για κινητές συσκευές
ΓΚΠΔ της ΕΕ	5(1)(f), 25, 32	Υποχρεωτικές απαιτήσεις για την ιδιωτικότητα, την κρυπτογράφηση δεδομένων και την ασφάλεια της επεξεργασίας
Οδηγία NIS2 της ΕΕ	21(2)(d)	Τεχνικά και οργανωτικά μέτρα προστασίας για κινητή πρόσβαση
Κανονισμός DORA της ΕΕ	9, 10	Απαιτήσεις διαχείρισης κινδύνων ΤΠΕ και ασφάλειας για κινητές συσκευές
COBIT 2019	APO13.02, DSS01.04, BAI09	Σχέδια ασφάλειας πληροφοριών, διαχείριση ρυθμίσεων περιουσιακών στοιχείων και έλεγχοι για περιβάλλοντα κινητής εργασίας

1. Σκοπός

1.1 Η παρούσα πολιτική καθορίζει τις απαιτήσεις ασφάλειας, συμμόρφωσης και λειτουργίας για τη χρήση κινητών συσκευών και προσωπικών συσκευών (BYOD) κατά την πρόσβαση σε συστήματα, εφαρμογές ή δεδομένα του οργανισμού.

1.2 Στόχος της είναι η διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των εταιρικών πληροφοριών στις οποίες αποκτάται πρόσβαση ή οι οποίες υφίστανται επεξεργασία μέσω κινητών τερματικών, συμπεριλαμβανομένων έξυπνων τηλεφώνων, tablets, φορητών υπολογιστών και υβριδικών συσκευών.

1.3 Η παρούσα πολιτική επιβάλλει επίσης τους τεχνικούς και διαδικαστικούς ελέγχους που απαιτούνται για τον μετριασμό κινδύνων όπως η διαρροή δεδομένων, η μη εξουσιοδοτημένη πρόσβαση, η απώλεια ή κλοπή συσκευής και ο συμβιβασμός εφαρμογών κινητών συσκευών.

1.4 Η παρούσα πολιτική υποστηρίζει τη συμμόρφωση με κανονιστικές και συμβατικές υποχρεώσεις, επιτρέποντας παράλληλα την ασφαλή κινητή εργασία για εργαζομένους, αναδόχους και εξουσιοδοτημένα τρίτα μέρη.

2. Πεδίο εφαρμογής

2.1 Η παρούσα πολιτική εφαρμόζεται σε όλο το προσωπικό, συμπεριλαμβανομένων εργαζομένων, αναδόχων, ασκουμένων και τρίτων παρόχων υπηρεσιών, που χρησιμοποιούν κινητές συσκευές για πρόσβαση σε εταιρικά δεδομένα, συστήματα, εφαρμογές ή πλατφόρμες επικοινωνίας.

2.2 Καλύπτει όλες τις κινητές υπολογιστικές συσκευές, συμπεριλαμβανομένων ενδεικτικά και όχι περιοριστικά των εξής:

2.2.1 Έξυπνα τηλέφωνα και tablets (iOS, Android κ.λπ.)

2.2.2 Φορητούς υπολογιστές και ultrabooks (Windows, macOS, Linux)

2.2.3 Φορετές συσκευές και υβριδικές έξυπνες συσκευές με δυνατότητα συγχρονισμού δεδομένων

2.3 Εφαρμόζεται ανεξάρτητα από το αν η συσκευή ανήκει στην εταιρεία ή είναι προσωπική συσκευή που χρησιμοποιείται βάσει συμφωνίας BYOD.

2.4 Η πολιτική καλύπτει όλα τα κανάλια πρόσβασης, συμπεριλαμβανομένων VPN, εικονικών επιφανειών εργασίας, εφαρμογών νέφους, ηλεκτρονικού ταχυδρομείου, πλατφορμών συνεργασίας (π.χ. SharePoint, Teams) και εργαλείων συγχρονισμού αρχείων (π.χ. OneDrive, Dropbox, εφόσον είναι εγκεκριμένα).

2.5 Περιλαμβάνει τη χρήση σε καθεστώς τηλεργασίας, εντός εγκαταστάσεων, κατά τη διάρκεια ταξιδιών ή σε υβριδικές ρυθμίσεις εργασίας.

3. Στόχοι

3.1 Η μείωση του κινδύνου συμβιβασμού, διαρροής ή απώλειας δεδομένων λόγω μη ασφαλούς χρήσης κινητών συσκευών.

3.2 Η εφαρμογή συνεπών και εκτελεστών ελέγχων ασφάλειας σε όλα τα κινητά τερματικά, ανεξαρτήτως μοντέλου ιδιοκτησίας (εταιρικό ή BYOD).

3.3 Η διασφάλιση ότι η χρήση κινητών συσκευών συμμορφώνεται με το ISO/IEC 27001 και άλλα κανονιστικά πλαίσια που εφαρμόζονται στην ιδιωτικότητα, την προστασία δεδομένων και την κυβερνοασφάλεια.

3.4 Η διευκόλυνση της ασφαλούς ενσωμάτωσης των κινητών συσκευών στις λειτουργικές ροές, την επικοινωνία και τις ροές συνεργασίας του οργανισμού.

3.5 Η παροχή σαφώς καθορισμένων αρμοδιοτήτων και διαδικασιών για τη διαχείριση κινητών συσκευών (MDM), συμπεριλαμβανομένων της ένταξης, της απομακρυσμένης διαγραφής, της κρυπτογράφησης, της αυθεντικοποίησης και της παρακολούθησης.

3.6 Η προστασία των δικαιωμάτων ιδιωτικότητας των προσώπων που χρησιμοποιούν τις δικές τους συσκευές, με παράλληλη διασφάλιση της προστασίας των ευαίσθητων πληροφοριών του οργανισμού.

4. Ρόλοι και αρμοδιότητες

4.1 Επικεφαλής Ασφάλειας Πληροφοριών (CISO) / Επικεφαλής Ασφάλειας Πληροφορικής

4.1.1 Καθορίζει την πολιτική και τα τεχνικά πρότυπα για τη χρήση κινητών συσκευών και BYOD.

4.1.2 Ασκεί εποπτεία στη συμμόρφωση, στην απόκριση σε περιστατικά και στη διαχείριση εξαιρέσεων για τους ελέγχους κινητών συσκευών.

4.1.3 Συντονίζεται με το Τμήμα Ανθρώπινου Δυναμικού και τη Νομική Υπηρεσία, ώστε η εφαρμογή της πολιτικής να είναι νομικά ορθή και οργανωτικά ευθυγραμμισμένη.

4.2 Διαχειριστές ΤΠ / Διαχειριστής MDM

4.2.1 Διαχειρίζονται τη χορήγηση πρόσβασης, την ένταξη και τη διαμόρφωση κινητών συσκευών μέσω λύσεων MDM.

4.2.2 Εφαρμόζουν ελέγχους σε επίπεδο συσκευής (π.χ. κρυπτογράφηση, κωδικοί PIN, έλεγχοι εφαρμογών).

4.2.3 Εκτελούν απομακρυσμένη διαγραφή, κλείδωμα συσκευής και ανάκληση πρόσβασης όταν 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 ανασκοπείται τουλάχιστον ετησίως από τον Επικεφαλής Ασφάλειας Πληροφοριών ή τον ορισμένο Υπεύθυνο Ασφάλειας Πληροφοριών, ώστε να διασφαλίζεται η ευθυγράμμιση με:

9.1.1 Αλλαγές σε πλατφόρμες κινητών λειτουργικών συστημάτων, τεχνολογίες MDM ή πρότυπα αυθεντικοποίησης

9.1.2 Κανονιστικές ή συμβατικές αλλαγές που επηρεάζουν την προστασία δεδομένων σε κινητές συσκευές (π.χ. ΓΚΠΔ της ΕΕ, Κανονισμός DORA της ΕΕ, Οδηγία NIS2 της ΕΕ)

9.1.3 Αναθεωρήσεις των συνόλων ελέγχων ISO/IEC 27001:2022, ISO/IEC 27002:2022 ή NIST SP 800-53 Rev.5

9.1.4 Ανατροφοδότηση από ελέγχους, αναλύσεις μετά από περιστατικά ή αναφορές εργαζομένων

9.2 Έκτακτες ανασκοπήσεις μπορεί να ενεργοποιούνται από:

9.2.1 Περιστατικά ασφάλειας που αφορούν κινητές συσκευές ή πλατφόρμες BYOD

9.2.2 Ειδοποίηση προμηθευτή για ευπάθειες υψηλού κινδύνου σε υποστηριζόμενες πλατφόρμες

9.2.3 Εισαγωγή νέων εφαρμογών κινητών συσκευών ή πλατφορμών συνεργασίας που χρησιμοποιούνται για επιχειρησιακή λειτουργία

9.3 Οι επικαιροποιήσεις της πολιτικής πρέπει να:

9.3.1 Τεκμηριώνονται στο ιστορικό εκδόσεων της πολιτικής

9.3.2 Γνωστοποιούνται σε όλο το προσωπικό και στους επηρεαζόμενους αναδόχους

9.3.3 Επιβεβαιώνονται εκ νέου με επικαιροποιημένη αναγνώριση αποδοχής από όλους τους χρήστες BYOD

9.4 Όλες οι ανασκοπήσεις και αναθεωρήσεις πρέπει να εγκρίνονται επίσημα από την Ανώτατη Διοίκηση και να καταγράφονται στο Μητρώο Αλλαγών Πολιτικής.

10. Συναφείς πολιτικές και διασυνδέσεις

10.1 Η παρούσα πολιτική αλληλεξαρτάται με αρκετές βασικές πολιτικές στο πλαίσιο του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ISMS) του οργανισμού. Ενδεικτικά, οι κύριες διασυνδέσεις περιλαμβάνουν:

10.1.1 P1 – Πολιτική Ασφάλειας Πληροφοριών: Καθορίζει τις υπερκείμενες αρχές διακυβέρνησης για όλους τους ελέγχους ασφάλειας πληροφοριών, συμπεριλαμβανομένων εκείνων που διέπουν τη χρήση κινητών συσκευών.

10.1.2 P3 – Πολιτική Αποδεκτής Χρήσης: Καθορίζει τις επιτρεπόμενες συμπεριφορές και τους περιορισμούς σχετικά με τη χρήση της τεχνολογίας, οι οποίοι εφαρμόζονται άμεσα στην κινητή πρόσβαση και το BYOD.

10.1.3 P9 – Πολιτική Τηλεργασίας: Καλύπτει πρόσθετες υποχρεώσεις ασφάλειας για περιβάλλοντα κινητής εργασίας, συμπληρώνοντας τους ειδικούς ελέγχους για κινητές συσκευές που ορίζονται στην παρούσα πολιτική.

10.1.4 P13 – Πολιτική Ταξινόμησης και Επισήμανσης Δεδομένων: Διέπει τον τρόπο με τον οποίο πρέπει να γίνεται η διαχείριση δεδομένων σε κινητές συσκευές βάσει του επιπέδου ταξινόμησης, επηρεάζοντας την αποθήκευση, τη μεταφορά και την εφαρμογή της κρυπτογράφησης.

10.1.5 P22 – Πολιτική Καταγραφής και Παρακολούθησης: Υποστηρίζει τη συλλογή και ανασκόπηση των αρχείων καταγραφής κινητής πρόσβασης για τον εντοπισμό ανωμαλιών ή παραβιάσεων.

10.1.6 P30 – Πολιτική Αντιμετώπισης Περιστατικών (P30): Καθορίζει τον τρόπο με τον οποίο τα περιστατικά που σχετίζονται με κινητές συσκευές (π.χ. απώλεια συσκευής, μη εξουσιοδοτημένη πρόσβαση) αντιμετωπίζονται και κλιμακώνονται.

10.1.7 P33 – Πολιτική Ελέγχου και Παρακολούθησης Συμμόρφωσης: Παρέχει τη βάση για περιοδικούς ελέγχους της συμμόρφωσης ασφάλειας κινητών συσκευών, συμπεριλαμβανομένης της τήρησης της πολιτικής BYOD.

11. Πρότυπα και πλαίσια αναφοράς

11.1 Η παρούσα πολιτική είναι ευθυγραμμισμένη με διεθνώς αναγνωρισμένα πλαίσια κυβερνοασφάλειας και νομικές υποχρεώσεις, προκειμένου να διασφαλίζεται η ασφαλής χρήση κινητών συσκευών και προσωπικών τεχνολογιών (BYOD) σε εταιρικά περιβάλλοντα.

11.2 ISO/IEC 27001:

11.2.1 Ρήτρα 5.10 – Αποδεκτή χρήση πληροφοριών και περιουσιακών στοιχείων: Απαιτεί ελέγχους για την υπεύθυνη χρήση εταιρικών περιουσιακών στοιχείων, συμπεριλαμβανομένων των κινητών συσκευών.

11.2.2 Ρήτρα 5.11 – Τηλεργασία: Διέπει ασφαλείς πρακτικές κατά την πρόσβαση σε συστήματα εκτός των εγκαταστάσεων της εταιρείας.

11.2.3 Ρήτρα 5.12 – Χρήση κινητών συσκευών: Επιβάλλει ελέγχους βάσει κινδύνου για κινητά τερματικά και ρυθμίσεις BYOD.

11.2.4 Ρήτρα 5.13 – Μεταφορά πληροφοριών: Επιβάλλει την προστασία των πληροφοριών που μεταφέρονται μέσω κινητών καναλιών.

11.3 ISO/IEC 27002:2022 – Έλεγχοι 5.10 έως 5.13:

11.3.1 Οι έλεγχοι του Παραρτήματος Α 5.10 έως 5.13 καθορίζουν τον τρόπο με τον οποίο πρέπει να εφαρμόζονται, στο πλαίσιο ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ISMS), η κινητή πρόσβαση, η κρυπτογράφηση, η παρακολούθηση και ο μετριασμός απώλειας. Οι έλεγχοι αυτοί παρέχουν αναλυτική καθοδήγηση υλοποίησης για την ασφάλεια κινητών τερματικών, την εφαρμογή απομόνωσης σε container, την παρακολούθηση της ακεραιότητας των συσκευών και τη διασφάλιση ρυθμίσεων BYOD με σεβασμό στην ιδιωτικότητα.

11.4 NIST SP 800-53 Rev.5:

11.4.1 AC-19 – Έλεγχος πρόσβασης για κινητές συσκευές: Καθορίζει βασικές γραμμές προστασίας, συμπεριλαμβανομένων της κρυπτογράφησης, της αυθεντικοποίησης και της εφαρμογής MDM.

11.4.2 AC-17 – Απομακρυσμένη πρόσβαση: Απαιτεί ασφαλή αυθεντικοποίηση και προστασία συνεδρίας για απομακρυσμένους χρήστες κινητών συσκευών.

11.4.3 CM-7 – Ελάχιστη λειτουργικότητα: Υποστηρίζει την αφαίρεση περιττών εφαρμογών και λειτουργιών από κινητά τερματικά για μείωση του κινδύνου.

11.4.4 MP-5 – Προστασία μεταφοράς μέσων: Διέπει την ασφαλή μεταφορά δεδομένων από κινητά συστήματα προς εξωτερικούς προορισμούς ή υπηρεσίες νέφους.

11.4.5 SC-12 – Καθιέρωση κρυπτογραφικών κλειδιών: Επιβάλλει τη χρήση ασφαλών κρυπτογραφικών πρωτοκόλλων για κινητή επικοινωνία και αποθήκευση.

11.5 ΓΚΠΔ της ΕΕ (2016/679):

11.5.1 Άρθρο 5(1)(f) – Ακεραιότητα και εμπιστευτικότητα: Απαιτεί από τους οργανισμούς να προστατεύουν τα δεδομένα προσωπικού χαρακτήρα σε κινητές συσκευές έναντι μη εξουσιοδοτημένης ή παράνομης πρόσβασης.

11.5.2 Άρθρο 25 – Προστασία δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού: Απαιτεί η ιδιωτικότητα να ενσωματώνεται στις διαδικασίες BYOD και MDM.

11.5.3 Άρθρο 32 – Ασφάλεια της επεξεργασίας: Επιβάλλει ελέγχους βάσει κινδύνου (π.χ. κρυπτογράφηση, αυθεντικοποίηση, έλεγχος πρόσβασης) για δεδομένα προσωπικού χαρακτήρα σε κινητές πλατφόρμες.

11.6 Οδηγία NIS2 της ΕΕ (2022/2555):

11.6.1 Άρθρο 21(2)(d): Επιβάλλει η κινητή πρόσβαση σε κρίσιμα συστήματα και πληροφορίες να προστατεύεται μέσω κατάλληλων τεχνικών και οργανωτικών μέτρων, όπως έλεγχος τερματικών, κρυπτογράφηση και παρακολούθηση.

11.7 Κανονισμός DORA της ΕΕ (2022/2554):

11.7.1 Άρθρο 9 – Πλαίσιο διαχείρισης κινδύνων ΤΠΕ: Απαιτεί από τις οντότητες του χρηματοπιστωτικού τομέα να μετριάζουν τους κινδύνους κινητής και απομακρυσμένης πρόσβασης στο πλαίσιο της λειτουργικής ανθεκτικότητας.

11.7.2 Άρθρο 10 – Απαιτήσεις ασφάλειας συστημάτων ΤΠΕ: Απαιτεί ασφαλή αρχιτεκτονική κινητών συσκευών, παρακολούθηση και μηχανισμούς απόκρισης για κυβερνοαπειλές που προέρχονται από κινητές συσκευές.

11.8 COBIT 2019:

11.8.1 APO13.02 – Καθιέρωση και διατήρηση σχεδίου ασφάλειας πληροφοριών: Απαιτεί η χρήση κινητών συσκευών, συμπεριλαμβανομένου του BYOD, να ενσωματώνεται στις στρατηγικές ασφάλειας του οργανισμού.

11.8.2 DSS01.04 – Διαχείριση διαμόρφωσης και ακεραιότητας περιουσιακών στοιχείων: Εφαρμόζεται στον έλεγχο των ρυθμίσεων και στην ασφαλή εγκατάσταση κινητών συσκευών.

11.8.3 BAI09.01 – Καθιέρωση και διατήρηση ελέγχων: Υποστηρίζει την εφαρμογή τεχνικών και διαδικαστικών δικλίδων ασφαλείας για ασφαλή κινητή και απομακρυσμένη λειτουργία.