					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P34S					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**

Ευθυγραμμισμένη με πρότυπα και κανονιστικές απαιτήσεις

Πρότυπο/Κανονισμός	**Ρήτρα/Άρθρο**	**Σχόλιο**
ISO/IEC 27001:2022	Ρήτρες 5.1, 5.2, 6.1, 6.2, 8	Γενικές απαιτήσεις ΣΔΑΠ και ελέγχων για κινητές συσκευές/BYOD
ISO/IEC 27002:2022	Έλεγχοι 5.10–5.13	Αναλυτικοί έλεγχοι για κινητές συσκευές/BYOD και απομακρυσμένη πρόσβαση
NIST SP 800-53 Rev.5	AC-19, AC-20, CM-6, MP-7	Ομοσπονδιακοί έλεγχοι για συσκευές, μέσα και ρυθμίσεις παραμέτρων
ΓΚΠΔ της ΕΕ	Άρθρο 5(1)(f)	Προστασία δεδομένων προσωπικού χαρακτήρα και κινητών τερματικών
Οδηγία NIS2 της ΕΕ	Άρθρο 21(2)(d)	Προστασία επιχειρησιακά κρίσιμων συσκευών, συμπεριλαμβανομένου του BYOD
Κανονισμός DORA της ΕΕ	Άρθρα 9, 10	Κίνδυνος ΤΠΕ / επιχειρησιακή συνέχεια για κινητά τερματικά
COBIT 2019	APO13, DSS01, DSS05	Διακυβέρνηση ΤΠ, λειτουργία και έλεγχοι υπηρεσιών ασφάλειας

1. Σκοπός

1.1. Η παρούσα πολιτική καθορίζει τις υποχρεωτικές απαιτήσεις ασφάλειας για τη χρήση κινητών συσκευών, συμπεριλαμβανομένων smartphones, tablets και φορητών υπολογιστών, κατά την πρόσβαση σε εταιρικές πληροφορίες, συστήματα ή υπηρεσίες.

1.2. Ρυθμίζει επίσης τη χρήση προσωπικών συσκευών (BYOD), ώστε να διασφαλίζεται η προστασία των δεδομένων πελατών και των επιχειρησιακών δεδομένων, ανεξάρτητα από την ιδιοκτησία της συσκευής.

1.3. Η παρούσα πολιτική επιβάλλει συνεπείς δικλίδες ασφαλείας για την κινητή πρόσβαση, υποστηρίζει την επίτευξη των στόχων πιστοποίησης κατά ISO/IEC 27001 και προλαμβάνει απώλεια δεδομένων ή περιστατικά παραβίασης της ασφάλειας λόγω απώλειας, κλοπής ή κακής χρήσης κινητών τερματικών.

1.4. Διασφαλίζει ότι εφαρμόζονται τόσο τεχνικά όσο και διαδικαστικά μέτρα ασφάλειας για τη χρήση κινητών συσκευών σε ΜΜΕ χωρίς αποκλειστικές ομάδες Πληροφορικής, συμπεριλαμβανομένων περιβαλλόντων τηλεργασίας και πλατφορμών που βασίζονται σε υπολογιστικό νέφος.

2. Πεδίο εφαρμογής

2.1. Η παρούσα πολιτική εφαρμόζεται σε όλους τους εργαζομένους, αναδόχους, ασκούμενους και παρόχους υπηρεσιών που:

2.1.1. Χρησιμοποιούν κινητή συσκευή για πρόσβαση, επεξεργασία ή αποθήκευση εταιρικών δεδομένων ή συστημάτων.

2.1.2. Συνδέονται σε εταιρικές υπηρεσίες, συμπεριλαμβανομένων ηλεκτρονικού ταχυδρομείου, κοινόχρηστων φακέλων, εφαρμογών νέφους ή εσωτερικών συστημάτων μέσω VPN.

2.2. Καλύπτει:

2.2.1. Όλες τις κινητές συσκευές: smartphones, tablets, φορητούς υπολογιστές (εταιρικά εκδιδόμενους ή προσωπικούς στο πλαίσιο BYOD).

2.2.2. Όλα τα λειτουργικά συστήματα (π.χ. iOS, Android, Windows, macOS).

2.2.3. Όλες τις τοποθεσίες (γραφείο, οικία, απομακρυσμένη εργασία, δημόσιοι χώροι).

2.3. Η πολιτική εφαρμόζεται σε όλα τα περιβάλλοντα εργασίας και τηρείται ανεξάρτητα από την ιδιοκτησία της συσκευής.

3. Στόχοι

3.1. Πρόληψη απώλειας δεδομένων: Να διασφαλίζεται ότι η χρήση κινητών συσκευών δεν εκθέτει ευαίσθητα εταιρικά δεδομένα ή δεδομένα πελατών σε μη εξουσιοδοτημένη πρόσβαση, κλοπή ή κακή χρήση.

3.2. Καθορισμός σαφών κανόνων για BYOD: Να καθορίζονται εφαρμοστέοι όροι για τη χρήση προσωπικών συσκευών για επιχειρησιακούς σκοπούς, με κατάλληλες νομικές και τεχνικές δικλίδες ασφαλείας.

3.3. Υποστήριξη κανονιστικής συμμόρφωσης: Να ικανοποιούνται οι απαιτήσεις των ISO/IEC 27001, ΓΚΠΔ της ΕΕ, Οδηγίας NIS2 της ΕΕ και λοιπών νομικών υποχρεώσεων μέσω εφαρμόσιμων πρακτικών ασφάλειας για κινητές συσκευές.

3.4. Ελαχιστοποίηση επιχειρησιακού κινδύνου: Να μειώνεται η πιθανότητα επιχειρησιακής διακοπής που προκαλείται από κακή χρήση, παραβίαση ή αστοχία κινητών συσκευών.

3.5. Διατήρηση της εμπιστοσύνης των πελατών: Να αποδεικνύεται σε πελάτες και συνεργάτες ότι τα δεδομένα τους παραμένουν προστατευμένα ακόμη και όταν η πρόσβαση πραγματοποιείται από κινητές ή προσωπικές συσκευές.

4. Ρόλοι και αρμοδιότητες

4.1. Γενικός Διευθυντής (GM):

4.1.1. Διατηρεί τη συνολική λογοδοσία για την παρούσα πολιτική.

4.1.2. Εγκρίνει κάθε χρήση κινητής πρόσβασης και BYOD στα εταιρικά συστήματα.

4.1.3. Διασφαλίζει ότι οι συμφωνίες BYOD υπογράφονται, τηρούνται και παρακολουθούνται.

4.1.4. Επαληθεύει ότι οι εξωτερικοί πάροχοι υπηρεσιών Πληροφορικής εφαρμόζουν τις απαιτούμενες δικλίδες προστασίας για κινητές συσκευές.

4.2. Ορισμένο προσωπικό ή υποστήριξη Πληροφορικής:

4.2.1. Υποστηρίζει τη ρύθμιση, καταχώριση και παραμετροποίηση των κινητών συσκευών που χρησιμοποιούνται για εργασία.

4.2.2. Εφαρμόζει ελέγχους πρόσβασης σχετικούς με κινητές συσκευές, περιορισμούς εφαρμογών και ελέγχους παρακολούθησης.

4.2.3. Υποστηρίζει την απόκριση σε περιστατικά που αφορούν κινητές συσκευές (απώλεια, κλοπή, παραβίαση).

[... 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. Ετήσια ανασκόπηση

9.1.1. Ο Γενικός Διευθυντής (GM) πρέπει να ανασκοπεί την παρούσα πολιτική τουλάχιστον μία φορά κάθε 12 μήνες.

9.1.2. Η ανασκόπηση πρέπει να επιβεβαιώνει τη συνεχιζόμενη ευθυγράμμιση με τις απαιτήσεις του ISO/IEC 27001, τις εξελισσόμενες τεχνολογίες κινητών συσκευών και τις αλλαγές στις επιχειρησιακές λειτουργίες.

9.1.3. Οι επικαιροποιήσεις πρέπει επίσης να λαμβάνουν υπόψη πρόσφατα περιστατικά, αποτελέσματα ελέγχων ή κανονιστικές εξελίξεις (π.χ. ΓΚΠΔ της ΕΕ, Οδηγία NIS2 της ΕΕ, Κανονισμός DORA της ΕΕ).

9.2. Γεγονότα ενεργοποίησης ενδιάμεσης ανασκόπησης

9.2.1. Η παρούσα πολιτική πρέπει να επικαιροποιείται άμεσα εάν συμβεί οποιοδήποτε από τα ακόλουθα:

9.2.1.1. Σημαντικό περιστατικό ασφάλειας κινητής συσκευής (π.χ. παραβίαση μέσω χαμένης ή παραβιασμένης συσκευής).

9.2.1.2. Αλλαγή στις υποστηριζόμενες πλατφόρμες ή στα εργαλεία διαχείρισης κινητών συσκευών.

9.2.1.3. Νομική ή κανονιστική αλλαγή που επηρεάζει τη χρήση προσωπικών συσκευών ή την προστασία δεδομένων.

9.2.1.4. Εισαγωγή νέων εφαρμογών, υπηρεσιών ή εργαλείων τρίτων μερών που χρησιμοποιούνται σε κινητές συσκευές.

9.3. Τεκμηρίωση αλλαγών

9.3.1. Όλες οι ανασκοπήσεις και οι επικαιροποιήσεις πρέπει να τεκμηριώνονται, συμπεριλαμβανομένων της ημερομηνίας ανασκόπησης, των αλλαγών που πραγματοποιήθηκαν και της έγκρισης του GM.

9.3.2. Πρέπει να διατηρείται ιστορικό ελέγχου εκδόσεων για ελεγκτικούς σκοπούς.

9.4. Επικοινωνία και πρόσβαση

9.4.1. Ο GM πρέπει να διασφαλίζει ότι όλοι οι χρήστες (εργαζόμενοι, ανάδοχοι, τρίτα μέρη) ενημερώνονται για τις αλλαγές.

9.4.2. Οι επικαιροποιημένες εκδόσεις πρέπει να είναι εύκολα προσβάσιμες, όπως σε κοινόχρηστους φακέλους ή εσωτερικές πλατφόρμες.

10. Συναφείς πολιτικές και διασυνδέσεις

10.1. Η παρούσα πολιτική αποτελεί μέρος του συνολικού πλαισίου πολιτικών ασφάλειας πληροφοριών της ΜΜΕ και πρέπει να εφαρμόζεται σε συνδυασμό με τις ακόλουθες:

10.1.1. P4S – Πολιτική Ελέγχου Πρόσβασης: Καθορίζει απαιτήσεις για τη διαχείριση ασφαλούς πρόσβασης σε συστήματα, συμπεριλαμβανομένων όσων είναι προσβάσιμα μέσω κινητών συσκευών. Επιβάλλει ορθή πρακτική διαχείρισης κωδικών πρόσβασης και έλεγχο συνεδριών.

10.1.2. P8S – Πολιτική Εκπαίδευσης Ευαισθητοποίησης για την Ασφάλεια Πληροφοριών: Διασφαλίζει ότι οι χρήστες εκπαιδεύονται στην ασφαλή χρήση κινητών συσκευών, στην αναφορά περιστατικών και στους όρους BYOD.

10.1.3. P17S – Πολιτική Προστασίας Δεδομένων και Ιδιωτικότητας: Καθορίζει τον χειρισμό δεδομένων προσωπικού χαρακτήρα και εταιρικών δεδομένων σε κινητές πλατφόρμες σύμφωνα με τον ΓΚΠΔ της ΕΕ, ιδίως όταν προσωπικές συσκευές χρησιμοποιούνται για εργασία.

10.1.4. P9S – Πολιτική Τηλεργασίας: Ευθυγραμμίζεται με τις απαιτήσεις χρήσης κινητών συσκευών κατά την εργασία εκτός εγκαταστάσεων ή από την οικία, συμπεριλαμβανομένου του χειρισμού συσκευών και των δικλίδων πρόσβασης δικτύου.

10.1.5. P30S – Πολιτική Αντιμετώπισης Περιστατικών: Παρέχει το πλαίσιο απόκρισης για περιστατικά που σχετίζονται με κινητές συσκευές, συμπεριλαμβανομένων συσκευών που έχουν παραβιαστεί ή χαθεί.

10.2. Οι συναφείς αυτές πολιτικές λειτουργούν συμπληρωματικά ώστε να συγκροτούν ένα πλήρες σύνολο ελέγχων για την ασφάλεια κινητών συσκευών σε ΜΜΕ χωρίς αποκλειστικό προσωπικό Πληροφορικής, διασφαλίζοντας δυνατότητα εφαρμογής, διαφάνεια και ετοιμότητα για πιστοποίηση.

11. Πρότυπα και πλαίσια αναφοράς

11.1. Η παρούσα πολιτική υποστηρίζει πλήρη ευθυγράμμιση με τα ακόλουθα πρότυπα ασφάλειας και συμμόρφωσης:

11.2. ISO/IEC 27001:

11.2.1. Ρήτρα 5.1 – Ηγεσία και δέσμευση: Διασφαλίζει διοικητική εποπτεία και λογοδοσία για την κινητή πρόσβαση και το BYOD.

11.2.2. Ρήτρα 6.1 – Ενέργειες για την αντιμετώπιση κινδύνων: Απαιτεί την αξιολόγηση και αντιμετώπιση των κινδύνων ασφάλειας που σχετίζονται με κινητές συσκευές.

11.2.3. Ρήτρα 8.1 – Επιχειρησιακός σχεδιασμός και έλεγχος: Απαιτεί συνεπείς διαδικασίες κινητής πρόσβασης για την προστασία των επιχειρησιακών δεδομένων.

11.3. ISO/IEC 27002:

11.3.1. Έλεγχοι 5.10 (Χρήση κινητών συσκευών), 5.11 (Τηλεργασία), 5.12 (Απομακρυσμένη πρόσβαση) και 5.13 (BYOD): Παρέχουν κατευθύνσεις εφαρμογής για τη διαχείριση των κινδύνων συσκευών στο πλαίσιο μικρής επιχείρησης.

11.4. NIST SP 800-53 Rev.5:

11.4.1. AC-19 – Έλεγχος πρόσβασης για κινητές συσκευές: Απαιτεί ρυθμίσεις ασφάλειας για εξουσιοδοτημένη χρήση κινητών συσκευών.

11.4.2. AC-20 – Χρήση εξωτερικών συστημάτων: Ρυθμίζει τους κινδύνους BYOD και απομακρυσμένης πρόσβασης.

11.4.3. CM-6 – Ρυθμίσεις παραμέτρων: Επιβάλλει ασφαλείς προεπιλεγμένες και προσαρμοσμένες ρυθμίσεις σε κινητές πλατφόρμες.

11.4.4. MP-7 – Χρήση μέσων: Καλύπτει την ορθή χρήση και τους περιορισμούς για κινητή αποθήκευση και πρόσβαση σε δεδομένα.

11.5. ΓΚΠΔ της ΕΕ (2016/679):

11.5.1. Άρθρο 5(1)(f) – Ακεραιότητα και εμπιστευτικότητα: Απαιτεί προστασία των δεδομένων μέσω κατάλληλης ασφάλειας των δεδομένων προσωπικού χαρακτήρα, ιδίως σε κινητές πλατφόρμες.

11.5.2. Άρθρο 32 – Ασφάλεια της επεξεργασίας: Επιβάλλει τη χρήση κατάλληλων τεχνικών και οργανωτικών μέτρων για την ασφάλεια δεδομένων στα οποία αποκτάται πρόσβαση ή τα οποία αποθηκεύονται σε κινητές συσκευές.

11.6. Οδηγία NIS2 της ΕΕ (2022/2555):

11.6.1. Άρθρο 21(2)(d) – Μέτρα ασφάλειας συσκευών: Απαιτεί ελέγχους ασφάλειας για υλικό και λογισμικό που χρησιμοποιούνται για πρόσβαση σε κρίσιμα επιχειρησιακά συστήματα, συμπεριλαμβανομένων προσωπικών συσκευών.

11.7. Κανονισμός DORA της ΕΕ (2022/2554):

11.7.1. Άρθρο 9 – Πλαίσιο διαχείρισης κινδύνων ΤΠΕ: Απαιτεί την προστασία κινητών τερματικών που χρησιμοποιούνται για κρίσιμες επιχειρησιακές επικοινωνίες και υπηρεσίες νέφους.

11.7.2. Άρθρο 10 – Επιχειρησιακή συνέχεια ΤΠΕ: Επιβάλλει τη διατήρηση ασφαλούς πρόσβασης σε επιχειρησιακά συστήματα ακόμη και κατά τη διάρκεια διαταραχών ή τηλεργασίας.

11.8. COBIT 2019:

11.8.1. APO13 – Διαχείριση ασφάλειας: Απαιτεί από τον οργανισμό να εφαρμόζει πολιτικές για κινητές συσκευές και BYOD ευθυγραμμισμένες με τον επιχειρησιακό κίνδυνο.

11.8.2. DSS01 – Διαχείριση λειτουργιών: Διασφαλίζει την τεχνική εφαρμογή μηχανισμών ασφαλούς πρόσβασης.

11.8.3. DSS05 – Διαχείριση υπηρεσιών ασφάλειας: Ρυθμίζει τη συμμετοχή τρίτων μερών στη διατήρηση ασφαλών περιβαλλόντων κινητών συσκευών και στον συντονισμό της απόκρισης σε περιστατικά.