					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P09S					Τίτλος εγγράφου: **Πολιτική Τηλεργασίας**							
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, 6.2, 8	
ISO/IEC 27002:2022	Έλεγχος 6	
NIST SP 800-53 Rev.5	AC-17, AC-2	
Οδηγία NIS2 της ΕΕ	Άρθρα 21(2)(b), 21(2)(h)	Οδηγία NIS2 της ΕΕ
Κανονισμός DORA της ΕΕ	Άρθρο 9	Κανονισμός DORA της ΕΕ
COBIT 2019	DSS05, APO13	COBIT 2019
ΓΚΠΔ της ΕΕ	Άρθρο 32	ΓΚΠΔ της ΕΕ

1. Σκοπός

1.1 Η παρούσα πολιτική καθορίζει τις απαιτήσεις ασφάλειας για εργαζομένους και αναδόχους που εργάζονται εξ αποστάσεως, συμπεριλαμβανομένης της εργασίας από την οικία, από κοινόχρηστους χώρους εργασίας ή κατά τη διάρκεια ταξιδιών.

1.2 Στόχος της είναι η προστασία της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των επιχειρησιακών πληροφοριών στις οποίες παρέχεται πρόσβαση εκτός περιβαλλόντων που ελέγχονται από την εταιρεία.

1.3 Η παρούσα πολιτική διασφαλίζει τη συμμόρφωση με διεθνή πρότυπα και μειώνει κινδύνους, όπως η μη εξουσιοδοτημένη πρόσβαση, η απώλεια δεδομένων και η διακοπή υπηρεσιών.

2. Πεδίο εφαρμογής

2.1 Η παρούσα πολιτική εφαρμόζεται σε όλα τα μέλη του προσωπικού (εργαζομένους, αναδόχους, συμβούλους και προσωρινό προσωπικό) που αποκτούν πρόσβαση σε συστήματα, δίκτυα ή δεδομένα της εταιρείας κατά την εργασία εκτός εγκαταστάσεων.

2.2 Καλύπτει:

2.2.1 Τη χρήση εταιρικών και προσωπικών συσκευών

2.2.2 Την πρόσβαση μέσω VPN, απομακρυσμένης επιφάνειας εργασίας ή υπηρεσιών υπολογιστικού νέφους

2.2.3 Τον ασφαλή χειρισμό πληροφοριών εκτός των εγκαταστάσεων της εταιρείας

2.2.4 Την παρακολούθηση, τη διαχείριση εξαιρέσεων και την εφαρμογή της πολιτικής

2.3 Εφαρμόζεται τόσο σε καθεστώς πλήρους όσο και μερικής τηλεργασίας, συμπεριλαμβανομένης της έκτακτης απομακρυσμένης πρόσβασης.

3. Στόχοι

3.1 Να αποτρέπεται η μη εξουσιοδοτημένη πρόσβαση σε συστήματα της εταιρείας ή σε ευαίσθητα δεδομένα κατά την τηλεργασία.

3.2 Να διασφαλίζεται ότι οι συσκευές και οι δίαυλοι επικοινωνίας που χρησιμοποιούνται εκτός γραφείου πληρούν τις απαιτήσεις της βασικής γραμμής ασφάλειας.

3.3 Να διατηρείται ο έλεγχος των δικαιωμάτων απομακρυσμένης πρόσβασης και της παρακολούθησης.

3.4 Να παρέχονται σαφείς οδηγίες στους εργαζομένους και στους προϊσταμένους για ασφαλείς πρακτικές τηλεργασίας.

3.5 Να τηρούνται οι απαιτήσεις των ISO, NIS2, ΓΚΠΔ, DORA και COBIT για την απομακρυσμένη και κινητή εργασία.

4. Ρόλοι και αρμοδιότητες

4.1 Γενικός Διευθυντής

4.1.1 Εγκρίνει τις ρυθμίσεις τηλεργασίας και παρακολουθεί τη συμμόρφωση.

4.1.2 Κλιμακώνει περιστατικά ασφάλειας ή επαναλαμβανόμενη μη συμμόρφωση.

4.1.3 Ανασκοπεί εξαιρέσεις και διασφαλίζει την παρακολούθηση των περιστατικών.

4.2 Τμήμα Πληροφορικής ή Εξωτερικός Πάροχος Υπηρεσιών Πληροφορικής

4.2.1 Ρυθμίζει την ασφαλή απομακρυσμένη πρόσβαση (π.χ. VPN, πολυπαραγοντική αυθεντικοποίηση).

4.2.2 Εφαρμόζει ασφάλεια τερματικών σημείων, κρυπτογράφηση και ρυθμίσεις παραμετροποίησης συσκευών.

4.2.3 Υποστηρίζει τους χρήστες και διερευνά τυχόν τεχνικά ζητήματα ασφάλειας.

[... 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 πολιτικής

9.1.1 Ο Γενικός Διευθυντής και το Τμήμα Πληροφορικής πρέπει να ανασκοπούν την παρούσα πολιτική ετησίως, ώστε να παραμένει ευθυγραμμισμένη με τεχνολογικές, εργασιακές και νομικές αλλαγές.

9.2 Μηχανισμοί έγκαιρης επικαιροποίησης

9.2.1 Απαιτείται άμεση ανασκόπηση μετά από:

9.2.1.1 Σημαντικό περιστατικό ασφάλειας που σχετίζεται με την τηλεργασία

9.2.1.2 Αλλαγές στις απαιτήσεις NIS2, ΓΚΠΔ ή DORA

9.2.1.3 Μετάβαση σε νέα τεχνολογία απομακρυσμένης πρόσβασης (π.χ. διαφορετική πλατφόρμα VPN)

9.3 Έλεγχος εκδόσεων και αρχειοθέτηση

9.3.1 Όλες οι εκδόσεις της παρούσας πολιτικής πρέπει να είναι:

9.3.1.1 Χρονολογημένες και εγκεκριμένες από τον Γενικό Διευθυντή

9.3.1.2 Αριθμημένες ως προς την έκδοση

9.3.1.3 Αρχειοθετημένες για τουλάχιστον τρία έτη

9.4 Επικοινωνία προς το προσωπικό

9.4.1 Οι επικαιροποιήσεις της πολιτικής πρέπει να γνωστοποιούνται σε όλους τους απομακρυσμένους χρήστες. Για κάθε ουσιώδη αλλαγή απαιτείται αποδοχή.

10. Σχετικές πολιτικές και διασυνδέσεις

10.1 Η παρούσα πολιτική συνδέεται και υποστηρίζει τα ακόλουθα:

10.1.1 P2S – Πολιτική Ρόλων και Αρμοδιοτήτων Διακυβέρνησης: Καθορίζει ποιος εξουσιοδοτεί και ασκεί εποπτεία στην απομακρυσμένη πρόσβαση

10.1.2 P4S – Πολιτική Ελέγχου Πρόσβασης: Καθορίζει τη ρύθμιση της ασφαλούς απομακρυσμένης πρόσβασης και τις διαδικασίες ανάκλησης

10.1.3 P6S – Πολιτική Διαχείρισης Κινδύνων: Παρακολουθεί και αξιολογεί τους κινδύνους που σχετίζονται με την πρόσβαση εκτός εγκαταστάσεων

10.1.4 P8S – Πολιτική Ευαισθητοποίησης και Εκπαίδευσης για την Ασφάλεια Πληροφοριών: Εκπαιδεύει τους χρήστες στους κινδύνους της τηλεργασίας και στις βέλτιστες πρακτικές

10.1.5 P30S – Πολιτική Αντιμετώπισης Περιστατικών: Διαχειρίζεται την απόκριση σε περιστατικά απομακρυσμένης πρόσβασης, όπως διαρροή διαπιστευτηρίων ή απώλεια συσκευής

11. Πρότυπα και πλαίσια αναφοράς

11.1 ISO/IEC 27001

11.1.1 Ρήτρα 6.1 – Σχεδιασμός βάσει κινδύνου για σενάρια απομακρυσμένης πρόσβασης

11.1.2 Ρήτρα 6.2 – Καλύπτει τις αρμοδιότητες του Ανθρώπινου Δυναμικού σε πλαίσια κινητής και απομακρυσμένης εργασίας

11.1.3 Ρήτρα 8.1 – Επιχειρησιακός σχεδιασμός και έλεγχος απομακρυσμένων διεργασιών

11.2 ISO/IEC 27002

11.2.1 Έλεγχος 6.7 – Παρέχει πρακτική καθοδήγηση για την ασφάλεια της απομακρυσμένης και κινητής εργασίας

11.3 NIST SP 800-53 Rev.5

11.3.1 AC-17 – Έλεγχος απομακρυσμένης πρόσβασης, προστασία συνόδων και παρακολούθηση ασφάλειας

11.3.2 AC-2 – Διαχείριση λογαριασμών για χρήστες εκτός εγκαταστάσεων

11.4 ΓΚΠΔ της ΕΕ

11.4.1 Άρθρο 32 – Απαιτεί προστασία δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού, συμπεριλαμβανομένων των ρυθμίσεων απομακρυσμένης πρόσβασης

11.5 Οδηγία NIS2 της ΕΕ

11.5.1 Άρθρο 21(2)(b) – Απαιτεί την ασφαλή χρήση δικτύων και πληροφοριακών συστημάτων

11.5.2 Άρθρο 21(2)(h) – Προβλέπει μέτρα ασφάλειας που σχετίζονται με το ανθρώπινο δυναμικό, συμπεριλαμβανομένων ελέγχων εκτός εγκαταστάσεων

11.6 Κανονισμός DORA της ΕΕ

11.6.1 Άρθρο 9 – Απαιτεί από τις χρηματοοικονομικές οντότητες να διατηρούν την ανθεκτικότητα των ΤΠΕ σε όλους τους τρόπους λειτουργίας, συμπεριλαμβανομένης της απομακρυσμένης πρόσβασης

11.7 COBIT 2019

11.7.1 DSS05 – Διαχείριση Υπηρεσιών Ασφάλειας: Περιλαμβάνει την ασφάλεια τερματικών σημείων και ασφαλείς πρακτικές τηλεργασίας

11.7.2 APO13 – Διαχείριση Ασφάλειας: Διασφαλίζει την ασφαλή χορήγηση πρόσβασης και την εποπτεία κινδύνων για κινητή και απομακρυσμένη πρόσβαση