					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P21S					Τίτλος εγγράφου: **Πολιτική Ασφάλειας Δικτύου**							
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**

Ευθυγράμμιση με πρότυπα και κανονιστικές απαιτήσεις

Πρότυπο/Κανονισμός	Ρήτρα/Άρθρο	Σχόλιο
ISO/IEC 27001:2022	Clause 8	-
ISO/IEC 27002:2022	Control 8	-
NIST SP 800-53 Rev.5	AC-4, SC-7	-
ΓΚΠΔ της ΕΕ	Άρθρο 32	-
Οδηγία NIS2 της ΕΕ	Άρθρα 21(2)(d), (e)	-
Κανονισμός DORA της ΕΕ	Άρθρα 9, 10	-
COBIT 2019	DSS05.02, APO13	-

1. Σκοπός

1.1. Σκοπός της παρούσας πολιτικής είναι να διασφαλίζει ότι όλες οι εσωτερικές και εξωτερικές επικοινωνίες δικτύου προστατεύονται από μη εξουσιοδοτημένη πρόσβαση, παραποίηση, υποκλοπή ή κακή χρήση, μέσω σαφώς καθορισμένων ελέγχων ασφάλειας.

1.2. Καθορίζει κανόνες για τον ασφαλή σχεδιασμό, τη χρήση και τη διαχείριση της υποδομής δικτύου, συμπεριλαμβανομένων των δρομολογητών, των ασύρματων σημείων πρόσβασης, των συνδέσεων απομακρυσμένης πρόσβασης και των τμηματοποιημένων δικτύων.

1.3. Στοχεύει στην ελαχιστοποίηση της έκθεσης σε απειλές που προέρχονται από το διαδίκτυο, στη διασφάλιση της εμπιστευτικότητας των δεδομένων που διαβιβάζονται μέσω εσωτερικών και εξωτερικών δικτύων και στη διατήρηση της διαθεσιμότητας κρίσιμων υπηρεσιών.

1.4. Η παρούσα πολιτική υποστηρίζει την πιστοποίηση κατά ISO/IEC 27001:2022 και συμβάλλει άμεσα στην εκπλήρωση νομικών και κανονιστικών υποχρεώσεων βάσει του ΓΚΠΔ της ΕΕ, της Οδηγίας NIS2 της ΕΕ και του Κανονισμού DORA της ΕΕ, ενώ παρέχει τεχνική διασφάλιση σε πελάτες και ελεγκτές.

2. Πεδίο εφαρμογής

2.1. Η παρούσα πολιτική εφαρμόζεται σε όλα τα στοιχεία του δικτύου πληροφορικής του οργανισμού, συμπεριλαμβανομένων των εξής:

2.1.1. Ενσύρματη και ασύρματη υποδομή στις εγκαταστάσεις γραφείων

2.1.2. Δρομολογητές, μεταγωγείς, σημεία πρόσβασης, τείχη προστασίας και πύλες

2.1.3. Συνδέσεις απομακρυσμένης πρόσβασης (VPN, διαχείριση φορητών συσκευών), συμπεριλαμβανομένων VPN, RDP και σηράγγων νέφους

2.1.4. Εφαρμογές που βασίζονται σε περιβάλλον νέφους, στις οποίες η πρόσβαση γίνεται από εσωτερικά ή εξωτερικά δίκτυα

2.1.5. Συσκευές που συνδέονται στο δίκτυο από εργαζομένους, αναδόχους, παρόχους υπηρεσιών τρίτων μερών ή επισκέπτες

2.2. Η παρούσα πολιτική διέπει τόσο τα φυσικά όσο και τα λογικά τμήματα δικτύου, συμπεριλαμβανομένων ζωνών επισκεπτών, συσκευών IoT και συστημάτων back-office.

2.3. Η πολιτική καλύπτει όλο το προσωπικό που έχει πρόσβαση στο δίκτυο του οργανισμού, συμπεριλαμβανομένων των εξής:

2.3.1. Εσωτερικοί εργαζόμενοι

2.3.2. Τηλεργαζόμενοι και υβριδικά εργαζόμενο προσωπικό

2.3.3. Εξωτερικοί προμηθευτές, σύμβουλοι και τρίτοι πάροχοι υπηρεσιών

2.3.4. Επισκέπτες που χρησιμοποιούν προσωρινή πρόσβαση Wi-Fi

3. Στόχοι

3.1. Να διασφαλίζεται ότι το δίκτυο του οργανισμού προστατεύεται από μη εξουσιοδοτημένη πρόσβαση και εξωτερικές κυβερνοαπειλές

3.2. Να εφαρμόζεται κατάλληλη τμηματοποίηση μεταξύ έμπιστων και μη έμπιστων δικτύων (π.χ. Wi-Fi επισκεπτών, πρόσβαση προμηθευτών)

3.3. Να παρέχεται ασφαλής απομακρυσμένη συνδεσιμότητα χωρίς να τίθενται σε κίνδυνο τα εσωτερικά συστήματα

3.4. Να προλαμβάνεται η διάδοση κακόβουλου λογισμικού και η εξαγωγή δεδομένων μέσω διαύλων δικτύου

3.5. Να παρέχονται παρακολούθηση, ειδοποίηση και έλεγχος της δραστηριότητας δικτύου προς υποστήριξη της ανίχνευσης και κλιμάκωσης περιστατικών και της συμμόρφωσης

3.6. Να διασφαλίζεται ότι μόνο εγκεκριμένες και ασφαλείς συσκευές επιτρέπεται να συνδέονται στα εσωτερικά δίκτυα

3.7. Να εκπληρώνονται οι υποχρεώσεις βάσει ISO 27001, ΓΚΠΔ της ΕΕ και συναφών πλαισίων κυβερνοασφάλειας

4. Ρόλοι και αρμοδιότητες

4.1. Γενικός Διευθυντής (GM)

4.1.1. Έχει την κυριότητα της παρούσας πολιτικής και διασφαλίζει ότι διατίθενται οι κατάλληλοι πόροι για τον ασφαλή σχεδιασμό και τη διαχείριση του δικτύου

4.1.2. Ανασκοπεί εξαιρέσεις από τους ελέγχους ασφάλειας δικτύου και εγκρίνει συμφωνίες πρόσβασης προμηθευτών στο δίκτυο

4.1.3. Ανασκοπεί περιστατικά ή ευρήματα ελέγχου που σχετίζονται με αδυναμίες ασφάλειας δικτύου

4.2. Πάροχος Υποστήριξης Πληροφορικής / Εσωτερική λειτουργία Πληροφορικής

4.2.1. Υλοποιεί, παραμετροποιεί και συντηρεί όλα τα τείχη προστασίας, τους δρομολογητές, τους μεταγωγείς και τους ασύρματους ελεγκτές

4.2.2. Διαχειρίζεται την τμηματοποίηση μεταξύ εσωτερικών δικτύων, δικτύων επισκεπτών και εξωτερικών δικτύων

4.2.3. Παρακολουθεί τα αρχεία καταγραφής και τις ειδοποιήσεις για απόπειρες μη εξουσιοδοτημένης πρόσβασης ή ανωμαλίες δικτύου

4.2.4. Διασφαλίζει ότι οι ενημερώσεις υλικολογισμικού και οι αλλαγές ρυθμίσεων εφαρμόζονται με ασφαλή και έγκαιρο τρόπο

[... 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. Η παρούσα πολιτική πρέπει να ανασκοπείται τουλάχιστον μία φορά ετησίως από τον Γενικό Διευθυντή σε συνεργασία με τον Πάροχο Υποστήριξης Πληροφορικής και τον Υπεύθυνο Ιδιωτικότητας.

9.2. Εναύσματα ενδιάμεσης ανασκόπησης

9.2.1. Η ανασκόπηση της πολιτικής πρέπει επίσης να ενεργοποιείται από τα ακόλουθα:

9.2.1.1. Σημαντικές αλλαγές στην αρχιτεκτονική δικτύου (π.χ. νέα συστήματα VPN ή τείχους προστασίας)

9.2.1.2. Περιστατικό σχετιζόμενο με το δίκτυο (π.χ. εισβολή, εξάπλωση ransomware ή εξαγωγή δεδομένων)

9.2.1.3. Νομικές, κανονιστικές ή πλαισιακές επικαιροποιήσεις που επηρεάζουν την προστασία δικτύου

9.2.1.4. Νέες πλατφόρμες προμηθευτών που απαιτούν εναλλακτικές μεθόδους πρόσβασης ή πρωτόκολλα

9.3. Διαχείριση εκδόσεων και τεκμηρίωση

9.3.1. Οι αναθεωρήσεις της πολιτικής πρέπει να καταγράφονται με αριθμό έκδοσης, ημερομηνία και σύνοψη αλλαγών

9.3.2. Οι προηγούμενες εκδόσεις πρέπει να αρχειοθετούνται για διάστημα τουλάχιστον 3 ετών

9.3.3. Οι επικαιροποιήσεις πρέπει να γνωστοποιούνται στους επηρεαζόμενους εργαζομένους, με απαιτούμενη επιβεβαίωση παραλαβής όπου εισάγονται σημαντικές αλλαγές συμπεριφοράς

10. Συναφείς πολιτικές και διασυνδέσεις

10.1. Η παρούσα πολιτική πρέπει να εφαρμόζεται σε συνδυασμό με τις ακόλουθες πολιτικές ασφάλειας για ΜΜΕ:

10.1.1. P9S – Πολιτική Τηλεργασίας: Εφαρμόζει ασφαλείς μεθόδους απομακρυσμένης πρόσβασης, απαιτήσεις VPN και προστασία τερματικών για χρήστες εκτός εγκαταστάσεων.

10.1.2. P12S – Πολιτική Διαχείρισης Περιουσιακών Στοιχείων: Διασφαλίζει ότι όλα τα συστήματα που είναι συνδεδεμένα στο δίκτυο αναγνωρίζονται, κατηγοριοποιούνται και παρακολουθούνται με επικαιροποιημένη κατάσταση ασφάλειας.

10.1.3. P17S – Πολιτική Προστασίας Δεδομένων και Ιδιωτικότητας: Διασφαλίζει ότι η τμηματοποίηση δικτύου, οι έλεγχοι πρόσβασης και η καταγραφή υποστηρίζουν τις αρχές ιδιωτικότητας και προστασίας δεδομένων βάσει του ΓΚΠΔ της ΕΕ.

10.1.4. P22S – Πολιτική Καταγραφής και Παρακολούθησης: Καθορίζει απαιτήσεις για τη συλλογή και ανασκόπηση αρχείων καταγραφής από συσκευές δικτύου, απομακρυσμένες συνδέσεις και ασύρματους ελεγκτές.

10.1.5. P30S – Πολιτική Αντιμετώπισης Περιστατικών: Ορίζει τις απαιτούμενες ενέργειες για την απόκριση σε παραβιάσεις δικτύου, απόπειρες μη εξουσιοδοτημένης πρόσβασης ή διάδοση κακόβουλου λογισμικού μέσω εσωτερικών δικτύων.

11. Πρότυπα και πλαίσια αναφοράς

11.1. ISO/IEC 27001

11.1.1. Clause 8.1 – Απαιτεί την εφαρμογή ελέγχων για τη διασφάλιση ασφαλών και ανθεκτικών λειτουργιών, συμπεριλαμβανομένων των δικτύων.

11.2. ISO/IEC 27002

11.2.1. Control 8.20 – Παρέχει τεχνική και διαδικαστική καθοδήγηση για την ασφάλεια της πρόσβασης δικτύου, της τμηματοποίησης και της παρακολούθησης.

11.3. NIST SP 800-53 Rev.5

11.3.1. AC-4 – Επιβάλλει τον έλεγχο της ροής πληροφοριών εντός των δικτύων και μεταξύ συστημάτων.

11.3.2. SC-7 – Απαιτεί προστασία περιμέτρου, ασφαλή δρομολόγηση και τμηματοποίηση δικτύου για τη μείωση του κινδύνου μη εξουσιοδοτημένης πρόσβασης.

11.4. ΓΚΠΔ της ΕΕ

11.4.1. Άρθρο 32 – Απαιτεί κατάλληλα τεχνικά και οργανωτικά μέτρα για τη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας δικτυωμένων συστημάτων και υπηρεσιών που επεξεργάζονται προσωπικά δεδομένα.

11.5. Οδηγία NIS2 της ΕΕ

11.5.1. Άρθρο 21(2)(d) – Επιβάλλει τεχνικά μέτρα βάσει κινδύνου, συμπεριλαμβανομένης της ασφάλειας δικτύου και του ελέγχου πρόσβασης.

11.5.2. Άρθρο 21(2)(e) – Απαιτεί τμηματοποίηση και απομόνωση συστημάτων για την αποτροπή διάδοσης κυβερνοπεριστατικών.

11.6. Κανονισμός DORA της ΕΕ

11.6.1. Άρθρο 9 – Απαιτεί από τους οργανισμούς να εφαρμόζουν ελέγχους διαχείρισης κινδύνων ΤΠΕ, συμπεριλαμβανομένων εκείνων για ασφαλή δίκτυα και επικοινωνίες.

11.6.2. Άρθρο 10 – Απαιτεί οι στρατηγικές ψηφιακής ανθεκτικότητας να περιλαμβάνουν προστασία της υποδομής δικτύου και της απομακρυσμένης συνδεσιμότητας.

11.7. COBIT 2019

11.7.1. DSS05.02 – Απαιτεί αποτελεσματική προστασία της υποδομής πληροφορικής και των περιβαλλόντων δικτύου από εσωτερικές και εξωτερικές απειλές.

11.7.2. APO13.01 – Απαιτεί στρατηγικές διαχείρισης κινδύνων που περιλαμβάνουν τμηματοποίηση δικτύου και παρακολούθηση ως μέρος του μετριασμού απειλών.