					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P21					Τίτλος εγγράφου: **Πολιτική Ασφάλειας Δικτύων**							
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	Ρήτρα 8	N/A
ISO/IEC 27002:2022	Έλεγχοι 8.20-8.22	N/A
NIST SP 800-53 Rev.5	SC-7, AC-4, SC-32	N/A
ΓΚΠΔ της ΕΕ	Άρθρο 32	N/A
Οδηγία NIS2 της ΕΕ	Άρθρο 21(2)(d)	N/A
Κανονισμός DORA της ΕΕ	Άρθρο 9	N/A
COBIT 2019	DSS01.03, DSS05.01, MEA03	N/A

1. Σκοπός

1.1 Σκοπός της παρούσας πολιτικής είναι να καθορίσει τις απαιτήσεις του οργανισμού για την προστασία των εσωτερικών και εξωτερικών δικτύων του από μη εξουσιοδοτημένη πρόσβαση, διακοπή υπηρεσιών, υποκλοπή δεδομένων και κακή χρήση.

1.2 Διασφαλίζει ότι το σύνολο της δικτυακής υποδομής —συμπεριλαμβανομένων φυσικών, εικονικών, νεφοϋπολογιστικών και υβριδικών υποδομών— προστατεύεται μέσω πολυεπίπεδων ελέγχων, όπως η τμηματοποίηση δικτύου, η εφαρμογή κανόνων τείχους προστασίας, η ασφαλής δρομολόγηση και η κεντρική παρακολούθηση.

1.3 Η παρούσα πολιτική επιβάλλει τις απαιτήσεις της Ρήτρας 8.1 του ISO/IEC 27001 και των ελέγχων 8.20 έως 8.22 του Παραρτήματος Α, διασφαλίζοντας συμμόρφωση με τις εφαρμοστέες νομικές και κανονιστικές υποχρεώσεις σύμφωνα με το Άρθρο 32 του ΓΚΠΔ της ΕΕ, το Άρθρο 21 της Οδηγίας NIS2 της ΕΕ και το Άρθρο 9 του Κανονισμού DORA της ΕΕ.

2. Πεδίο εφαρμογής

2.1 Η παρούσα πολιτική εφαρμόζεται σε όλα τα δίκτυα και τα συναφή στοιχεία υποδομής, συμπεριλαμβανομένων των εξής:

2.1.1 Δρομολογητές, μεταγωγείς, ασύρματα σημεία πρόσβασης και τείχη προστασίας

2.1.2 Εικονικά δίκτυα σε περιβάλλον νέφους (π.χ. AWS VPC, Azure VNET), συγκεντρωτές VPN και συστήματα SD-WAN

2.1.3 Εσωτερικά LAN, ζώνες DMZ, διαδρομές απομακρυσμένης πρόσβασης και διασυνδέσεις μεταξύ εγκαταστάσεων ή με τρίτα μέρη

2.1.4 Υποστηρικτικά συστήματα, όπως DNS, DHCP, διακομιστές μεσολάβησης και συσκευές παρακολούθησης

2.2 Η πολιτική είναι δεσμευτική για όλο το προσωπικό και τους τρίτους παρόχους υπηρεσιών που διαχειρίζονται, ρυθμίζουν, παρακολουθούν ή διασυνδέονται με τα δίκτυα του οργανισμού, είτε εντός εγκαταστάσεων είτε σε περιβάλλον νέφους.

2.3 Όλα τα συστήματα και οι εφαρμογές που είναι συνδεδεμένα στα δίκτυα του οργανισμού — ανεξαρτήτως τοποθεσίας ή ιδιοκτησίας— πρέπει να συμμορφώνονται με τις παρούσες απαιτήσεις ασφάλειας δικτύων.

3. Στόχοι

3.1 Να διασφαλίζεται η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα των δεδομένων που διακινούνται μέσω των δικτύων, με ισχυρούς ελέγχους πρόσβασης, ασφαλή δρομολόγηση και παρακολούθηση.

3.2 Να αποτρέπεται η μη εξουσιοδοτημένη πρόσβαση, η πλευρική μετακίνηση και η εκμετάλλευση δικτυακών πόρων μέσω της εφαρμογής τμηματοποίησης, ζωνοποίησης και προστασίας περιμέτρου.

3.3 Να διατηρούνται συνεπείς διαμορφώσεις δικτύου, βασισμένες σε πρότυπα του κλάδου και πληροφορίες απειλών, ώστε να αντιμετωπίζονται οι εξελισσόμενες κυβερνοαπειλές.

3.4 Να προστατεύονται οι εξωτερικές επικοινωνίες, η διασυνδεσιμότητα με περιβάλλον νέφους και η απομακρυσμένη πρόσβαση με χρήση κρυπτογραφημένων διαύλων, ισχυρής αυθεντικοποίησης και επικύρωσης τερματικών σημείων.

3.5 Να παρέχεται ορατότητα στη δραστηριότητα του δικτύου μέσω κεντρικής καταγραφής, επιθεώρησης δικτυακής κίνησης σε πραγματικό χρόνο και αυτοματοποιημένης ειδοποίησης.

3.6 Να διασφαλίζεται η κανονιστική συμμόρφωση με την ευθυγράμμιση όλων των λειτουργιών δικτύου με τις απαιτήσεις των ISO/IEC 27001:2022, ΓΚΠΔ της ΕΕ, Οδηγίας NIS2 της ΕΕ, Κανονισμού DORA της ΕΕ και COBIT 2019.

4. Ρόλοι και αρμοδιότητες

4.1 Επικεφαλής Ασφάλειας Πληροφοριών (CISO)

4.1.1 Έχει την κυριότητα της παρούσας πολιτικής και διασφαλίζει ότι ανασκοπείται και ευθυγραμμίζεται με τη συνολική στρατηγική κυβερνοασφάλειας του οργανισμού.

4.1.2 Εγκρίνει τα μοντέλα τμηματοποίησης δικτύου, τα σύνολα κανόνων τείχους προστασίας για ευαίσθητα συστήματα και τα αιτήματα εξαίρεσης.

4.2 Υπεύθυνος Ασφάλειας Δικτύων / Επικεφαλής Ασφάλειας Υποδομών

4.2.1 Διαχειρίζεται την αρχιτεκτονική άμυνας δικτύου, συμπεριλαμβανομένων τειχών προστασίας, συστημάτων ανίχνευσης/αποτροπής εισβολών (IDS/IPS), VPN και ασφαλούς δρομολόγησης.

4.2.2 Ασκεί εποπτεία στην τμηματοποίηση δικτύου, στις αναθέσεις VLAN, στη ζωνοποίηση της κίνησης και στην εξωτερική διασυνδεσιμότητα.

4.2.3 Διασφαλίζει τη συνεχή ανασκόπηση του φιλτραρίσματος εισερχόμενης/εξερχόμενης κίνησης και την εφαρμογή της αρχής της μηδενικής εμπιστοσύνης σε όλα τα επίπεδα του δικτύου.

[... 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 ετησίως από τον Υπεύθυνο Ασφάλειας Δικτύων σε συνεργασία με τον Επικεφαλής Ασφάλειας Πληροφοριών και να επικαιροποιείται βάσει:

9.1.1 Αναδυόμενων κινδύνων (π.χ. νέες τεχνικές επιθέσεων, ευπάθειες πρωτοκόλλων)

9.1.2 Αλλαγών στην υποδομή (π.χ. μεταφορά υπηρεσιών σε περιβάλλον νέφους, υλοποιήσεις SD-WAN)

9.1.3 Κανονιστικών ή προτυπικών επικαιροποιήσεων που επηρεάζουν την προστασία δικτύων

9.1.4 Ευρημάτων ελέγχου, τάσεων περιστατικών ή υποβάθμισης απόδοσης που προκαλείται από ελέγχους

9.2 Οι ανασκοπήσεις πρέπει επίσης να ενεργοποιούνται από:

9.2.1 Σημαντικές αλλαγές στην αρχιτεκτονική δικτύου

9.2.2 Υλοποίηση νέων πλατφορμών τείχους προστασίας, VPN ή δικτύου σε περιβάλλον νέφους

9.2.3 Παροπλισμό κρίσιμων περιουσιακών στοιχείων ή αξιόπιστων ζωνών

9.3 Οι επικαιροποιήσεις πρέπει να καταγράφονται στο Μητρώο Ελέγχου Εγγράφων του ISMS και να κοινοποιούνται σε:

9.3.1 Τις ομάδες Υποδομών και Λειτουργίας Δικτύου

9.3.2 Το SOC και τις ομάδες Μηχανικής Ασφάλειας

9.3.3 Τις ομάδες εφαρμογών με εξαρτήσεις συστημάτων από δικτυακές ροές

9.3.4 Όλους τους προμηθευτές ή λοιπά τρίτα μέρη με ενεργές διασυνδέσεις

9.4 Όλες οι προηγούμενες εκδόσεις της πολιτικής πρέπει να αρχειοθετούνται με ασφαλή τρόπο, με σημειώσεις ιστορικού μεταβολών, ώστε να διατηρείται η δυνατότητα ελέγχου και η ιχνηλασιμότητα των αλλαγών.

10. Συναφείς πολιτικές και διασυνδέσεις

10.1 P1 - Πολιτική Ασφάλειας Πληροφοριών. Καθορίζει θεμελιώδεις αρχές ασφάλειας και επιβάλλει πολυεπίπεδη προστασία, συμπεριλαμβανομένων ελέγχων πρόσβασης και αντιμετώπισης απειλών σε επίπεδο δικτύου.

10.2 P4 - Πολιτική Ελέγχου Πρόσβασης. Διασφαλίζει ότι η τμηματοποίηση δικτύου εφαρμόζεται σε ευθυγράμμιση με τους ρόλους χρηστών, την αρχή του ελάχιστου προνομίου και τους κανόνες χορήγησης πρόσβασης.

10.3 P5 - Πολιτική Διαχείρισης Αλλαγών. Ρυθμίζει τις τροποποιήσεις τειχών προστασίας, τις προσαρμογές κανόνων VPN και τις αλλαγές δρομολόγησης μέσω τεκμηριωμένης και ελέγξιμης διαδικασίας.

10.4 P12 - Πολιτική Διαχείρισης Περιουσιακών Στοιχείων. Υποστηρίζει την αναγνώριση και την ταξινόμηση δικτυωμένων συστημάτων και διασφαλίζει ότι όλα τα συνδεδεμένα περιουσιακά στοιχεία διαχειρίζονται εντός των καθορισμένων από τις πολιτικές ορίων εφαρμογής.

10.5 P22 - Πολιτική Καταγραφής και Παρακολούθησης. Διέπει τη συλλογή, τη συσχέτιση και τη διατήρηση αρχείων καταγραφής δικτύου, συμπεριλαμβανομένων συμβάντων τείχους προστασίας, προσπαθειών πρόσβασης και ανιχνεύσεων ανωμαλιών.

10.6 P30 - Πολιτική Αντιμετώπισης Περιστατικών. Καθορίζει τις διαδικασίες κλιμάκωσης, περιορισμού και εξάλειψης ως απόκριση σε απειλές ή εισβολές που μεταφέρονται μέσω του δικτύου, όπως DDoS, πλευρική μετακίνηση ή μη εξουσιοδοτημένη πρόσβαση.

11. Πρότυπα και πλαίσια αναφοράς

11.1 Η παρούσα πολιτική ευθυγραμμίζεται με διεθνή πρότυπα και κανονιστικές απαιτήσεις που καθορίζουν την ασφαλή λειτουργία δικτύων, την τμηματοποίηση, την προστασία περιμέτρου και την ασφαλή απομακρυσμένη πρόσβαση.

11.2 ISO/IEC 27001

11.2.1 Ρήτρα 8.1 - Επιχειρησιακός σχεδιασμός και έλεγχος: Απαιτεί την ενσωμάτωση τεχνικών ελέγχων, συμπεριλαμβανομένων δικλίδων ασφάλειας δικτύου, στις επιχειρησιακές διαδικασίες.

11.3 ISO/IEC 27002:2022

11.3.1 Έλεγχοι 8.20-8.22: Παρέχουν καθοδήγηση για την προστασία δικτύων, την τμηματοποίηση υπηρεσιών και την ασφάλεια υπηρεσιών δικτύου μέσω ελέγχων πρόσβασης και παρακολούθησης.

11.4 NIST SP 800-53 Rev.5

11.4.1 SC-7 - Προστασία ορίων: Απαιτεί ελέγχους περιμέτρου, τμηματοποίηση και ασφαλείς διασυνδέσεις.

11.4.2 AC-4 - Επιβολή ροής πληροφοριών: Υποστηρίζει τη ζωνοποίηση και τους περιορισμούς κίνησης βάσει κανόνων.

11.4.3 SC-32 - Τμηματοποίηση πληροφοριακών συστημάτων: Προωθεί τον λογικό διαχωρισμό πληροφοριακών συστημάτων.

11.5 ΓΚΠΔ της ΕΕ (2016/679)

11.5.1 Άρθρο 32 - Ασφάλεια της επεξεργασίας: Απαιτεί τεχνικά μέτρα —όπως τείχη προστασίας και τμηματοποίηση— για την προστασία δεδομένων προσωπικού χαρακτήρα.

11.6 Οδηγία NIS2 της ΕΕ (2022/2555)

11.6.1 Άρθρο 21(2)(d): Απαιτεί αποτελεσματική ασφάλεια δικτύων και πληροφοριακών συστημάτων, προστασία περιμέτρου, ασφαλή διαμόρφωση και ελέγχους διαχωρισμού.

11.7 Κανονισμός DORA της ΕΕ (2022/2554)

11.7.1 Άρθρο 9 - Διαχείριση κινδύνων ΤΠΕ: Υποχρεώνει τις χρηματοοικονομικές οντότητες να προστατεύουν τα δίκτυα και τις διασυνδέσεις τους από μη εξουσιοδοτημένη πρόσβαση, διαρροή δεδομένων και επιχειρησιακή διακοπή.

11.8 COBIT 2019

11.8.1 DSS01.03 - Παρακολούθηση υποδομής: Απαιτεί προληπτικό έλεγχο της κατάστασης και της διασυνδεσιμότητας του δικτύου.

11.8.2 DSS05.01 - Προστασία από κακόβουλο λογισμικό: Περιλαμβάνει τμηματοποίηση και προστασία ορίων για την ελαχιστοποίηση της διάδοσης.

11.8.3 MEA03 - Παρακολούθηση, αξιολόγηση και εκτίμηση της συμμόρφωσης: Ενισχύει την εφαρμογή της πολιτικής δικτύου και τις αξιολογήσεις συμμόρφωσης.