					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P04S					Τίτλος εγγράφου: **Πολιτική Ελέγχου Πρόσβασης P04S**							
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 5	
ISO/IEC 27002:2022	Έλεγχοι: 5.15, 5.16, 5	
NIST SP 800-53 Rev.5	AC-1 έως AC-5	
ΓΚΠΔ της ΕΕ	Άρθρο 32	
Οδηγία NIS2 της ΕΕ	Άρθρο 21(2)(b)	
Κανονισμός DORA της ΕΕ	Άρθρο 9	
COBIT 2019	APO07, DSS	

1. Σκοπός

1.1. Η παρούσα πολιτική ορίζει τον τρόπο με τον οποίο ο οργανισμός διαχειρίζεται την πρόσβαση σε συστήματα, δεδομένα και εγκαταστάσεις, ώστε να διασφαλίζεται ότι μόνο εξουσιοδοτημένα πρόσωπα αποκτούν πρόσβαση σε πληροφορίες βάσει επιχειρησιακής ανάγκης.

1.2. Καθορίζει σαφείς κανόνες για τη χορήγηση, την τροποποίηση, την παρακολούθηση και την αφαίρεση της πρόσβασης χρηστών, με σκοπό την ελαχιστοποίηση του κινδύνου μη εξουσιοδοτημένης πρόσβασης και την υποστήριξη της συμμόρφωσης με την ισχύουσα νομοθεσία και τα εφαρμοστέα πρότυπα.

1.3. Η πολιτική καθιερώνει την αρχή του ελάχιστου απαιτούμενου δικαιώματος, σύμφωνα με την οποία η πρόσβαση περιορίζεται στο ελάχιστο αναγκαίο επίπεδο για την εκτέλεση των καθηκόντων κάθε θέσης.

2. Πεδίο εφαρμογής

2.1. Η παρούσα πολιτική εφαρμόζεται σε όλα τα πρόσωπα που χρησιμοποιούν ή διαχειρίζονται πρόσβαση στα πληροφοριακά συστήματα, τα δίκτυα, τα δεδομένα ή τις εγκαταστάσεις του οργανισμού, συμπεριλαμβανομένων των εξής:

2.1.1. Εργαζομένων

2.1.2. Εξωτερικών συνεργατών

2.1.3. Προσωρινού προσωπικού

2.1.4. Εξωτερικών παρόχων υπηρεσιών πληροφορικής

2.2. Καλύπτει την πρόσβαση σε:

2.2.1. Εταιρικές εφαρμογές, κοινόχρηστους φακέλους και βάσεις δεδομένων

2.2.2. Συστήματα ηλεκτρονικού ταχυδρομείου, VPN και απομακρυσμένης πρόσβασης

2.2.3. Υπηρεσίες νέφους που χρησιμοποιούνται για επιχειρησιακούς σκοπούς

2.2.4. Φυσική πρόσβαση σε ασφαλείς χώρους, όπως γραφεία ή αίθουσες διακομιστών

2.3. Η παρούσα πολιτική εφαρμόζεται σε όλες τις συσκευές (εταιρικές ή εγκεκριμένες συσκευές BYOD), τις πλατφόρμες και τις τοποθεσίες.

3. Στόχοι

3.1. Να διασφαλίζεται ότι τα δικαιώματα πρόσβασης χορηγούνται μόνο κατόπιν επίσημης έγκρισης, βάσει ρόλου και τεκμηριωμένης επιχειρησιακής ανάγκης.

3.2. Να αποτρέπεται η μη εξουσιοδοτημένη ή υπερβολική πρόσβαση σε ευαίσθητα δεδομένα, συστήματα ή υποδομές.

3.3. Να ορίζονται σαφείς διαδικασίες για τη χορήγηση, την τροποποίηση και την κατάργηση της πρόσβασης χρηστών.

3.4. Να απαιτούνται τακτικές ανασκοπήσεις πρόσβασης και αυτοματοποιημένη ή χειροκίνητη καταγραφή ενεργειών, προς υποστήριξη των ελεγκτικών δραστηριοτήτων.

3.5. Να υποστηρίζεται η τεχνική εφαρμογή των περιορισμών πρόσβασης μέσω κατάλληλων ρυθμίσεων και παρακολούθησης.

4. Ρόλοι και αρμοδιότητες

4.1. Γενικός Διευθυντής

4.1.1. Εγκρίνει την παρούσα πολιτική και διασφαλίζει τη διάθεση των απαραίτητων πόρων για την εφαρμογή αποτελεσματικών ελέγχων πρόσβασης.

4.1.2. Εγκρίνει εξαιρέσεις και ανασκοπεί τους ετήσιους ελέγχους πρόσβασης.

4.2. Υπεύθυνος Πληροφορικής / Εξωτερικός Πάροχος Υπηρεσιών Πληροφορικής

4.2.1. Διαχειρίζεται τη χορήγηση, την τροποποίηση και την κατάργηση λογαριασμών χρηστών.

4.2.2. Τηρεί Μητρώο Ελέγχου Πρόσβασης με όλες τις σχετικές ενέργειες (δημιουργία, αλλαγή, αφαίρεση).

4.2.3. Εφαρμόζει έλεγχο πρόσβασης βάσει ρόλων (RBAC) και ισχυρή αυθεντικοποίηση (π.χ. MFA).

4.2.4. Ανασκοπεί τα αρχεία καταγραφής πρόσβασης για ύποπτη δραστηριότητα και αναφέρει ζητήματα στον Γενικό Διευθυντή.

[... 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 της πολιτικής

9.1.1. Ο Υπεύθυνος Πληροφορικής πρέπει να ανασκοπεί την παρούσα πολιτική ετησίως. Κάθε μεταβολή στο νομικό, τεχνικό ή οργανωτικό πλαίσιο πρέπει να οδηγεί σε άμεση επικαιροποίησή της.

9.2. Εναύσματα ανασκόπησης

9.2.1. Η πολιτική πρέπει επίσης να ανασκοπείται εάν συμβεί οποιοδήποτε από τα ακόλουθα:

9.2.2. Σημαντικές αλλαγές συστημάτων ή μεταφορά υπηρεσιών σε περιβάλλον νέφους

9.2.3. Αλλαγές σε ρόλους ή στην οργανωτική δομή

9.2.4. Περιστατικό ασφάλειας που αφορά μη εξουσιοδοτημένη πρόσβαση

9.2.5. Κανονιστικές αλλαγές (π.χ. επικαιροποιήσεις του ΓΚΠΔ, της NIS2 ή του DORA)

9.3. Τεκμηρίωση και κοινοποίηση αλλαγών

9.3.1. Οι αναθεωρήσεις πρέπει να καταγράφονται με ιστορικό εκδόσεων, να εγκρίνονται από τον Γενικό Διευθυντή και να κοινοποιούνται σε όλο το επηρεαζόμενο προσωπικό.

9.4. Διαθεσιμότητα και εκπαίδευση

9.4.1. Η παρούσα πολιτική πρέπει να είναι διαθέσιμη σε όλο το προσωπικό και να παρέχεται σχετική εκπαίδευση κατά την ένταξη και, στη συνέχεια, σε ετήσια βάση.

10. Συναφείς πολιτικές και διασυνδέσεις

10.1. Η παρούσα πολιτική πρέπει να εφαρμόζεται σε συντονισμό με τις ακόλουθες πολιτικές SME, ώστε να διασφαλίζεται η πλήρης εφαρμογή ασφαλών πρακτικών πρόσβασης:

10.1.1. P3S – Πολιτική Αποδεκτής Χρήσης: Διασφαλίζει ότι οι χρήστες κατανοούν τη συμπεριφορά που είναι αποδεκτή κατά τη χρήση της χορηγημένης πρόσβασης.

10.1.2. P5S – Πολιτική Διαχείρισης Αλλαγών: Διασφαλίζει ότι τα δικαιώματα πρόσβασης ευθυγραμμίζονται με εγκεκριμένες αλλαγές συστημάτων.

10.1.3. P7S – Πολιτική Ένταξης και Αποχώρησης Προσωπικού: Ορίζει τα σημεία ενεργοποίησης για τη χορήγηση και την αφαίρεση πρόσβασης χρηστών.

10.1.4. P17S – Πολιτική Προστασίας Δεδομένων και Ιδιωτικότητας: Διασφαλίζει ότι οι έλεγχοι πρόσβασης ευθυγραμμίζονται με τα μέτρα προστασίας δεδομένων προσωπικού χαρακτήρα.

10.1.5. P30S – Πολιτική Απόκρισης σε Περιστατικά: Ορίζει τον τρόπο με τον οποίο διαχειρίζονται και διερευνώνται τα περιστατικά που σχετίζονται με την πρόσβαση (π.χ. κακή χρήση ή παραβιάσεις).

11. Πρότυπα και πλαίσια αναφοράς

11.1. ISO/IEC 27001

11.1.1. Ρήτρα 5.15 – Απαιτεί τυποποιημένες πολιτικές και διαδικασίες ελέγχου πρόσβασης.

11.2. ISO/IEC 27002

11.2.1. Έλεγχοι 5.15–5.17 – Παρέχουν αναλυτική καθοδήγηση για πρόσβαση βάσει ρόλων, διαχείριση του κύκλου ζωής χρηστών και διαχείριση προνομιούχας πρόσβασης.

11.3. NIST SP 800-53 Rev.

11.3.1. AC-1 έως AC-5 – Απαιτούν δομημένες πολιτικές για τη διαχείριση πρόσβασης, συμπεριλαμβανομένων της εξουσιοδότησης λογαριασμών, της ανασκόπησης και της παρακολούθησης.

11.4. ΓΚΠΔ της ΕΕ

11.4.1. Άρθρο 32 – Απαιτεί τεχνικά και οργανωτικά μέτρα (όπως η διαχείριση πρόσβασης) για τη διασφάλιση της ασφάλειας και της εμπιστευτικότητας των δεδομένων.

11.5. Οδηγία NIS2 της ΕΕ

11.5.1. Άρθρο 21(2)(b) – Επιβάλλει επιχειρησιακό έλεγχο πρόσβασης και συστήματα διαχείρισης ταυτοτήτων για την αποτροπή μη εξουσιοδοτημένης πρόσβασης σε συστήματα.

11.6. Κανονισμός DORA της ΕΕ

11.6.1. Άρθρο 9 – Τονίζει την ασφαλή διαχείριση κινδύνων ΤΠΕ, συμπεριλαμβανομένου του ισχυρού ελέγχου πρόσβασης για τις χρηματοοικονομικές οντότητες.

11.7. COBIT 2019

11.7.1. APO07 – Managed Security: Απαιτεί καθορισμένες και εφαρμοζόμενες αρμοδιότητες πρόσβασης.

11.7.2. DSS01 – Manage Operations: Περιλαμβάνει διαδικασίες για τη διαχείριση λογικής πρόσβασης και τη διατήρηση ασφαλών λειτουργικών περιβαλλόντων.