					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P04					Τίτλος εγγράφου: **Πολιτική Ελέγχου Πρόσβασης**							
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	Ρήτρες 5.15, 5.17, 5.18	Διαχείριση λογικής και φυσικής πρόσβασης
ISO/IEC 27002:2022	Έλεγχοι 8.2, 8.3	Έλεγχος πρόσβασης βάσει ρόλων και διαχείριση ταυτοτήτων
NIST SP 800-53 Rev. 5	AC-1 έως AC-20, IA-1 έως IA-8	Έλεγχοι λογαριασμών και πρόσβασης, ταυτότητας και αυθεντικοποίησης
ΓΚΠΔ της ΕΕ	Άρθρα 5(1)(f), 32(1)(b), Αιτιολογική σκέψη 39	Προστασία δεδομένων και ελαχιστοποίηση
Οδηγία NIS2 της ΕΕ	Άρθρο 21(2)(c–e)	Έλεγχος πρόσβασης, αυθεντικοποίηση χρηστών και προστασία στοιχείων ενεργητικού
Κανονισμός DORA της ΕΕ	Άρθρα 6, 9(2)	Πρόσβαση χρηστών στις ΤΠΕ και ισχυροί έλεγχοι, συμπεριλαμβανομένης της διαχείρισης τρίτων μερών
COBIT 2019	APO07, BAI03, DSS01, DSS05, MEA03	Ένταξη, λειτουργίες, παρακολούθηση και συμμόρφωση

1. Σκοπός

1.1 Η παρούσα πολιτική καθορίζει υποχρεωτικές αρχές, αρμοδιότητες και απαιτήσεις ελέγχου για τη διαχείριση της πρόσβασης σε πληροφοριακά συστήματα, εφαρμογές, φυσικές εγκαταστάσεις και δεδομένα σε όλο τον οργανισμό.

1.2 Διασφαλίζει ότι η πρόσβαση χορηγείται βάσει επιχειρησιακής ανάγκης, εργασιακού ρόλου και επιπέδου κινδύνου, με την εφαρμογή αρχών όπως το ελάχιστο απαιτούμενο δικαίωμα, η ανάγκη γνώσης και ο διαχωρισμός καθηκόντων.

1.3 Η πολιτική υποστηρίζει την εφαρμογή της ρήτρας 5.15 του ISO/IEC 27001:2022 και των σχετικών ελέγχων που διέπουν τη λογική και φυσική πρόσβαση, την αυθεντικοποίηση χρηστών και τη διαχείριση του κύκλου ζωής της πρόσβασης.

1.4 Η παρούσα πολιτική υποστηρίζει την προστασία των ψηφιακών και φυσικών πόρων από μη εξουσιοδοτημένη χρήση, κατάχρηση ή παραβίαση.

2. Πεδίο εφαρμογής

2.1 Η παρούσα πολιτική εφαρμόζεται σε όλους τους χρήστες, τα συστήματα και τις εγκαταστάσεις που εμπίπτουν στο πεδίο εφαρμογής του ΣΔΑΠ, συμπεριλαμβανομένων των εξής:

2.1.1 Εργαζόμενοι, ανάδοχοι, προμηθευτές και προσωρινό προσωπικό

2.1.2 Υποδομές εντός εγκαταστάσεων, συστήματα που φιλοξενούνται σε περιβάλλον νέφους και υβριδικά περιβάλλοντα

2.1.3 Όλα τα εταιρικά στοιχεία ενεργητικού — υλισμικό, λογισμικό, δεδομένα και ασφαλείς φυσικές περιοχές

2.1.4 Λογική πρόσβαση (π.χ. συστήματα, δίκτυα, εφαρμογές, διεπαφές προγραμματισμού εφαρμογών) και φυσική πρόσβαση (π.χ. κτίρια, κέντρα δεδομένων)

2.2 Διέπει την πρόσβαση σε όλο τον κύκλο ζωής της ταυτότητας και της αλληλεπίδρασης με πόρους, από την ένταξη και την παροχή πρόσβασης έως τις αλλαγές ρόλου και την αποχώρηση.

2.3 Η πολιτική καλύπτει επίσης τη χρήση προσωπικών συσκευών για επαγγελματικούς σκοπούς (BYOD) και την απομακρυσμένη πρόσβαση, διασφαλίζοντας ότι οι έλεγχοι εφαρμόζονται με συνέπεια ανεξαρτήτως τοποθεσίας και μοντέλου ιδιοκτησίας της συσκευής.

3. Στόχοι

3.1 Η εφαρμογή ασφαλών ελέγχων πρόσβασης βάσει ρόλων που υποστηρίζουν τη λειτουργική ακεραιότητα και τη συμμόρφωση με τις κανονιστικές απαιτήσεις.

3.2 Η διασφάλιση ότι τα δικαιώματα πρόσβασης εγκρίνονται, παρακολουθούνται και ανακαλούνται έγκαιρα και κατάλληλα.

3.3 Η αποτροπή μη εξουσιοδοτημένης πρόσβασης, κλιμάκωσης δικαιωμάτων ή διατήρησης παρωχημένων δικαιωμάτων πρόσβασης.

3.4 Η υποστήριξη των αρχών μηδενικής εμπιστοσύνης με προεπιλεγμένη άρνηση πρόσβασης, εκτός εάν έχει χορηγηθεί ρητή έγκριση και υπάρχει σχετική τεκμηρίωση.

3.5 Η παροχή διασφάλισης προς ελεγκτές και ενδιαφερόμενα μέρη μέσω τεκμηριωμένων, αυτοματοποιημένων ανασκοπήσεων πρόσβασης και της εφαρμογής της πολιτικής.

3.6 Η ενσωμάτωση του ελέγχου πρόσβασης στις επιχειρησιακές διαδικασίες, στα γεγονότα του κύκλου ζωής του ανθρώπινου δυναμικού και στις τεχνικές αρχιτεκτονικές.

4. Ρόλοι και αρμοδιότητες

4.1 Ανώτατη Διοίκηση

4.1.1 Εγκρίνει την Πολιτική Ελέγχου Πρόσβασης και διασφαλίζει επαρκή προϋπολογισμό και στελέχωση για την εφαρμογή της.

4.1.2 Ανασκοπεί τους κινδύνους που σχετίζονται με τον έλεγχο πρόσβασης κατά τις ανασκοπήσεις διοίκησης και κατανέμει τη λογοδοσία σε στρατηγικό επίπεδο.

4.2 CISO / Υπεύθυνος ΣΔΑΠ

4.2.1 Είναι υπεύθυνος για το πλαίσιο ελέγχου πρόσβασης και διασφαλίζει την ευθυγράμμισή του με το ISO/IEC 27001 και τα σχετικά πρότυπα.

4.2.2 Συντονίζει την εφαρμογή της πολιτικής, τις δοκιμές των ελέγχων και την αναφορά μετρικών ελέγχου πρόσβασης.

4.2.3 Ασκεί εποπτεία στη μοντελοποίηση πρόσβασης βάσει κινδύνου και παρακολουθεί συστημικά κενά ελέγχου.

[... 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 Εναύσματα και συχνότητα ανασκόπησης

9.1.1 Η παρούσα πολιτική πρέπει να ανασκοπείται:

9.1.1.1 Ετησίως, ή

9.1.1.2 Μετά από σημαντική αλλαγή στην υποδομή Πληροφορικής, στις κανονιστικές απαιτήσεις ή στο επίπεδο κινδύνου

9.1.1.3 Μετά από περιστατικά που αποκαλύπτουν αδυναμίες στους ελέγχους πρόσβασης

9.1.1.4 Όταν προκύπτουν σημαντικές μεταβολές στις τεχνολογίες αυθεντικοποίησης ή στις πλατφόρμες ταυτότητας

9.2 Αρμοδιότητα και διαδικασία ανασκόπησης

9.2.1 Ο CISO ή ο ορισμένος επικεφαλής του ΣΔΑΠ οφείλει να διαχειρίζεται τον κύκλο ανασκόπησης, ενσωματώνοντας:

9.2.1.1 Ευρήματα εσωτερικού ελέγχου

9.2.1.2 Αποτελέσματα και μετρικές ανασκόπησης πρόσβασης

9.2.1.3 Νομικές και κανονιστικές επικαιροποιήσεις

9.2.1.4 Αλλαγές στις τεχνολογικές πλατφόρμες

9.2.2 Κάθε αναθεώρηση πρέπει να εγκρίνεται από την Ανώτατη Διοίκηση και να γνωστοποιείται σε όλα τα ενδιαφερόμενα μέρη.

9.2.3 Οι επηρεαζόμενοι χρήστες ενδέχεται να υποχρεούνται να αποδεχθούν εκ νέου την πολιτική μετά από ουσιώδεις επικαιροποιήσεις.

9.3 Έλεγχος εκδόσεων και τεκμηρίωση

9.3.1 Η κύρια έκδοση τηρείται στο Αποθετήριο Εγγράφων ΣΔΑΠ με τα ακόλουθα μεταδεδομένα:

9.3.1.1 Αριθμός έκδοσης και αρχείο μεταβολών

9.3.1.2 Ημερομηνία έναρξης ισχύος και επόμενη ημερομηνία ανασκόπησης

9.3.1.3 Ιδιοκτήτης και αρμόδιο όργανο έγκρισης

9.3.1.4 Αρχεία διανομής και αποδοχής

9.3.2 Οι καταργημένες εκδόσεις πρέπει να αρχειοθετούνται και να παραμένουν προσβάσιμες για τουλάχιστον 3 έτη.

10. Συναφείς πολιτικές και διασυνδέσεις

10.1 Η παρούσα πολιτική εξαρτάται λειτουργικά από τις ακόλουθες πολιτικές και πρέπει να ερμηνεύεται σε συνδυασμό με αυτές:

10.1.1 P01 – Πολιτική Ασφάλειας Πληροφοριών: Καθορίζει τη δέσμευση του οργανισμού για την ασφάλεια και τις απαιτήσεις υψηλού επιπέδου για τον έλεγχο πρόσβασης.

10.1.2 P03 – Πολιτική Αποδεκτής Χρήσης: Καθορίζει τους κανόνες συμπεριφοράς για την πρόσβαση και τη λογοδοσία των χρηστών για την υπεύθυνη χρήση των συστημάτων.

10.1.3 P05 – Πολιτική Διαχείρισης Αλλαγών: Διέπει τον τρόπο με τον οποίο οι αλλαγές στις ρυθμίσεις πρόσβασης, στους ρόλους ή στις δομές ομάδων πρέπει να υλοποιούνται και να δοκιμάζονται με ασφάλεια.

10.1.4 P07 – Πολιτική Ένταξης και Αποχώρησης: Καθοδηγεί την έναρξη και την ανάκληση δικαιωμάτων πρόσβασης σύμφωνα με τα γεγονότα του κύκλου ζωής των χρηστών.

10.1.5 P11 – Πολιτική Διαχείρισης Λογαριασμών Χρηστών και Δικαιωμάτων: Εξειδικεύει τους ελέγχους σε επίπεδο λογαριασμού και συμπληρώνει την παρούσα πολιτική με τεχνικές οδηγίες εφαρμογής ελέγχου πρόσβασης.

10.2 Από κοινού, οι πολιτικές αυτές συγκροτούν ένα συνεκτικό και εφαρμόσιμο πλαίσιο διακυβέρνησης πρόσβασης σε όλες τις επιχειρησιακές μονάδες και τεχνολογίες.

11. Πρότυπα και πλαίσια αναφοράς

11.1 ISO/IEC 27001:2022:

11.1.1 Ρήτρα 5.15 – Έλεγχος Πρόσβασης: Η παρούσα πολιτική καλύπτει την απαίτηση ελέγχου της πρόσβασης σε πληροφορίες και λοιπά συναφή στοιχεία ενεργητικού, βάσει επιχειρησιακών απαιτήσεων και απαιτήσεων ασφάλειας πληροφοριών.

11.1.2 Ρήτρα 5.17 – Διαχείριση Ταυτοτήτων και Ρήτρα 5.18 – Πληροφορίες Αυθεντικοποίησης: Υλοποιούνται μέσω της παροχής ταυτοτήτων, των μηχανισμών αυθεντικοποίησης και των αναθέσεων δικαιωμάτων.

11.1.3 Έλεγχοι Παραρτήματος Α 8.2 (Πολιτική Ελέγχου Πρόσβασης) και 8.3 (Διαχείριση Ταυτοτήτων): Παρέχουν τη βάση για τους στόχους ελέγχου της παρούσας πολιτικής, συμπεριλαμβανομένης της πρόσβασης βάσει ρόλων, της ενσωμάτωσης του κύκλου ζωής χρηστών και της προστασίας της προνομιακής πρόσβασης.

11.2 NIST SP 800-53 Rev. 5:

11.2.1 Οικογένεια AC (AC-1 έως AC-20): Η παρούσα πολιτική υποστηρίζει τις απαιτήσεις ελέγχου πρόσβασης του NIST για φυσικά και λογικά συστήματα, συμπεριλαμβανομένου του καθορισμού πολιτικής (AC-1), της διαχείρισης λογαριασμών (AC-2) και του διαχωρισμού καθηκόντων (AC-5).

11.2.2 Οικογένεια IA (IA-1 έως IA-8): Παρέχει καθοδήγηση για την αυθεντικοποίηση ταυτότητας, την προστασία διαπιστευτηρίων και το MFA.

11.2.3 AU-2, AU-12: Οι απαιτήσεις καταγραφής και ελέγχου που εφαρμόζονται στο πλαίσιο της παρούσας πολιτικής υποστηρίζουν τη λογοδοσία των χρηστών και τη διερεύνηση περιστατικών.

11.2.4 PE-2 έως PE-6: Αφορούν περιορισμούς φυσικής πρόσβασης, τους οποίους η παρούσα πολιτική εφαρμόζει εν μέρει μέσω ελέγχων καρτών πρόσβασης και δικαιωμάτων πρόσβασης σε κτίρια.

11.3 ΓΚΠΔ της ΕΕ (2016/679):

11.3.1 Άρθρο 5(1)(f): Τα δεδομένα προσωπικού χαρακτήρα πρέπει να προστατεύονται από μη εξουσιοδοτημένη πρόσβαση. Η παρούσα πολιτική διασφαλίζει την τεχνική και διαδικαστική εφαρμογή της αρχής αυτής.

11.3.2 Άρθρο 32(1)(b): Απαιτεί την εφαρμογή ελέγχων πρόσβασης, ψευδωνυμοποίησης και κρυπτογράφησης για την αποτροπή μη εξουσιοδοτημένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα.

11.3.3 Αιτιολογική σκέψη 39: Επιβάλλει την ελαχιστοποίηση της πρόσβασης σε δεδομένα προσωπικού χαρακτήρα, η οποία εφαρμόζεται εδώ μέσω του ελάχιστου απαιτούμενου δικαιώματος και των απαιτήσεων αιτιολόγησης πρόσβασης.

11.4 Οδηγία NIS2 της ΕΕ (2022/2555):

11.4.1 Άρθρο 21(2)(c–e): Η παρούσα πολιτική επιτρέπει την εφαρμογή τεχνικών και οργανωτικών μέτρων για τον έλεγχο πρόσβασης, την αυθεντικοποίηση χρηστών και την προστασία στοιχείων ενεργητικού σε ουσιώδεις και σημαντικές οντότητες.

11.5 Κανονισμός DORA της ΕΕ (2022/2554):

11.5.1 Άρθρο 6: Απαιτεί πολιτικές διαχείρισης κινδύνων ΤΠΕ που περιλαμβάνουν ρητά τη διαχείριση πρόσβασης χρηστών και τους ελέγχους του κύκλου ζωής ταυτότητας. Η παρούσα πολιτική καλύπτει την απαίτηση αυτή για τους χρηματοοικονομικούς τομείς και τους τομείς υπηρεσιών ΤΠΕ.

11.5.2 Άρθρο 9(2): Η παρούσα πολιτική υποστηρίζει την εφαρμογή ισχυρών ελέγχων πρόσβασης ως μέρος της διαχείρισης υπηρεσιών ΤΠΕ τρίτων μερών και εντός ομίλου.

11.6 COBIT 2019:

11.6.1 APO07 – Διαχείριση Ανθρώπινου Δυναμικού: Εφαρμόζει ελέγχους ένταξης και αποχώρησης για την υποστήριξη της διακυβέρνησης πρόσβασης.

11.6.2 BAI03 – Διαχείριση Προσδιορισμού και Ανάπτυξης Λύσεων: Ενσωματώνει απαιτήσεις ελέγχου πρόσβασης στον σχεδιασμό συστημάτων και στις διαδικασίες αλλαγών.

11.6.3 DSS01 – Διαχείριση Λειτουργιών και DSS05 – Διαχείριση Υπηρεσιών Ασφάλειας: Διέπουν την εφαρμογή περιορισμών λογικής πρόσβασης και την παρακολούθηση παραβιάσεων.

11.6.4 MEA03 – Παρακολούθηση, Αξιολόγηση και Αποτίμηση Συμμόρφωσης: Υποστηρίζει μηχανισμούς ελέγχου και διασφάλισης για την επικύρωση της αποτελεσματικότητας του ελέγχου πρόσβασης.