					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P11					Τίτλος εγγράφου: **Πολιτική Διαχείρισης Λογαριασμών Χρηστών και Προνομίων**							
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 6.1.3, Ρήτρα 8	-
ISO/IEC 27002:2022	Έλεγχοι 5.15-5.18	-
NIST SP 800-53 Rev.5	AC-1, AC-2, AC-5, AC-6, IA-2 - IA-5, AU-2, AU-12	-
ΓΚΠΔ της ΕΕ	Άρθρα 5(1)(f), 32· Αιτιολογική σκέψη 39	-
Οδηγία NIS2 της ΕΕ	Άρθρα 21(2)(a, d), 21(3)	-
Κανονισμός DORA της ΕΕ	Άρθρα 5, 9	-
COBIT 2019	DSS01, DSS05, APO13	-

1. Σκοπός

1. Η παρούσα πολιτική θεσπίζει υποχρεωτικούς ελέγχους για τη διαχείριση λογαριασμών χρηστών και προνομίων σε όλα τα πληροφοριακά συστήματα και τις υπηρεσίες. Διασφαλίζει ότι η πρόσβαση στους πόρους του οργανισμού χορηγείται βάσει επαληθευμένης ταυτότητας, επιχειρησιακής αναγκαιότητας και των αρχών του ελαχίστου προνομίου και του διαχωρισμού καθηκόντων.

1.1 Υποστηρίζει τη δέσμευση του οργανισμού για την ασφάλεια πληροφοριών μέσω της εφαρμογής δομημένων και ελέγξιμων διαδικασιών για τη χορήγηση πρόσβασης, την ανάθεση προνομίων, την παρακολούθηση της χρήσης και την ανάκληση πρόσβασης λογαριασμών.

1.2 Η παρούσα πολιτική είναι κρίσιμη για τη μείωση του κινδύνου μη εξουσιοδοτημένης πρόσβασης, κατάχρησης προνομίων, εσωτερικών απειλών και μη συμμόρφωσης με τα εφαρμοστέα κανονιστικά πλαίσια.

2. Πεδίο εφαρμογής

2.1 Η παρούσα πολιτική εφαρμόζεται σε όλους τους εργαζομένους, αναδόχους, τρίτους παρόχους υπηρεσιών, συμβούλους και κάθε άλλο πρόσωπο στο οποίο χορηγείται πρόσβαση στους πόρους ΤΠ, στις εφαρμογές ή στα δεδομένα του οργανισμού.

2.2 Διέπει όλα τα συστήματα και περιβάλλοντα στα οποία εφαρμόζονται μηχανισμοί αυθεντικοποίησης χρηστών και έλεγχος πρόσβασης, συμπεριλαμβανομένων ενδεικτικά των εξής:

2.2.1 Επιχειρησιακές εφαρμογές και βάσεις δεδομένων

2.2.2 Πλατφόρμες υπολογιστικού νέφους και περιβάλλοντα SaaS

2.2.3 Λειτουργικά συστήματα και διαχειριστικές κονσόλες

2.2.4 Εργαλεία απομακρυσμένης πρόσβασης και VPN

2.2.5 Συστήματα διαχείρισης ταυτοτήτων και πρόσβασης (IAM)

2.3 Η πολιτική καλύπτει τόσο τους τυπικούς όσο και τους προνομιούχους λογαριασμούς χρηστών και περιλαμβάνει ελέγχους για:

2.3.1 Δημιουργία, τροποποίηση και απενεργοποίηση λογαριασμών

2.3.2 Κλιμάκωση και εκχώρηση προνομίων

2.3.3 Έλεγχο και παρακολούθηση συνεδριών

2.3.4 Μεθόδους αυθεντικοποίησης και διαχείριση διαπιστευτηρίων

3. Στόχοι

3.1 Να διασφαλίζεται ότι όλοι οι λογαριασμοί χρηστών είναι μοναδικά αναγνωρίσιμοι, δεόντως εξουσιοδοτημένοι και ανατίθενται μόνο κατόπιν επίσημης επικύρωσης της ανάγκης.

3.2 Να εφαρμόζονται οι αρχές του ελαχίστου προνομίου και να αποτρέπεται η περιττή ή υπερβολική πρόσβαση μέσω αυστηρών ελέγχων στη χορήγηση και χρήση προνομιούχων λογαριασμών.

3.3 Να απαιτείται η έγκαιρη επικαιροποίηση της κατάστασης των λογαριασμών βάσει αλλαγών στην εργασιακή σχέση ή στον ρόλο, συμπεριλαμβανομένης της άμεσης απενεργοποίησης κατά την αποχώρηση.

3.4 Να καθίσταται δυνατή η προληπτική ανίχνευση και αποκατάσταση ανενεργών, καταχρηστικά χρησιμοποιούμενων ή μη εξουσιοδοτημένων λογαριασμών μέσω καταγραφής, ανασκοπήσεων και αυτοματισμών.

3.5 Να διατηρείται η ευθυγράμμιση με το ISO/IEC 27001:2022 και τα συναφή πρότυπα, καθώς και η κάλυψη υποχρεώσεων που απορρέουν από σχετικά νομικά και κανονιστικά πλαίσια, όπως ο ΓΚΠΔ, η NIS2, ο DORA και το COBIT 2019.

4. Ρόλοι και αρμοδιότητες

4.1 Επικεφαλής Ασφάλειας Πληροφοριών (CISO)

4.1.1 Έχει την κυριότητα της παρούσας πολιτικής και διασφαλίζει την εφαρμογή της σε όλο τον οργανισμό.

4.1.2 Ανασκοπεί και εγκρίνει κάθε επίσημη εξαίρεση ή περίπτωση έκτακτης πρόσβασης.

4.1.3 Αναφέρει ευρήματα ελέγχου που σχετίζονται με λογαριασμούς και κλιμακώνει τους κινδύνους προς την Ανώτατη Διοίκηση.

4.2 Υπεύθυνος Ελέγχου Πρόσβασης / Διαχειριστής Πληροφοριακών Συστημάτων

4.2.1 Διατηρεί και λειτουργεί τους τεχνικούς ελέγχους για τη διαχείριση του κύκλου ζωής των λογαριασμών χρηστών.

4.2.2 Εκτελεί ενέργειες χορήγησης, ανάκλησης και διαχείρισης προνομίων κατόπιν εγκεκριμένου αιτήματος.

4.2.3 Τηρεί έγκυρο μητρώο όλων των λογαριασμών χρηστών, της κατάστασής τους και του επιπέδου προνομίων τους.

4.2.4 Υποστηρίζει ελέγχους και ανασκοπήσεις συμμόρφωσης με αρχεία καταγραφής και αναφορές δραστηριότητας.

[... 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 τουλάχιστον ετησίως ή σε περίπτωση σημαντικών αλλαγών στα εξής:

9.1.1 Οργανωτική δομή ή επιχειρησιακές διεργασίες

9.1.2 Συστήματα ΤΠ, πλατφόρμες ταυτοτήτων ή μέθοδοι πρόσβασης

9.1.3 Κανονιστικές ή συμβατικές απαιτήσεις σχετικές με τη διαχείριση ταυτοτήτων και πρόσβασης

9.2 Ο Επικεφαλής Ασφάλειας Πληροφοριών (CISO), σε συνεργασία με τον Υπεύθυνο Ελέγχου Πρόσβασης, είναι υπεύθυνος για την έναρξη της διαδικασίας ανασκόπησης και τον συντονισμό της ανατροφοδότησης από τα ενδιαφερόμενα μέρη.

9.3 Έκτακτες ανασκοπήσεις μπορούν να ενεργοποιούνται από:

9.3.1 Περιστατικά ασφάλειας που σχετίζονται με κατάχρηση λογαριασμών

9.3.2 Ευρήματα ελέγχου που αναδεικνύουν αδυναμίες στη διαχείριση του κύκλου ζωής λογαριασμών

9.3.3 Εγκατάσταση νέων εργαλείων διαχείρισης ταυτοτήτων ή προνομιούχας πρόσβασης

9.4 Οι επικαιροποιήσεις της παρούσας πολιτικής πρέπει να:

9.4.1 Υπόκεινται σε έλεγχο εκδόσεων και να καταγράφονται στη βιβλιοθήκη τεκμηρίωσης του ISMS

9.4.2 Κοινοποιούνται σε όλα τα σχετικά ενδιαφερόμενα μέρη, συμπεριλαμβανομένων των Επικεφαλής Τμημάτων, των λειτουργιών Πληροφορικής και του HR

9.4.3 Υποστηρίζονται από επικαιροποιημένο εκπαιδευτικό υλικό και διαδικαστικούς οδηγούς

9.5 Όλες οι αλλαγές πρέπει να εγκρίνονται από την Ανώτατη Διοίκηση ή την Επιτροπή Ασφάλειας Πληροφοριών και να καταγράφονται για σκοπούς ελέγχου.

10. Συναφείς πολιτικές και διασυνδέσεις

10.1 Η παρούσα πολιτική συνδέεται λειτουργικά με τις ακόλουθες συναφείς πολιτικές της δέσμης του ISMS και υποστηρίζεται από αυτές:

10.1.1 P4 Πολιτική Ελέγχου Πρόσβασης: Καθορίζει τις υπερκείμενες αρχές και τους μηχανισμούς ελέγχου πρόσβασης, συμπεριλαμβανομένων των ελέγχων βάσει κανόνων και βάσει ρόλων.

10.1.2 P7 Πολιτική Ένταξης και Αποχώρησης: Παρέχει τα διαδικαστικά βήματα για την έναρξη και τον τερματισμό της πρόσβασης χρηστών σε ευθυγράμμιση με ενέργειες του HR.

10.1.3 P8 Πολιτική Ευαισθητοποίησης και Εκπαίδευσης για την Ασφάλεια Πληροφοριών: Ενισχύει τις ευθύνες των χρηστών για την ασφάλεια λογαριασμών και την προστασία των διαπιστευτηρίων.

10.1.4 P13 Πολιτική Ταξινόμησης και Επισήμανσης Δεδομένων: Καθοδηγεί τα επίπεδα πρόσβασης βάσει της ταξινόμησης δεδομένων, διασφαλίζοντας ότι τα όρια προνομίων ευθυγραμμίζονται με τα επίπεδα ευαισθησίας.

10.1.5 P22 Πολιτική Καταγραφής και Παρακολούθησης: Διασφαλίζει ότι συλλέγονται ίχνη ελέγχου για όλες τις δραστηριότητες που σχετίζονται με λογαριασμούς και ότι ανασκοπούνται για την ανίχνευση ανωμαλιών ή μη εξουσιοδοτημένης χρήσης.

10.1.6 P30 Πολιτική Αντιμετώπισης Περιστατικών: Διέπει την κλιμάκωση, τον περιορισμό και τις ενέργειες μετά το περιστατικό σε περιπτώσεις κατάχρησης προνομίων ή μη εξουσιοδοτημένης δραστηριότητας λογαριασμών.

10.2 Καθεμία από αυτές τις πολιτικές λειτουργεί συμπληρωματικά για την εφαρμογή ενός συνεκτικού πλαισίου διαχείρισης ταυτοτήτων και πρόσβασης βάσει κινδύνου σε όλο τον οργανισμό.

11. Πρότυπα και πλαίσια αναφοράς

11.1 Η παρούσα πολιτική είναι ευθυγραμμισμένη με διεθνώς αναγνωρισμένα πρότυπα κυβερνοασφάλειας και κανονιστικά πλαίσια που επιβάλλουν την ασφαλή διαχείριση ταυτοτήτων, πρόσβασης και προνομίων ως βασικό στοιχείο της ασφάλειας πληροφοριών του οργανισμού.

11.2 ISO/IEC 27001:

11.2.1 Η Ρήτρα 6.1.3 απαιτεί από τους οργανισμούς να προσδιορίζουν, να αξιολογούν και να αντιμετωπίζουν τους κινδύνους ασφάλειας πληροφοριών, καθιστώντας τη διαχείριση πρόσβασης και προνομίων επίσημο έλεγχο βάσει κινδύνου, ενσωματωμένο στη διαδικασία σχεδιασμού του ISMS.

11.2.2 Η Ρήτρα 8.1 - Επιχειρησιακός σχεδιασμός και έλεγχος: ενισχύει την εφαρμογή τεχνικών και διαδικαστικών δικλίδων ασφαλείας που διέπουν την πρόσβαση χρηστών και την προνομιούχα πρόσβαση.

11.3 ISO/IEC 27002:2022 - Έλεγχοι 5.15 έως 5.18:

11.3.1 Ο Έλεγχος 5.15 - Διαχείριση πρόσβασης χρηστών: υποστηρίζει επίσημες διαδικασίες για τη χορήγηση πρόσβασης λογαριασμών, την εξουσιοδότηση πρόσβασης και την περιοδική ανασκόπηση των δικαιωμάτων πρόσβασης.

11.3.2 Ο Έλεγχος 5.16 - Διαχείριση ταυτοτήτων: καθιερώνει τη μοναδικότητα ταυτότητας, ελέγχους κύκλου ζωής και επιβολή ασφαλούς αυθεντικοποίησης.

11.3.3 Ο Έλεγχος 5.17 διασφαλίζει ότι η χορήγηση και η χρήση δικαιωμάτων προνομιούχας πρόσβασης ελέγχονται αυστηρά, είναι ιχνηλάσιμες και ευθυγραμμίζονται με την αρχή του ελαχίστου προνομίου σε όλο τον κύκλο ζωής του λογαριασμού χρήστη.

11.3.4 Ο Έλεγχος 5.18 - Δικαιώματα προνομιούχας πρόσβασης: καλύπτεται πλήρως μέσω ανάθεσης προνομίων βάσει ρόλων, ελέγχου και απαιτήσεων έγκρισης αυξημένης πρόσβασης.

11.4 Οι έλεγχοι αυτοί καθοδηγούν τη δομημένη εφαρμογή της καταχώρισης και διαγραφής λογαριασμών, του διαχωρισμού προνομίων και της χρήσης πληροφοριών αυθεντικοποίησης. Η πολιτική επιβάλλει διακυβέρνηση του κύκλου ζωής ταυτοτήτων, πρόσβαση Just-in-Time και παρακολούθηση αυξημένων συνεδριών, ώστε να αποτρέπεται η μη εξουσιοδοτημένη χρήση συστημάτων.

11.5 NIST SP 800-53 Rev.5:

11.5.1 Τα AC-1 (Πολιτική Ελέγχου Πρόσβασης) και AC-2 (Διαχείριση λογαριασμών) αντιστοιχίζονται στις απαιτήσεις της πολιτικής για εγκρίσεις πρόσβασης, αντιστοίχιση ρόλων και έλεγχο λογαριασμών χρηστών.

11.5.2 Τα AC-5 (Διαχωρισμός καθηκόντων) και AC-6 (Ελάχιστο προνόμιο) ικανοποιούνται μέσω περιορισμού προνομίων, ευθυγράμμισης με τον εργασιακό ρόλο και διπλής έγκρισης για εργασίες υψηλού κινδύνου.

11.5.3 Τα IA-2 έως IA-5 (Αναγνώριση και αυθεντικοποίηση) εφαρμόζονται μέσω ισχυρών μηχανισμών αυθεντικοποίησης, κανόνων κύκλου ζωής διαπιστευτηρίων και απαιτήσεων MFA.

11.5.4 Τα AU-2 και AU-12 (Καταγραφή ελέγχου και ανάλυση) καλύπτονται μέσω καταγραφής συνεδριών και παρακολούθησης προνομιούχας δραστηριότητας σε ευαίσθητα περιβάλλοντα.

11.6 ΓΚΠΔ της ΕΕ (2016/679):

11.6.1 Άρθρο 32 - Ασφάλεια επεξεργασίας: απαιτεί ελέγχους πρόσβασης και μηχανισμούς επαλήθευσης ταυτότητας για την προστασία δεδομένων προσωπικού χαρακτήρα. Η απαίτηση αυτή καλύπτεται μέσω υποχρεωτικών εγκρίσεων λογαριασμών, ανασκοπήσεων προνομίων και ισχυρών δικλίδων αυθεντικοποίησης.

11.6.2 Άρθρο 5(1)(f) - Ακεραιότητα και εμπιστευτικότητα: διασφαλίζει ότι η πρόσβαση σε δεδομένα προσωπικού χαρακτήρα παρέχεται μόνο σε εξουσιοδοτημένους χρήστες με νόμιμους ρόλους, γεγονός που ενισχύεται από την εφαρμογή της διαχείρισης λογαριασμών.

11.6.3 Αιτιολογική σκέψη 39: απαιτεί σαφή περιορισμό πρόσβασης και λογοδοσία — η παρούσα πολιτική υποστηρίζει πλήρη ιχνηλασιμότητα των ταυτοτήτων χρηστών και των αναθέσεων προνομίων.

11.7 Οδηγία NIS2 της ΕΕ (2022/2555):

11.7.1 Άρθρο 21(2)(a, d): απαιτεί από τις οντότητες να εφαρμόζουν πολιτικές διαχείρισης πρόσβασης και ασφαλή διαχείριση διαπιστευτηρίων και προνομιούχων συνεδριών, κάτι που υποστηρίζεται μέσω των ελέγχων χορήγησης πρόσβασης, παρακολούθησης και εξαιρέσεων της παρούσας πολιτικής.

11.7.2 Άρθρο 21(3): προάγει την πειθαρχία πρόσβασης και την ισχυρή διασφάλιση ταυτότητας σε κρίσιμους τομείς, απαιτήσεις που καλύπτονται μέσω της χρήσης μοναδικών αναγνωριστικών, RBAC και χρονικά περιορισμένης αυξημένης πρόσβασης.

11.8 Κανονισμός DORA της ΕΕ (2022/2554):

11.8.1 Άρθρο 5 - Διακυβέρνηση και έλεγχος ΤΠΕ: επιβάλλει τυποποιημένες διαδικασίες για τη διαχείριση χρηστών ΤΠΕ, οι οποίες καλύπτονται μέσω τεκμηριωμένης χορήγησης πρόσβασης, απενεργοποίησης και διαχείρισης εξαιρέσεων.

11.8.2 Άρθρο 9 - Διαχείριση κινδύνων ΤΠΕ: καθοδηγεί τους οργανισμούς να προστατεύουν τα συστήματα μέσω περιορισμών πρόσβασης και παρακολούθησης, απαίτηση που αντιμετωπίζεται μέσω MFA, καταγραφής προνομιούχας πρόσβασης και κεντρικών ανασκοπήσεων.

11.9 COBIT 2019:

11.9.1 DSS01 - Διαχειριζόμενες λειτουργίες: προωθεί την εφαρμογή τυποποιημένων επιχειρησιακών ελέγχων, συμπεριλαμβανομένης της διαχείρισης του κύκλου ζωής λογαριασμών χρηστών και της τεκμηρίωσης πρόσβασης.

11.9.2 DSS05 - Διαχειριζόμενες υπηρεσίες ασφάλειας: αποτυπώνει την ασφαλή διαχείριση προνομίων χρηστών και συστημάτων, υποστηρίζοντας τον μετριασμό του κινδύνου μέσω ελαχίστου προνομίου και επικύρωσης του ίχνους ελέγχου.

11.9.3 APO13 - Διαχειριζόμενη ασφάλεια: απαιτεί διακυβέρνηση πρόσβασης σε ψηφιακά περιουσιακά στοιχεία, η οποία καλύπτεται μέσω τυποποιημένων πρακτικών εξουσιοδότησης λογαριασμών και ρόλων με υποχρεωτικές περιοδικές ανασκοπήσεις.