					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P11S					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**

Νομική σημείωση (πνευματικά δικαιώματα και περιορισμοί χρήσης)

(C) 2025 Clarysec LLC. All rights reserved.

Το παρόν έγγραφο αποτελεί πνευματική ιδιοκτησία της Clarysec LLC. Απαγορεύεται η αντιγραφή, επαναχρησιμοποίηση, διανομή ή τροποποίησή του, εν όλω ή εν μέρει, για εμπορικούς ή σκοπούς υλοποίησης χωρίς προηγούμενη ρητή έγγραφη άδεια.
Η μη εξουσιοδοτημένη χρήση απαγορεύεται αυστηρά και ενδέχεται να επιφέρει νομικές ενέργειες.
Για θέματα αδειοδότησης, επικοινωνήστε με: info@clarysec.com

Ευθυγραμμισμένη με πρότυπα και κανονιστικές απαιτήσεις

Πρότυπο/Κανονισμός	Ρήτρα/Άρθρο	Σχόλιο
ISO/IEC 27001:2022	Ρήτρες 5.3, 8	Ρόλοι, αρμοδιότητες και επιχειρησιακός σχεδιασμός/έλεγχος για τη διαχείριση της πρόσβασης χρηστών
ISO/IEC 27002:2022	Έλεγχος 8	Έλεγχοι για την ανάθεση, την ανασκόπηση και την αφαίρεση αυξημένων προνομίων
NIST SP 800-53 Rev.5	AC-2, AC-5, AC-6	Δημιουργία λογαριασμών, παρακολούθηση, ελάχιστο προνόμιο και διαχωρισμός καθηκόντων
Οδηγία NIS2 της ΕΕ	Άρθρο 21(2)(d)	Διαχείριση της πρόσβασης χρηστών για ουσιώδεις και σημαντικές οντότητες
Κανονισμός DORA της ΕΕ	Άρθρο 9(2)(b)	Έλεγχος προνομιούχας πρόσβασης σε χρηματοοικονομικές οντότητες
COBIT 2019	DSS05.03, DSS05.04	Χορήγηση πρόσβασης, κατάργηση πρόσβασης και περιοδική ανασκόπηση της πρόσβασης χρηστών
ΓΚΠΔ της ΕΕ	Άρθρο 32	Κατάλληλοι έλεγχοι πρόσβασης για την προστασία δεδομένων προσωπικού χαρακτήρα

1. Σκοπός

1.1 Η παρούσα πολιτική καθορίζει κανόνες για τη διαχείριση λογαριασμών χρηστών και δικαιωμάτων πρόσβασης με ασφαλή, συνεπή και ιχνηλάσιμο τρόπο. Διασφαλίζει ότι μόνο εξουσιοδοτημένοι χρήστες έχουν πρόσβαση σε συστήματα και δεδομένα και ότι η πρόσβαση είναι κατάλληλη για τον ρόλο και τις αρμοδιότητές τους.

1.2 Η αποτελεσματική διαχείριση λογαριασμών και προνομίων είναι ουσιώδης για την πρόληψη μη εξουσιοδοτημένης πρόσβασης, τον περιορισμό εσωτερικών απειλών και τη διασφάλιση της συμμόρφωσης με το ISO/IEC 27001, τον ΓΚΠΔ της ΕΕ και άλλες κανονιστικές απαιτήσεις.

1.3 Η παρούσα πολιτική επιτρέπει στον οργανισμό να αναθέτει ιδιοκτησία και ευθύνη για τη χρήση λογαριασμών, να παρακολουθεί και να ελέγχει την κλιμάκωση προνομίων και να απενεργοποιεί ή να ανακαλεί με ασφαλή τρόπο την πρόσβαση όταν αυτή δεν απαιτείται πλέον.

1.4 Παράλληλα, προστατεύει τις επιχειρησιακές λειτουργίες από λειτουργικά σφάλματα ή κακή χρήση που προκαλούνται από υπερβολική ή μη παρακολουθούμενη πρόσβαση και συμβάλλει στη μείωση του κινδύνου τυχαίας διαρροής δεδομένων, κατάχρησης προνομίων ή κανονιστικής μη συμμόρφωσης.

2. Πεδίο εφαρμογής

2.1 Η παρούσα πολιτική εφαρμόζεται σε:

2.1.1 Όλους τους εργαζομένους, ασκούμενους, αναδόχους και χρήστες τρίτων μερών που έχουν πρόσβαση στα πληροφοριακά συστήματα του οργανισμού

2.1.2 Όλα τα συστήματα, τις συσκευές, τις υπηρεσίες και τις πλατφόρμες που διαχειρίζεται ο οργανισμός ή διαχειρίζονται για λογαριασμό του, συμπεριλαμβανομένων των πλατφορμών υπολογιστικού νέφους, της επιτόπιας υποδομής και εργαλείων τρίτων μερών

2.2 Καλύπτει όλους τους τύπους λογαριασμών χρηστών, συμπεριλαμβανομένων των εξής:

2.2.1 Ονομαστικοί λογαριασμοί χρηστών (π.χ. λογαριασμοί ηλεκτρονικού ταχυδρομείου, συνδέσεις σε συστήματα)

2.2.2 Λογαριασμοί διαχειριστή και λογαριασμοί συστήματος

2.2.3 Προσωρινά διαπιστευτήρια πρόσβασης, λογαριασμοί επισκεπτών ή λογαριασμοί τρίτων μερών

2.2.4 Λογαριασμοί υπηρεσίας που χρησιμοποιούνται από εφαρμογές ή συστήματα αυτοματισμού

2.3 Η πολιτική εφαρμόζεται σε όλο τον κύκλο ζωής του λογαριασμού, από τη δημιουργία και την έγκριση έως την τροποποίηση, την παρακολούθηση και την απενεργοποίηση. Αυτό περιλαμβάνει την αρχική χορήγηση πρόσβασης κατά τη διαδικασία ένταξης, τις αναθεωρήσεις δικαιωμάτων πρόσβασης κατά τις αλλαγές ρόλου και την ανάκληση κατά την αποχώρηση.

3. Στόχοι

3.1 Ανάθεση μοναδικών και ιχνηλάσιμων ταυτοτήτων χρήστη σε όλους τους χρήστες συστημάτων, με διασφάλιση της λογοδοσίας και εξάλειψη της εξάρτησης από κοινόχρηστα διαπιστευτήρια.

3.2 Εφαρμογή της αρχής του ελαχίστου προνομίου, ώστε στους χρήστες να χορηγείται μόνο το ελάχιστο επίπεδο πρόσβασης που είναι απαραίτητο για την εκτέλεση των καθηκόντων τους.

3.3 Πρόληψη μη εξουσιοδοτημένης πρόσβασης σε ευαίσθητα συστήματα ή δεδομένα μέσω σαφώς τεκμηριωμένων διαδικασιών έγκρισης και ανασκόπησης.

3.4 Διασφάλιση της έγκαιρης απενεργοποίησης λογαριασμών χρηστών όταν αυτοί δεν απαιτούνται πλέον, π.χ. σε περίπτωση αποχώρησης, ολοκλήρωσης σύμβασης ή αλλαγής ρόλου.

3.5 Διατήρηση ασφαλούς περιβάλλοντος με ετοιμότητα ελέγχου μέσω τεκμηρίωσης όλων των αλλαγών λογαριασμών, των εγκρίσεων και των περιοδικών ανασκοπήσεων.

3.6 Διασφάλιση ότι η κλιμάκωση προνομίων ελέγχεται αυστηρά, εγκρίνεται ανεξάρτητα και καταγράφεται, και ότι η αυξημένη πρόσβαση ανακαλείται άμεσα όταν δεν απαιτείται πλέον.

4. Ρόλοι και αρμοδιότητες

4.1 Γενικός Διευθυντής (GM)

4.1.1 Έχει τη συνολική λογοδοσία για την εφαρμογή της παρούσας πολιτικής.

4.1.2 Διασφαλίζει ότι οι πρακτικές διαχείρισης λογαριασμών ευθυγραμμίζονται με τις απαιτήσεις πιστοποίησης ISO/IEC 27001 και τις σχετικές νομικές υποχρεώσεις (π.χ. ΓΚΠΔ της ΕΕ).

4.1.3 Ενημερώνεται άμεσα για κάθε μη εξουσιοδοτημένη πρόσβαση, περιστατικό ασφάλειας ή παραβίαση πολιτικής που σχετίζεται με λογαριασμούς χρηστών.

4.1.4 Ασκεί εποπτεία στις ανασκοπήσεις της πολιτικής, στους ελέγχους και στις ενέργειες εφαρμογής της πολιτικής.

4.2 Επικεφαλής Πληροφορικής ή Εξωτερικός Πάροχος Υπηρεσιών Πληροφορικής

4.2.1 Είναι υπεύθυνος για την τεχνική εφαρμογή των ελέγχων λογαριασμών και προνομίων σε όλα τα συστήματα που χρησιμοποιεί ο οργανισμός.

4.2.2 Χορηγεί, τροποποιεί και απενεργοποιεί λογαριασμούς χρηστών μόνο βάσει τεκμηριωμένων εγκρίσεων.

4.2.3 Εφαρμόζει απαιτήσεις πολυπλοκότητας κωδικών πρόσβασης, χρονικό όριο αδράνειας οθόνης, πολυπαραγοντικό έλεγχο ταυτότητας (όπου είναι διαθέσιμος) και καταγραφή συμβάντων συστημάτων.

4.2.4 Τηρεί ασφαλή αρχεία για όλες τις εγκρίσεις πρόσβασης, την ιδιοκτησία λογαριασμών, τις κλιμακώσεις προνομίων και τις ανακλήσεις.

4.2.5 Παρακολουθεί για μη εξουσιοδοτημένους ή ορφανούς λογαριασμούς και αναφέρει τυχόν αποκλίσεις στον GM.

[... 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 από τον GM και τον Επικεφαλής Πληροφορικής, ώστε να διασφαλίζεται η συμμόρφωση με:

9.1.1 Τους ισχύοντες ελέγχους και την καθοδήγηση του ISO/IEC 27001:2022

9.1.2 Κανονιστικές επικαιροποιήσεις (π.χ. ΓΚΠΔ της ΕΕ, DORA, NIS2)

9.1.3 Αλλαγές σε συστήματα, υπηρεσίες ή στην επιχειρησιακή δομή

9.2 Ανασκοπήσεις πρέπει επίσης να διενεργούνται μετά από:

9.2.1 Σημαντικά περιστατικά ασφάλειας ή ευρήματα ελέγχου

9.2.2 Μείζονες αλλαγές στα πληροφοριακά συστήματα ή στην αρχιτεκτονική λογαριασμών

9.2.3 Εισαγωγή νέων πλατφορμών που απαιτούν ενσωμάτωση ελέγχου πρόσβασης

9.3 Όλες οι αλλαγές πρέπει να εγκρίνονται από τον GM και να κοινοποιούνται με σαφήνεια στο επηρεαζόμενο προσωπικό.

10. Συναφείς πολιτικές και διασυνδέσεις

10.1 P2S – Πολιτική Ρόλων και Αρμοδιοτήτων Διακυβέρνησης: Καθορίζει τη λογοδοσία και την αρμοδιότητα λήψης αποφάσεων για εγκρίσεις πρόσβασης και εποπτεία.

10.2 P4S – Πολιτική Ελέγχου Πρόσβασης: Διέπει την εφαρμογή του ελέγχου πρόσβασης σε όλο το εύρος των συστημάτων και τις μεθόδους αυθεντικοποίησης.

10.3 P7S – Πολιτική Ένταξης και Αποχώρησης: Διασφαλίζει ότι η δημιουργία και η αφαίρεση λογαριασμών ενσωματώνονται στις μεταβολές προσωπικού που διαχειρίζεται η λειτουργία Ανθρώπινου Δυναμικού (HR).

10.4 P8S – Πολιτική Ευαισθητοποίησης και Εκπαίδευσης στην Ασφάλεια Πληροφοριών: Εκπαιδεύει τους χρήστες στις ασφαλείς πρακτικές διαχείρισης λογαριασμών και στις απαιτήσεις χρήσης.

10.5 P30S – Πολιτική Αντιμετώπισης Περιστατικών: Ορίζει τις ενέργειες που πρέπει να ληφθούν εάν η κακή χρήση λογαριασμού οδηγήσει σε περιστατικό ασφάλειας ή μη εξουσιοδοτημένη γνωστοποίηση.

11. Πρότυπα και πλαίσια αναφοράς

11.1 ISO/IEC 27001

11.1.1 Ρήτρα 5.3: Απαιτεί οι ρόλοι και οι αρμοδιότητες για την ασφάλεια πληροφοριών να ανατίθενται με σαφήνεια και να εφαρμόζονται.

11.1.2 Ρήτρα 8.1: Ο επιχειρησιακός σχεδιασμός και έλεγχος πρέπει να περιλαμβάνουν τη διαχείριση της πρόσβασης χρηστών.

11.2 ISO/IEC 27002

11.2.1 Έλεγχος 8.2: Περιγράφει τεχνικούς και διαδικαστικούς ελέγχους για την ανάθεση, την ανασκόπηση και την αφαίρεση αυξημένων προνομίων.

11.3 NIST SP 800-53 Rev.5

11.3.1 AC-2: Απαιτεί τη δημιουργία, την παρακολούθηση και την ανάκληση λογαριασμών βάσει καθορισμένων ρόλων και διαδικασιών.

11.3.2 AC-5: Καλύπτει τον διαχωρισμό καθηκόντων για την πρόληψη σύγκρουσης ή κατάχρησης προνομίων.

11.3.3 AC-6: Επιβάλλει την εφαρμογή της αρχής του ελαχίστου προνομίου σε όλα τα δικαιώματα πρόσβασης.

11.4 ΓΚΠΔ της ΕΕ

11.4.1 Άρθρο 32: Απαιτεί κατάλληλους ελέγχους πρόσβασης για την προστασία δεδομένων προσωπικού χαρακτήρα από μη εξουσιοδοτημένη πρόσβαση ή αλλοίωση.

11.5 Οδηγία NIS2 της ΕΕ

11.5.1 Άρθρο 21(2)(d): Επιβάλλει τη διαχείριση της πρόσβασης χρηστών ως μέρος των βασικών ελέγχων ασφάλειας για ουσιώδεις και σημαντικές οντότητες.

11.6 Κανονισμός DORA της ΕΕ

11.6.1 Άρθρο 9(2)(b): Απαιτεί από τις χρηματοοικονομικές οντότητες να εφαρμόζουν ελέγχους πρόσβασης που περιορίζουν και παρακολουθούν τα προνομιούχα δικαιώματα.

11.7 COBIT 2019

11.7.1 DSS05.03: Προσδιορίζει τη χορήγηση πρόσβασης και την κατάργηση πρόσβασης χρηστών ως μέρος της διακυβέρνησης ΤΠ.

11.7.2 DSS05.04: Απαιτεί συνεχή ανασκόπηση και ευθυγράμμιση της πρόσβασης χρηστών με τους οργανωτικούς ρόλους.