					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P07S					Τίτλος εγγράφου: **Πολιτική Ένταξης και Αποχώρησης**							
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 κανονισμούς

Πρότυπο/Κανονισμός	Ρήτρα/Άρθρο	Σχόλιο
ISO/IEC 27001:2022	Ρήτρες 6.2, 7	Απαιτήσεις ασφάλειας ανθρώπινου δυναμικού και ευαισθητοποίησης
ISO/IEC 27002:2022	Έλεγχοι 6.2, 6.5	Πρακτικές ασφάλειας για την ένταξη και αποχώρηση προσωπικού
NIST SP 800-53 Rev.5	PS-4, AC-2, PL-4	Αποχώρηση προσωπικού, κύκλος ζωής λογαριασμών, σχεδιασμός
Οδηγία NIS2 της ΕΕ	Άρθρο 21(2)(h)	Ασφάλεια ανθρώπινου δυναμικού και κύκλος ζωής πρόσβασης
Κανονισμός DORA της ΕΕ	Άρθρο 12	Έλεγχος πρόσβασης και ανάκληση για συστήματα ΤΠΕ
COBIT 2019	APO07, DSS01	Ασφάλεια προσωπικού, έλεγχοι λογικής/φυσικής πρόσβασης
ΓΚΠΔ της ΕΕ	Άρθρο 32	Ασφάλεια δεδομένων προσωπικού χαρακτήρα κατά τη διάρκεια της απασχόλησης

1. Σκοπός

1.1 Η παρούσα πολιτική ορίζει τη διαδικασία για την ένταξη νέων εργαζομένων ή αναδόχων και την ασφαλή αφαίρεση δικαιωμάτων πρόσβασης όταν τα πρόσωπα αποχωρούν ή αλλάζουν ρόλο.

1.2 Διασφαλίζει ότι η πρόσβαση χορηγείται σύμφωνα με την αρχή του ελάχιστου απαιτούμενου δικαιώματος, ότι όλα τα περιουσιακά στοιχεία καταγράφονται και ότι κρίσιμες ενέργειες, όπως η απενεργοποίηση συστημάτων και η ανάκτηση δεδομένων, ολοκληρώνονται έγκαιρα.

1.3 Η παρούσα πολιτική υποστηρίζει τη συμμόρφωση, την επιχειρησιακή ακεραιότητα και την προστασία δεδομένων μέσω δομημένων και ελέγξιμων δραστηριοτήτων ένταξης και αποχώρησης.

2. Πεδίο εφαρμογής

2.1 Η παρούσα πολιτική εφαρμόζεται σε:

2.1.1 Όλους τους μόνιμους και προσωρινούς εργαζομένους

2.1.2 Αναδόχους, συμβούλους και ασκούμενους

2.1.3 Εξωτερικούς παρόχους υπηρεσιών με πρόσβαση σε συστήματα ή φυσική πρόσβαση

2.2 Καλύπτει:

2.2.1 Ένταξη: δημιουργία λογαριασμών χρηστών, χορήγηση πρόσβασης, διάθεση εξοπλισμού

2.2.2 Αποχώρηση: αφαίρεση δικαιωμάτων πρόσβασης, ανάκτηση εταιρικών περιουσιακών στοιχείων και ασφαλής κατάργηση ψηφιακών ταυτοτήτων

2.2.3 Εσωτερικές αλλαγές ρόλου που απαιτούν αναδιαμόρφωση πρόσβασης ή επαναδιάθεση περιουσιακών στοιχείων

2.3 Εφαρμόζεται σε όλες τις συσκευές, τις πλατφόρμες και τις τοποθεσίες που χρησιμοποιούνται για επίσημες επιχειρησιακές λειτουργίες.

3. Στόχοι

3.1 Να διασφαλίζεται ότι το νέο προσωπικό λαμβάνει πρόσβαση και πόρους βάσει επαληθευμένων ρόλων και αρμοδιοτήτων.

3.2 Να επιβεβαιώνεται ότι οι αποχωρούντες χρήστες αφαιρούνται πλήρως από τα συστήματα και τις εγκαταστάσεις έως το τέλος της τελευταίας εργάσιμης ημέρας τους.

3.3 Να αποτρέπεται η ύπαρξη ορφανών λογαριασμών και μη επιστραφέντων περιουσιακών στοιχείων, τα οποία συνιστούν κίνδυνο ασφάλειας.

3.4 Να τηρούνται τεκμηριωμένα αρχεία ενεργειών ένταξης, μετακίνησης και αποχώρησης.

3.5 Να ενισχύεται η λογοδοσία μέσω λιστών ελέγχου και διατμηματικού συντονισμού ρόλων.

4. Ρόλοι και αρμοδιότητες

4.1 Γενικός Διευθυντής

4.1.1 Εγκρίνει την πρόσβαση για ρόλους υψηλών προνομίων και ασκεί εποπτεία στο πρόγραμμα ένταξης και αποχώρησης.

4.1.2 Διασφαλίζει ότι οι εξαιρέσεις τεκμηριώνονται επαρκώς και ότι λαμβάνονται διορθωτικά μέτρα όταν δεν τηρούνται οι διαδικασίες.

4.2 Υπεύθυνος Γραφείου / Ανθρώπινο Δυναμικό (HR)

4.2.1 Εκκινεί τη διαδικασία ένταξης για νέες προσλήψεις και ενημερώνει την Πληροφορική για αποχωρήσεις.

4.2.2 Διασφαλίζει την ολοκλήρωση των νομικών εγγράφων (π.χ. NDA) και των δηλώσεων αποδοχής των πολιτικών ασφάλειας.

4.2.3 Τηρεί τις λίστες ελέγχου ένταξης/αποχώρησης και παρακολουθεί τη συμμόρφωση με την πολιτική.

[... 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

9.1.1 Η παρούσα πολιτική πρέπει να ανασκοπείται τουλάχιστον μία φορά ετησίως από τον Γενικό Διευθυντή και τους επικεφαλής HR/IT.

9.2 Παράγοντες ενεργοποίησης πρόωρης ανασκόπησης

9.2.1 Πρέπει να πραγματοποιείται επικαιροποίηση εάν:

9.2.1.1 Εισάγονται νέα συστήματα HR ή Πληροφορικής

9.2.1.2 Υπάρχει αλλαγή Εξωτερικού Παρόχου Υπηρεσιών Πληροφορικής ή διαχειριζόμενης υπηρεσίας HR

9.2.1.3 Οι έλεγχοι ασφάλειας αποκαλύπτουν κενά διαδικασιών

9.2.1.4 Οι ρυθμιστικές υποχρεώσεις μεταβάλλονται (π.χ. επικαιροποιήσεις του ΓΚΠΔ της ΕΕ)

9.2.1.5 Προκύπτει κρίσιμη αστοχία αποχώρησης ή παραβίαση

9.3 Έλεγχος εκδόσεων και έγκριση

9.3.1 Κάθε έκδοση της παρούσας πολιτικής πρέπει να περιλαμβάνει:

9.3.1.1 Αριθμό έκδοσης και ημερομηνία

9.3.1.2 Σύνοψη αλλαγών

9.3.1.3 Έγκριση από τον Γενικό Διευθυντή

9.3.1.4 Αρχειοθετημένες προηγούμενες εκδόσεις που διατηρούνται για τουλάχιστον τρία έτη

9.4 Επικοινωνία και επιβεβαίωση

9.4.1 Όλο το προσωπικό που είναι αρμόδιο για την ένταξη ή την αποχώρηση πρέπει να ενημερώνεται για κάθε επικαιροποίηση της πολιτικής. Η ετήσια ευαισθητοποίηση ή επαναληπτική εκπαίδευση είναι υποχρεωτική.

10. Σχετικές πολιτικές και διασυνδέσεις

10.1 Η παρούσα πολιτική υποστηρίζει και υποστηρίζεται από τις ακόλουθες:

10.1.1 P2S – Πολιτική ρόλων και αρμοδιοτήτων διακυβέρνησης: Διασφαλίζει τη λογοδοσία στις διαδικασίες πρόσβασης και ένταξης

10.1.2 P4S – Πολιτική Ελέγχου Πρόσβασης: Καθορίζει την τεχνική εφαρμογή της χορήγησης πρόσβασης βάσει ρόλων και της απενεργοποίησης

10.1.3 P6S – Πολιτική Διαχείρισης Κινδύνων: Αξιολογεί τους κινδύνους που προκύπτουν από αστοχίες ελέγχων ένταξης και αποχώρησης

10.1.4 P8S – Πολιτική Ευαισθητοποίησης και Εκπαίδευσης για την Ασφάλεια Πληροφοριών: Επιβάλλει τις απαιτήσεις ενημέρωσης προσωπικού κατά την ένταξη

10.1.5 P30S – Πολιτική Αντιμετώπισης Περιστατικών: Αντιμετωπίζει ως περιστατικά ασφάλειας την αποτυχία αφαίρεσης δικαιωμάτων πρόσβασης ή την κλοπή περιουσιακών στοιχείων

11. Πρότυπα και πλαίσια αναφοράς

11.1 ISO/IEC 27001

11.1.1 Ρήτρα 6.2 – Καθορίζει απαιτήσεις ασφάλειας ανθρώπινου δυναμικού

11.1.2 Ρήτρα 7.2 – Επιβάλλει εκπαίδευση ευαισθητοποίησης για νέο προσωπικό

11.2 ISO/IEC 27002

11.2.1 Οι έλεγχοι 6.2 και 6.5 – Εξειδικεύουν τις πρακτικές ασφάλειας για την ένταξη και την αποχώρηση εργαζομένων

11.3 NIST SP 800-53 Rev. 5

11.3.1 PS-4 – Διαδικασίες αποχώρησης προσωπικού, συμπεριλαμβανομένης της απενεργοποίησης πρόσβασης

11.3.2 AC-2 – Διασφαλίζει τη διαχείριση του κύκλου ζωής λογαριασμών για την πρόσβαση χρηστών

11.3.3 PL-4 – Απαιτεί σχεδιασμό για μεταβάσεις προσωπικού

11.4 ΓΚΠΔ της ΕΕ

11.4.1 Άρθρο 32 – Διασφαλίζει κατάλληλη ασφάλεια κατά τη διάρκεια και μετά την απασχόληση, ιδίως ως προς την πρόσβαση σε δεδομένα προσωπικού χαρακτήρα

11.5 Οδηγία NIS2 της ΕΕ

11.5.1 Άρθρο 21(2)(h) – Απαιτεί ελέγχους ασφάλειας ανθρώπινου δυναμικού και κύκλου ζωής πρόσβασης

11.6 Κανονισμός DORA της ΕΕ

11.6.1 Άρθρο 12 – Απαιτεί από τις ρυθμιζόμενες χρηματοοικονομικές οντότητες να ελέγχουν την πρόσβαση του προσωπικού σε συστήματα ΤΠΕ, συμπεριλαμβανομένων των διαδικασιών ανάκλησης

11.7 COBIT 2019

11.7.1 APO07 – Διαχείριση Ανθρώπινου Δυναμικού: Καθορίζει απαιτήσεις ασφάλειας για τον κύκλο ζωής του προσωπικού

11.7.2 DSS01 – Διαχείριση Λειτουργιών: Καλύπτει τον έλεγχο λογικής και φυσικής πρόσβασης κατά τις μεταβάσεις απασχόλησης