					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P07					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	Ρήτρα 7.2, Ρήτρα 6	Ικανότητα προσωπικού, ασφαλής ένταξη, εφαρμογή αρμοδιοτήτων κατά την αποχώρηση/αλλαγή ρόλου.
ISO/IEC 27002:2022	Έλεγχοι 6.2, 6.5, 5	Ένταξη, πρόσβαση και έλεγχοι κύκλου ζωής προσωπικού.
NIST SP 800-53 Rev.5	PS-4, PS-5, AC-2, AC-6, IA-4, IA-5, CM-5, AU-2, AU-6	Μετάβαση και αποχώρηση προσωπικού, αρχή του ελάχιστου απαιτούμενου δικαιώματος, καταγραφή ελέγχου, διαχείριση πρόσβασης κατά τη διάρκεια και μετά από αλλαγές προσωπικού.
ΓΚΠΔ της ΕΕ	Άρθρα 5(1)(f), 25, 32, Αιτιολογική σκέψη 39	Περιορισμός πρόσβασης, εμπιστευτικότητα, προστασία και κατάλληλοι έλεγχοι για δεδομένα προσωπικού χαρακτήρα.
Οδηγία NIS2 της ΕΕ	Άρθρο 21(2)(b, c, d)	Μέτρα ασφάλειας προσωπικού/λειτουργίας, μετριασμός εσωτερικών απειλών, διεργασίες κύκλου ζωής.
Κανονισμός DORA της ΕΕ	Άρθρα 5, 8, 9	Διακυβέρνηση, εσωτερικός έλεγχος ΤΠΕ, κίνδυνος ΤΠΕ, διαχείριση περιστατικών κατά τη μετάβαση προσωπικού.
COBIT 2019	APO07, BAI08, DSS05, MEA03	Ανθρώπινοι πόροι, διαχείριση γνώσης, ασφάλεια και συμμόρφωση κατά την ένταξη/αποχώρηση.

1. Σκοπός

1.1 Η παρούσα πολιτική καθορίζει τυποποιημένες διαδικασίες για τη διαχείριση της ένταξης, των εσωτερικών μετακινήσεων και των αποχωρήσεων για όλους τους τύπους χρηστών.

1.2 Διασφαλίζει την έγκαιρη και ασφαλή χορήγηση πρόσβασης και την αφαίρεση δικαιωμάτων φυσικής και λογικής πρόσβασης, εφαρμόζοντας παράλληλα την εμπιστευτικότητα, τη λογοδοσία και την ανάκτηση περιουσιακών στοιχείων.

1.3 Η παρούσα πολιτική μετριάζει τους κινδύνους που συνδέονται με μη εξουσιοδοτημένη πρόσβαση, διαρροή δεδομένων και μη επιστραφέντα περιουσιακά στοιχεία, ενσωματώνοντας ελέγχους ένταξης και αποχώρησης στις διεργασίες του Ανθρώπινου Δυναμικού (HR), της Πληροφορικής και της ασφάλειας.

1.4 Υποστηρίζει το ISO/IEC 27001:2022, Παράρτημα Α, Έλεγχο 6.5, διασφαλίζοντας ότι οι υποχρεώσεις ασφάλειας προσωπικού εφαρμόζονται κατά τη διάρκεια και μετά την απασχόληση ή τη συνεργασία.

2. Πεδίο εφαρμογής

2.1 Η παρούσα πολιτική εφαρμόζεται σε όλους τους εργαζομένους, αναδόχους, συμβούλους, προμηθευτές και λοιπά τρίτα μέρη στα οποία παρέχεται πρόσβαση στα συστήματα, δίκτυα, εγκαταστάσεις ή δεδομένα του οργανισμού.

2.2 Καλύπτει τον πλήρη κύκλο ζωής των εξής:

2.2.1 διαδικασία ένταξης (πρόσληψη, σύναψη σύμβασης ή προσωρινή συνεργασία)

2.2.2 εσωτερικές μετακινήσεις ή αλλαγές ρόλου

2.2.3 διαδικασία αποχώρησης (παραίτηση, συνταξιοδότηση, λύση συνεργασίας, λήξη σύμβασης)

2.3 Η πολιτική καλύπτει:

2.3.1 λογική πρόσβαση (συστήματα, εφαρμογές, υπηρεσίες νέφους, VPN)

2.3.2 φυσική πρόσβαση (κάρτες πρόσβασης, κλειδιά, συστήματα εισόδου κτιρίων)

2.3.3 ανατεθειμένα περιουσιακά στοιχεία (φορητοί υπολογιστές, τηλέφωνα, διακριτικά, διαπιστευτήρια)

2.3.4 βεβαίωση αποδοχής πολιτικών και υποχρεώσεις εμπιστευτικότητας

2.4 Όλα τα τμήματα (HR, Πληροφορική, Εγκαταστάσεις, Ασφάλεια και Διοίκηση) είναι υπεύθυνα για την εκτέλεση του ρόλου τους στις ροές εργασιών ένταξης και αποχώρησης.

3. Στόχοι

3.1 Να διασφαλίζεται ότι σε όλο το προσωπικό παρέχεται πρόσβαση μόνο μετά την ικανοποίηση των προαπαιτούμενων ασφάλειας, εκπαίδευσης και συμβατικών απαιτήσεων.

3.2 Να ανακαλούνται τα δικαιώματα πρόσβασης και να ανακτώνται τα περιουσιακά στοιχεία του οργανισμού αμέσως μετά από αλλαγή ρόλου ή αποχώρηση.

3.3 Να διατηρούνται η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα των περιουσιακών στοιχείων του οργανισμού κατά τις μεταβάσεις προσωπικού.

3.4 Να υποστηρίζεται η δυνατότητα ελέγχου και η νομική τεκμηρίωση μέσω πλήρων αρχείων ένταξης και αποχώρησης.

3.5 Να μειώνεται η έκθεση σε εσωτερικές απειλές με την επικύρωση και τεκμηρίωση όλων των συμβάντων πρόσβασης που σχετίζονται με το προσωπικό.

3.6 Να ευθυγραμμίζεται ο κύκλος ζωής του ανθρώπινου δυναμικού του οργανισμού με πρακτικές ασφάλειας βάσει κινδύνου και κανονιστικές απαιτήσεις.

4. Ρόλοι και αρμοδιότητες

4.1 Εκτελεστική Διοίκηση

4.1.1 Εγκρίνει την παρούσα πολιτική και διαθέτει αρμοδιότητες και πόρους για τις διαδικασίες ένταξης, αποχώρησης και ελέγχου πρόσβασης.

4.1.2 Διασφαλίζει ότι οι μεταβάσεις προσωπικού δεν εκθέτουν τον οργανισμό σε αδικαιολόγητο κίνδυνο ασφάλειας ή νομικό κίνδυνο.

4.2 Ανθρώπινο Δυναμικό (HR)

4.2.1 Εκκινεί τις ροές εργασιών ένταξης και αποχώρησης για εργαζομένους και γνωστοποιεί τις αλλαγές στα σχετικά τμήματα.

4.2.2 Διασφαλίζει ότι οι έλεγχοι ιστορικού, οι συμβάσεις, οι συμφωνίες εμπιστευτικότητας (NDA) και οι βεβαιώσεις αποδοχής πολιτικών έχουν ολοκληρωθεί πριν από τη χορήγηση πρόσβασης.

4.2.3 Ενημερώνει την Πληροφορική και τις Εγκαταστάσεις για αποχωρήσεις προσωπικού σύμφωνα με τη συμφωνία επιπέδου υπηρεσιών για την ειδοποίηση.

4.2.4 Συντονίζεται με το Νομικό Τμήμα για την εφαρμογή υποχρεώσεων μετά τη λήξη της απασχόλησης (π.χ. ρήτρες μη γνωστοποίησης).

[... 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 Συχνότητα ανασκόπησης πολιτικής

9.1.1 Η παρούσα πολιτική πρέπει να ανασκοπείται:

9.1.1.1 ετησίως, ή

9.1.1.2 μετά από κάθε ουσιώδες περιστατικό που αφορά κακή χρήση πρόσβασης, απώλεια περιουσιακών στοιχείων ή αστοχία διαδικασίας

9.1.1.3 κατά την υλοποίηση σημαντικών αλλαγών σε πλατφόρμες HR ή IAM

9.1.1.4 μετά από κανονιστικές ή νομικές επικαιροποιήσεις που επηρεάζουν δεδομένα προσωπικού ή σχετικές υποχρεώσεις

9.2 Διαδικασία ανασκόπησης και ιδιοκτησία

9.2.1 Ο Υπεύθυνος ΣΔΑΠ και ο Διευθυντής HR οφείλουν να συντονίζουν την ανασκόπηση, με συνεισφορά από την Ασφάλεια Πληροφοριών, τη Νομική Υπηρεσία και Συμμόρφωση.

9.2.2 Όλες οι αλλαγές πρέπει να εγκρίνονται από την Εκτελεστική Διοίκηση και την Επιτροπή Καθοδήγησης ΣΔΑΠ.

9.2.3 Οι αναθεωρημένες εκδόσεις πρέπει να αναδιανέμονται στα επηρεαζόμενα τμήματα και στο προσωπικό για νέα επιβεβαίωση αποδοχής.

9.3 Έλεγχος εγγράφου και διατήρηση

9.3.1 Η παρούσα πολιτική πρέπει να περιλαμβάνει:

9.3.2 έλεγχο εκδόσεων, ιστορικό αλλαγών και ημερομηνία έναρξης ισχύος

9.3.3 υπεύθυνο ιδιοκτήτη και ανασκοπούντες

9.3.4 ταξινόμηση πολιτικής και αρχείο έγκρισης

9.3.5 Οι παρωχημένες εκδόσεις πρέπει να αρχειοθετούνται για τουλάχιστον 3 έτη σύμφωνα με την Πολιτική Διαχείρισης Εγγράφων.

10. Σχετικές πολιτικές και διασυνδέσεις

10.1.1 Η παρούσα πολιτική διασυνδέεται άμεσα με:

10.1.2 P1 – Πολιτική Ασφάλειας Πληροφοριών: Καθορίζει τους στόχους ασφάλειας του οργανισμού, συμπεριλαμβανομένης της διακυβέρνησης της πρόσβασης προσωπικού.

10.1.3 P4 – Πολιτική Ελέγχου Πρόσβασης: Καθορίζει τις λειτουργικές απαιτήσεις για τη χορήγηση και ανάκληση πρόσβασης σε συστήματα και φυσική πρόσβαση βάσει ενεργοποιητών ένταξης και αποχώρησης.

10.1.4 P3 – Πολιτική Αποδεκτής Χρήσης: Απαιτεί βεβαίωση αποδοχής κατά τη διαδικασία ένταξης και υποστηρίζει την εφαρμογή της πολιτικής μετά την αποχώρηση.

10.1.5 P6 – Πολιτική Διαχείρισης Κινδύνων: Διασφαλίζει ότι οι κίνδυνοι πρόσβασης χρηστών και μεταβάσεων αξιολογούνται και μετριάζονται σύμφωνα με τις αρχές του ΣΔΑΠ.

10.1.6 P11 – Πολιτική Διαχείρισης Λογαριασμών Χρηστών και Προνομίων: Διέπει τους τεχνικούς ελέγχους για τη χορήγηση πρόσβασης και την αφαίρεση δικαιωμάτων πρόσβασης προς υποστήριξη της παρούσας πολιτικής.

10.2 Οι πολιτικές αυτές συγκροτούν ένα ολοκληρωμένο σύστημα ελέγχων για την ασφαλή και υπόλογη διαχείριση συμβάντων του κύκλου ζωής ανθρώπινου δυναμικού.

11. Πρότυπα και πλαίσια αναφοράς

11.1 Η παρούσα πολιτική ευθυγραμμίζεται με διεθνώς αναγνωρισμένα πλαίσια ασφάλειας, ιδιωτικότητας και διακυβέρνησης ΤΠ, ώστε οι διαδικασίες ένταξης και αποχώρησης να είναι ασφαλείς, να παρέχουν ιχνηλασιμότητα και να συμμορφώνονται με νομικές και οργανωτικές απαιτήσεις.

11.2 ISO/IEC 27001:

11.2.1 Ρήτρα 7.2 – Competence και Ρήτρα 6.2 – Information Security Objectives: Η παρούσα πολιτική υποστηρίζει τη διασφάλιση της ικανότητας του προσωπικού και την ασφαλή ένταξη ατόμων σε ρόλους που επηρεάζουν τους στόχους του ΣΔΑΠ.

11.2.2 Παράρτημα Α, Έλεγχος 6.5 – Responsibilities After Termination or Change of Employment: Η παρούσα πολιτική εφαρμόζει πλήρως ελέγχους για υπολειπόμενα δικαιώματα πρόσβασης, κατοχή δεδομένων και συμβατικές υποχρεώσεις κατά την αποχώρηση.

11.2.3 Παράρτημα Α, Έλεγχος 5.9 – Screening και 6.2 – Terms and Conditions of Employment: Οι διαδικασίες ένταξης ενσωματώνουν μηχανισμούς επαλήθευσης ιστορικού και βεβαίωσης αποδοχής πολιτικών σύμφωνα με τις εν λόγω ρήτρες.

11.3 NIST SP 800-53 Rev.5:

11.3.1 PS-4 (Personnel Termination) και PS-5 (Personnel Transfer): Η παρούσα πολιτική εφαρμόζει δομημένη αφαίρεση ή τροποποίηση δικαιωμάτων πρόσβασης, φυσικών καρτών πρόσβασης και περιουσιακών στοιχείων.

11.3.2 AC-2 (Account Management) και AC-6 (Least Privilege): Οι σχετικές προβλέψεις διασφαλίζουν ότι η πρόσβαση ευθυγραμμίζεται με τον ρόλο και ανακαλείται άμεσα όταν δεν είναι πλέον αναγκαία.

11.3.3 IA-4 (Identifier Management) και IA-5 (Authenticator Management): Υποστηρίζεται η ασφαλής διαχείριση διαπιστευτηρίων κατά τη διάρκεια και μετά από αλλαγές προσωπικού.

11.3.4 CM-5 (Access Restrictions for Change): Αποτρέπει μη εξουσιοδοτημένες αλλαγές μετά την αποχώρηση με την ανάκληση αυξημένων δικαιωμάτων πρόσβασης.

11.3.5 AU-2 και AU-6: Η καταγραφή και η ιχνηλασιμότητα συμβάντων πρόσβασης ενισχύονται μέσω της ενοποίησης IAM και του ίχνους ελέγχου.

11.4 ΓΚΠΔ της ΕΕ (2016/679):

11.4.1 Άρθρο 5(1)(f): Προστατεύει τα προσωπικά δεδομένα από μη εξουσιοδοτημένη πρόσβαση, κάτι που εφαρμόζεται εδώ μέσω της ανάκλησης της πρόσβασης χρηστών κατά τη διαδικασία αποχώρησης.

11.4.2 Άρθρο 32: Επιβάλλει κατάλληλα τεχνικά και οργανωτικά μέτρα για την ασφάλεια των προσωπικών δεδομένων κατά τον κύκλο ζωής της απασχόλησης.

11.4.3 Άρθρο 25 – Προστασία δεδομένων ήδη από τον σχεδιασμό: Διασφαλίζει ότι η ένταξη και η αποχώρηση ενσωματώνουν ελαχιστοποίηση δεδομένων, διατήρηση και νόμιμους ελέγχους πρόσβασης.

11.4.4 Αιτιολογική σκέψη 39: Τονίζει τον περιορισμό της πρόσβασης και την εμπιστευτικότητα, στοιχεία που υποστηρίζονται από τη δομή της παρούσας πολιτικής.

11.5 Οδηγία NIS2 της ΕΕ (2022/2555):

11.5.1 Άρθρο 21(2)(b, c, d): Απαιτεί μέτρα ασφάλειας προσωπικού και λειτουργίας για την αντιμετώπιση του ελέγχου πρόσβασης, του μετριασμού εσωτερικών απειλών και των διεργασιών κύκλου ζωής, τα οποία αποτυπώνονται στην παρούσα πολιτική.

11.6 Κανονισμός DORA της ΕΕ (2022/2554):

11.6.1 Άρθρο 5 – Διακυβέρνηση και εσωτερικός έλεγχος: Η παρούσα πολιτική υποστηρίζει την εσωτερική διακυβέρνηση ΤΠΕ που σχετίζεται με τον ανθρώπινο κίνδυνο και τη διαχείριση πρόσβασης.

11.6.2 Άρθρο 8 – Διαχείριση κινδύνων ΤΠΕ: Εφαρμόζει ελέγχους σε μεταβάσεις προσωπικού που θα μπορούσαν να εκθέσουν κρίσιμα περιουσιακά στοιχεία ή ρυθμιζόμενα περιβάλλοντα.

11.6.3 Άρθρο 9 – Ταξινόμηση και διαχείριση περιστατικών: Διασφαλίζει ότι παραβιάσεις που σχετίζονται με αποχώρηση είναι κοινοποιήσιμες και μετριάζονται μέσω ορθής αποπαροχοποίησης και χειρισμού περιουσιακών στοιχείων.

11.7 COBIT 2019:

11.7.1 APO07 – Managed Human Resources: Καθορίζει τους ρόλους, τις αρμοδιότητες και τις ενέργειες κύκλου ζωής για ένταξη και αποχώρηση σε ευθυγράμμιση με τους στόχους διακυβέρνησης.

11.7.2 BAI08 – Knowledge Management: Ενισχύει την τεκμηρίωση διαδικασιών, τη διατήρηση γνώσης και τη μεταβίβαση ελέγχου στο τέλος της απασχόλησης.

11.7.3 DSS05 – Managed Security Services: Εφαρμόζει απενεργοποίηση χρηστών, έλεγχο περιουσιακών στοιχείων και λογοδοσία κατά τις μεταβάσεις ρόλων.

11.7.4 MEA03 – Monitor, Evaluate, and Assess Compliance: Διασφαλίζει ότι οι έλεγχοι ένταξης και αποχώρησης αξιολογούνται στο πλαίσιο εσωτερικών και εξωτερικών ελέγχων.