					[Insert Registered Legal Entity Name Here]									
Document number: P7					Document Title: **Onboarding and Termination Policy**									
Version: 1.0		Effective Date: 01.01.2025			Document Owner:									
X	Policy		Standard		Procedure		Form		Register		Other			

Revision history				
Revision number	**Revision Date**	**Changes**	**Reviewed by**	**Process owner**

Approvals			
Name	**Title**	**Date**	**Signature**

Aligned with standards and regulations where applicable		
Standard/Regulation	**Clause/Article**	**Comment**
ISO/IEC 27001:2022	Clause 7.2, Clause 6.2	
ISO/IEC 27002:2022	Controls 6.2, 6.5, 5.9	
NIST SP 800-53 Rev.5	PS-4, PS-5	
EU GDPR	Articles 5(1)(f), 25, 32; Recital 39	
EU NIS2	Article 21(2)(b, c, d)	
EU DORA	Articles 5, 8, 9	
COBIT 2019	APO07, BAI08, DSS05, MEA03	

					[Insert Registered Legal Entity Name Here]								
Document number: P7					Document Title: **Onboarding and Termination Policy**								
Version: 1.0		Effective Date: 01.01.2025			Document Owner:								
X	Policy		Standard		Procedure		Form		Register		Other		

1. Purpose

1.1 This policy establishes standardized procedures to manage onboarding, internal transfers, and terminations across all user types.

1.2 It ensures timely and secure provisioning and deprovisioning of physical and logical access, while enforcing confidentiality, accountability, and asset recovery.

1.3 This policy mitigates risks associated with unauthorized access, data leakage, and unreturned assets by embedding onboarding and termination controls into HR, IT, and security processes.

1.4 It supports ISO/IEC 27001:2022 Annex A Control 6.5 by ensuring personnel security obligations are enforced during and after employment or engagement.

2. Scope

2.1 This policy applies to all employees, contractors, consultants, vendors, and other third parties granted access to the organization's systems, networks, facilities, or data.

2.2 It governs the full lifecycle of:

2.2.1 Onboarding (hiring, contracting, or temporary engagement)

2.2.2 Internal transfers or role changes

2.2.3 Offboarding (resignation, retirement, termination, contract expiry)

2.3 The policy covers:

2.3.1 Logical access (systems, applications, cloud, VPN)

2.3.2 Physical access (badges, keys, building entry systems)

2.3.3 Assigned assets (laptops, phones, tokens, credentials)

2.3.4 Acknowledgment of policies and confidentiality obligations

2.4 All departments (HR, IT, Facilities, Security, and Management) are responsible for executing their role in onboarding and offboarding workflows.

3. Objectives

3.1 To ensure that all personnel are granted access only after satisfying security, training, and contractual prerequisites.

3.2 To revoke access rights and recover organizational assets immediately upon role change or termination.

3.3 To preserve the confidentiality, integrity, and availability of organizational assets during personnel transitions.

3.4 To support auditability and legal defensibility through complete records of onboarding and termination events.

3.5 To reduce insider threat exposure by validating and documenting all personnel-related access events.

3.6 To align the organization's people lifecycle with risk-based security practices and regulatory mandates.

4. Roles and Responsibilities

4.1 **Executive Management**

4.1.1 Approves this policy and allocates authority and resources for onboarding, offboarding, and access control processes.

4.1.2 Ensures that personnel transitions do not expose the organization to undue security or legal risk.

4.2 **Human Resources (HR)**

4.2.1 Initiates onboarding and termination workflows for employees and notifies relevant departments of changes.

4.2.2 Ensures that background checks, contracts, NDAs, and policy acknowledgments are completed prior to access being granted.

[.....]

11. Reference Standards and Frameworks

This policy is aligned with internationally recognized security, privacy, and IT governance frameworks to ensure that onboarding and termination processes are secure, traceable, and compliant with legal and organizational requirements.

ISO/IEC 27001:2022

Clause 7.2 – Competence and **Clause 6.2 – Information Security Objectives**: This policy supports the establishment of personnel competence and the secure integration of individuals into roles where they influence ISMS objectives.

Annex A Control 6.5 – Responsibilities After Termination or Change of Employment: This policy fully enforces controls over residual access rights, data custody, and contractual obligations upon departure.

Annex A Control 5.9 – Screening and **6.2 – Terms and Conditions of Employment**: Onboarding procedures incorporate background verification and policy acknowledgment mechanisms consistent with these clauses.

NIST SP 800-53 Rev.5

PS-4 (Personnel Termination) and **PS-5 (Personnel Transfer)**: This policy enforces structured removal or modification of access rights, physical badges, and assets.

AC-2 (Account Management) and **AC-6 (Least Privilege)**: Provisions ensure access is role-aligned and promptly revoked when no longer necessary.

IA-4 (Identifier Management) and **IA-5 (Authenticator Management)**: Supports secure management of credentials during and after personnel changes.

CM-5 (Access Restrictions for Change): Prevents unauthorized post-termination changes by revoking elevated access rights.

AU-2 and AU-6: Logging and traceability of access events are reinforced through IAM and audit trail integration.

EU GDPR (2016/679)

Article 5(1)(f): Protects personal data against unauthorized access, enforced here by revoking user access during offboarding.

Article 32: Mandates appropriate technical and organizational controls to secure personal data during the employment lifecycle.

Article 25 – Data Protection by Design: Ensures that onboarding and termination integrate data minimization, retention, and lawful access controls.

Recital 39: Emphasizes access limitation and confidentiality, supported by the structure of this policy.

EU NIS2 Directive (2022/2555)

Article 21(2)(b, c, d): Requires personnel and operational security measures to address access control, insider threat mitigation, and lifecycle processes, all of which are reflected in this policy.

EU DORA (2022/2554)

Article 5 – Governance and Internal Control: This policy supports internal ICT governance related to human risk and access management.

Article 8 – ICT Risk Management: Applies controls to personnel transitions that could expose critical assets or regulated environments.

Article 9 – Incident Classification and Management: Ensures termination-related breaches are reportable and mitigated through proper deprovisioning and asset handling.

COBIT 2019

APO07 – Managed Human Resources: Defines the roles, responsibilities, and lifecycle actions for onboarding and termination aligned to governance objectives.

BAI08 – Knowledge Management: Reinforces the documentation of procedures, retention of knowledge, and control transfer at the end of employment.

DSS05 – Managed Security Services: Enforces user deactivation, asset control, and accountability during role transitions.

MEA03 – Monitor, Evaluate, and Assess Compliance: Ensures onboarding and offboarding controls are assessed during internal and external audits.