					Insert Registered Legal Entity Name Here							
Document number: P07					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

Standard/Regulation	Clause/Article	Comment
ISO/IEC 27001:2022	Clause 7.2, Clause 6	Personnel competence, secure integration, and enforcement of responsibilities on termination or change of employment.
ISO/IEC 27002:2022	Controls 6.2, 6.5, 5	Onboarding, access, and personnel lifecycle controls.
NIST SP 800-53 Rev.5	PS-4, PS-5, AC-2, AC-6, IA-4, IA-5, CM-5, AU-2, AU-6	Personnel transition and termination, least privilege, audit logging, and access management during and after personnel changes.
EU GDPR	Articles 5(1)(f), 25, 32; Recital 39	Access limitation, confidentiality, protection, and appropriate controls for personnel data.
EU NIS2	Article 21(2)(b, c, d)	Personnel and operational security measures; insider threat mitigation; lifecycle processes.
EU DORA	Articles 5, 8, 9	Governance, internal ICT control, ICT risk, and incident management during personnel transition.
COBIT 2019	APO07, BAI08, DSS05, MEA03	Human resources, knowledge management, security, and compliance in onboarding and termination.

1. Purpose

1.1 This policy establishes standardized procedures for managing 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 Human Resources (HR), IT, and security processes.

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

2. Scope

2.1 This policy applies to all personnel, contractors, third-party service providers, 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 services, corporate VPN)

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

2.3.3 assigned assets (laptops, phones, MFA/SSO tokens, authentication credentials)

2.3.4 mandatory acknowledgments of policies and confidentiality obligations

2.4 All departments (Human Resources (HR), IT, Facilities and Asset Management, 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 privileges 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 audit readiness and legal defensibility through complete records of onboarding and termination events.

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

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

4. Roles and Responsibilities

4.1 Top Management

4.1.1 Approves this policy and allocates authority, accountability, 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, Non-Disclosure Agreements (NDAs), and mandatory acknowledgments are completed before access is granted.

4.2.3 Informs IT and Facilities of staff departures in accordance with the notification service level agreement.

4.2.4 Coordinates with Legal and Compliance to enforce post-employment obligations (e.g., non-disclosure clauses).

[... Sections 4.3–8 are not included in this preview. Purchase the full document to access the complete policy content. ...]

9. Review and Update Requirements

9.1 Policy Review Frequency

9.1.1 This policy must be reviewed:

9.1.1.1 annually, or

9.1.1.2 after any material incident involving access misuse, asset loss, or procedural failure

9.1.1.3 when implementing major changes to Human Resources (HR) or the IAM platform

9.1.1.4 upon regulatory or legal updates affecting personnel data or obligations

9.2 Review Process and Ownership

9.2.1 The ISMS Manager and Human Resources (HR) Director shall coordinate the review, with input from IT Security, Legal, and Compliance.

9.2.2 All changes must be approved by Top Management and the ISMS Steering Committee.

9.2.3 Revised versions must be redistributed to affected departments and personnel for re-acknowledgment.

9.3 Document Control and Retention

9.3.1 This policy shall include:

9.3.2 version control, change history, and effective date

9.3.3 responsible owner and reviewer(s)

9.3.4 policy classification and approval record

9.3.5 Obsolete versions shall be archived for a minimum of 3 years in accordance with the Document Management Policy.

10. Related Policies and Linkages

10.1.1 This policy directly integrates with:

10.1.2 P1 – Information Security Policy: Establishes the organization's security objectives, including personnel access governance.

10.1.3 P4 – Access Control Policy: Provides operational requirements for assigning and revoking system and physical access based on onboarding and termination triggers.

10.1.4 P3 – Acceptable Use Policy: Requires acknowledgment during onboarding and supports enforcement after termination.

10.1.5 P6 – Risk Management Policy: Ensures that user access and transition risks are evaluated and mitigated in line with ISMS principles.

10.1.6 P11 – User Account and Privilege Management Policy: Governs the technical controls for user provisioning and deprovisioning in support of this policy.

10.2 These policies form an integrated control system for managing personnel lifecycle events securely and accountably.

11. Reference Standards and Frameworks

11.1 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.

11.2 ISO/IEC 27001:

11.2.1 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.

11.2.2 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.

11.2.3 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 controls.

11.3 NIST SP 800-53 Rev.5:

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

11.3.2 AC-2 (Account Management) and AC-6 (Least Privilege): Requirements ensure that access is aligned to role and promptly revoked when no longer needed.

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

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

11.3.5 AU-2 and AU-6: Audit logging and traceability of access events are reinforced through integration between the Identity and Access Management platform and the audit trail.

11.4 EU GDPR (2016/679):

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

11.4.2 Article 32: Requires appropriate technical and organizational controls to secure personal data throughout the employment lifecycle.

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

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

11.5 EU NIS2 Directive (2022/2555):

11.5.1 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.

11.6 EU DORA (2022/2554):

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

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

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

11.7 COBIT 2019:

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

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

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

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