					Insert Registered Legal Entity Name Here							
Document number: P07S					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	Clauses 6.2, 7	HR security and awareness requirements
ISO/IEC 27002:2022	Controls 6.2, 6.5	Onboarding and termination security practices
NIST SP 800-53 Rev.5	PS-4, AC-2, PL-4	Personnel termination, account lifecycle, and planning
EU NIS2	Article 21(2)(h)	HR security and access lifecycle
EU DORA	Article 12	Access controls and revocation for ICT systems
COBIT 2019	APO07, DSS01	Personnel security and logical/physical access controls
EU GDPR	Article 32	Security of personal data during employment

1. Purpose

1.1 This policy defines the process for onboarding new employees and contractors and for securely removing access when individuals leave the organization or change roles.

1.2 It ensures that access is provisioned according to the principle of least privilege, that all assets are accounted for, and that critical actions such as account deactivation and data recovery are completed promptly.

1.3 This policy supports compliance, operational integrity, and data protection through structured and auditable onboarding and termination activities.

2. Scope

2.1 This policy applies to:

2.1.1 All permanent and temporary workers

2.1.2 Contractors, consultants, and interns

2.1.3 External service providers with system or physical access

2.2 It covers:

2.2.1 Onboarding: user account creation, access provisioning, and equipment issuance

2.2.2 Offboarding: access removal, recovery of company assets, and secure closure of digital identities

2.2.3 Internal role changes requiring access reconfiguration or asset reassignment

2.3 This policy applies to all devices, platforms, and locations used for official business activities.

3. Objectives

3.1 Ensure that new personnel receive access and resources based on verified roles and responsibilities.

3.2 Confirm that departing users are fully removed from systems and facilities by the end of their last working day.

3.3 Prevent orphaned accounts and unreturned assets that present security risk.

3.4 Maintain documented records of onboarding, internal transfers, and offboarding activities.

3.5 Promote accountability through checklists and cross-functional coordination.

4. Roles and Responsibilities

4.1 General Manager

4.1.1 Approves access for high-privilege roles and oversees the onboarding and termination program.

4.1.2 Ensures that exceptions are justified and that corrective actions are taken when processes are not followed.

4.2 Office Manager / Human Resources (HR)

4.2.1 Initiates onboarding for new hires and notifies IT of departures.

4.2.2 Ensures completion of required legal documents (e.g., Non-Disclosure Agreement (NDA)) and security policy acknowledgements.

4.2.3 Maintains onboarding and offboarding checklists and monitors compliance with this policy.

[... 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 Annual Review

9.1.1 This policy must be reviewed at least annually by the General Manager and the HR and IT leads.

9.2 Early Review Triggers

9.2.1 Updates must be made if:

9.2.1.1 New Human Resources (HR) or IT systems are introduced

9.2.1.2 There is a change in the External IT Provider or managed HR service

9.2.1.3 Security audits identify process gaps

9.2.1.4 Regulatory obligations change (e.g., GDPR updates)

9.2.1.5 A critical offboarding failure or security breach occurs

9.3 Version Control and Approval

9.3.1 Every version of this policy must include:

9.3.1.1 Version number and date

9.3.1.2 Summary of changes

9.3.1.3 Approval by the General Manager

9.3.1.4 Archived previous versions retained for at least three years

9.4 Communication and Acknowledgment

9.4.1 All personnel responsible for onboarding or termination must be informed of any policy updates. Annual awareness or refresher training is mandatory.

10. Related Policies and Linkages

10.1 This policy supports and is supported by the following:

10.1.1 P2S – Governance Roles and Responsibilities Policy: Ensures accountability in access and onboarding processes

10.1.2 P4S – Access Control Policy: Establishes technical enforcement of role-based provisioning and deactivation

10.1.3 P6S – Risk Management Policy: Assesses risks arising from failures in onboarding and termination controls

10.1.4 P8S – Information Security Awareness and Training Policy: Establishes personnel orientation requirements during onboarding

10.1.5 P30S – Incident Response Policy: Treats failures to deprovision access or asset theft as security incidents

11. Reference Standards and Frameworks

11.1 ISO/IEC 27001

11.1.1 Clause 6.2 – Establishes HR security requirements

11.1.2 Clause 7.2 – Requires awareness training for new personnel

11.2 ISO/IEC 27002

11.2.1 Controls 6.2 and 6.5 – Describe security practices for onboarding and termination of employment

11.3 NIST SP 800-53 Rev. 5

11.3.1 PS-4 – Personnel termination procedures, including access deactivation

11.3.2 AC-2 – Ensures account lifecycle management for user access

11.3.3 PL-4 – Requires planning for personnel transitions

11.4 EU GDPR

11.4.1 Article 32 – Requires appropriate security during and after employment, particularly for access to personal data

11.5 EU NIS2 Directive

11.5.1 Article 21(2)(h) – Requires HR security and access lifecycle controls

11.6 EU DORA

11.6.1 Article 12 – Requires regulated financial entities to control personnel access to ICT systems, including revocation procedures

11.7 COBIT 2019

11.7.1 APO07 – APO07 Manage Human Resources: Establishes personnel lifecycle security requirements

11.7.2 DSS01 – Manage Operations: Covers control of logical and physical access during employment transitions