					[Insert Registered Legal Entity Name Here]							
Document number: P7S					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	Clauses 6.2, 7.2	
ISO/IEC 27002:2022	Controls 6.2, 6.5	
NIST SP 800-53 Rev.5	PS-4, AC-2, PL-4	
EU NIS2	Article 21(2)(h)	
EU DORA	Article 12	
COBIT 2019	APO07, DSS01	
EU GDPR	Article 32	

					[Insert Registered Legal Entity Name Here]								
Document number: P7S					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 defines the process for onboarding new employees or contractors and securely removing access when individuals leave or change roles.

1.2. It ensures that access is provisioned with the least privilege necessary, all assets are accounted for, and critical actions such as system 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 employees

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: creation of user accounts, access granting, equipment issuance

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

2.2.3. Internal role changes requiring access reconfiguration or asset reassignment

2.3. Applies to all devices, platforms, and locations used in official business functions.

3. Objectives

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

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

3.3. Prevent orphaned accounts and unreturned assets, which pose a security risk.

3.4. Maintain documented records of onboarding, transfers, and offboarding actions.

3.5. Promote accountability through checklists and cross-functional role 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 exceptions are justified and corrective actions are taken when processes are not followed.

4.2. **Office Manager / HR**

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

4.2.2. Ensures completion of legal documents (e.g., NDA) and security policy acknowledgements.

4.2.3. Maintains onboarding/offboarding checklists and monitors policy compliance.

4.3. **IT Support / External IT Provider**

4.3.1. Creates, adjusts, or disables system accounts.

4.3.2. Grants least-privilege access and updates the Access Log and Asset Inventory.

4.3.3. Retrieves company-issued devices and revokes credentials on exit.

4.4. **Department Managers**

4.4.1. Notify HR/IT of role changes or departures.

4.4.2. Validate that old permissions are removed and new ones correctly applied during transitions.

4.5. **Employees and Contractors**

4.5.1. Must complete onboarding requirements (e.g., security training, signing policy documents).

4.5.2. Must return all company assets and access credentials on departure.

5. Governance Requirements

5.1. **Onboarding Checklists**

5.1.1. A checklist must be used for each new hire, covering:

5.1.1.1. Security orientation

5.1.1.2. NDA and policy acknowledgment