					Insert Registered Legal Entity Name Here							
Document number: P04S					Document Title: **Access Control 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 5	
ISO/IEC 27002:2022	Controls: 5.15, 5.16, 5	
NIST SP 800-53 Rev.5	AC-1 to AC-5	
EU GDPR	Article 32	
EU NIS2	Article 21(2)(b)	
EU DORA	Article 9	
COBIT 2019	APO07, DSS	

1. Purpose

1.1. This policy defines how the organization manages access to systems, data, and facilities to ensure that only authorized individuals can access information based on business need.

1.2. It establishes clear rules for user provisioning, modification, monitoring, and removal to minimize the risk of unauthorized access and support compliance with applicable laws and standards.

1.3. This policy enforces the principle of least privilege and requires that access be limited to the minimum necessary to perform job functions.

2. Scope

2.1. This policy applies to all individuals who use or manage access to the organization's IT systems, networks, data, or facilities, including:

2.1.1. Employees

2.1.2. Contractors

2.1.3. Temporary workers

2.1.4. External IT service providers

2.2. It covers access to:

2.2.1. Company applications, file shares, and databases

2.2.2. Email, VPN, and remote access systems

2.2.3. Cloud-based services used for business purposes

2.2.4. Physical access to secure facilities, such as offices or server rooms

2.3. This policy applies across all devices (company-issued or approved BYOD), platforms, and locations.

3. Objectives

3.1. Ensure that access rights are granted only after formal approval based on role and business justification.

3.2. Prevent unauthorized or excessive access to sensitive data, systems, or infrastructure.

3.3. Define clear procedures for provisioning, modification, and termination of user access.

3.4. Require regular access reviews and automated or manual logging to support audits.

3.5. Support the technical enforcement of access restrictions through configuration and monitoring.

4. Roles and Responsibilities

4.1. General Manager

4.1.1. Approves this policy and ensures that resources are available to implement effective access controls.

4.1.2. Approves exceptions and reviews annual access audits.

4.2. IT Manager / External IT Provider

4.2.1. Manages the provisioning, modification, and termination of user accounts.

4.2.2. Maintains an access control register that records all activity (creations, changes, and removals).

4.2.3. Implements role-based access controls (RBAC) and enforces strong authentication (e.g., multi-factor authentication (MFA)).

4.2.4. Reviews access logs for suspicious activity and reports issues to the General Manager.

[... 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 Policy Review

9.1.1. The IT Manager must review this policy annually. Any change in the legal, technical, or organizational context must trigger an immediate update.

9.2. Review Triggers

9.2.1. This policy must also be reviewed if any of the following occur:

9.2.2. Major system changes or cloud migrations

9.2.3. Changes to roles or organizational structure

9.2.4. A security incident involving unauthorized access

9.2.5. Regulatory changes (e.g., GDPR, NIS2, or DORA updates)

9.3. Documenting and Communicating Changes

9.3.1. Revisions must be logged with version history, approved by the General Manager, and communicated to all affected personnel.

9.4. Accessibility and Training

9.4.1. This policy must be made available to all staff, and relevant training should be provided as part of onboarding and annually thereafter.

10. Related Policies and Linkages

10.1. This policy should be applied in conjunction with the following SME policies to ensure the full enforcement of secure access practices:

10.1.1. P3S – Acceptable Use Policy (AUP): Ensures users understand acceptable behavior associated with granted access.

10.1.2. P5S – Change Management Policy: Ensures access rights remain aligned with approved system changes.

10.1.3. P7S – Onboarding and Termination Policy: Defines the trigger points for provisioning and deprovisioning user access.

10.1.4. P17S – Data Protection and Privacy Policy: Ensures access controls align with personal data protection requirements.

10.1.5. P30S – Incident Response Policy: Defines how access-related incidents (e.g., misuse or breaches) are managed and investigated.

11. Reference Standards and Frameworks

11.1. ISO/IEC 27001

11.1.1. Clause 5.15 – Requires formalized access control policies and processes.

11.2. ISO/IEC 27002

11.2.1. Controls 5.15–5.17 – Provide detailed guidance on role-based access, user lifecycle management, and the handling of privileged access.

11.3. NIST SP 800-53 Rev.

11.3.1. AC-1 to AC-5 – Require structured policies for access management, including account authorization, review, and monitoring.

11.4. EU GDPR

11.4.1. Article 32 – Requires technical and organizational controls (such as access management) to ensure data security and confidentiality.

11.5. EU NIS2 Directive

11.5.1. Article 21(2)(b) – Requires operational access control and identity management measures to prevent unauthorized system access.

11.6. EU DORA

11.6.1. Article 9 – Emphasizes the secure management of ICT risks, including robust access control for financial entities.

11.7. COBIT 2019

11.7.1. APO07 – Managed Security: Requires defined and enforced access responsibilities.

11.7.2. DSS01 – Manage Operations: Includes procedures for managing logical access and maintaining secure operational environments.