| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Insert Registered Legal Entity Name Here | | | | | | | |
| Document number:<br>P04 | | | | | Document Title:<br>**Access Control Policy** | | | | | | | |
| Version:<br>1.0 | | Effective Date:<br>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 5.15, 5.17, 5.18 | Logical and physical access management |
| ISO/IEC 27002:2022 | Controls 8.2, 8.3 | Role-based access and identity management |
| NIST SP 800-53 Rev. 5 | AC-1 to AC-20, IA-1 to IA-8 | Account and access controls, identity and authentication |
| EU GDPR | Articles 5(1)(f), 32(1)(b); Recital 39 | Data protection and data minimization |
| EU NIS2 | Article 21(2)(c–e) | Access control, user authentication, and asset protection |
| EU DORA | Articles 6, 9(2) | ICT and user access, strong controls, and third-party management |
| COBIT 2019 | APO07, BAI03, DSS01, DSS05, MEA03 | Onboarding, operations, monitoring, and compliance |

**1. Purpose**

1.1 This policy establishes mandatory principles, responsibilities, and control requirements for managing access to information systems, applications, physical facilities, and data assets across the organization.

1.2 It ensures that access is granted based on business need, job function, and risk posture, and enforces principles such as least privilege, need to know, and segregation of duties.

1.3 This policy supports implementation of ISO/IEC 27001:2022 Clause 5.15 and related controls governing logical and physical access, user authentication, and access lifecycle management.

1.4 This policy supports the protection of digital and physical resources from unauthorized use, misuse, or compromise.

**2. Scope**

**2.1 This policy applies to all users, systems, and facilities within the scope of the ISMS, including:**

2.1.1 Employees, contractors, vendors, and temporary personnel

2.1.2 On-premises infrastructure, cloud-hosted systems, and hybrid environments

2.1.3 All corporate assets—hardware, software, data, and secure physical areas

2.1.4 Logical access (e.g., systems, networks, applications, Application Programming Interfaces (APIs)) and physical access (e.g., buildings, data centers)

2.2 It governs access across the full identity and resource interaction lifecycle, from onboarding and provisioning to role changes and termination.

2.3 This policy also applies to Bring Your Own Device (BYOD) and remote access scenarios, ensuring that controls are applied consistently across locations and device ownership models.

**3. Objectives**

3.1 To implement secure, role-based access controls that support operational integrity and regulatory compliance.

3.2 To ensure that access privileges are appropriately approved, monitored, and revoked in a timely manner.

3.3 To prevent unauthorized access, privilege escalation, or the persistence of outdated access privileges.

3.4 To support zero trust principles by denying access by default unless explicitly approved and justified.

3.5 To provide assurance to auditors and stakeholders through evidence-based, automated access reviews and policy enforcement.

3.6 To embed access control into business processes, Human Resources lifecycle events, and technical architectures.

## 4. Roles and Responsibilities

### 4.1 Top Management

4.1.1 Approves the access control policy and ensures appropriate budget and staffing for its enforcement.

4.1.2 Reviews access control risks during management reviews and assigns accountability at a strategic level.

### 4.2 CISO / ISMS Manager

4.2.1 Owns the Access Control Framework and ensures alignment with ISO/IEC 27001 and related standards.

4.2.2 Coordinates policy enforcement, control testing and remediation, and reporting of access control metrics.

4.2.3 Oversees risk-based access modelling and monitors for systemic control gaps.

[ ... 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 Review Triggers and Frequency

#### 9.1.1 This policy must be reviewed:

9.1.1.1 Annually, or

9.1.1.2 Following a major change to IT infrastructure, regulatory requirements, or risk posture

9.1.1.3 After incidents that reveal weaknesses in access controls

9.1.1.4 When significant changes occur in authentication technologies or identity platforms

### 9.2 Review Authority and Process

#### 9.2.1 The CISO or designated ISMS lead shall manage the review cycle, incorporating:

9.2.1.1 Internal audit findings

9.2.1.2 Access review results and metrics

9.2.1.3 Legal and regulatory updates

9.2.1.4 Technology platform changes

9.2.2 All revisions must be approved by Top Management and communicated to all stakeholders.

9.2.3 Affected users may be required to re-acknowledge the policy following material updates.

### 9.3 Version Control and Documentation

#### 9.3.1 The master version shall be stored in the ISMS Document Repository with the following metadata:

9.3.1.1 Version number and change log

9.3.1.2 Effective date and next review date

9.3.1.3 Owner and approval authority

9.3.1.4 Distribution and acknowledgment records

9.3.2 Superseded versions must be archived and remain accessible for a minimum of 3 years.

## 10. Related Policies and Linkages

### 10.1 This policy is functionally dependent on, and must be interpreted alongside:

10.1.1 P01 – Information Security Policy: Defines the organization's security commitment and high-level access control expectations.

10.1.2 P03 – Acceptable Use Policy (AUP): Establishes behavioural requirements for access and user accountability for responsible system use.

10.1.3 P05 – Change Management Policy: Governs how changes to access configurations, roles, or group structures must be implemented and tested securely.

10.1.4 P07 – Onboarding and Termination Policy: Governs the granting and revocation of access rights in accordance with user lifecycle events.

10.1.5 P11 – User Account and Privilege Management Policy: Operationalizes account-level controls and complements this policy with technical access enforcement requirements.

10.2 Together, these policies provide a cohesive and enforceable access governance framework across business units and technologies.

## 11. Reference Standards and Frameworks

### 11.1 ISO/IEC 27001:2022:

11.1.1 Clause 5.15 – Access Control: This policy fulfills the requirement to control access to information and other associated assets based on business and information security requirements.

11.1.2 Clause 5.17 – Identity Management and Clause 5.18 – Authentication Information: These are operationalized through identity provisioning, authentication mechanisms, and privilege assignments.

11.1.3 Annex A Controls 8.2 (Access Control Policy) and 8.3 (Identity Management): These provide the foundation for this policy's control objectives, including role-based access, user lifecycle integration, and privileged access protection.

### 11.2 NIST SP 800-53 Rev. 5:

11.2.1 AC Family (AC-1 through AC-20): This policy supports NIST access control requirements for both physical and logical systems, including policy definition (AC-1), account management (AC-2), and separation of duties (AC-5).

11.2.2 IA Family (IA-1 through IA-8): Provides guidance for identity authentication, credential protection, and multi-factor authentication (MFA).

11.2.3 AU-2, AU-12: Logging and auditing requirements enforced under this policy support user accountability and incident investigation.

11.2.4 PE-2 through PE-6: Address physical access restrictions, which this policy partially enforces through badge controls and building access permissions.

### 11.3 EU GDPR (2016/679):

11.3.1 Article 5(1)(f): Personal data must be protected against unauthorized access. This policy ensures technical and procedural enforcement of that principle.

11.3.2 Article 32(1)(b): Requires the implementation of access controls, pseudonymization, and encryption to prevent unauthorized processing of personal data.

11.3.3 Recital 39: Requires minimization of access to personal data, enforced here through least privilege and access justification requirements.

**11.4 EU NIS2 Directive (2022/2555):**

11.4.1 Article 21(2)(c–e): This policy enables technical and organizational measures for access control, user authentication, and asset protection across essential and important entities.

**11.5 EU DORA (2022/2554):**

11.5.1 Article 6: Requires ICT risk management policies that explicitly include user access management and identity lifecycle controls. This policy satisfies that requirement for financial entities and ICT service sectors.

11.5.2 Article 9(2): This policy supports enforcement of strong access controls as part of third-party and intra-group ICT service management.

**11.6 COBIT 2019:**

11.6.1 APO07 – Managed Human Resources: Enforces onboarding and offboarding controls to support access governance.

11.6.2 BAI03 – Managed Solutions Identification and Build: Embeds access control requirements into system design and change processes.

11.6.3 DSS01 – Managed Operations and DSS05 – Managed Security Services: Govern the enforcement of logical access restrictions and monitoring for violations.

11.6.4 MEA03 – Monitor, Evaluate, and Assess Compliance: Supports audit and assurance mechanisms for validating access control effectiveness.