					[Insert Registered Legal Entity Name Here]						
Document number: P4					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 where applicable		
Standard/Regulation	**Clause/Article**	**Comment**
ISO/IEC 27001:2022	Clauses 5.15, 5.17, 5.18	
ISO/IEC 27002:2022	Controls 8.2, 8.3	
NIST SP 800-53 Rev.5	AC-1 to AC-20, IA-1 to IA-8	
EU GDPR	Articles 5(1)(f), 32(1)(b); Recital 39	
EU NIS2	Article 21(2)(c–e)	
EU DORA	Articles 6, 9(2)	
COBIT 2019	APO07, BAI03, DSS01, DSS05, MEA03	

PREVIEW ONLY

Legal Notice (Copyright & Usage Restrictions)

© 2025 Clarysec LLC. All rights reserved.

This document is the intellectual property of Clarysec LLC. No part may be copied, reused, redistributed, or modified for commercial or implementation purposes without explicit written permission.

Unauthorized use is strictly prohibited and may lead to legal action.

For licensing, contact: info@clarysec.com

					[Insert Registered Legal Entity Name Here]						
Document number: P4					Document Title: **Access Control Policy**						
Version: 1.0		Effective Date: 01.01.2025			Document Owner:						
X	Policy		Standard		Procedure		Form		Register		Other

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—enforcing principles such as least privilege, need-to-know, and segregation of duties.

1.3. The 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 underpins the protection of digital and physical resources from unauthorized use, abuse, or compromise.

2. Scope

2.1. This policy applies to all users, systems, and facilities within the ISMS scope, 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, APIs) and physical access (e.g., buildings, data centers)

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

2.3. The policy also covers Bring Your Own Device (BYOD) and remote access contexts, ensuring controls are consistent 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 access rights are appropriately approved, monitored, and revoked in a timely manner.

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 To prevent unauthorized access, escalation of privileges, or persistence of outdated access rights.

3.4. To support zero trust principles by defaulting to deny access 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, HR lifecycle events, and technical architectures.

4. Roles and Responsibilities

4.1. Executive Management

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

4.1.2. Reviews access control risks during management reviews and allocates 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 access control metrics reporting.

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

PREVIEW ONLY

4.3. **System Owners and Application Owners**

4.3.1. Define the access levels and roles permitted within their systems, aligned to the principle of least privilege.

[……]

11. Reference Standards and Frameworks

This Access Control Policy aligns with leading international frameworks to ensure secure, auditable, and risk-based identity and access governance across all systems, assets, and user roles.

ISO/IEC 27001:2022

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.

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

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

NIST SP 800-53 Rev.5

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

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

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

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

EU GDPR (2016/679)

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

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

PREVIEW ONLY

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

EU NIS2 Directive (2022/2555)

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.

EU DORA (2022/2554)

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

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

COBIT 2019

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

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

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

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

PREVIEW ONLY