					Insert Registered Legal Entity Name Here							
Document number: P11					Document Title: **User Account and Privilege Management 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 6.1.3, Clause 8	-
ISO/IEC 27002:2022	Controls 5.15-5	-
NIST SP 800-53 Rev.5	AC-1, AC-2, AC-5, AC-6, IA-2 - IA-5, AU-2, AU-12	-
EU GDPR	Articles 5(1)(f), 32; Recital 39	-
EU NIS2	Articles 21(2)(a, d), 21(3)	-
EU DORA	Articles 5, 9	-
COBIT 2019	DSS01, DSS05, APO	-

1. Purpose

1 This policy establishes mandatory controls for managing user accounts and privileges across all information systems and services. It ensures that access to organizational resources is granted based on validated identity, role-based need, and the principles of Least Privilege and segregation of duties.

1.1 It supports the organization's commitment to information security by implementing structured, auditable processes for user provisioning, role and permission assignment, usage monitoring, and account deactivation.

1.2 This policy is critical to reducing the risk of unauthorized access, privilege misuse, insider threats, and non-compliance with applicable regulatory frameworks.

2. Scope

2.1 This policy applies to all employees, contractors, third-party service providers, consultants, and other individuals granted access to the organization's IT resources, applications, or data.

2.2 It governs all systems and environments where user authentication and access control mechanisms are applied, including but not limited to:

2.2.1 Enterprise applications and databases

2.2.2 Cloud platforms and SaaS environments

2.2.3 Operating systems and administrative consoles

2.2.4 Remote access tools and VPNs

2.2.5 Identity and Access Management platforms

2.3 This policy covers both standard and privileged user accounts and includes controls over:

2.3.1 Account creation, modification, and deactivation

2.3.2 Privilege escalation and delegation of responsibilities

2.3.3 Session control and monitoring

2.3.4 Authentication methods and management of authentication credentials

3. Objectives

3.1 Ensure that all user accounts are uniquely identifiable, properly authorized, and assigned only after formal validation of need.

3.2 Implement Least Privilege principles and prevent unnecessary or excessive access by enforcing strict controls over the issuance and use of privileged accounts.

3.3 Require timely updates to account status based on employment or role changes, including immediate access revocation upon termination.

3.4 Enable proactive detection and remediation of dormant credentials, misused accounts, and unauthorized accounts through logging, access reviews, and automation.

3.5 Maintain alignment with ISO/IEC 27001:2022 and associated standards, and satisfy obligations under applicable legal and regulatory frameworks such as the GDPR, NIS2, DORA, and COBIT 2019.

4. Roles and Responsibilities

4.1 Chief Information Security Officer (CISO)

4.1.1 Owns this policy and ensures its enforcement and compliance across the organization.

4.1.2 Reviews and approves any formal exceptions or emergency access cases.

4.1.3 Reports account-related audit findings and escalates risks to Top Management.

4.2 Access Control Manager / IT Administrator

4.2.1 Maintains and operates the technical controls for user account lifecycle management.

4.2.2 Executes user provisioning, deprovisioning, and privilege management activities upon approved request.

4.2.3 Maintains an authoritative register of all user accounts, their status, and privilege levels.

4.2.4 Supports audits and compliance reviews with logs and activity reports.

[... 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 This policy shall be reviewed at least annually or upon significant changes to:

9.1.1 Organizational structure or business processes

9.1.2 IT systems, identity platforms, or access methods

9.1.3 Regulatory or contractual requirements related to identity and access management

9.2 The Chief Information Security Officer (CISO), in conjunction with the Access Control Manager, is responsible for initiating the review process and coordinating stakeholder feedback.

9.3 Interim reviews may be triggered by:

9.3.1 Security incidents related to account misuse

9.3.2 Audit findings identifying deficiencies in account lifecycle management

9.3.3 Deployment of new identity or Privileged Access Management (PAM) tools

9.4 Updates to this policy must be:

9.4.1 Version-controlled and recorded in the ISMS documentation library

9.4.2 Communicated to all relevant stakeholders, including department heads, IT Operations, and Human Resources (HR)

9.4.3 Supported by updated training materials and procedural guidance

9.5 All changes must be approved by Top Management or the Information Security Steering Committee and logged for audit purposes.

10. Related Policies and Linkages

10.1 This policy is operationally linked to and supported by the following related policies within the ISMS suite:

10.1.1 P4 Access Control Policy: Establishes overarching access control principles and mechanisms, including rule-based and role-based controls.

10.1.2 P7 Onboarding and Termination Policy: Provides procedural steps for initiating and terminating user access in alignment with Human Resources (HR) actions.

10.1.3 P8 Information Security Awareness and Training Policy: Reinforces user responsibilities for account security and safeguarding authentication credentials.

10.1.4 P13 Data Classification and Labeling Policy: Guides access levels based on data classification, ensuring that privilege boundaries align with sensitivity tiers.

10.1.5 P22 Logging and Monitoring Policy: Ensures that audit trail records are collected for all account-related activities and reviewed to detect anomalies or unauthorized use.

10.1.6 P30 Incident Response Policy: Governs escalation, containment, and post-incident actions in cases of privilege misuse or unauthorized account activity.

10.2 These policies operate together to enforce a coherent, risk-based identity and access management framework across the organization.

11. Reference Standards and Frameworks

11.1 This policy is aligned with globally recognized cybersecurity standards and regulatory frameworks that require secure identity, access, and privilege management as a core component of organizational information security.

11.2 ISO/IEC 27001:

11.2.1 Clause 6.1.3 requires organizations to identify, assess, and treat information security risks, making access and privilege management a formal, risk-based control embedded within the ISMS planning process.

11.2.2 Clause 8.1 - Operational Planning and Control: Reinforces the implementation of technical and procedural safeguards governing user and privileged access.

11.3 ISO/IEC 27002:2022 - Controls 5.15 to 5:

11.3.1 Control 5.15 - User Access Management: Supports formal processes for user provisioning, access authorization, and periodic review of access rights.

11.3.2 Control 5.16 - Identity Management: Establishes identity uniqueness, lifecycle controls, and enforcement of secure authentication.

11.3.3 Control 5.17 ensures that the allocation and use of privileged access rights are strictly controlled, traceable, and aligned with the principle of Least Privilege throughout the user account lifecycle.

11.3.4 Control 5.18 - Privileged Access Rights: Addressed through role-based privilege assignment, auditing, and approval requirements for elevated access.

11.4 These controls guide the structured implementation of account registration, de-registration, privilege separation, and the use of authentication information. This policy enforces identity lifecycle governance, just-in-time access, and elevated session monitoring to prevent unauthorized system use.

11.5 NIST SP 800-53 Rev.5:

11.5.1 AC-1 (Access Control Policy) and AC-2 (Account Management): Mapped through policy requirements for access approvals, role mapping, and user account auditing.

11.5.2 AC-5 (Separation of Duties) and AC-6 (Least Privilege): Fulfilled through privilege restriction, job-role alignment, and dual approval for high-risk tasks.

11.5.3 IA-2 to IA-5 (Identification and Authentication): Enforced through strong authentication mechanisms, credential lifecycle rules, and MFA requirements.

11.5.4 AU-2, AU-12 (Audit Logging and Analysis): Addressed through session recording and monitoring of privileged activity across sensitive environments.

11.6 EU GDPR (2016/679):

11.6.1 Article 32 - Security of Processing: Requires access controls and identity verification mechanisms to protect personal data. This is fulfilled by mandating account approvals, privilege reviews, and strong authentication safeguards.

11.6.2 Article 5(1)(f) - Integrity and Confidentiality: Ensures that personal data is accessed only by authorized users with legitimate roles, reinforced through account management controls.

11.6.3 Recital 39: Calls for clear access limitation and accountability; this policy supports full traceability of user identities and privilege assignments.

11.7 EU NIS2 Directive (2022/2555):

11.7.1 Article 21(2)(a, d): Requires entities to enforce access management policies and secure handling of authentication credentials and privileged sessions, supported by this policy's user provisioning, monitoring, and exception controls.

11.7.2 Article 21(3): Promotes access discipline and strong identity assurance in critical sectors, met through the use of unique IDs, RBAC, and time-restricted elevated access.

11.8 EU DORA (2022/2554):

11.8.1 Article 5 - ICT Governance and Control: Mandates formalized processes for ICT user management, addressed through documented user provisioning, account deactivation, and exception handling.

11.8.2 Article 9 - ICT Risk Management: Directs organizations to secure systems through access restrictions and monitoring, addressed through MFA, privileged access logging, and centralized reviews.

11.9 COBIT 2019:

11.9.1 DSS01 - Managed Operations: Promotes enforcement of standardized operational controls, including user account lifecycle management and access documentation.

11.9.2 DSS05 - Managed Security Services: Reflects secure administration of user and system privileges, supporting risk mitigation through Least Privilege and audit trail validation.

11.9.3 APO13 - Managed Security: Requires access governance across digital identities, fulfilled through formalized account and role authorization practices with periodic review requirements.