					Insert Registered Legal Entity Name Here							
Document number: P11S					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	Clauses 5.3, 8	Roles, responsibilities, and operational planning/control for user access management
ISO/IEC 27002:2022	Control 8	Controls for the assignment, review, and removal of elevated privileges
NIST SP 800-53 Rev.5	AC-2, AC-5, AC-6	Account creation, monitoring, least privilege, and segregation of duties
EU NIS2	Article 21(2)(d)	User access management for essential and important entities
EU DORA	Article 9(2)(b)	Privileged access control in financial entities
COBIT 2019	DSS05.03, DSS05.04	Provisioning, deprovisioning, and periodic review of user access
EU GDPR	Article 32	Appropriate access controls for the protection of personal data

1. Purpose

1.1 This policy establishes rules for managing user accounts and access privileges in a secure, consistent, and traceable manner. It ensures that only authorized users have access to systems and data and that such access is appropriate to their role and responsibilities.

1.2 Effective account and privilege management is essential to prevent unauthorized access, minimize insider threats, and ensure compliance with ISO/IEC 27001, GDPR, and other applicable regulatory requirements.

1.3 This policy enables the organization to assign ownership and responsibility for account usage, monitor and audit privilege escalations, and securely disable or revoke access when it is no longer required.

1.4 It also protects business operations against operational errors or misuse caused by excessive or unmonitored access and helps reduce the risk of accidental data leakage, privilege misuse, or regulatory non-compliance.

2. Scope

2.1 This policy applies to:

2.1.1 All personnel, including employees, interns, contractors, third-party service providers, and third-party users with access to the organization’s IT systems

2.1.2 All systems, devices, services, and platforms managed by or on behalf of the organization, including cloud platforms, on-premises IT infrastructure, and third-party tools

2.2 It covers all types of user accounts, including:

2.2.1 Named user accounts (e.g., email accounts, system logins)

2.2.2 Administrator and system-level accounts

2.2.3 Temporary, guest, or third-party authentication credentials

2.2.4 Service accounts used by applications or automation systems

2.3 This policy applies throughout the entire account lifecycle, from creation and approval through modification, monitoring, and deactivation. This includes initial user provisioning during onboarding, access reviews during role changes, and revocation during offboarding.

3. Objectives

3.1 Assign unique, traceable digital identities to all system users to ensure accountability and eliminate reliance on shared authentication credentials.

3.2 Enforce the principle of least privilege, ensuring users are granted only the minimum level of access necessary to perform their duties.

3.3 Prevent unauthorized access to sensitive systems or data through clearly documented approval workflows and review processes.

3.4 Ensure timely deactivation of user accounts when they are no longer required, for example upon termination, contract completion, or role changes.

3.5 Maintain a secure, audit-ready environment by documenting all account changes, approvals, and periodic reviews.

3.6 Ensure privilege elevation is strictly controlled, independently approved, and logged, and that elevated access is revoked promptly when no longer needed.

4. Roles and Responsibilities

4.1 General Manager

4.1.1 Has overall accountability for enforcing this policy.

4.1.2 Ensures account management practices align with ISO/IEC 27001 certification requirements and applicable legal obligations (e.g., GDPR).

4.1.3 Must be informed immediately of any unauthorized access, security incident, or policy violation related to user accounts.

4.1.4 Oversees policy reviews, audits, and enforcement actions.

4.2 IT Lead or External IT Provider

4.2.1 Is responsible for the technical implementation of account and privilege controls across systems used by the organization.

4.2.2 Must provision, modify, and deactivate user accounts only in accordance with documented controls and approvals.

4.2.3 Must enforce the Password Policy, screen timeout settings, multi-factor authentication (MFA), where available, and system logging.

4.2.4 Must maintain secure audit records of all access approvals, account ownership, privilege escalations, and revocations.

4.2.5 Must monitor for unauthorized or orphaned accounts and report discrepancies 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 This policy must be reviewed at least annually by the General Manager and IT Lead to ensure compliance with:

9.1.1 Current ISO/IEC 27001:2022 controls and guidance

9.1.2 Regulatory updates (e.g., GDPR, DORA, NIS2)

9.1.3 Changes in systems, services, or business structure

9.2 Reviews must also be conducted following:

9.2.1 Significant security incidents or audit findings

9.2.2 Major changes in IT systems or account architecture

9.2.3 Introduction of new platforms requiring access control integration

9.3 All changes must be approved by the General Manager and clearly communicated to affected staff.

10. Related Policies and Linkages

10.1 P2S – Governance Roles and Responsibilities Policy: Establishes accountability and decision-making authority for access approvals and oversight.

10.2 P4S – Access Control Policy: Governs organization-wide implementation of access controls and authentication methods.

10.3 P7S – Onboarding and Termination Policy: Ensures account creation and removal are integrated into Human Resources-managed personnel changes.

10.4 P8S – Information Security Awareness and Training Policy: Trains users on secure account practices and expected usage.

10.5 P30S – Incident Response Policy: Defines the actions to be taken if account misuse results in a security breach or unauthorized disclosure.

11. Reference Standards and Frameworks

11.1 ISO/IEC 27001

11.1.1 Clause 5.3: Requires roles and responsibilities for information security to be clearly assigned and enforced.

11.1.2 Clause 8.1: Operational planning and control must include user access management.

11.2 ISO/IEC 27002

11.2.1 Control 8.2: Details technical and procedural controls for assigning, reviewing, and removing elevated privileges.

11.3 NIST SP 800-53 Rev.5

11.3.1 AC-2: Requires account creation, monitoring, and revocation based on defined roles and processes.

11.3.2 AC-5: Addresses segregation of duties to prevent conflicts of interest or abuse of privilege.

11.3.3 AC-6: Requires application of the principle of least privilege to all access privileges.

11.4 EU GDPR

11.4.1 Article 32: Requires appropriate access controls to protect personal data against unauthorized access or alteration.

11.5 EU NIS

11.5.1 Article 21(2)(d): Requires user access management as part of core security controls for essential and important entities.

11.6 EU DORA

11.6.1 Article 9(2)(b): Requires financial entities to implement access controls that restrict and monitor privileged rights.

11.7 COBIT 2019

11.7.1 DSS05.03: Specifies provisioning and deprovisioning of user access as part of IT governance.

11.7.2 DSS05.04: Requires ongoing review and alignment of user access with organizational roles.