					[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 where applicable		
Standard/Regulation	**Clause/Article**	**Comment**
ISO/IEC 27001:2022	Clauses 5.3, 8.1	
ISO/IEC 27002:2022	Control 8.2	
NIST SP 800-53 Rev.5	AC-2, AC-5, AC-6	
EU NIS2	Article 21(2)(d)	
EU DORA	Article 9(2)(b)	
COBIT 2019	DSS05.03, DSS05.04	
EU GDPR	Article 32	

					[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			

1. **Purpose**
   1.1. This policy establishes rules for managing user accounts and access rights in a secure, consistent, and traceable manner. It ensures that only authorized users have access to systems and data, and that access is appropriate to their role and responsibilities.
   1.2. Effective account and privilege management is essential for preventing unauthorized access, minimizing insider threats, and ensuring compliance with ISO/IEC 27001, GDPR, and other 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 no longer needed.
   1.4. It also protects business operations from operational errors or misuse caused by excessive or unmonitored access, and helps reduce the risk of accidental data leaks, privilege misuse, or regulatory non-compliance.
2. **Scope**
   2.1. This policy applies to:
      2.1.1. All employees, interns, contractors, 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 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 access credentials
      2.2.4. Service accounts used by applications or automation systems
   2.3. The policy applies throughout the entire account lifecycle—from creation and approval to modification, monitoring, and deactivation. This includes initial provisioning during onboarding, access reviews during role changes, and revocation during offboarding.
3. **Objectives**
   3.1. Assign unique, traceable user identities to all system users, ensuring accountability and eliminating reliance on shared 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 and review processes.
   3.4. Ensure timely deactivation of user accounts when they are no longer required—e.g., 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 (GM)**

4.1.1. Holds overall accountability for enforcing this policy.

4.1.2. Ensures account management practices align with ISO/IEC 27001 certification requirements and relevant 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 technically implementing account and privilege controls across systems used by the organization.

4.2.2. Must provision, modify, and deactivate user accounts based only on documented approvals.

4.2.3. Must enforce password complexity, screen timeout, multi-factor authentication (if available), and system logging.

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

4.2.5. Is required to monitor for unauthorized or orphaned accounts and report discrepancies to the GM.

4.3. **Line Managers**

4.3.1. Must request user accounts in writing and approve access based on job duties.

4.3.2. Are responsible for reviewing access during onboarding and ensuring prompt updates when employees change roles or depart.

4.3.3. Must assist in regular access reviews and verify the continuing need for system access among their team members.

4.3.4. Must communicate immediately with the IT Lead or GM when a staff member no longer requires access.

4.4. **Employees and Contractors**

4.4.1. Must only use accounts assigned to them; shared use of credentials is strictly prohibited.

4.4.2. Are required to lock their screen or log off before leaving their device unattended.

4.4.3. Must maintain password confidentiality and adhere to the organization's password policies.

4.4.4. Must report any account misuse, unauthorized access, or suspicious activity immediately.

4.4.5. Are accountable for any actions taken through their assigned account credentials.

5. Governance Requirements

5.1. Account creation must be based on a formal, documented request from a line manager, with approval logged in a central register or system.

5.2. All accounts must be uniquely identifiable and associated with a specific individual or process. Generic, untraceable usernames are prohibited unless justified and approved in writing.

5.3. A list of all active user accounts must be maintained and reviewed by the IT Lead at least every six months, or more frequently if required by risk assessments.

5.4. Any user assigned elevated privileges (e.g., administrator or root access) must receive explicit approval from the GM or IT Lead, with the justification and duration recorded.

5.5. Default accounts, system setup accounts, and legacy or unused accounts must be disabled or deleted. If technically required, these accounts must be renamed, secured, and tightly monitored.

5.6. All changes to user access (e.g., promotion requiring admin access, or role changes requiring reduced access) must be documented and approved.

6. Policy Implementation Requirements

6.1. **Account Provisioning**

6.1.1. User accounts may only be created after receiving written approval from the requesting user's manager.

6.1.2. Each account must be unique and traceable to a specific individual, and linked to a business role.

6.1.3. The IT Lead must verify identity and job requirements before granting access.

6.2. **Privilege Allocation**

6.3.

[……]

Reference Standards and Frameworks

ISO/IEC 27001:2022

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

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

ISO/IEC 27002:2022

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

NIST SP 800-53 Rev.5

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

AC-5: Addresses separation of duties to prevent conflict or abuse of privilege.

AC-6: Mandates application of the least privilege principle to all access rights.

EU GDPR

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

EU NIS2

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

EU DORA

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

COBIT 2019

DSS05.03: Specifies provisioning and de-provisioning of user access as part of IT governance.

DSS05.04: Calls for ongoing review and alignment of user access with organizational roles.