					[Insert Registered Legal Entity Name Here]							
Document number: P3					Document Title: **Acceptable Use 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	Clause 5.10	
ISO/IEC 27002:2022	Controls 6.1, 6.2, 8.1, 8.12	
NIST SP 800-53 Rev.5	AC-19, AC-20, AT-2	
EU GDPR	Articles 5(1)(f), 32; Recital 39	
EU NIS2	Article 21(2)(a–d)	
EU DORA	Article 5	
COBIT 2019	APO07, BAI05, DSS05, MEA01	

1. Purpose

1.1. This policy defines the acceptable and unacceptable use of the organization's information systems, computing resources, communication tools, and data-handling practices.

1.2. It ensures that all users understand their responsibilities when using corporate IT assets and that their actions support the confidentiality, integrity, availability, and lawful processing of information.

1.3. The policy fulfills ISO/IEC 27001:2022 Clause 5.10 by establishing behavioral norms for system use and applies technical and procedural safeguards to minimize the risk of misuse, negligence, or abuse.

1.4. It also supports investigation and enforcement activities, including incident response and disciplinary measures for violations.

2. **Scope**

2.1. This policy applies to all individuals and entities granted access to the organization's information systems and assets, including but not limited to:

2.1.1. Employees, contractors, consultants, interns, and agency staff

2.1.2. Third-party vendors with system access or delegated administrative roles

2.1.3. Guests or partners using organization-owned or authorized IT infrastructure

2.2. The scope includes all organizational technology and data assets, including:

2.2.1. Workstations, laptops, mobile devices, and servers

2.2.2. Network infrastructure and cloud-hosted services

2.2.3. Email, messaging, file storage, collaboration platforms, and VPNs

2.2.4. Data at rest, in transit, or being processed, regardless of format or location

2.2.5. Any personal device used under a BYOD (Bring Your Own Device) arrangement that connects to organizational systems

2.3. This policy is enforceable across all work environments including:

2.3.1. Corporate offices and production sites

2.3.2. Remote work locations or hybrid setups

2.3.3. Field-based operations or third-party-managed premises

2.4. All users are required to acknowledge and comply with this policy as a condition of accessing company systems or handling corporate data.

3. **Objectives**

3.1. To define and enforce rules for acceptable use of organizational IT resources.

3.2. To prevent unauthorized access, data leakage, or damage resulting from negligent or malicious use.

3.3. To protect company networks, assets, and data from threats introduced through user behavior.

3.4. To support legal and contractual obligations by demonstrating due diligence in IT resource governance.

3.5. To ensure consistency and clarity in applying disciplinary actions and exception management processes.

3.6. To promote a culture of ethical, secure, and responsible use of digital and physical computing resources.

4. **Roles and Responsibilities**

4.1. Executive Management

4.1.1. Approves the Acceptable Use Policy (AUP) and ensures that it is aligned with business objectives, regulatory requirements, and organizational values.

4.1.2. Allocates resources for enforcement, training, monitoring, and policy review.

4.1.3. Reviews compliance status and disciplinary actions associated with policy violations as part of ISMS governance.

4.2. **IT and Information Security Teams**

4.2.1. Implement technical safeguards to enforce this policy, including:

4.2.2. Content filtering, malware protection, endpoint security, and network monitoring tools

[…..]

11. Reference Standards and Frameworks

This Acceptable Use Policy (AUP) is aligned with internationally recognized standards and legal frameworks to ensure enforceable, auditable, and risk-based behavioral controls across all digital and physical information system usage.

ISO/IEC 27001:2022

Clause 5.10 – Acceptable Use of Information and Other Associated Assets: This policy directly fulfills the requirement to define, communicate, and enforce rules governing the appropriate use of IT resources.

Annex A Control 6.1 – Responsibility for Information Security: Assigns clear responsibilities for user behavior and compliance oversight.

Annex A Control 6.2 – Information Security Awareness, Education, and Training: Embedded training and policy acknowledgment processes are part of AUP enforcement.

Annex A Control 8.1 – User Endpoint Devices and **8.12 – Data Loss Prevention**: Addresses acceptable behavior on user devices and governs activities that could lead to data exposure or leakage.

NIST SP 800-53 Rev.5

AC-19 (Access Control for Mobile Devices) and **AC-20 (Use of External Information Systems)**: This policy defines user obligations and restrictions for BYOD and third-party system access.

PL-4 (Rules of Behavior): Provides detailed acceptable use requirements consistent with this policy.

AT-2 (Security Awareness Training): Supported through user training and documented policy acknowledgment.

AU-2 (Audit Events) and **AU-12 (Audit Generation)**: Enforcement relies on monitoring user actions and alerting on violations.

EU GDPR (2016/679)

Article 5(1)(f): Enforces the security and integrity of personal data; this policy mitigates risks introduced by human behavior and unauthorized use.

Article 32: Mandates technical and organizational measures—such as behavior controls and usage restrictions—to protect personal data.

Recital 39: Highlights the need to ensure only necessary access and lawful use of data by authorized individuals.

EU NIS2 Directive (2022/2555)

Article 21(2)(a–d): Requires operational policies and training for secure system use, which this AUP delivers by defining behavior, monitoring, and enforcement processes.

EU DORA (2022/2554)

Article 5: This policy supports the ICT risk management framework by defining rules for human-system interaction and minimizing behavior-based cyber risk exposure.

COBIT 2019

APO07 – Managed Human Resources: Enforces user responsibilities and awareness across the employee lifecycle.

BAI05 – Managed Organizational Change: Embeds acceptable use governance into change processes affecting user behavior.

DSS05 – Managed Security Services: Supports user activity monitoring, behavioral alerts, and automated response mechanisms.

MEA01 – Monitor, Evaluate, and Assess Performance and Conformance: The policy defines metrics and mechanisms to validate user compliance with behavioral expectations.