					Insert Registered Legal Entity Name Here							
Document number: P03S					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

Standard/Regulation	Clause/Article	Comment
ISO/IEC 27001:2022	Clause 5	Relevant to the overall policy scope and implementation
ISO/IEC 27002:2022	5.10, 5.11, 5	Provides guidance on acceptable use requirements and controls
NIST SP 800-53 Rev.5	AC-19, AC-20, AT-2	Covers system and device use, monitoring, and user training
EU GDPR	Articles 5(1)(f), 32	Integrity and confidentiality of data, and security measures
EU NIS2	Article 21(2)(b)	Requires appropriate security and acceptable use policies
EU DORA	Article 9	ICT risk management policy, controls, and enforcement
COBIT 2019	DSS05, BAI08	Security services and knowledge management

1. Purpose

1.1. This policy defines the acceptable, responsible, and secure use of company-provided systems, devices, internet access, email, cloud services, and any personally owned devices used for business purposes.

1.2. It ensures that individuals understand their obligations when using organizational IT resources, and supports the protection of data integrity, privacy, and operational continuity.

1.3. This policy supports compliance with ISO/IEC 27001:2022 by establishing clear standards of user behavior aligned with legal, contractual, and regulatory requirements.

2. Scope

2.1. This policy applies to all individuals who access, manage, or interact with company systems or data, including:

2.1.1. Employees and contractors

2.1.2. Temporary workers and interns

2.1.3. External IT service providers

2.2. It covers:

2.2.1. Company-owned computers, phones, and tablets

2.2.2. Personally owned devices approved for business use (BYOD)

2.2.3. Company networks, cloud platforms, and software services

2.2.4. Internet access, email systems, shared storage, and business applications

2.3. This policy applies across all working environments—onsite, remote, and hybrid—and at all times.

3. Objectives

3.1. Define what constitutes acceptable and unacceptable use of IT systems.

3.1.1. Reduce security risks arising from misuse, unauthorized access, or the introduction of malware.

3.1.2. Protect business data, customer information, and the company’s reputation.

3.1.3. Establish enforceable rules and accountability for all users.

3.1.4. Support monitoring and compliance activities to detect violations early and enable corrective action.

4. Roles and Responsibilities

4.1. General Manager

4.1.1. Approves this policy and is responsible for ensuring that sufficient resources and authority are in place for its enforcement.

4.1.2. Reviews and authorizes any exceptions to this policy.

4.2. IT Manager or External IT Provider

4.2.1. Maintains inventories of approved software and hardware.

4.2.2. Configures devices to enforce acceptable use requirements (e.g., content filtering, audit logging).

4.2.3. Monitors usage for potential violations and investigates incidents.

4.2.4. Ensures that personal devices (BYOD) used for business are authorized and secured.

[... 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. Annual Review

9.1.1. This policy must be reviewed annually by the IT Manager, with final approval by the General Manager, to ensure that it remains aligned with technology usage patterns, emerging risks, and compliance obligations.

9.2. Interim Review Triggers

9.2.1. Reviews must also be conducted in response to:

9.2.2. New systems or technologies (e.g., a new cloud service or endpoint platform)

9.2.3. Significant policy violations

9.2.4. Changes to laws or contractual terms affecting IT use

9.3. Change Documentation

9.3.1. All updates must be recorded in a version log that includes:

9.3.1.1. Version number

9.3.1.2. Review date

9.3.1.3. Summary of changes

9.3.1.4. Approving authority

9.4. Policy Communication

9.4.1. Revised versions of this policy must be communicated to all affected users. Employees must acknowledge receipt and understanding as part of their security awareness obligations.

10. Related Policies and Linkages

10.1. This policy operates in conjunction with several other SME policies to ensure comprehensive coverage of security responsibilities:

10.1.1. P4S – Access Control Policy: Defines the technical and procedural enforcement of permitted use and account restrictions.

10.1.2. P8S – Information Security Awareness and Training Policy: Provides user education on acceptable use boundaries and reporting obligations.

10.1.3. P9S – Remote Work Policy: Governs the use of company systems in offsite or home-working environments.

10.1.4. P17S – Data Protection and Privacy Policy: Establishes personal data handling requirements that intersect with acceptable use monitoring and BYOD.

10.1.5. P30S – Incident Response Policy: Governs procedures for investigating and responding to misuse or violations of acceptable use requirements.

11. Reference Standards and Frameworks

11.1. ISO/IEC 27001

11.1.1. Clause 5.10 – Requires organizations to define and enforce the acceptable use of information assets.

11.2. ISO/IEC 27002

11.2.1. Control 5.10 – Provides guidance on the acceptable use of systems, including permitted and prohibited behaviors.

11.3. NIST SP 800-53 Rev.5

11.3.1. AC-19 – Addresses control over system use, including personally owned devices.

11.3.2. AC-20 – Requires authorization and monitoring of external systems.

11.3.3. AT-2 – Emphasizes user training on acceptable use practices.

11.4. EU GDPR

11.4.1. Article 5(1)(f) – Requires the integrity and confidentiality of personal data, which may be compromised by user misuse.

11.4.2. Article 32 – Requires the implementation of technical and organizational measures to secure systems and data.

11.5. EU NIS2

11.5.1. Article 21(2)(b) – Requires appropriate security policies, including acceptable use requirements, to mitigate cyber threats.

11.6. EU DORA

11.6.1. Article 9 – Requires ICT risk management policies, including usage controls and enforcement mechanisms.

11.7. COBIT 2019

11.7.1. DSS05 – Manage Security Services: Emphasizes policy-based control of user behavior.

11.7.2. BAI08 – Manage Knowledge: Addresses awareness of policy responsibilities and acceptable use training.