					[Insert Registered Legal Entity Name Here]							
Document number: P3S					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	Clauses 5.10	
ISO/IEC 27002:2022	5.10, 5.11, 5.12	
NIST SP 800-53 Rev.5	AC-19, AC-20, AT-2	
EU GDPR	Articles 5(1)(f), 32	
EU NIS2	Article 21(2)(b)	
EU DORA	Article 9	
COBIT 2019	DSS05, BAI08	

					[Insert Registered Legal Entity Name Here]							
Document number: P3S					Document Title: **Acceptable Use Policy**							
Version: 1.0		Effective Date: 01.01.2025			Document Owner:							
X	Policy		Standard		Procedure		Form		Register		Other	

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.

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

1.3. This policy supports ISO/IEC 27001:2022 compliance by enforcing clear user behavior standards, 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 or 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 work environments—onsite, remote, hybrid—and all business hours.

3. Objectives

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

3.1.1. Reduce security risks posed by misuse, unauthorized access, or introduction of malware.

3.1.2. Protect business data, customer information, and company reputation.

3.1.3. Set enforceable rules and enable accountability for all users.

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

4. Roles and Responsibilities

4.1. **General Manager**

4.1.1. Approves this policy and is responsible for ensuring that resources and authority exist for enforcement.

4.1.2. Reviews and authorizes any exceptions to this policy.

4.2. **IT Manager or External IT Provider**

4.2.1. Maintains approved software and hardware inventories.

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

4.2.3. Monitors usage for potential violations and investigates incidents.

4.2.4. Ensures personal devices (BYOD) are authorized and secure if used for business.

4.3. **Department Managers**

4.3.1. Ensure their teams understand and follow acceptable use rules.

4.3.2. Approve job-related access and report observed misuse.

4.4. **Employees and Contractors**

4.4.1. Must use IT systems responsibly and only for legitimate business purposes.

4.4.2. Must not circumvent security controls, install unauthorized tools, or engage in prohibited activities.

4.4.3. [……]