				[Insert Registered Legal Entity Name Here]							
Document number: P27S				Document Title: **Cloud Usage 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 8.1	
ISO/IEC 27002:2022	Controls 5.23–5.25	
NIST SP 800-53 Rev.5	AC-20, SC-12, SC-13, SR-5	
EU GDPR	Article 28, 32, and Chapter V	
EU NIS2	Articles 21(2)(f), (i)	
EU DORA	Articles 5(2), 28	
COBIT 2019	DSS01, DSS05, BAI04	

					[Insert Registered Legal Entity Name Here]						
Document number: P27S					Document Title: **Cloud Usage Policy**						
Version: 1.0		Effective Date: 01.01.2025			Document Owner:						
X	Policy		Standard		Procedure		Form		Register		Other

1. Purpose

1.1. This policy defines how cloud services may be used securely within the organization. It ensures that data processed or stored in the cloud is protected, access is controlled, and risks are managed responsibly.

1.2. It helps SMEs meet legal obligations and customer expectations for protecting sensitive information, preventing data leaks, and managing cloud-based risks effectively without requiring enterprise-scale infrastructure.

1.3. This policy supports ISO/IEC 27001 certification, GDPR compliance, and supply chain assurance through consistent governance of all third-party cloud services.

2. Scope

2.1. This policy applies to:

2.1.1. Any cloud-based service used to store, process, or transmit company data

2.1.2. All staff, contractors, or service providers using cloud tools on behalf of the organization

2.1.3. Free and paid cloud solutions, including email platforms, document sharing, SaaS tools, backup platforms, video conferencing, and customer platforms

2.1.4. Any device (desktop, mobile, tablet) accessing company information via cloud applications

2.2. This includes, but is not limited to:

2.2.1. Microsoft 365, Google Workspace, Dropbox Business

2.2.2. Zoom, Microsoft Teams, Google Meet

2.2.3. AWS, Azure, GCP

2.2.4. Cloud-based backup and disaster recovery tools

2.2.5. Shared folders or apps used for invoicing, project management, or customer communication

3. Objectives

3.1. Prevent unauthorized or high-risk use of unapproved cloud services.

3.2. Ensure sensitive or regulated data stored in the cloud is secured using appropriate technical and administrative controls.

3.3. Define clear roles for approving, configuring, monitoring, and decommissioning cloud services.

3.4. Control data flows and enforce retention, deletion, and privacy obligations for cloud-stored information.

3.5. Reduce reliance on personal accounts or untracked tools by requiring approval of all cloud systems used for business purposes.

3.6. Comply with ISO/IEC 27001:2022, GDPR, NIS2, and DORA requirements for managing external cloud dependencies.

4. Roles and Responsibilities

4.1. **General Manager (GM)**

4.1.1. Approves the use of all new cloud services

4.1.2. Reviews risks related to cloud vendors and service types

4.1.3. Enforces policy and oversees exception decisions

[……]

					[Insert Registered Legal Entity Name Here]						
Document number: P27S					Document Title: **Cloud Usage Policy**						
Version: 1.0		Effective Date: 01.01.2025			Document Owner:						
X	Policy		Standard		Procedure		Form		Register		Other

Reference Standards and Frameworks

ISO/IEC 27001:2022

Clause 8.1 – Requires organizations to implement operational controls for data handling, including those related to cloud-based systems.

ISO/IEC 27002:2022

Control 5.23 – Mandates governance over the use of cloud services and third-party SaaS tools.

Control 5.24 – Requires a defined cloud usage policy aligned with risk and regulatory requirements.

Control 5.25 – Requires organizations to ensure that security controls in cloud environments meet organizational needs.

NIST SP 800-53 Rev.5

AC-20 – Requires formal use policies for external systems such as cloud services.

SC-12, SC-13 – Address encryption for data in transit and at rest within cloud environments.

SR-5 – Covers cloud and third-party risk controls within the supply chain.

EU GDPR (2016/679)

Article 28 – Requires cloud providers acting as data processors to follow binding contractual obligations.

Article 32 – Mandates technical and organizational controls for cloud-based data processing.

Chapter V – Prohibits unauthorized international transfers of personal data stored in the cloud.

EU NIS2 Directive (2022/2555)

Article 21(2)(f), (i**) – Requires essential and important entities to implement appropriate policies for cloud service** security and supply chain control.

EU DORA (2022/2554)

Article 5(2) – Requires financial SMEs to integrate cloud security into their ICT risk management frameworks.

Article 28 – Establishes oversight rules for critical third-party ICT service providers, including cloud vendors.

COBIT 2019

DSS01 – “Manage Operations” addresses the operational integrity of cloud services.

DSS05 – “Manage Security Services” includes cloud-specific protections and monitoring.

BAI04 – “Manage Availability and Capacity” ensures business continuity and performance in cloud environments.