					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

Standard/Regulation	Clause/Article	Comment
ISO/IEC 27001:2022	Clause 8	
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	

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 appropriately.

1.2 It supports SMEs in meeting legal obligations and customer expectations for protecting sensitive information, preventing data leakage, and managing cloud-related 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 personnel, 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 through 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 applications 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 that sensitive or regulated data stored in the cloud is protected through appropriate technical and administrative controls.

3.3 Define clear responsibilities 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 for 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 associated with cloud providers and service types

4.1.3 Enforces this policy and oversees exception decisions

4.2 IT Provider or Technical Support

4.2.1 Assesses and implements secure configurations for cloud services

4.2.2 Provisions accounts, access controls, and backups

4.2.3 Monitors compliance with password, MFA, and security configuration requirements

[... 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 This policy must be reviewed at least annually by the General Manager, in coordination with the IT provider.

9.2 A formal review must also take place:

9.2.1 Following a cloud-related security incident (e.g., breach, data loss)

9.2.2 When a new major cloud platform is introduced

9.2.3 If legal or regulatory requirements change (e.g., GDPR, NIS2, DORA updates)

9.2.4 If monitoring activities identify misuse or new risks

9.3 The GM must ensure:

9.3.1 The Cloud Service Register is updated to reflect new or retired services

9.3.2 Legal and privacy requirements continue to be met

9.3.3 All changes are communicated to relevant users and stakeholders

9.4 Archived versions must be stored securely, and superseded policy versions must be handled in accordance with the organization’s P14S – Data Retention Policy and Disposal Policy.

10. Related Policies and Linkages

10.1 This policy must be used in conjunction with the following SME-aligned information security policies:

10.1.1 P2S – Governance Roles and Responsibilities Policy: Defines accountability for approving cloud services and managing provider relationships.

10.1.2 P4S – Access Control Policy: Supports secure authentication, session management, and access revocation practices required for cloud platforms.

10.1.3 P14S – Data Retention Policy and Disposal Policy: Governs how cloud-based data is backed up, retained, and deleted in accordance with legal obligations.

10.1.4 P17S – Data Protection and Privacy Policy: Ensures that any personal data stored in cloud services is handled in accordance with GDPR principles.

10.1.5 P30S – Incident Response Policy: Provides structured procedures for responding to cloud security incidents, including evidence collection and external notification.

10.2 Together, these policies ensure that cloud usage is secure, compliant, and operationally resilient.

11. Reference Standards and Frameworks

11.1 ISO/IEC 27001

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

11.2 ISO/IEC 27002

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

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

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

11.3 NIST SP 800-53 Rev. 5

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

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

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

11.4 EU GDPR (2016/679)

11.4.1 Article 28 – Requires cloud providers acting as data processors to comply with binding contractual obligations.

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

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

11.5 EU NIS2 Directive (2022/2555)

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

11.6 EU DORA (2022/2554)

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

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

11.7 COBIT 2019

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

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

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