					Insert Registered Legal Entity Name Here							
Document number: P27					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	Cloud operational planning and control requirements.
ISO/IEC 27002:2022	Controls 5.23–5.25	Requirements for the use, policy, and security of cloud services.
NIST SP 800-53 Rev.5	AC-20, SA-9(5), SC-12 – SC-28, SR-5	External system use, contractual and technical requirements, cryptographic protections, supply chain protection.
EU GDPR	Articles 28, 32, Chapter V	Cloud processor requirements, security of processing, data transfers.
EU NIS2	Article 21(2)(f, i)	Third-party risk and supply chain requirements.
EU DORA	Articles 5(2), 28	ICT and third-party (cloud) oversight for financial entities.
COBIT 2019	BAI04, DSS01, DSS05	Cloud availability, operations, and security management.

1. Purpose

1.1 This policy establishes the organization's mandatory requirements for the secure, compliant, and responsible use of cloud computing services across Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS) delivery models.

1.2 This policy is intended to ensure that cloud services are adopted and governed in a manner that protects the confidentiality, integrity, and availability of information assets while meeting regulatory, legal, and contractual obligations.

1.3 It defines controls to manage cloud risk, protect data, monitor provider compliance, and eliminate unauthorized use. It also supports business innovation through cloud platforms by aligning security, operational reliability, and cost efficiency.

2. Scope

2.1 This policy applies to all employees, contractors, third-party service providers, and external consultants who provision, configure, access, manage, or use cloud services on behalf of the organization.

2.2 It applies to all environments in which the organization's data or workloads are processed, including:

2.2.1 Public, private, hybrid, and community cloud deployments

2.2.2 All cloud service models (IaaS, PaaS, SaaS)

2.2.3 Multi-cloud and federated architectures

2.2.4 Use of shadow IT or personal cloud accounts for business purposes

2.3 It covers all data classification levels and applies to internal systems as well as vendor-hosted platforms where organization-owned or regulated data is stored or processed.

3. Objectives

3.1 To ensure the secure and consistent use of cloud technologies through clearly defined usage requirements, security baselines, and governance roles.

3.2 To minimize operational and regulatory risks associated with cloud computing, including unauthorized access, data breaches, misconfigurations, non-compliance, and service outages.

3.3 To enforce security and data privacy requirements for all cloud vendors and verify compliance through contractual clauses, assessments, and audit rights.

3.4 To enable scalable and resilient cloud adoption without compromising the enterprise risk posture, legal requirements, or Business Continuity Policy requirements.

3.5 To align cloud governance and usage with the organization's ISMS framework, legal obligations (e.g., GDPR, DORA), sector-specific guidance, and industry best practices (e.g., NIST, COBIT).

4. Roles and Responsibilities

4.1 Top Management

4.1.1 Approves the Cloud Usage Policy and the strategic cloud adoption roadmap.

4.1.2 Reviews and approves high-risk exceptions to standard cloud governance requirements.

4.1.3 Ensures cloud initiatives receive adequate funding, oversight, and integration with enterprise risk management frameworks.

4.2 Chief Information Security Officer (CISO)

4.2.1 Owns this policy and the organizational Cloud Services Register.

4.2.2 Approves the onboarding of new cloud providers based on due diligence and security risk assessment.

4.2.3 Reviews provider compliance attestations and validates security alignment.

[... 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 shall be reviewed at least annually and updated as necessary to ensure continued alignment with:

9.1.1 Evolving legal and regulatory requirements (e.g., GDPR, NIS2, DORA)

9.1.2 Changes to ISO/IEC 27001 or ISO/IEC 27002 standards

9.1.3 Updates to the organization's cloud architecture, threat landscape, or service portfolio

9.1.4 Incident investigations, audit results, or lessons learned from operational use

9.2 The CISO is responsible for initiating the review and convening relevant stakeholders, including:

9.2.1 Cloud Security Architect

9.2.2 Legal and Compliance Team

9.2.3 Procurement and Vendor Managers

9.2.4 Service Owners and IT Operations

9.3 All updates must be:

9.3.1 Version-controlled and dated

9.3.2 Approved by Top Management

9.3.3 Communicated to affected parties, including employees, contractors, and third parties

9.3.4 Archived in accordance with internal documentation policies

9.4 Interim reviews may be triggered by:

9.4.1 New CSP engagements or major migrations

9.4.2 Emerging threats to cloud infrastructure

9.4.3 Material changes in contractual, legal, or sector-specific obligations

10. Related Policies and Linkages

10.1 This policy is closely linked to, and dependent on, the following internal policies:

10.1.1 P1 – Information Security Policy: Establishes the overarching principles governing the secure operation of systems and services, which this policy enforces in the cloud context.

10.1.2 P5 – Change Management Policy: All cloud configuration changes must follow the change control procedures set out in P5.

10.1.3 P13 – Data Classification and Labeling Policy: Determines how data is assessed before cloud transfer and how controls such as encryption and residency are applied.

10.1.4 P18 – Cryptographic Controls Policy: Provides standards for encryption, key management, and cryptographic algorithm use, which apply directly to cloud service configurations.

10.1.5 P22 – Logging and Monitoring Policy: Specifies requirements for log collection, retention, and analysis that must be enforced in cloud environments.

10.1.6 P30 – Incident Response Policy: Defines escalation, containment, and remediation procedures for cloud-related security events.

10.1.7 P33 – Audit and Compliance Monitoring Policy: Supports audit readiness and continuous assurance that cloud controls are implemented and monitored.

11. Reference Standards and Frameworks

11.1 ISO/IEC 27001: Clause 8.1 – Operational Planning and Control: Requires organizations to implement and control the processes needed to meet information security requirements, including those involving cloud environments.

11.2 ISO/IEC 27002:2022 – Controls 5.23 to 5.25:

11.2.1 Annex A Control 5.23 – Use of Cloud Services: Requires risk-based assessment, formal authorization, and documentation of cloud service usage.

11.2.2 Annex A Control 5.24 – Cloud Use Policy: Requires the establishment and enforcement of formal cloud usage policies aligned with organizational needs and risks.

11.2.3 Annex A Control 5.25 – Security in Cloud Services: Requires security integration, contractual protections, and monitoring of cloud-hosted systems, workloads, and data.

11.3 NIST SP 800-53 Rev.5:

11.3.1 AC-20 – Use of External Systems: Requires defined rules and conditions for accessing organizational resources from external or cloud-based systems.

11.3.2 SA-9(5) – External Information System Services: Requires contractual security requirements, oversight, and continuous monitoring for third-party cloud systems.

11.3.3 SC-12 to SC-28 – Cryptographic Protections, Boundary Defense, and Transmission Integrity: Align with encryption, identity, and access requirements for cloud-hosted systems, services, and data in transit.

11.3.4 SR-5 – Supply Chain Protection: Supports due diligence and contractual control over CSPs involved in service delivery.

11.4 EU GDPR (2016/679):

11.4.1 Article 28 – Processor Obligations: Requires formal contracts with cloud providers to ensure the security, confidentiality, and auditability of personal data processing.

11.4.2 Article 32 – Security of Processing: Supports the application of encryption, access controls, logging capabilities, and other safeguards in cloud environments.

11.4.3 Chapter V – International Data Transfers: Requires the lawful transfer of data outside the EU/EEA using safeguards such as SCCs or adequacy decisions.

11.5 EU NIS2 Directive (2022/2555):

11.5.1 Article 21(2)(f, i): Requires entities to manage risks arising from third-party cloud service providers and ensure digital supply chain integrity through contractual and technical measures.

11.6 EU DORA (2022/2554):

11.6.1 Article 5(2) – Governance of ICT Risks: Requires integration of ICT third-party risk, including cloud services, into overall risk governance.

11.6.2 Article 28 – Oversight of Critical ICT Third-Party Providers: Requires financial entities to monitor, control, and report on cloud provider dependencies, security posture, and ICT resilience.

11.7 COBIT 2019:

11.7.1 BAI04 – Manage Availability and Capacity: Ensures cloud services are resilient, monitored, and meet defined performance criteria.

11.7.2 DSS01 – Manage Operations: Supports operational integration, incident handling, and configuration baselines across cloud-hosted platforms.

11.7.3 DSS05 – Manage Security Services: Directs the implementation of cloud-specific security controls, monitoring, and incident prevention across digital services.