					[Insert Registered Legal Entity Name Here]							
Document number: P15					Document Title: **Backup and Restore 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 6.1.3, 8.1	
ISO/IEC 27002:2022	Controls 8.13, 5.28, 5.29	
NIST SP 800-53 Rev.5	CP-9, CP-10, SI-12, MP-6	
EU GDPR	Article 32, Recital 49	
EU NIS2	Article 21(2)(c-e)	
EU DORA	Articles 10, 11	
COBIT 2019	DSS01, DSS04, MEA03	

					[Insert Registered Legal Entity Name Here]							
Document number: P15					Document Title: **Backup and Restore Policy**							
Version: 1.0		Effective Date: 01.01.2025			Document Owner:							
X	Policy		Standard		Procedure		Form		Register		Other	

1. Purpose

1.1 The purpose of this policy is to define the mandatory requirements for the backup and restoration of data, systems, and applications to support operational resilience, data integrity, and business continuity.

1.2 The policy establishes a standardized framework to:

1.2.1 Protect organizational data from loss due to deletion, corruption, failure, or cyberattacks

1.2.2 Define recovery expectations through clear RTO (Recovery Time Objective) and RPO (Recovery Point Objective) parameters

1.2.3 Integrate backup operations with the broader ISMS and Business Continuity Plans (BCP/DRP)

1.2.4 Ensure compliance with applicable laws and sectoral regulations on availability and recoverability

1.3 The policy enforces ISO/IEC 27001:2022 controls related to secure data disposal (5.28), resilience (5.29), and operational recovery (8.13), and maps to best practices from ISO/IEC 27002:2022, NIST SP 800-53 Rev.5, GDPR, DORA, and NIS2.

2. Scope

2.1 This policy applies to:

2.1.1 All business-critical and operational systems within the scope of the ISMS

2.1.2 All structured and unstructured business data including databases, files, emails, and configurations

2.1.3 All environments—on-premises, cloud, hybrid, and remote/offsite storage

2.1.4 All personnel responsible for managing, executing, verifying, or restoring backup processes

2.2 It also applies to:

2.2.1 Backup media and infrastructure, including physical tapes, virtual appliances, disk snapshots, and cloud-based backup solutions

2.2.2 Third-party providers contracted to host, manage, or process organizational backups

2.2.3 Backup of logs, configurations, audit trails, and continuity-critical operational documentation

2.3 Systems explicitly excluded from backup must be documented, risk-assessed, and formally accepted by the ISMS Manager and system owner.

3. Objectives

3.1 Ensure that all critical systems and data are reliably backed up with sufficient frequency, redundancy, and security controls.

3.2 Provide mechanisms for restoration that meet defined RTO and RPO expectations in alignment with business impact assessments.

3.3 Maintain complete documentation of backup procedures, retention schedules, roles, and technologies.

3.4 Validate the effectiveness of backup operations through systematic restore testing, failure logging, and remediation tracking.

3.5 Protect backup data from unauthorized access, modification, or destruction throughout its lifecycle.

3.6 Enable compliance with:

3.6.1 ISO/IEC 27001 operational and continuity control requirements

3.6.2 NIST SP 800-53 CP and MP families for backup and sanitization

3.6.3 GDPR Articles 32 and Recital 49 for restoration of access to personal data

3.6.4 DORA Article 10 and NIS2 Article 21 for ICT continuity and resilience

3.7 Ensure that third-party backup services meet contractual and regulatory security obligations, including encryption, disposal, and notification protocols.

4. Roles and Responsibilities

4.1 Executive Management

4.1.1 Endorses this policy and ensures that business-critical systems are adequately protected by approved backup and restoration practices.

[….]

11. Reference Standards and Frameworks

This policy aligns with internationally accepted frameworks, ensuring compliant, secure, and resilient backup and recovery operations.

ISO/IEC 27001:2022

Clause 6.1.3 - Risk Treatment Plan: Supports risk-based backup prioritization and restoration planning.

Clause 8.1 - Operational Planning and Control: Integrates recovery and continuity controls as part of operational safeguards.

Annex A Control 5.28 - Secure Disposal or Reuse of Equipment: Addresses secure sanitization of backup media.

Annex A Control 5.29 - Information Security during Disruption: Ensures restoration capabilities during incidents or disasters.

Annex A Control 8.13 - Information Backup: Directly addressed via scheduled, tested, and secure backup operations.

ISO/IEC 27002:2022 - Controls 8.13, 5.28, 5.29

These controls reinforce the requirement for regular backups, integrity validation, and restoration planning across all IT environments.

NIST SP 800-53 Rev.5

CP-9 - System Backup: Establishes comprehensive backup procedures, including offsite storage and restoration testing.

CP-10 - System Recovery and Restoration: Requires validated procedures for full or partial restoration aligned with recovery objectives.

MP-6 - Media Sanitization: Ensures secure handling of obsolete backup media.

SI-12 - Information Handling Procedures: Reinforces backup and recovery responsibilities for sensitive data.

EU GDPR (2016/679)

Article 32 - Security of Processing: Mandates restoration capabilities and data availability safeguards, especially for personal data.

Recital 49: Supports business continuity and disaster recovery measures, including secure backup as part of organizational resilience.

EU NIS2 Directive (2022/2555)

Article 21(2)(c-e): Requires technical and organizational measures, including backup and continuity controls, to ensure service resilience.

EU DORA (2022/2554)

Article 10 - ICT Business Continuity: Requires financial entities to have full data backup, recovery, and continuity planning.

Article 11 - Testing of ICT Business Continuity Plans: Emphasizes recovery capability validation through regular testing.

COBIT 2019

DSS01 - Managed Operations: Supports reliable delivery of services through protected data availability.

DSS04 - Managed Continuity: Defines strategic and operational continuity controls, including verified backups.

MEA03 - Monitor, Evaluate, and Assess Compliance: Mandates periodic review of continuity measures, including backup control effectiveness.