					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

Standard/Regulation	Clause/Article	Comment
ISO/IEC 27001:2022	Clauses 6.1.3, 8.1	Risk treatment, planning, and operational backup controls
ISO/IEC 27002:2022	Controls 8.13, 5.28, 5.29	Backup management, secure disposal, and information security during disruption
NIST SP 800-53 Rev.5	CP-9, CP-10, SI-12, MP-6	System backup, recovery, and media sanitization requirements
EU GDPR	Article 32, Recital 49	Restoration and availability of personal data, business continuity
EU NIS2	Article 21(2)(c-e)	Backup and continuity controls for resilience
EU DORA	Articles 10, 11	Financial sector backup, recovery, and testing requirements
COBIT 2019	DSS01, DSS04, MEA03	Backup operations, continuity, and compliance monitoring

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 This policy establishes a standardized framework to:

1.2.1 Protect organizational data from loss resulting from 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 Information Security Management System (ISMS) and Business Continuity Plans (BCP/DRP)

1.2.4 Ensure compliance with applicable laws and sector-specific regulations relating to availability and recoverability

1.3 This policy implements ISO/IEC 27001:2022 controls related to secure disposal or reuse of equipment (5.28), information security during disruption (5.29), and information backup (8.13), and aligns with industry 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 ISMS scope

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

2.1.3 All environments—on-premises, cloud, hybrid environments, and remote access/off-site storage

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

2.2 This policy 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 Backups of logs, configurations, audit trail records, and continuity-critical operational documentation

2.3 Systems explicitly excluded from backup must be documented, subject to a security risk assessment, and formally approved by the ISMS Manager and the 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 restoration mechanisms that meet defined RTO and RPO requirements 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 restoration testing, failure logging, and tracking of corrective actions.

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 control families for backup and media sanitization

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

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

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

4. Roles and Responsibilities

4.1 Top Management

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

4.1.2 Is accountable for ensuring that backup operations are adequately resourced and periodically reviewed for regulatory compliance.

4.2 CISO

4.2.1 Owns this policy and ensures alignment with broader information security, risk management, and continuity frameworks.

4.2.2 Oversees integration of backup procedures into BCP/DRP, incident reporting and management, and resilience planning.

4.2.3 Reviews backup exceptions and evaluates residual risk acceptance proposals for exclusions relating to critical systems.

[... 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, or sooner if triggered by:

9.1.1 Changes in business continuity or disaster recovery strategy

9.1.2 New regulatory or legal obligations affecting backup frequency or data retention

9.1.3 Changes in system architecture, backup tooling, or service providers

9.1.4 Significant incidents or audit findings related to data loss or recovery failures

9.2 The review shall be coordinated by the CISO in collaboration with:

9.2.1 IT Infrastructure and Operations

9.2.2 Internal Audit

9.2.3 Data Protection Officer (DPO)

9.2.4 Business continuity and disaster recovery teams

9.3 Backup schedules, system inclusion lists, restoration documentation, and exception logs shall be reviewed in parallel to ensure:

9.3.1 Accuracy of backup coverage for all critical assets

9.3.2 Compliance with RTO/RPO and retention requirements

9.3.3 Completeness of testing logs and incident reports

9.3.4 Remediation of previously identified control gaps

9.4 All updates must:

9.4.1 Be version-controlled and retained in the ISMS document repository

9.4.2 Include a summary of changes and justification

9.4.3 Be approved by Top Management

9.4.4 Be communicated to all affected technical and business personnel

10. Related Policies and Linkages

10.1 This policy directly supports and interfaces with the following related documents:

10.1.1 P6 - Risk Management Policy: Identifies risk-based prioritization of backup protection for systems and services.

10.1.2 P12 - Asset Management Policy: Ensures that systems eligible for backup are included in the Asset Inventory and linked to lifecycle tracking and classification.

10.1.3 P13 - Data Classification and Labeling Policy: Determines which data categories require backup, including labeling metadata used for prioritization.

10.1.4 P14 - Data Retention and Disposal Policy: Aligns backup retention with regulatory retention limits and the secure disposal of expired media.

10.1.5 P16 - Data Masking and Pseudonymization Policy: Supports data protection and data minimization during backup of sensitive datasets.

10.1.6 P30 - Incident Response Policy: Is activated in the event of backup failures, restoration issues, or compromise of backup data repositories.

10.2 These interlinked policies form a cohesive framework that ensures backup governance is embedded in the organization’s broader ISMS and operational resilience strategy.

11. Reference Standards and Frameworks

11.1 ISO/IEC 27001:

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

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

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

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

11.1.5 Annex A Control 8.13 - Information Backup: Is addressed directly through scheduled, tested, and secure backup operations.

11.2 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.

11.3 NIST SP 800-53 Rev.5:

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

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

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

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

11.4 EU GDPR (2016/679):

11.4.1 Article 32 - Security of Processing: Requires restoration capabilities and safeguards for data availability, particularly for personal data.

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

11.5 EU NIS2 Directive (2022/2555):

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

11.6 EU DORA (2022/2554):

11.6.1 Article 10 - ICT Business Continuity: Requires financial entities to maintain comprehensive data backup, recovery, and continuity planning.

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

11.7 COBIT 2019:

11.7.1 DSS01 - Managed Operations: Supports reliable service delivery through protected data availability.

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

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