					Insert Registered Legal Entity Name Here							
Document number: P14					Document Title: **Data Retention and Disposal 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	
ISO/IEC 27002:2022	Controls 5.10, 5.12, 5.30, 5	
NIST SP 800-53 Rev. 5	AU-11, MP-6, SI-12, PL-2	
EU GDPR	Articles 5(1)(e), 17, 32	
EU NIS2	Article 21(2)(a-e)	
EU DORA	Articles 5, 9	
COBIT 2019	DSS01, DSS05, MEA	

1. Purpose

1.1 The purpose of this policy is to define the organizational requirements for data retention and secure disposal across all phases of the information asset lifecycle. It ensures compliance with applicable legal, regulatory, and contractual obligations and prevents the unnecessary or risky accumulation of data.

1.2 This policy supports the implementation of ISO/IEC 27001:2022 by enforcing control over data retention periods and irreversible disposal practices. It enables traceable recordkeeping, enforces retention aligned with information classification sensitivity, and ensures audit readiness for internal audits, regulatory inspections, and legal discovery.

1.3 It further aims to uphold the confidentiality, integrity, and availability of data while minimizing business risk, operational inefficiencies, and exposure to data privacy violations resulting from improper data retention or destruction.

2. Scope

2.1 This policy applies to all physical and digital information assets owned, processed, or retained by the organization, including those under the control of third parties, subsidiaries, or outsourcing partners.

2.2 The scope includes, but is not limited to:

2.2.1 Documents, files, and records (digital and paper-based)

2.2.2 Databases and archives

2.2.3 Emails and instant messaging logs

2.2.4 Backups, system logs, and audit trails

2.2.5 Source code, application data, and cloud-hosted assets

2.2.6 Removable media and obsolete hardware containing data

2.3 This policy governs both operational records and regulated datasets (e.g., financial, legal, HR, customer-related, and audit-relevant content), regardless of storage location or system.

2.4 This policy applies to all organizational departments and all employees, contractors, and vendors engaged in creating, storing, managing, or disposing of data.

3. Objectives

3.1 To ensure that data is retained only for as long as legally, contractually, or operationally necessary, and securely disposed of when no longer required.

3.2 To prevent the premature, unauthorized, or accidental deletion of records needed for ongoing operations, mandatory compliance, litigation, or audit purposes.

3.3 To establish and enforce consistent retention schedules based on information classification, asset type, applicable laws, and risk exposure.

3.4 To safeguard data privacy and confidentiality during the retention period and at the point of disposal, including fulfillment of data subject rights (e.g., erasure under GDPR Article 17).

3.5 To ensure that all data disposal methods are irreversible, appropriately documented, and compliant with recognized standards such as NIST SP 800-88.

3.6 To minimize operational inefficiencies, cost overhead, and legal exposure caused by over-retention or untracked legacy data.

3.7 To support business continuity and disaster recovery objectives through integrated backup retention governance and defensible data archiving practices.

4. Roles and Responsibilities

4.1 Top Management

4.1.1 Approves this policy and ensures appropriate funding, resourcing, and integration into enterprise governance, risk management, and compliance programs.

4.1.2 Holds overall accountability for legal and regulatory compliance related to data retention and secure disposal.

4.2 Chief Information Security Officer (CISO)

4.2.1 Owns this policy and is responsible for defining and reviewing retention and disposal governance in alignment with the Information Security Management System (ISMS).

4.2.2 Ensures that classification-based retention and disposal requirements are implemented within business units and technical systems.

4.2.3 Monitors compliance with this policy and enforces corrective actions where necessary.

[... 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 annually or when any of the following conditions are met:

9.1.1 Changes to applicable laws or regulations affecting data retention (e.g., updates to the GDPR, tax codes, or DORA)

9.1.2 Revisions to the classification framework or business processes affecting data lifecycle stages

9.1.3 Introduction of new IT systems, archiving platforms, or media disposal technologies

9.1.4 Internal audit findings or regulatory recommendations identifying gaps in retention or disposal practices

9.2 The review shall be led by the CISO and the Data Protection Officer (DPO), with input from Legal, Compliance, IT, and business units.

9.3 The Master Data Retention Schedule (MDRS) and Disposal Register shall be reviewed in parallel to ensure:

9.3.1 Schedules remain accurate and reflect operational, legal, and regulatory requirements

9.3.2 Disposal documentation is complete and auditable

9.3.3 Legal hold and deletion suspension records are validated and released when appropriate

9.4 Any updates to this policy must:

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

9.4.2 Include revision history and change justification

9.4.3 Be approved by Top Management

9.4.4 Be communicated to relevant personnel with updated training or guidance materials

9.5 Where significant policy changes occur, affected employees must complete targeted training within 30 days of release to ensure continued compliance.

9.6 Related Policies and Linkages

10. Related Policies and Linkages

10.1.1 P4 - Access Control Policy: Ensures that only authorized individuals can access data during its retention period and that expired data is restricted pending disposal.

10.1.2 P12 - Asset Management Policy: Identifies which assets contain data requiring scheduled disposal and tracks their lifecycle from acquisition to destruction.

10.1.3 P13 - Data Classification and Labeling Policy: Guides classification decisions that directly influence retention periods and required disposal methods.

10.1.4 P15 - Backup and Restore Policy: Defines retention periods and disposal procedures for backup media and replicated data assets.

10.1.5 P18 - Cryptographic Controls Policy: Supports cryptographic erasure for disposal and enforces encryption during data storage until destruction.

10.1.6 P30 - Incident Response Policy: Is activated in cases where improper disposal results in potential data loss, breach, or regulatory violation.

10.2 Each linked policy plays a role in enforcing a coherent data governance model across classification, lifecycle control, access management, and audit readiness.

11. Reference Standards and Frameworks

11.1 This policy aligns with globally recognized standards and regulatory frameworks that define secure, compliant, and efficient data lifecycle practices.

11.2 ISO/IEC 27001:

11.2.1 Clause 6.1.3 - Risk Treatment Plan: Supports mitigation of risks associated with over-retention, data breaches, or disposal failures.

11.2.2 Clause 8.1 - Operational Planning and Control: Establishes lifecycle controls governing storage, archiving, and destruction.

11.3 ISO/IEC 27002:2022 - Controls 5.10, 5.12, 5.30, 5: Provide practical guidance on acceptable data use, retention justification, controlled deletion, and defensible recordkeeping aligned with the organization's risk tolerance.

11.4 NIST SP 800-53 Rev. 5:

11.4.1 AU-11 - Audit Record Retention: Ensures sufficient retention of audit logs and compliance evidence.

11.4.2 MP-6 - Media Sanitization: Requires secure, documented destruction methods for physical and electronic media.

11.4.3 SI-12 - Information Handling: Enforces appropriate data handling aligned with retention and disposal controls.

11.4.4 PL-2 - System Security and Privacy Plan: Requires system-specific documentation of data lifecycle handling and secure disposal provisions.

11.5 EU GDPR (2016/679):

11.5.1 Article 5(1)(e) - Storage Limitation: Requires that data not be retained longer than necessary.

11.5.2 Article 17 - Right to Erasure (“Right to be Forgotten”): Requires prompt and permanent deletion of personal data upon a valid request.

11.5.3 Article 32 - Security of Processing: Reinforces data protection during retention and mandates secure destruction of expired records.

11.6 EU NIS2 Directive (2022/2555):

11.6.1 Article 21(2)(a-e): Requires entities to adopt policies and technical measures for secure data handling, including storage limitation and disposal methods.

11.7 EU DORA (2022/2554):

11.7.1 Article 5 - Governance and Control: Mandates structured ICT risk management, including secure information lifecycle handling.

11.7.2 Article 9 - ICT Risk Management Framework: Requires policies for data retention, destruction, and legal/regulatory compliance of digital operations.

11.8 COBIT 2019:

11.8.1 DSS01 - Managed Operations: Supports retention tracking and consistency across data systems.

11.8.2 DSS05 - Managed Security Services: Ensures protection of stored and archived data until secure disposal.

11.8.3 MEA03 - Monitor, Evaluate, and Assess Compliance: Enables auditing of retention enforcement, deletion procedures, and regulatory compliance.