					[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 where applicable		
Standard/Regulation	**Clause/Article**	**Comment**
ISO/IEC 27001:2022	Clauses 6.1.3, 831	
ISO/IEC 27002:2022	Controls 5.10, 5.12, 5.30, 5.33	
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, MEA03	

					[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	

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 lifecycle. It ensures compliance with applicable legal, regulatory, and contractual obligations, and prevents unnecessary or risky accumulation of data.

1.2 This policy supports the implementation of ISO/IEC 27001:2022 by enforcing control over data storage duration and irreversible disposal practices. It enables traceable documentation of records, enforces retention aligned with classification sensitivity, and ensures readiness for audit, regulatory inspection, and legal discovery.

1.3 It further aims to uphold confidentiality, integrity, and availability of data while minimizing business risk, operational inefficiencies, and exposure to 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 The 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 It applies to all organizational departments and individual employees, contractors, 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 premature, unauthorized, or accidental deletion of records needed for ongoing operations, 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 the privacy and confidentiality of data during its 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 Executive Management

4.1.1 Approves this policy and ensures appropriate funding, resourcing, and integration into enterprise 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)

[.....]

11. Reference Standards and Frameworks

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

ISO/IEC 27001:2022

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

Clause 8.1 – Operational Planning and Control: Establishes lifecycle controls that govern storage, archival, and destruction.

ISO/IEC 27002:2022 – Controls 5.10, 5.12, 5.30, 5.33

Provide practical guidance on acceptable data use, retention justification, controlled deletion, and defensible recordkeeping aligned with organizational risk tolerance.

NIST SP 800-53 Rev.5

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

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

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

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

EU GDPR (2016/679)

Article 5(1)(e) – Data Minimization and Storage Limitation: Requires that data not be retained longer than necessary.

Article 17 – Right to Erasure ("Right to be Forgotten"): Requires prompt and permanent deletion of personal data upon valid request.

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

EU NIS2 Directive (2022/2555)

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

EU DORA (2022/2554)

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

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

COBIT 2019

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

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

MEA03 – Monitor, Evaluate, and Assess Compliance: Enables auditing of retention enforcement, deletion procedures, and regulatory fulfillment.