					Insert Registered Legal Entity Name Here							
Document number: P14S					Document Title: **Data Retention Policy and Secure 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	Covers risk treatment, operational controls, and retention requirements
ISO/IEC 27002:2022	Control 5	Guidance on retention periods and secure destruction methods
NIST SP 800-53 Rev.5	AU-11, MP-6, SI-12	Audit record retention, media sanitization, data retention limits, and enforcement
EU NIS2	Article 21(2)(a)	Requires a risk-appropriate lifecycle management policy
EU DORA	Article 5(1)	ICT risk management: data availability and removal
COBIT 2019	BAI03.04, DSS01	Information lifecycle controls and secure disposal
EU GDPR	Article 5(1)(e), 17	Data must not be kept longer than necessary; right to erasure

1. Purpose

1.1 The purpose of this policy is to define enforceable requirements for the retention and secure disposal of information within an SME environment. It ensures that records are retained only for the period required by law, contractual obligation, or business need, and are securely destroyed thereafter.

1.2 This policy is intended to reduce information risk, manage legal exposure, and limit the storage of redundant or obsolete data. It supports compliance with ISO/IEC 27001 and data protection frameworks such as the GDPR by minimizing the unauthorized retention of personal or sensitive information.

1.3 A well-structured retention and disposal framework reduces operating costs, improves system performance, and enhances audit readiness. For SMEs with limited IT capacity, it provides a practical means of managing digital and physical information assets responsibly.

2. Scope

2.1 This policy applies to:

2.1.1 All records, files, logs, communications, and data sets created, collected, processed, or stored by the organization

2.1.2 All employees, contractors, and external providers handling organizational data

2.1.3 All data formats (e.g., paper, electronic, image, audio, or log) and all storage media (e.g., local drives, cloud services, email servers, backups)

2.2 The scope includes:

2.2.1 Business documents (e.g., invoices, contracts, project reports)

2.2.2 Operational records (e.g., logs, access history, backup snapshots)

2.2.3 Personal data (e.g., Human Resources (HR) files, client communications, support records)

2.2.4 Data hosted internally, externally, or in hybrid environments

2.2.5 Archived and backup data, whether active or dormant

2.3 All stages of the data lifecycle are in scope, from creation through authorized disposal.

3. Objectives

3.1 Define consistent retention requirements based on legal, operational, and regulatory criteria.

3.2 Prevent the premature deletion of critical records and eliminate unnecessary data accumulation.

3.3 Ensure the secure and irreversible disposal of data when retention is no longer required.

3.4 Assign accountability for enforcing retention and deletion decisions within SME staffing constraints.

3.5 Provide audit-ready documentation to demonstrate due diligence under ISO 27001, the GDPR, NIS2, and other applicable frameworks.

3.6 Promote secure lifecycle management of data without imposing unnecessary technical burden on non-specialist personnel.

4. Roles and Responsibilities

4.1 General Manager (GM)

4.1.1 Approves and owns this policy.

4.1.2 Ensures retention and disposal procedures are implemented in a manner consistent with legal obligations and business risk.

4.1.3 Authorizes exceptions and Legal Hold and Deletion Suspension where necessary.

4.1.4 Initiates policy reviews and approves updates based on business or regulatory changes.

4.2 Designated Data Owner

4.2.1 Is assigned for each data category (e.g., financial, Human Resources (HR), client records).

4.2.2 Classifies records and determines the appropriate retention period based on this policy and legal guidance.

4.2.3 Authorizes deletion when retention requirements have been met.

4.2.4 Supports internal audits by providing context on retention rationale and disposal events.

[... 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 must be reviewed at least annually, or upon:

9.1.1 Changes in applicable laws (e.g., data protection, financial reporting)

9.1.2 Adoption of new systems or processes that affect the data lifecycle

9.1.3 Audit findings or incidents identifying gaps in retention practices

9.2 Reviews must ensure that the Retention Register remains complete and reflects all major record categories.

9.3 Policy updates must be approved by the GM and communicated to affected staff. The most recent version must be accessible and subject to version control.

10. Related Policies and Linkages

10.1 P2S – Governance Roles and Responsibilities Policy: Defines policy ownership and authority for exceptions.

10.2 P13S – Data Classification and Labeling Policy: Determines how retention requirements align with data classification.

10.3 P12S – Asset Management Policy: Governs storage media containing data subject to retention and disposal requirements.

10.4 P17S – Data Protection and Privacy Policy: Ensures data protection and minimization and supports lawful processing under the GDPR.

10.5 P30S – Incident Response Policy: Applies where disposal or retention failures result in potential data exposure.

11. Reference Standards and Frameworks

11.1 ISO/IEC 27001

11.1.1 Clause 6.1.3: Requires the treatment of information-related risks, including retention risks.

11.1.2 Clause 8.1: Defines lifecycle operational controls.

11.2 ISO/IEC 27002

11.2.1 Control 5.33: Provides guidance on setting retention periods and secure destruction methods.

11.3 NIST SP 800-53 Rev. 5

11.3.1 AU-11: Requires audit record retention.

11.3.2 MP-6: Defines media sanitization procedures.

11.3.3 SI-12: Addresses data retention limits and enforcement.

11.4 EU GDPR

11.4.1 Article 5(1)(e): Data must be kept no longer than necessary.

11.4.2 Article 17: The right to erasure applies where data is no longer lawfully retained.

11.5 EU NIS

11.5.1 Article 21(2)(a): Requires risk-appropriate organizational policies, including lifecycle management.

11.6 EU DORA

11.6.1 Article 5(1): ICT risk management includes data availability and removal.

11.7 COBIT 2019

11.7.1 BAI03.04: Requires information lifecycle controls.

11.7.2 DSS01.06: Requires secure disposal procedures as part of safeguarding information assets.