					[Insert Registered Legal Entity Name Here]							
Document number: P15S					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	Clause 8.1	
ISO/IEC 27002:2022	Controls 5.29, 8.13	
NIST SP 800-53 Rev.5	CP-9, MP-6	
EU NIS2	Article 21(2)(c)	
EU DORA	Article 10(1)	
COBIT 2019	BAI04.05, DSS04.07	
EU GDPR	Articles 5(1)(f), 32(1)(c)	

1. **Purpose**
   1.1. This policy defines how the organization performs and manages backups to ensure business continuity, protect against data loss, and enable timely recovery from incidents.
   1.2. It establishes enforceable rules for how systems and data must be backed up, stored, and restored, particularly in SMEs without complex IT infrastructure.
   1.3. This policy supports audit readiness and ISO/IEC 27001 certification by ensuring that essential backup controls are in place, consistently applied, and reviewed regularly.
   1.4. The organization's ability to recover from technical failures, accidental deletion, or cyber incidents depends on strict adherence to this policy.
2. **Scope**
   2.1. This policy applies to all business systems and data, including:
      2.1.1. Financial records, customer information, and HR data
      2.1.2. Desktops, laptops, servers, and cloud applications used in business operations
      2.1.3. Backup media such as USB drives, external storage, or cloud-based backups
   2.2. It also applies to all individuals with responsibility for handling or managing backup processes, including:
      2.2.1. The General Manager (GM) or designated responsible person
      2.2.2. External IT support providers or consultants
      2.2.3. All employees responsible for saving data to approved locations
3. **Objectives**
   3.1. Ensure all critical business data and systems are securely backed up at appropriate intervals based on risk and operational need.
   3.2. Guarantee that data can be recovered in a timely and complete manner following disruptions.
   3.3. Prevent unauthorized access, tampering, or loss of backup data through effective storage controls.
   3.4. Clearly assign and enforce roles and responsibilities for implementing and testing backup procedures.
   3.5. Support compliance with ISO/IEC 27001, GDPR, and other regulatory obligations through structured, documented backup practices.
4. **Roles and Responsibilities**
   4.1. **General Manager (GM)**
      4.1.1. Approves this policy and ensures it is enforced
      4.1.2. Allocates resources and designates responsibility for backup and restore activities
      4.1.3. Reviews backup failures, incidents, or policy deviations
      4.1.4. Leads annual policy reviews and ensures audit readiness
   4.2. **External IT Support Provider (if applicable)**
      4.2.1. Implements and manages backup solutions (local or cloud-based)
   4.3. […..]

10. **Related Policies and Linkages**
    10.1. This policy aligns with and depends on the following SME policies:

10.1.1. **P14S – Data Retention and Disposal Policy**: Defines how long backup data should be stored and securely deleted.

10.1.2. **P13S – Data Classification and Labeling Policy**: Helps prioritize which data must be backed up based on classification levels.

10.1.3. **P30S – Incident Response Policy**: Covers procedures if backups fail or if data recovery is required after a breach or outage.

10.1.4. **P2S – Governance Roles & Responsibilities Policy**: Assigns clear authority for backup oversight and policy enforcement.

10.1.5. **P17S – Data Protection and Privacy Policy**: Ensures backup handling of personal data aligns with legal and privacy regulations.

11. Reference Standards and Frameworks

This policy supports compliance with the following frameworks:

ISO/IEC 27001:2022

Clause 8.1: Operational planning and control of backup systems as part of ISMS

ISO/IEC 27002:2022

Control 8.13: Prescribes best practices for backup scheduling, monitoring, and restoration

Annex A Control 5.29: Backup integration with business continuity and restore readiness

NIST SP 800-53 Rev.5

CP-9 *(Contingency Planning)*: Defines structured backup strategies for business resilience

MP-6 *(Media Protection)*: Requires secure handling and destruction of backup media

EU GDPR

Article 5(1)(f*)*: Mandates integrity and availability of personal data

Article 32(1)(c): Requires the ability to restore access to personal data in a timely manner

EU NIS2 Directive

Article 21(2)(c): Requires backup and recovery as part of resilience and continuity planning

EU DORA

Article 10(1*)*: Financial sector organizations must ensure backup as part of ICT continuity measures

COBIT 2019

BAI04.05: Requires documented backup strategies

DSS04.07: Emphasizes routine testing and control over data backup and recovery processes