					Insert Registered Legal Entity Name Here							
Document number: P15S					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	Clause 8	Backup controls in accordance with ISMS requirements
ISO/IEC 27002:2022	Controls 5.29, 8.13	Best practices for backup and integration with business continuity planning
NIST SP 800-53 Rev.5	CP-9, MP-6	Backup and media protection
EU NIS2	Article 21(2)(c)	Resilience and continuity through backup
EU DORA	Article 10(1)	ICT continuity - backup for financial sector organizations
COBIT 2019	BAI04.05, DSS04	Documentation and testing of backups and control processes
EU GDPR	Articles 5(1)(f), 32(1)(c)	Integrity, availability, and timely restoration of data

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 mandatory requirements 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, applied consistently, 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 Human Resources (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 responsible 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 that all critical business data and systems are securely backed up at appropriate intervals based on risk and operational need.

3.2 Ensure that data can be recovered in a timely and complete manner following disruptions.

3.3 Prevent unauthorized access to, tampering with, 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 and documented backup practices.

4. Roles and Responsibilities

4.1 General Manager (GM)

4.1.1 Approves this policy and ensures its enforcement

4.1.2 Allocates resources and assigns responsibility for backup and restore activities

4.1.3 Reviews backup failures, incidents, or policy deviations

4.1.4 Leads the annual policy review and ensures audit readiness

4.2 External IT Support Provider (if applicable)

4.2.1 Implements and manages backup solutions (local or cloud-based)

4.2.2 Monitors backup success and schedules restore tests

4.2.3 Reports failures and incidents directly to the GM

4.2.4 Ensures encryption, access restrictions, and proper handling of backup media

[... 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 by the GM. Triggers for interim reviews include:

9.1.1 Major changes to systems or storage methods

9.1.2 Introduction of new cloud or IT platforms

9.1.3 Legal or regulatory changes affecting data recovery

9.1.4 Findings from audits or incidents

9.2 The GM is responsible for initiating the review, approving changes, and communicating updates.

9.3 Policy versions must be tracked and archived. Superseded versions must have restricted access to prevent confusion during audits or business continuity events.

10. Related Policies and Linkages

10.1 This policy aligns with and depends on the following SME policies:

10.1.1 P14S – Data Retention Policy: Defines how long backup data must be retained and when it must be securely deleted.

10.1.2 P13S – Data Classification and Labeling Policy: Supports prioritization of data to be backed up based on classification levels.

10.1.3 P30S – Incident Response Policy: Defines procedures where backups fail or data recovery is required following a breach or outage.

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

10.1.5 P17S – Data Protection and Privacy Policy: Ensures that the handling of personal data in backups is aligned with legal and privacy requirements.

11. Reference Standards and Frameworks

11.1 ISO/IEC 27001

11.1.1 Clause 8.1: Operational planning and control of backup systems as part of the Information Security Management System (ISMS)

11.2 ISO/IEC 27002

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

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

11.3 NIST SP 800-53 Rev.5

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

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

11.4 EU GDPR

11.4.1 Article 5(1)(f): Requires integrity and availability of personal data

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

11.5 EU NIS2 Directive

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

11.6 EU DORA

11.6.1 Article 10(1): Requires financial sector organizations to ensure backup as part of ICT continuity measures

11.7 COBIT 2019

11.7.1 BAI04.05: Requires documented backup strategies

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