					Insert Registered Legal Entity Name Here							
Document number: P32S					Document Title: **Business Continuity Policy and Disaster Recovery 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, 6.3, 8	
ISO/IEC 27002:2022	Controls 5.29, 5.30	
NIST SP 800-53 Rev.5	CP-2, CP-4, CP-6, CP-7	
EU GDPR	Articles 32, 33	
EU NIS2	Article 21(2)(f)	
EU DORA	Article 10	
COBIT 2019	DSS04	

1. Purpose

1.1 This policy ensures that the organization can maintain business operations and recover critical IT services during and after disruptive events such as power outages, cyberattacks, ransomware infections, or system failures.

1.2 It provides a clear framework for Business Continuity and Disaster Recovery Plans (BCP/DRP), tailored for SMEs without dedicated IT teams.

1.3 This policy supports the organization in meeting mandatory compliance requirements under ISO/IEC 27001:2022, GDPR, NIS2, DORA, and COBIT 2019, while strengthening operational resilience and customer trust.

2. Scope

2.1 This policy applies to:

2.1.1 all mission-critical systems and services (e.g., email, cloud storage, invoicing platforms, customer records)

2.1.2 all employees and external IT service providers responsible for BC/DR readiness and execution

2.1.3 all types of disruption, including cyber incidents, hardware failure, power loss, flooding, and office inaccessibility

2.2 It covers:

2.2.1 backup management

2.2.2 business continuity planning (BCP)

2.2.3 disaster recovery operations

2.2.4 staff training and testing

2.2.5 legal and regulatory response procedures

3. Objectives

3.1 Protect the organization’s ability to deliver key services despite unplanned disruptions.

3.2 Ensure timely recovery of systems and data against predefined Recovery Time Objectives (RTOs).

3.3 Enable all staff to follow continuity procedures during crises with minimal confusion.

3.4 Maintain compliance with data protection and operational resilience requirements, including GDPR Article 32 and NIS2 Article 21.

3.5 Establish a practical, testable continuity and recovery strategy suitable for SMEs.

4. Roles and Responsibilities

4.1 General Manager (GM)

4.1.1 Owns the BC/DR process and this policy.

4.1.2 Approves the Business Continuity and Disaster Recovery Plans (BCP/DRP).

4.1.3 Coordinates incident reporting, incident management, and internal communication during disruptions.

4.1.4 Makes regulatory notifications where required (e.g., GDPR breach notifications).

4.2 IT Support Provider / System Administrators

4.2.1 Maintain and test backups.

4.2.2 Execute disaster recovery procedures when triggered.

4.2.3 Document all recovery actions and system restoration events.

4.2.4 Report critical IT incidents to the GM immediately.

[... 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 Annual Review of Policy and Plan

9.1.1 The General Manager (GM) must ensure this policy and its associated Business Continuity and Disaster Recovery Plans (BCP/DRP) are formally reviewed at least once per year.

9.1.2 The review must include:

9.1.2.1 evaluation of new or emerging risks

9.1.2.2 revalidation of RTOs and RPOs

9.1.2.3 verification of supplier and contact information

9.1.2.4 alignment with changes in IT systems, legal obligations, or operations

9.2 Trigger-Based Updates

9.2.1 This policy must also be updated in response to:

9.2.1.1 major incidents or disruptions, especially where objectives were not met

9.2.1.2 new legal or regulatory obligations (e.g., DORA amendments)

9.2.1.3 changes in critical systems, cloud platforms, or personnel

9.2.1.4 findings from annual BCP/DR tests

9.3 Change Control Process

9.3.1 All changes must be approved by the GM.

9.3.2 A version history log must be maintained, including the date, description of the change, and approver.

9.3.3 The updated policy must be redistributed to all relevant personnel, including the IT Support Provider and Department Heads.

9.4 Documentation of Lessons Learned

9.4.1 After tests or actual disruptions, documented lessons learned must inform future revisions.

9.4.2 These reviews must also include supplier performance evaluations and checks of response adequacy.

10. Related Policies and Linkages

10.1 This policy is closely integrated with the following SME policies:

10.1.1 P1S – Information Security Policy: Defines the high-level security objectives that continuity and recovery practices must support.

10.1.2 P4S – Access Control Policy: Enables emergency revocation or restoration of user access during business disruption scenarios.

10.1.3 P6S – Risk Management Policy: Provides the foundation for identifying, evaluating, and prioritizing continuity-related risks.

10.1.4 P8S – Information Security Awareness and Training Policy: Ensures employees are prepared to act during disruptions and understand the BCP.

10.1.5 P15S – Backup and Restore Policy: Provides specific technical procedures for safeguarding data availability and recovery.

10.1.6 P17S – Data Protection and Privacy Policy: Ensures continuity planning respects personal data protections and complies with GDPR during and after incidents.

10.1.7 P22S – Logging and Monitoring Policy: Supports detection of events that may trigger BC/DR processes and provides a forensic audit trail following disruptions.

10.1.8 P30S – Incident Response Policy: Directly precedes activation of the recovery process in the event of cyber or operational incidents.

10.1.9 P31S – Evidence Collection and Forensics Policy: Ensures digital evidence is captured during continuity scenarios for compliance, insurance, or investigative purposes.

10.2 These policies form a cohesive, audit-ready framework for resilience, accountability, and continuity of control across all SME operations.

11. Reference Standards and Frameworks

11.1 ISO/IEC 27001:

11.1.1 Clause 6.1 – Requires risk-based planning and treatment, including business continuity and recovery.

11.1.2 Clause 6.3 – Emphasizes continual improvement following disruptions.

11.1.3 Clause 8.1 – Requires operational controls, including documented continuity measures.

11.2 ISO/IEC 27002:

11.2.1 Control 5.29 – Requires the establishment and maintenance of business continuity arrangements.

11.2.2 Control 5.30 – Requires testing and review of those arrangements.

11.3 NIST SP 800-53 Rev.5:

11.3.1 CP-2 – Defines requirements for contingency planning.

11.3.2 CP-4 – Requires contingency training for organizational personnel.

11.3.3 CP-6 – Covers alternate storage site requirements.

11.3.4 CP-7 – Governs alternate processing site expectations.

11.4 EU GDPR:

11.4.1 Article 32 – Requires measures to ensure the ongoing availability and resilience of processing systems and services.

11.4.2 Article 33 – Triggers breach notification obligations where continuity failure results in compromise of personal data.

11.5 EU NIS2 Directive (2022/2555):

11.5.1 Article 21(2)(f) – Requires continuity planning and crisis management capabilities as a condition of cyber risk preparedness.

11.6 EU DORA Regulation (2022/2554):

11.6.1 Article 10 – Requires implementation of digital operational resilience testing and recovery capabilities, particularly for financial-sector SMEs.

11.7 COBIT 2019:

11.7.1 DSS04 – Manage Continuity: Provides enterprise governance guidance for maintaining and validating operational resilience, including ownership, testing, supplier integration, and post-event reviews.