| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | [Insert Registered Legal Entity Name Here] | | | | | | | |
| Document number:<br>P32S | | | | | Document Title:<br>**Business Continuity and Disaster Recovery Policy** | | | | | | | |
| Version:<br>1.0 | | Effective Date:<br>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, 6.3, 8.1 | |
| 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 the organization can maintain business operations and recover essential 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 (BC/DR) planning, tailored for SMEs without dedicated IT teams.

1.3. This policy helps the organization meet mandatory requirements under ISO/IEC 27001:2022, GDPR, NIS2, DORA, and COBIT 2019, while building operational resilience and customer trust.

**2. Scope**

2.1. This policy applies to:

2.1.1. All business-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 disruptions, 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 with predefined Recovery Time Objectives (RTOs).

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

3.4. Maintain regulatory compliance with data protection and operational resilience laws, 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 Plan (BCP)

4.1.3. Coordinates incident response and internal communication during disruptions

[…..]

**Related Policies and Linkages**

4.2. This policy is tightly integrated with the following SME policies:

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

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

4.2.3. **P6S – Risk Management Policy**: Forms the foundation for identifying, evaluating, and prioritizing continuity-related risks.

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

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

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

4.2.7. **P22S – Logging and Monitoring Policy**: Supports detection of events that may trigger BC/DR processes, and provides forensic audit trails post-disruption.

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

4.2.9. **P31S – Evidence Collection and Forensics Policy**: Ensures digital evidence is captured during continuity scenarios for compliance, insurance, or investigation needs.

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

## 5. Reference Standards and Frameworks

**ISO/IEC 27001:2022**

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

**Clause 6.3** – Emphasizes continual improvement following disruptions.

**Clause 8.1** – Mandates operational controls, which include documented continuity measures.

.

**ISO/IEC 27002:2022**

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

**Control 5.30** – Requires testing and review of those arrangements

**NIST SP 800-53 Rev.5**

**CP-2** – Defines requirements for contingency planning.

**CP-4** – Mandates contingency training for organizational personnel.

**CP-6** – Covers alternate storage site requirements.

**CP-7** – Governs alternate processing site expectations.

**EU GDPR**

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

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

**EU NIS2 Directive (2022/2555)**

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

**EU DORA Regulation (2022/2554)**

**Article 10** – Mandates the implementation of digital operational resilience testing and recovery capabilities, especially for financial sector SMEs.

**COBIT 2019**

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