					Insert Registered Legal Entity Name Here							
Document number: P32					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	Clause 8	
ISO/IEC 27002:2022	Controls 5.29, 5.30	
NIST SP 800-53 Rev.5	CP-1 to CP-11	
NIST SP 800-34 Rev.1	Contingency Planning	Framework
ISO 22301:2019		Business Continuity Management System Requirements
EU GDPR	Article 32	
EU NIS2	Article 21(2)(f)	
EU DORA	Article 10	
COBIT 2019	DSS	

1. Purpose

1.1. This policy defines the mandatory controls and responsibilities required to ensure the organization's ability to sustain or restore critical business operations and supporting ICT services during and after a disruptive incident.

1.2. It is intended to protect life, operational stability, legal obligations, customer commitments, and the organization's reputation by embedding resilience through proactive planning and validated recovery capabilities.

1.3. This policy establishes the foundation for the organization's Business Continuity Management (BCM) and Disaster Recovery (DR) framework and ensures compliance with applicable regulatory, contractual, and industry requirements.

2. Scope

2.1. This policy applies to all organizational units, information systems, business processes, personnel, and third-party services classified as critical or essential based on Business Impact Analysis (BIA) results.

2.2. This policy covers:

2.2.1. Natural and human-caused disruptions, including cyberattacks, infrastructure failures, data center outages, pandemics, and vendor service interruptions

2.2.2. The planning, testing, and continual improvement of Business Continuity Plans (BCPs) and Disaster Recovery Plans (DRPs)

2.2.3. Roles and responsibilities for emergency response, recovery coordination, and incident escalation

2.3. All personnel with continuity or recovery responsibilities, including IT, Business Process Owners, crisis managers, and vendors, are subject to this policy.

3. Objectives

3.1. Ensure continuity of business operations and services through predefined and tested procedures, minimizing operational, reputational, and legal impact.

3.2. Restore ICT services within defined Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs), aligned with business risk tolerance levels.

3.3. Assign ownership for business continuity and disaster recovery planning, execution, and governance across the enterprise.

3.4. Ensure continuity capabilities are regularly tested, maintained, and improved based on realistic scenarios and audit findings.

3.5. Fulfill compliance obligations under ISO, NIST, GDPR, DORA, and NIS2, supporting due diligence in operational resilience and availability.

4. Roles and Responsibilities

4.1. Top Management

4.1.1. Approves the Business Continuity Policy and Disaster Recovery Policy and ensures strategic alignment.

4.1.2. Allocates budget and resources to support business continuity, emergency response, and recovery exercises.

4.2. Business Continuity Manager (BCM Lead)

4.2.1. Owns the development and maintenance of organization-wide Business Continuity Plans (BCPs) and coordinates continuity testing.

4.2.2. Maintains the BIA schedule, facilitates training, and ensures documentation meets compliance requirements.

[... 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 shall be reviewed annually by the Business Continuity Manager and the CISO to ensure alignment with:

9.1.1. Changes in business operations, critical systems, or IT infrastructure

9.1.2. Lessons learned from incidents, audits, tabletop exercises, or DR tests

9.1.3. Updated regulatory or contractual obligations (e.g., DORA, GDPR, customer RTO/RPO requirements)

9.1.4. Changes to the organization’s risk appetite or continuity strategy

9.2. Reviews shall include:

9.2.1. Validation of plan relevance and contact details

9.2.2. Reassessment of RTOs, RPOs, and recovery tiering

9.2.3. Evaluation of backup and DR service capacity

9.2.4. Feedback from stakeholders who executed recent recovery plans or tests

9.3. All policy changes shall be:

9.3.1. Maintained under version control with documented rationale and stakeholder approval

9.3.2. Communicated to key personnel and teams with updated responsibilities

9.3.3. Reflected in updated training, awareness materials, and operating procedures

9.4. Emergency interim updates shall be issued if a major organizational change, legal requirement, or critical finding renders current plans or this policy ineffective.

10. Related Policies and Linkages

10.1. This policy operates in conjunction with the following key documents:

10.1.1. P1 – Information Security Policy: Establishes the requirement for risk-based, resilient operations under all conditions.

10.1.2. P5 – Change Management Policy: Ensures that any recovery-related configuration or IT infrastructure changes follow documented and approved workflows.

10.1.3. P14 – Data Retention Policy and Disposal Policy: Governs the lifecycle of backup media and recovered data used in continuity operations.

10.1.4. P15 – Backup and Restore Policy: Enforces controls over backup frequency, security, and restoration verification.

10.1.5. P18 – Cryptographic Controls Policy: Ensures that recovery processes maintain encryption and confidentiality requirements.

10.1.6. P22 – Logging and Monitoring Policy: Supports the detection and escalation of events affecting continuity.

10.1.7. P30 – Incident Response Policy: Defines containment, escalation, and root cause processes aligned with continuity triggers.

10.1.8. P33 – Audit and Compliance Monitoring Policy: Validates the integrity and effectiveness of continuity and recovery practices across systems and processes.

11. Reference Standards and Frameworks

11.1. This policy is aligned with internationally recognized business continuity and disaster recovery standards to support auditability, resilience, and legal compliance.

11.2. ISO/IEC 27002

11.2.1. Annex A Control 5.29 – Information Security During Disruption: Requires continuity of security controls under adverse conditions.

11.2.2. Annex A Control 5.30 – ICT Readiness for Business Continuity: Requires the preparation, testing, and validation of ICT recovery capabilities.

11.3. ISO 22301:2019 – Business Continuity Management Systems

11.3.1. Provides the framework for establishing, implementing, and maintaining BCM practices aligned with organizational objectives and risk thresholds.

11.4. NIST SP 800-34 Rev.1 – Contingency Planning Guide

11.4.1. Describes best practices for IT system contingency planning, including continuity strategy development, impact analysis, and plan testing.

11.5. EU GDPR (2016/679)

11.5.1. Article 32 – Security of Processing: Requires resilience of processing systems and timely restoration of availability and access to personal data (PII) following an incident.

11.6. EU NIS2 Directive (2022/2555)

11.6.1. Article 21(2)(f): Requires business continuity and crisis management measures to support the security of network and information systems.

11.7. EU DORA (2022/2554)

11.7.1. Article 10 – ICT Business Continuity: Requires financial entities to develop and test ICT continuity plans, including risk-based RTOs, RPOs, and failover capabilities.

11.8. COBIT 2019

11.8.1. DSS04 – Manage Continuity: Covers all aspects of continuity planning, including threat identification, impact analysis, recovery strategy, and regular testing.