					[Insert Registered Legal Entity Name Here]							
Document number: P32					Document Title: **Business Continuity 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 where applicable		
Standard/Regulation	**Clause/Article**	**Comment**
ISO/IEC 27001:2022	Clause 8.1	
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	DSS04	

1. **Purpose**
   1.1. This policy defines the mandatory controls and responsibilities for ensuring the organization's ability to sustain or recover critical business operations and supporting ICT services during and after a disruptive incident.
   1.2. It aims 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 provides the foundation for the organization's Business Continuity Management (BCM) and Disaster Recovery (DR) framework, ensuring 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 that are classified as critical or essential based on Business Impact Analysis (BIA) results.
   2.2. The policy covers:
      2.2.1. Natural and man-made disruptions, including cyberattacks, infrastructure failures, data center outages, pandemics, and vendor service interruptions
      2.2.2. Planning, testing, and continuous 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 staff with continuity or recovery responsibilities, including IT, business owners, crisis managers, and vendors, are subject to the provisions of this policy.
3. **Objectives**
   3.1. To ensure continuity of business operations and services through predefined and tested procedures, minimizing operational, reputational, and legal impact.
   3.2. To recover ICT services within defined Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs), aligned with business risk tolerance levels.
   3.3. To assign ownership for business continuity and disaster recovery planning, execution, and governance across the enterprise.
   3.4. To ensure that continuity capabilities are regularly tested, maintained, and improved based on realistic scenarios and audit findings.
   3.5. To meet compliance obligations under ISO, NIST, GDPR, DORA, and NIS2, supporting due diligence in operational resilience and availability.
4. **Roles and Responsibilities**
   4.1. **Executive Management**
      4.1.1. Approves the Business Continuity 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 BCPs and coordination of continuity testing.

[…..]

11. Reference Standards and Frameworks

This policy is aligned with internationally accepted business continuity and disaster recovery standards, supporting auditability, resilience, and legal compliance.

ISO/IEC 27002:2022

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

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

ISO 22301:2019 – Business Continuity Management Systems

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

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

Outlines best practices for IT system contingency plans, including continuity strategy development, impact analysis, and plan testing.

EU GDPR (2016/679)

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

EU NIS2 Directive (2022/2555)

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

EU DORA (2022/2554)

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

COBIT 2019

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