		[Insert Registered Legal Entity Name Here]
Document number: P5S		Document Title: **Change Management Policy**
Version: 1.0	Effective Date:	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 6.1, 8.1	
ISO/IEC 27002:2022	Control 8.32	
NIST SP 800-53 Rev.5	CM-2 to CM-5, CM-11	
EU NIS2	Article 21(2)(b)	
EU DORA	Articles 6(9), 8(4)(b)	
COBIT 2019	BAI06, DSS01	

					[Insert Registered Legal Entity Name Here]						
Document number: P5S					Document Title: **Change Management Policy**						
Version: 1.0		Effective Date:			Document Owner:						
X	Policy		Standard		Procedure		Form		Register		Other

Purpose

1.1. This policy ensures that all changes to IT systems, configurations, business applications, or cloud services are planned, risk-assessed, tested, and approved before implementation.

1.2. The goal is to reduce operational disruptions, security risks, and service outages by establishing a simplified but enforceable process that applies even to small businesses with limited resources.

1.3. This policy supports ISO/IEC 27001:2022 certification by formalizing how technical and operational changes are managed and documented.

2. Scope

2.1. This policy applies to:

2.1.1. Employees and department managers proposing or executing changes

2.1.2. External IT service providers managing systems or software

2.1.3. General Manager, who holds overall responsibility for change approvals

2.2. It covers changes to:

2.2.1. Software (updates, patches, new applications)

2.2.2. Hardware (replacements, upgrades)

2.2.3. Network and firewall configurations

2.2.4. Cloud services, user access permissions, or vendor integrations

2.2.5. Critical business process changes involving information systems

2.3. Both planned and emergency changes are within the scope of this policy.

3. Objectives

3.1. Ensure that all IT and business system changes are authorized, documented, and reversible if problems occur.

3.2. Prevent unplanned downtime, data loss, or security incidents caused by uncontrolled changes.

3.3. Define simple, repeatable procedures for change submission, approval, testing, and rollback.

3.4. Maintain an auditable Change Log that supports operational accountability and regulatory compliance.

3.5. Enable risk-based decision-making for significant or sensitive changes.

4. Roles and Responsibilities

4.1. **General Manager**

4.1.1. Holds ultimate accountability for all major changes.

4.1.2. Reviews and approves non-routine, critical, or high-risk changes.

4.1.3. Reviews the Change Log quarterly or after major incidents.

4.2. **IT Support or Outsourced IT Provider**

4.2.1. Implements changes, including configuration updates, patching, and system migrations.

4.2.2. Maintains a basic Change Log recording dates, types of change, outcomes, and approvers.

4.2.3. Tests changes prior to implementation and applies rollback steps as needed.

4.2.4. Notifies affected users before and after major changes.

4.3. **Department Managers**

4.3.1. Propose needed changes related to their business area.

4.3.2. Ensure employees do not bypass change procedures.

4.4. **Employees**

4.4.1. Report issues or requests requiring system changes.

4.4.2. Must not make unauthorized changes to software, hardware, or system settings.

4.5. **Security or Compliance Contact (if assigned)**

4.5.1. Reviews change requests that could impact data security or regulatory compliance.

4.5.2. Recommends additional protections when necessary (e.g., encryption, access logging).

5. Governance Requirements

5.1. **Change Submission**

5.1.1. All changes must be submitted as a Change Request (email, form, or helpdesk ticket).

[……]