					Insert Registered Legal Entity Name Here							
Document number: P05S					Document Title: **Change Management 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, 8	
ISO/IEC 27002:2022	Control 8	
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, DSS	

1. 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 purpose is to reduce operational disruption, security risk, and service outages by establishing a simplified but enforceable process that remains applicable to small businesses with limited resources.

1.3 This policy supports ISO/IEC 27001:2022 certification by formalizing the management and documentation of technical and operational changes.

2. Scope

2.1 This policy applies to:

2.1.1 Employees and department managers who propose or implement changes

2.1.2 External IT service providers responsible for managing systems or software

2.1.3 The General Manager, who retains 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 changes to IT and business systems are authorized, documented, and reversible if issues 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 Retains 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 following 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, change types, outcomes, and approvers.

4.2.3 Tests changes before implementation and executes rollback steps where required.

4.2.4 Notifies affected users before and after major changes.

[... 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

9.1.1 This policy must be reviewed annually by the General Manager or designated IT contact to ensure alignment with current systems, workflows, and regulatory requirements.

9.2 Interim Reviews

9.2.1 Reviews must also be triggered by:

9.2.1.1 Security incidents caused by inadequate change handling

9.2.1.2 Introduction of new IT systems

9.2.1.3 Changes to relevant standards such as ISO, NIS2, or DORA

9.3 Documentation of Updates

9.3.1 Changes to this policy must be version controlled and approved by the General Manager. Each version must record the date, summary of changes, and approver.

9.4 Policy Communication

9.4.1 Any updates must be communicated to all affected employees and external providers. Documentation must be updated in all reference locations (e.g. staff portal, shared drives).

10. Related Policies and Linkages

10.1 This policy is closely related to the following SME policies:

10.1.1 P2S – Governance Roles & Responsibilities Policy: Defines approval authority for changes.

10.1.2 P4S – Access Control Policy: Ensures that access changes resulting from system changes are documented and implemented correctly.

10.1.3 P7S – Onboarding and Termination Policy: Coordinates changes related to role transitions and access provisioning.

10.1.4 P15S – Backup and Restore Policy: Ensures that rollback and recovery steps can be executed if a change fails.

10.1.5 P30S – Incident Response Policy: Governs how failed or unauthorized changes are handled as security incidents.

11. Reference Standards and Frameworks

11.1 ISO/IEC 27001

11.1.1 Clause 6.1 – Risk-based planning must include change activities.

11.1.2 Clause 8.1 – Operational controls must be applied consistently to change-related activities to ensure service integrity.

11.2 ISO/IEC 27002

11.2.1 Control 8.32 – Provides guidance for secure change management processes, including documentation, testing, and approval.

11.3 NIST SP 800-53 Rev. 5

11.3.1 CM-2 – Baseline configuration for systems before change.

11.3.2 CM-3 – Configuration change control.

11.3.3 CM-4 – Security impact analysis.

11.3.4 CM-5 – Change approval and documentation.

11.3.5 CM-11 – Audit and monitoring of changes.

11.4 EU NIS2 Directive

11.4.1 Article 21(2)(b) – Requires formal procedures for technical and organizational security measures, including change management.

11.5 EU DORA

11.5.1 Articles 6(9) and 8(4)(b) – Require financial entities to maintain change and configuration management for ICT systems.

11.6 COBIT 2019

11.6.1 BAI06 – Manage Changes: Emphasizes planning, risk evaluation, and rollback capability.

11.6.2 DSS01 – Manage Operations: Ensures operational integrity during technical transitions and changes.