<table>
<tr><td colspan="4"></td><td colspan="8">[Insert Registered Legal Entity Name Here]</td></tr>
<tr><td colspan="4">Document number:
P5</td><td colspan="8">Document Title:
<b>Change Management Policy</b></td></tr>
<tr><td colspan="2">Version:
1.0</td><td colspan="2">Effective Date:
01.01.2025</td><td colspan="8">Document Owner:</td></tr>
<tr><td>X</td><td>Policy</td><td></td><td>Standard</td><td></td><td>Procedure</td><td></td><td>Form</td><td></td><td>Register</td><td></td><td>Other</td></tr>
</table>

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, 5.15	
ISO/IEC 27002:2022	Control 8.32	
NIST SP 800-53 Rev.5	CM-2 to CM-14	
EU GDPR	Articles 32(1)(b–d), 25; Recital 78	
EU NIS2	Article 21(2)(a, b, d, e)	
EU DORA	Articles 5, 8, 12	
COBIT 2019	BAI06, BAI02, BAI03, DSS01, MEA01, MEA03	

					[Insert Registered Legal Entity Name Here]						
Document number: P5					Document Title: **Change Management Policy**						
Version: 1.0		Effective Date: 01.01.2025			Document Owner:						
X	Policy		Standard		Procedure		Form		Register		Other

1. **Purpose**

1.1. This policy establishes a formal framework for initiating, assessing, approving, implementing, and reviewing changes to the organization’s information systems, infrastructure, applications, and related processes.

1.2. It ensures that all changes are executed in a controlled and auditable manner, minimizing the risk of disruption, security compromise, or regulatory non-compliance.

1.3. It supports ISO/IEC 27001:2022 Annex A Control 8.32 by enforcing secure, documented, and risk-aligned change management practices.

1.4. The policy also ensures traceability of change decisions and promotes operational resilience during planned or emergency modifications.

2. **Scope**

2.1. This policy applies to all changes affecting systems, data, and environments within the ISMS scope, including:

2.1.1. IT infrastructure (on-premises, cloud, hybrid)

2.1.2. Production, pre-production, and disaster recovery environments

2.1.3. Business applications, services, APIs, and integrations

2.1.4. Configuration settings, patching, software releases, and system migrations

2.1.5. Emergency fixes and project-based or planned changes

2.2. It governs changes initiated by:

2.2.1. Internal staff (IT operations, developers, system owners)

2.2.2. External vendors, managed service providers (MSPs), and contractors

2.2.3. Project teams during system implementation, upgrades, or service transitions

2.3. policy does not apply to:

2.3.1. Temporary test/dev environments with no access to production data

2.3.2. Personal user configurations (covered under Acceptable Use Policy)

2.3.3. Changes to systems outside the organization’s control boundary unless they affect integrated assets or compliance obligations

3. **Objectives**

3.1. To ensure that all changes are reviewed, approved, tested, and documented prior to execution.

3.2. To maintain system availability, data integrity, and service continuity during and after change activities.

3.3. To require defined change classifications, rollback plans, and risk assessments for all change types.

3.4. To enable transparent decision-making and escalation through structured governance.

3.5. To support audit readiness through traceable change records and post-implementation reviews.

3.6. To enforce separation of duties and reduce the risk of unauthorized or conflicting changes in critical systems.

4. **Roles and Responsibilities**

4.1. Executive Management

4.1.1. Endorses the Change Management Policy and ensures alignment with strategic goals and regulatory obligations.

4.1.2. Approves high-impact or cross-functional change programs as part of governance oversight.

[…..]

11. Reference Standards and Frameworks

This Change Management Policy aligns with globally recognized cybersecurity, operational resilience, and IT governance frameworks to ensure structured, secure, and auditable control over all modifications to systems, services, and infrastructure.

ISO/IEC 27001:2022

Clause 6.1 – Actions to Address Risks and Opportunities: This policy supports the identification, evaluation, and control of risks related to change.

Clause 5.15 – Access Control: Ensures access during changes is controlled and traceable.

Annex A Control 8.32 – Change Management: This policy fully implements the requirement to manage changes to information processing facilities and systems in a planned and controlled manner.

ISO/IEC 27002:2022 – Control 8.32

Reinforces the implementation of a structured change management process including change classification, approval, testing, rollback, and documentation. This policy incorporates those implementation guidelines into enforceable requirements.

NIST SP 800-53 Rev.5

CM Family (CM-1 through CM-14): This policy is tightly aligned with Configuration Management controls, including baseline configurations (CM-2), configuration change control (CM-3), security impact analysis (CM-4), and access restrictions (CM-5).

AU Family (AU-2, AU-6, AU-12): Logging and audit mechanisms referenced in this policy support event traceability and compliance review for change-related activity.

RA-3, RA-5: Change-driven risk assessments and vulnerability scans are embedded in the change evaluation process.

PM-11 (Mission/Business Process Definition): Ensures that business continuity and operational objectives are preserved during changes.

EU GDPR (2016/679)

Article 32(1)(b–d): This policy supports the requirement for appropriate technical and organizational measures to ensure data security, especially during system changes.

Article 25 – Data Protection by Design and by Default: Ensures that changes affecting personal data integrate privacy and security into design and rollout.

Recital 78: Requires that data controllers implement mechanisms—such as change control policies—to ensure ongoing confidentiality, integrity, and resilience of processing systems.

EU NIS2 Directive (2022/2555)

Article 21(2)(a, b, d, e): Mandates technical and organizational measures for managing ICT risks, including those arising from system changes, software updates, and infrastructure modifications. This policy enforces change discipline to ensure system integrity and service continuity.

EU DORA (2022/2554)

Article 5 – Governance and Internal Control Framework: This policy enforces operational risk management principles tied to ICT changes and updates.

Article 8 – ICT Risk Management Framework: Mandates that financial entities manage all changes impacting ICT systems under structured change management processes—mirrored in this policy's classification, testing, rollback, and documentation mandates.

Article 12 – Incident Reporting: Ensures that failed changes leading to ICT disruptions are traceable, documented, and reported where applicable.

COBIT 2019

BAI06 – Managed IT Changes: This policy directly fulfills BAI06 objectives by establishing structured workflows for change approval, impact assessment, communication, and testing.

BAI02 – Managed Requirements Definition and **BAI03 – Managed Solutions Identification and Build**: Ensure that business-driven changes are reviewed and implemented securely.

DSS01 – Managed Operations: Supports ongoing system integrity during change execution.

MEA01 and MEA03 – Monitor, Evaluate, and Assess Performance and Compliance: Enables continuous oversight of change management policy effectiveness and enforcement.