					Insert Registered Legal Entity Name Here							
Document number: P05					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, 5.15	Addresses risk treatment actions, access control, and change management
ISO/IEC 27002:2022	Control 8	Implements a structured change management process
NIST SP 800-53 Rev.5	CM-2 to CM-14	Configuration management controls
EU GDPR	Articles 32(1)(b–d), 25; Recital 78	Technical and organizational measures for system and data security during changes
EU NIS2	Article 21(2)(a, b, d, e)	Mandates risk management of ICT changes
EU DORA	Articles 5, 8, 12	Governs operational and ICT risk and incident reporting
COBIT 2019	BAI06, BAI02, BAI03, DSS01, MEA01, MEA03	Structured IT change management performance, compliance, and requirements

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. This 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, Application Programming Interfaces (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), contractors, and third-party service providers

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

2.3. This policy does not apply to:

2.3.1. Temporary test or development environments with no access to production data

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

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 segregation of duties and reduce the risk of unauthorized or conflicting changes in critical systems.

4. Roles and Responsibilities

4.1. Top Management

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

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

4.1.3. Allocates the necessary resources and budget for change control tooling and personnel training.

4.2. Change Advisory Board

4.2.1. Reviews and authorizes standard and major changes, ensuring appropriate evaluation of risk, impact, and dependencies.

4.2.2. Validates rollback plans, test results, stakeholder communications, and scheduling.

4.2.3. Is composed of system owners, Information Security, IT Operations, sales leads, and Compliance representatives.

4.2.4. May delegate decisions for low-risk or emergency changes under documented controls.

[... 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. Review Triggers and Frequency

9.1.1. This policy must be reviewed annually or upon:

9.1.1.1. Major IT or infrastructure changes

9.1.1.2. Significant incidents related to failed or unauthorized changes

9.1.1.3. Regulatory updates or new legal obligations related to change management

9.1.1.4. Implementation of new tooling or Change Management System platforms

9.2. Change Management Policy Review Process

9.2.1. The Change Manager will lead the review process in collaboration with:

9.2.1.1. IT, Security, and Operations

9.2.1.2. Internal Audit and Risk Management

9.2.1.3. Change Advisory Board representatives

9.2.2. Updates must be reviewed and approved by Top Management and the ISMS Steering Committee.

9.2.3. Reissued versions must be tracked in the Document Register and communicated to affected parties, with re-acknowledgment where required.

9.3. Document Control and Versioning

9.3.1. All versions must include:

9.3.1.1. Policy ID, title, and classification level

9.3.1.2. Owner and revision history

9.3.1.3. Change log and effective date

9.3.1.4. Approval authority

9.3.2. Archived versions must be retained in accordance with the Document Retention Policy (minimum of 3 years).

10. Related Policies and Linkages

10.1. This policy is directly linked to, and supports enforcement of:

10.1.1. P1 – Information Security Policy: Establishes the requirement for formal security controls and process-level accountability, including change management governance.

10.1.2. P2 – Governance Roles and Responsibilities Policy: Defines approval authorities and segregation of duties relevant to change authorization and oversight.

10.1.3. P4 – Access Control Policy: Ensures that access permissions for change implementers and reviewers follow least privilege principles.

10.1.4. P6 – Risk Management Policy: Ensures that all changes are subject to appropriate risk evaluation and mitigation strategies.

10.1.5. P33 – Audit and Compliance Monitoring Policy: Governs the validation and audit review of change management records and violations.

10.2. These policies collectively enable a defensible, traceable, and secure change management lifecycle within the ISMS framework.

11. Reference Standards and Frameworks

11.1. ISO/IEC 27001:2022

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

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

11.1.3. 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.

11.2. ISO/IEC 27002:2022 – Control 8

11.2.1. Reinforces implementation of a structured change management process, including change classification, approval, testing, rollback, and documentation.

11.3. NIST SP 800-53 Rev.5

11.3.1. CM Family (CM-1 through CM-14): This policy is closely 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).

11.3.2. 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.

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

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

11.4. EU GDPR (2016/679)

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

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

11.4.3. Recital 78: Requires that data controllers implement mechanisms, such as change control policies, to ensure the ongoing Confidentiality, Integrity, and Availability of processing systems.

11.5. EU NIS2 Directive (2022/2555)

11.5.1. 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.

11.6. EU DORA (2022/2554)

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

11.6.2. Article 8 – ICT Risk Management Framework: Mandates that financial entities manage all changes affecting ICT systems through structured change management processes, as reflected in this policy's classification, testing, rollback, and documentation requirements.

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

11.7. COBIT 2019

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

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

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

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