# 1. Introduction

This document outlines the Change Management Policy for [Organization Name], ensuring compliance with ISO/IEC 27001:2022 requirements. The policy establishes a framework for managing changes to systems, processes, and infrastructure in a controlled and systematic manner to protect the organization’s information security and operational integrity.

# 2. Purpose

The purpose of this policy is to:

- Ensure that all changes are evaluated for their impact on information security and organizational objectives. Examples include major system upgrades or policy amendments.

- Minimize risks associated with changes, such as service disruptions, data breaches, or compliance violations.

- Establish roles and responsibilities for the change management process.

- Provide a systematic approach to planning, approving, implementing, and reviewing changes.

# 3. Scope

This policy applies to all changes within [Organization Name] that could impact the organization’s information assets, including changes to:

- IT systems and applications

- Infrastructure and networks

- Business processes

- Policies and procedures

- Third-party services and vendor agreements.

# 4. Roles and Responsibilities

- Change Requester: Initiates the change request and provides detailed information about the proposed change.

- Change Advisory Board (CAB): Reviews and approves changes based on risk, impact, and resource availability.

- IT Department: Implements technical changes and ensures compliance with security policies.

- Information Security Officer (ISO): Assesses the impact of changes on information security and ensures alignment with ISO 27001 requirements.

- Change Manager: Oversees the change management process, ensuring that all changes are logged, evaluated, and implemented according to policy. Coordinates between CAB and implementation teams for smooth transitions.

# 5. Change Management Process

5.1 Change Request

- Changes must be initiated using the organization’s Change Request Form. A complete form should include:

- Description of the change

- Business justification

- Risk assessment

- Impact analysis

- Rollback plan

5.2 Review and Approval

- All change requests are reviewed by the Change Manager for completeness.

- The Change Advisory Board (CAB) evaluates the change based on:

- Strategic alignment

- Security impact

- Resource availability

- High-impact or high-risk changes require additional executive approval.

5.3 Implementation

- Approved changes are scheduled and implemented by the IT Department or relevant teams.

- Implementation must follow predefined procedures to ensure consistency and security.

- A rollback plan must be in place before implementation begins.

5.4 Testing and Validation

- Changes must be tested in a controlled environment to verify functionality and ensure no adverse effects.

- Validation results must be documented and submitted to the Change Manager.

5.5 Post-Implementation Review

- A review is conducted to evaluate the success of the change and identify lessons learned.

- The review findings are documented and shared with relevant stakeholders.

# 6. Emergency Change Management

- Emergency changes, such as those required to address critical security vulnerabilities, must follow an expedited process.

- The Change Manager and Information Security Officer must approve emergency changes.

- A post-implementation review must be conducted to assess the impact and effectiveness of the change.

# 7. Documentation and Reporting

- All change requests, approvals, and implementation details must be documented in the Change Log.

- Regular reports on change management activities and metrics (e.g., the number of successful changes vs. failed changes) must be submitted to executive leadership.

# 8. Policy Review

This policy will be reviewed annually or whenever significant changes occur in the organization’s operations or regulatory environment. Recommendations for updates will be considered by the Information Security Officer and Change Manager.

# 9. Acknowledgment

All employees and contractors involved in change management activities must acknowledge receipt and understanding of this policy. Signed acknowledgment forms will be retained for audit purposes.

# Appendices

## Appendix A: Change Request Form Template

| Request ID | Change Description | Requester | Impact Analysis | Risk Assessment | Rollback Plan | Approval Status |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |

## Appendix B: Post-Implementation Review Template

| Review ID | Change Description | Key Metrics | Outcomes | Lessons Learned | Recommendations |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |

## Appendix C: Policy Acknowledgment Form

I acknowledge that I have read and understood the Change Management Policy and agree to comply with its requirements.  
  
Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   
Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   
Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_