# Change Management Procedure Template

## Introduction

The Change Management Procedure establishes a structured approach to managing changes within the organization’s information systems and processes, including software updates, infrastructure modifications, and process enhancements. This ensures alignment with ISO 27001 standards, minimizes risks, and maintains system integrity and continuity.

## Purpose

The purpose of this procedure is to define the process for requesting, evaluating, approving, and implementing changes to information systems, applications, and infrastructure while minimizing disruption and ensuring security and compliance.

## Scope

This procedure applies to all employees, contractors, and third parties involved in initiating, approving, or implementing changes to the organization’s information systems, applications, and infrastructure.

## Policy Statement

The organization mandates that all changes to information systems and processes:  
1. Follow a documented and approved process.  
2. Be evaluated for potential risks, including security vulnerabilities, operational disruptions, and compliance impacts such as legal, regulatory, or contractual obligations.  
3. Be tested, documented, and approved before implementation.  
4. Include post-implementation reviews to confirm success and identify improvements.

## Roles and Responsibilities

- Change Requestor:  
 - Submits change requests with detailed descriptions, objectives, and potential impacts.  
 - Coordinates with relevant stakeholders for initial input.  
- Change Manager:  
 - Oversees the change management process, ensuring compliance with policies and procedures.  
 - Reviews and prioritizes change requests.  
- Change Advisory Board (CAB):  
 - Evaluates and approves high-impact or high-risk changes.  
 - Provides recommendations for mitigating risks associated with changes.  
- IT Team:  
 - Implements approved changes, including testing and deployment.  
 - Ensures proper documentation and communication throughout the process.  
- Information Security Team:  
 - Reviews changes for security risks and compliance with ISO 27001 requirements.  
 - Provides recommendations to mitigate identified risks.

## Procedure Steps

1. Change Request Submission:  
 - The Change Requestor submits a formal change request, including details of the proposed change, objectives, risks, and impact analysis.  
  
2. Initial Review:  
 - The Change Manager reviews the request for completeness and alignment with organizational objectives.  
 - Low-risk changes are expedited, while high-risk changes proceed to CAB review.  
  
3. Evaluation:  
 - The CAB and Information Security Team evaluate the change request, focusing on potential risks such as security vulnerabilities, operational disruptions, and compliance violations. Resource requirements, including personnel, budget, and time, are also assessed to ensure feasibility and alignment with organizational priorities.  
  
4. Approval:  
 - Approved changes receive documented authorization from the CAB or Change Manager.  
 - Changes not approved are returned with feedback for revision or rejection.  
  
5. Implementation:  
 - The IT Team plans, tests, and implements the approved change in a controlled manner.  
 - A rollback plan is prepared in case the change causes issues.  
  
6. Post-Implementation Review:  
 - The Change Manager conducts a review to confirm the change’s success and document lessons learned.  
 - Outcomes are reported to the CAB and relevant stakeholders.

## Compliance and Monitoring

Compliance with this procedure is ensured through:  
- Regular audits of the change management process.  
- Monitoring and reporting of change implementation outcomes.  
- Periodic reviews of change records to ensure alignment with ISO 27001 standards.

## Related Documentation

- Information Security Policy  
- Incident Management Procedure  
- Risk Management Framework  
- IT Operations Manual

## Review and Revision

This procedure is reviewed annually by the Change Advisory Board and Information Security Manager. Updates are made as needed to address changes in organizational requirements, regulatory standards, or industry practices.

## Narrative Guidance

This procedure aligns with ISO 27001 which emphasizes the need for a formal process to manage changes securely and efficiently. It helps mitigate risks associated with system modifications and ensures continuity of operations.