# Change Management Policy Template

## Document Control Information

- **Document Title:** Change Management Policy
- **Document Version:** 1.0
- **Last Updated:** [DATE]
- **Document Owner:** [ROLE/NAME]
- **Approved By:** [ROLE/NAME]
- **Next Review Date:** [DATE]

## 1. Introduction

### 1.1 Purpose

This Change Management Policy establishes [ORGANIZATION NAME]'s requirements for managing changes to information systems, processes, and services in accordance with ISO 27001:2022 requirements. It provides a framework for ensuring that changes are implemented in a controlled manner to minimize the risk of disruption to services and security incidents.

### 1.2 Scope

This policy applies to: - All changes to information systems, networks, applications, and infrastructure - All changes to business processes that impact information security - All changes to security controls and configurations - All personnel involved in requesting, approving, implementing, and reviewing changes - All environments, including development, testing, staging, and production

### 1.3 Policy Statement

[ORGANIZATION NAME] is committed to: - Implementing changes in a controlled and systematic manner - Assessing the security impact of changes before implementation - Testing changes before deployment to production environments - Documenting changes and maintaining change records - Communicating changes to affected stakeholders - Reviewing the effectiveness of the change management process

## 2. Change Management Process

### 2.1 Change Types

Changes shall be categorized as follows:

#### 2.1.1 Standard Changes

- Pre-approved changes that follow established procedures
- Low-risk, routine changes with predictable outcomes
- Changes that have been performed successfully multiple times
- Changes that do not require additional risk assessment

#### 2.1.2 Normal Changes

- Changes that require formal assessment and approval
- Changes that follow the complete change management process
- Changes with moderate risk or impact
- Changes that require testing before implementation

#### 2.1.3 Emergency Changes

- Changes required to resolve critical incidents or issues
- Changes that need expedited implementation
- Changes that may bypass normal approval processes
- Changes that require post-implementation review

### 2.2 Change Management Lifecycle

The change management process shall follow these stages: 1. Change Request 2. Change Assessment 3. Change Approval 4. Change Planning 5. Change Implementation 6. Change Verification 7. Change Documentation 8. Change Review

### 2.3 Change Advisory Board

- A Change Advisory Board (CAB) shall be established
- The CAB shall include representatives from:
  - IT Operations
  - Information Security
  - Application Development
  - Business Units
  - Risk Management
- The CAB shall review and approve significant changes
- The CAB shall meet regularly to review change requests

- Emergency CAB meetings may be called for urgent changes

## 3. Change Request and Assessment

### 3.1 Change Request

- Change requests shall be documented in a standardized format
- Change requests shall include:
  - Description of the change
  - Reason for the change
  - Systems and services affected
  - Requested implementation date
  - Requester information
  - Risk assessment
  - Rollback plan
- Change requests shall be submitted through the approved change management system
- Change requests shall be assigned a unique identifier

### 3.2 Change Assessment

- All changes shall be assessed before approval
- Assessment shall consider:
  - Technical impact
  - Security impact
  - Business impact
  - Resource requirements
  - Dependencies and conflicts
  - Compliance implications
  - Risk level
- Security impact assessment shall be performed for changes affecting security controls
- Assessment results shall be documented

### 3.3 Risk Assessment

- Changes shall be risk-assessed based on:
  - Likelihood of disruption
  - Potential impact on services
  - Security implications
  - Complexity of the change
  - Experience with similar changes
- Risk assessment shall determine the level of testing and approval required

- High-risk changes shall require additional scrutiny and controls
- Risk mitigation measures shall be identified

## 4. Change Approval and Planning

### 4.1 Approval Process

- Changes shall be approved before implementation
- Approval authority shall be based on change type and risk level
- Standard changes may be pre-approved
- Normal changes shall be approved by the CAB or designated approvers
- Emergency changes shall follow expedited approval procedures
- Approval decisions shall be documented

### 4.2 Change Schedule

- A change schedule shall be maintained
- The schedule shall include:
    - Planned changes
    - Implementation windows
    - Resource assignments
    - Dependencies between changes
- The schedule shall be communicated to stakeholders
- Changes shall be coordinated to minimize conflicts
- Change blackout periods shall be defined for critical business periods

### 4.3 Change Planning

- Implementation plans shall be developed for approved changes
- Plans shall include:
    - Step-by-step implementation procedures
    - Resource requirements
    - Timeline and milestones
    - Testing procedures
    - Verification methods
    - Rollback procedures
    - Communication plan
- Plans shall be reviewed and approved before implementation
- Plans shall be accessible to implementation teams

# 5. Change Implementation and Verification

## 5.1 Change Implementation

- Changes shall be implemented according to approved plans
- Changes shall be implemented during approved change windows
- Implementation shall be performed by authorized personnel
- Implementation progress shall be monitored
- Issues encountered during implementation shall be documented
- Emergency changes shall follow expedited implementation procedures

## 5.2 Testing

- Changes shall be tested before implementation in production
- Testing shall be appropriate to the nature and risk of the change
- Testing environments shall resemble production environments
- Testing shall verify:
    - Functionality
    - Performance
    - Security
    - Integration with other systems
- Test results shall be documented
- Failed tests shall result in change rejection or revision

## 5.3 Verification and Validation

- Changes shall be verified after implementation
- Verification shall confirm that:
    - The change was implemented as planned
    - The change meets its objectives
    - No unexpected issues have occurred
    - Security controls are functioning properly
- Verification results shall be documented
- Failed verification shall trigger rollback procedures

## 5.4 Rollback Procedures

- Rollback procedures shall be defined for all changes
- Rollback procedures shall be tested where feasible
- Rollback shall be initiated if:
    - Implementation fails
    - Verification fails
    - Unexpected issues occur

    - Security vulnerabilities are introduced
- Rollback execution shall be documented
- Lessons learned from rollbacks shall be captured

## 6. Change Documentation and Review

### 6.1 Change Documentation

- All changes shall be documented
- Documentation shall include:
    - Change request details
    - Assessment results
    - Approval information
    - Implementation details
    - Test results
    - Verification results
    - Issues encountered
    - Lessons learned
- Documentation shall be maintained in the change management system
- Documentation shall be accessible to authorized personnel

### 6.2 Change Records

- Change records shall be maintained for all changes
- Records shall include:
    - Change identifier
    - Change type
    - Systems affected
    - Implementation date
    - Implementer information
    - Approval information
    - Status information
- Records shall be retained according to retention policies
- Records shall be available for audit purposes

### 6.3 Post-Implementation Review

- Significant changes shall undergo post-implementation review
- Reviews shall assess:
    - Achievement of objectives
    - Adherence to procedures
    - Issues encountered
    - Effectiveness of testing

    - Effectiveness of rollback procedures
    - Opportunities for improvement
- Review results shall be documented
- Lessons learned shall be incorporated into future changes

## 7. Emergency Change Management

### 7.1 Emergency Change Process

- Emergency changes shall follow an expedited process
- The process shall include:
    - Expedited assessment
    - Expedited approval
    - Controlled implementation
    - Post-implementation review
- Emergency changes shall be limited to necessary actions
- Emergency changes shall be documented retrospectively if necessary
- Emergency changes shall be reviewed by the CAB after implementation

### 7.2 Emergency Change Authorization

- Authority to approve emergency changes shall be clearly defined
- Emergency approvers shall be available 24/7
- Emergency approval shall be documented
- Abuse of emergency procedures shall be prevented
- Emergency changes shall be monitored for security implications
- Regular reporting of emergency changes shall be provided to management

## 8. Change Management for Security Controls

### 8.1 Security Control Changes

- Changes to security controls shall follow the change management process
- Security control changes shall be assessed for:
    - Impact on security posture
    - Compliance implications
    - Risk introduction
- Security team shall be involved in security control changes
- Security testing shall be performed after changes
- Security control changes shall be documented

### 8.2 Configuration Management

- Configuration changes shall follow the change management process
- Baseline configurations shall be established and documented
- Configuration changes shall be tracked and controlled
- Configuration verification shall be performed regularly
- Unauthorized configuration changes shall be detected and addressed
- Configuration documentation shall be maintained

### 8.3 Patch Management

- Patch management shall follow the change management process
- Patches shall be assessed for:
  - Criticality
  - Applicability
  - Potential impact
- Patches shall be tested before deployment
- Patch deployment shall be scheduled and controlled
- Emergency patches shall follow expedited procedures
- Patch status shall be monitored and reported

## 9. Communication and Training

### 9.1 Change Communication

- Changes shall be communicated to affected stakeholders
- Communication shall include:
  - Nature of the change
  - Systems affected
  - Implementation schedule
  - Expected impact
  - Actions required by stakeholders
  - Support contact information
- Communication methods shall be appropriate to the audience
- Communication effectiveness shall be monitored

### 9.2 Change Management Training

- Personnel involved in change management shall receive training
- Training shall cover:
  - Change management policy and procedures
  - Roles and responsibilities
  - Risk assessment methods

    - Testing procedures
    - Documentation requirements
- Training shall be refreshed periodically
- Training effectiveness shall be evaluated

## 10. Roles and Responsibilities

### 10.1 Change Requester

- Submit change requests with required information
- Provide additional information as requested
- Participate in change assessment
- Verify change results
- Report issues with implemented changes

### 10.2 Change Manager

- Coordinate the change management process
- Facilitate CAB meetings
- Maintain the change schedule
- Monitor change implementation
- Report on change management performance
- Identify process improvements

### 10.3 Change Advisory Board

- Review and assess change requests
- Approve or reject changes
- Prioritize changes
- Resolve conflicts between changes
- Review emergency changes retrospectively
- Provide guidance on complex changes

### 10.4 Technical Teams

- Assess technical aspects of changes
- Develop implementation plans
- Test changes before implementation
- Implement approved changes
- Verify change results
- Execute rollback procedures when necessary

### 10.5 Information Security Team

- Assess security impact of changes
- Review changes to security controls
- Participate in CAB for security-related changes
- Verify security controls after changes
- Monitor for unauthorized changes
- Provide security guidance for changes

## 11. Compliance and Monitoring

### 11.1 Compliance Verification

- Compliance with this policy shall be regularly verified
- Verification methods may include:
  - Process audits
  - Change record reviews
  - System configuration checks
  - Post-implementation reviews
- Non-compliance shall be addressed through appropriate channels
- Compliance trends shall be analyzed and reported

### 11.2 Performance Measurement

- Change management performance shall be measured
- Metrics may include:
  - Change success rate
  - Failed changes
  - Emergency changes
  - Changes requiring rollback
  - Change backlog
  - Change cycle time
- Metrics shall be analyzed for trends
- Performance reports shall be provided to management

### 11.3 Continuous Improvement

- The change management process shall be regularly reviewed
- Improvement opportunities shall be identified from:
  - Performance metrics
  - Audit findings
  - Stakeholder feedback
  - Incident analysis

    - Industry best practices
- Process improvements shall be implemented through the change management process
- Effectiveness of improvements shall be measured

## 12. Exceptions

Exceptions to this policy shall be: - Documented with justification - Risk-assessed and approved by appropriate management - Time-limited and regularly reviewed - Accompanied by compensating controls where appropriate

## 13. Related Documents

- Information Security Policy
- Configuration Management Policy
- Incident Management Policy
- IT Operations Policy
- Risk Management Policy
- [LIST OTHER RELEVANT POLICIES AND PROCEDURES]

## 14. Approval

This Change Management Policy is approved by:

Name: ________________________ Position: ______________________ Date: _________________________ Signature: _____________________