Change Management Policy

Purpose

This Change Management Policy establishes a standardized process for requesting, evaluating, approving, and implementing changes to systems and infrastructure within our organization. The policy aims to minimize disruption to services, reduce the risk of unintended consequences, and ensure that all changes are properly documented and traceable.

Scope

This policy applies to:

- All IT systems and infrastructure
- Software applications and databases
- Network configurations and hardware
- Cloud-based services and platforms
- Security systems and controls
- All employees, contractors, and third-party vendors involved in making changes to the organization's IT environment

Policy Section

General Principles

All changes to IT systems and infrastructure must follow the established change management process. Changes must be properly documented, reviewed, and approved before implementation. The impact and risk of each change must be assessed before approval. All changes must be tested in a non-production environment before implementation in production. A rollback plan must be in place for all changes. Post-implementation reviews must be conducted for all significant changes.

Change Advisory Board (CAB)

A Change Advisory Board (CAB) shall be established to review and approve changes. The CAB shall consist of representatives from IT, security, and relevant business units. The CAB shall meet regularly to review and approve change requests.

Documentation Requirements

All change requests must be documented in the organization's designated change management system. Change documentation must include a detailed description of the change, justification

for the change, impact assessment, risk assessment, implementation plan, testing plan, and rollback plan.

Change Approval

All changes must be approved by the appropriate authority based on the change classification. High-impact or high-risk changes require CAB approval, while low-impact or low-risk changes may be approved by designated IT managers.

Change Implementation

Changes must be implemented within the approved change window. The implementation team must follow the approved implementation plan. Any deviations from the approved plan must be immediately reported and reassessed.

Post-Implementation Review

A post-implementation review must be conducted for all significant changes. The review must assess the success of the change and identify any lessons learned. Results of the review must be documented and used to improve future change processes.

Change Types and Classifications

Changes are classified into the following types:

1. Standard Changes: Pre-approved, low-risk changes that follow established procedures.
2. Normal Changes: Changes that require CAB review and approval.
3. Emergency Changes: Urgent changes required to restore service or mitigate significant risks.

Changes are further classified based on their impact and risk:

- Low Impact/Risk: Minimal disruption to services, affects few users.
- Medium Impact/Risk: Moderate disruption, affects multiple users or departments.
- High Impact/Risk: Significant disruption, affects critical systems or entire organization.

Change Request Process

1. Submission: Change requester submits a change request in the change management system.
2. Initial Review: Change manager reviews the request for completeness and assigns classification.
3. Risk and Impact Assessment: IT teams assess the potential risks and impacts of the change.

4. CAB Review (for Normal Changes): CAB reviews and approves or rejects the change request.
5. Scheduling: Approved changes are scheduled for implementation.
6. Implementation: Change is implemented according to the approved plan.
7. Post-Implementation Review: Results are reviewed and documented.

Implementation Planning

1. Develop a detailed implementation plan, including:
    - Step-by-step procedures
    - Resource requirements
    - Timeline and schedule
    - Communication plan
2. Create a test plan to verify the change in a non-production environment.
3. Develop a rollback plan in case of unexpected issues.
4. Identify and mitigate potential risks.
5. Obtain necessary approvals for the implementation plan.

Emergency Changes

1. Emergency changes must be approved by the designated Emergency Change Authority.
2. Documentation may be completed retrospectively but must be done within 24 hours of implementation.
3. Emergency changes must be reviewed by the CAB at the next scheduled meeting.
4. A post-implementation review is mandatory for all emergency changes.

Enforcement

Violations of this policy may result in disciplinary action, up to and including termination of employment. The IT Department is responsible for monitoring compliance with this policy and reporting violations to appropriate management.

Roles and Responsibilities

Role	**Description**
Change Requester	Initiates and documents change requests
Change Manager	Reviews and classifies change requests, facilitates CAB meetings
Change Advisory Board (CAB)	Reviews and approves normal changes

Role	Description
IT Teams	Assesses risks and impacts, implements changes
Emergency Change Authority	Approves emergency changes
Post-Implementation Reviewer	Conducts post-implementation reviews

Revision History

Version	Date	Author	Changes

Approval

Name	Title	Date	Signature