Change Management Process

This document outlines the **Change Management Process** for managing changes to the organization's information systems and processing facilities. The goal is to minimize disruption to services, ensure system integrity, and maintain security and compliance.

1. Scope and Policy

This process applies to **all proposed changes** to the organization's:

- **Information Systems:** Hardware, software, applications, databases, and configuration settings.
- **Processing Facilities:** Data centers, network infrastructure, cloud environments, and supporting environmental controls.

The policy is that **no change will be implemented** without following the steps defined in this process, including required authorization and testing.

2. Change Management Process Steps

The change management process follows a structured lifecycle: **Planning, Authorization, Implementation, and Review.**

2.1. Planning and Submission (Request for Change - RFC)

1. **Change Identification:** A need for a change is identified by a system owner, team member, or business requirement.
2. **RFC Submission:** A formal **Request for Change (RFC)** is submitted detailing:
    - **Type of Change:** (e.g., *Standard*, *Normal*, *Emergency*).
    - **Description:** The nature, purpose, and scope of the change.
    - **Configuration Items (CIs):** The specific systems, applications, or facilities affected.

- **Risk Assessment:** Preliminary assessment of security, performance, and operational risks.
- **Implementation Plan:** Step-by-step instructions for execution.
- **Backout Plan:** A detailed plan for reverting the change if implementation fails or causes unforeseen issues.
- **Testing Requirements:** Criteria and method for verifying success.

2.2. Review and Authorization (Change Advisory Board - CAB)

1. **Impact Documentation and Review:** The change initiator documents the **potential impact** of the proposed change on **information systems and business processes**. This documentation is reviewed to ensure all dependencies and downstream effects are understood.
2. **CAB Review:** The RFC is presented to the **Change Advisory Board (CAB)** (or designated change management team). The CAB reviews the RFC, risk assessment, impact documentation, and implementation/backout plans.
3. **CAB Decision:** The CAB either **Approve**, **Reject**, or **Defer** the RFC.
    - *Note:* **Emergency Changes** are typically implemented immediately to address critical incidents, but a formal RFC and an *after-the-fact* CAB review are mandatory.
4. **Authorization:** Upon CAB approval, the change is formally authorized, scheduled, and recorded in the change management system.

2.3. Testing and Verification

1. **Pre-Implementation Testing: All approved Normal and Standard changes** must undergo testing in a non-production environment (e.g., Development, Staging, or Sandbox) that closely mirrors the production environment.
2. **Testing Process:**
    - Execute the change using the documented implementation plan.
    - Perform specific tests outlined in the RFC to ensure the change delivers the desired outcome.
    - Perform **regression testing** to ensure the change hasn't negatively impacted existing functionality or security controls.

3. **Testing Documentation:** Test results are documented, demonstrating that the change is successful and stable. Successful test results are a prerequisite for deployment to the production environment.

2.4. Implementation and Closeout

1. **Implementation:** The authorized and tested change is implemented in the production environment according to the scheduled maintenance window and approved implementation plan.
2. **Verification:** Immediately following implementation, a final verification test is conducted in the production environment to ensure the change is successful and the system is operational.
3. **Backout Execution (If necessary):** If the change fails verification or causes severe unforeseen issues, the authorized **Backout Plan** is executed to restore the system to its pre-change state.
4. **Closure:** Once verified as successful, the RFC is marked as **Completed**. Implementation details, time spent, and lessons learned are recorded.

3. Recording and Categorization of Changes

All changes are recorded in the central change management system and categorized by **Type of Change**:

Change Type	Description	Authorization Requirement
Standard Change	Pre-approved, low-risk, frequent changes with a well-known procedure (e.g., routine patch installation, user account creation).	Requires minimal review; documented procedure must be pre-approved by the CAB.
Normal Change	Non-emergency changes that require full CAB review and testing (e.g., major application upgrade, significant network topology change).	Full CAB Review and formal authorization are mandatory.

Change Type	Description	Authorization Requirement
Emergency Change	Urgent changes required to resolve a critical incident or security vulnerability that severely impacts business operations or security.	Implementation is authorized immediately; *ex-post-facto* (after-the-fact) CAB review is required.