

## **POLICY: Configuration Change Management**

*(Use TAB Key to Navigate Table)*

**AS-OF-DATE: 01/01/2011**

### **PURPOSE:**

Healthy organizations are dynamic and require changes to remain competitive. Changes may be initiated to improve the business model or mediate problems. Changes to any established system or organization can be disruptive. Change management is the process that enables necessary and acceptable changes with minimum business disruption. Change management is the planning process for implementing, monitoring, and recording orderly and productive configuration changes.

### **SCOPE:**

This document addresses the minimum requirements for a Configuration and Change Management (C&CM) system and what a change management product or service should provide. This standard does, however, call out specific areas that require a C&CM process.

### **RESPONSIBILITY:**

The system or application owner is ultimately responsible for ensuring that a Configuration and Change Management process is in place. This is particularly true for mission critical and critical support systems and applications. However, the Change Control Board (CCB) is responsible for managing and overseeing the Configuration & Change Management (C&CM) process.

### **AUTHOR:**

**Name:** Billy Williams **Title/Role:** Change Control Manager **Phone:** 555.555.5555  
**Email:** b.d.williams@company.com **Location (Site):** Newark, DE

### **APPROVING AUTHORITY:**

**Name:** TBD **Title/Role:** Applications Control Manager **Phone:** TBD  
**Email:** N/A **Location (Site):** Newark, DE

### **REQUIREMENT:**

A formal C&CM process (automated or manual) must be established and operational for all mission critical and critical support systems and applications (e.g., programs, servers, operating systems, networks, etc.). The C&CM process should: 1) Accept changes that improve the work product in its target environment and reject those that do not; 2) Be capable of quickly returning to the pre-change environment (rollback change) with minimum business disruption; 3) Provide revision control and backup during the development and maintenance phases; 4) Provide a history or audit trail of the developing work product and all proposed changes; 5) Allow those with the likelihood of being affected by the proposed change to conduct and/or participate in an impact analysis of current and future systems and applications; 6) Allow for a formal approval or acceptance process at the initiation, selected milestones, and completion phases.

**STANDARD:**

This standard ensures that only necessary and accepted changes are made to company information assets. Additionally, a C&CM process curtails business disruption due to change activities. This can be accomplished - in part - by communicating pending changes to relevant personnel.

IMPLEMENTATION: The C&CM process must meet the following standards:

Be capable of returning to the pre-change environment with minimum business disruption.

Contain procedures or mechanisms to update backup, recovery, and contingency plans for systems and applications that are affected by change processes. This includes alternate or backup processes and facilities.

Changes to mission critical and critical systems and applications (e.g., hardware, software, network components, etc.) must be recorded and maintained by a C&CM process.

In compliance with the philosophy of separation and segregation of duties, the person or entity who authorizes the change must not be the person or entity who initiates or implements the change.

A Change Control Board (CCB) must be established to manage the C&CM process.

The CCB owns the C&CM process and decides what actions are to be taken with respect to proposed work product changes.

Changes to production systems or applications must be via source (instead of object or executable) code, scripts, or statements to prevent the introduction of malicious or erroneous code.

The change control process must control the recompilation or regeneration of the object or executable code for submission to the production environment.

The CCB is responsible for ensuring that change control records for production applications and systems are current and accurately reflect changes. Consequently, these records must be reviewed and validated regularly (i.e., monthly).

The change control process must include an impact statement.

All inputs or changes to production systems and applications must be authorized and pass edit checks before being implemented.

The C&CM process must include PCs, workstations, servers, routers, etc., especially when enterprise-wide hardware or software changes or updates are proposed.

**COMPLIANCE:**

Deviation from this standard must be approved and documented by the CCB, appropriate business unit manager, development manager, and/or application owner.

**ENFORCEMENT:**

A breach of standards, procedures, and/or guidelines established in support of this policy shall be directed to the appropriate manager for action that could result in employee termination and/or legal action.

**REFERENCES:**

**ISO 27002 Standard:**

10.1.2 Change management; 12.5.1 Change control procedures; and 12.5.3 Restrictions on changes to software packages.

**NIST SP 800 Standard:**

NIST SP 800-53: CM-1 CONFIGURATION MANAGEMENT POLICY AND PROCEDURES

**OTHER Standard:**

**COMMENTS, ADDITIONAL INFORMATION, EXAMPLES:**

SAMPLE