Configuration Management Procedure

|  |  |
| --- | --- |
| Policy Area | IT Policy Library |
| Approved Date | December 31, 20XX |
| Approved By | Policy Committee |
| Effective Date | January 1, 20XX |
| Current Version | 1.0 |

# I. Overview

Information Resource configurations must be planned and managed to optimize resources, mitigate risk, and maximize return on investment. This procedure specifies the steps and actions performed to meet the requirements of ABC Company’s Configuration Management Policy.

# II. Purpose

The purpose of this procedure is to formally document the series of steps taken to meet the requirements specified in ABC Company's Configuration Management Policy.

# III. Scope

This procedure applies to ABC Company’s Risk Management Officer, Chief Security Officer, and Director of IT.

# IV. Procedure

A. Risk Management

Executive Management are involved in risk management and mitigation decisions including how security processes are communicated throughout the organization. ABC Company’s Risk Management Officer (RMO) ensures a formal and documented Risk Management Framework has been established to manage risks related to Information Resources. For more information see the Risk Management Policy.

B. Configuration Management Processes

The Configuration Management Committee (Committee) consists of ABC Company’s Risk Management Officer, Chief Security Officer, and IT Director. The Committee develops, implements and maintains configuration management processes.

Established configuration management processes include:

* Baselines. Information Resources configuration baselines identify specifications that have been formally reviewed and agreed upon. Baselines are changed through change control procedures.
* Changes. Changes and updates (including patches) to Information Resources are implemented only with approval of the appropriate Resource Owner.
* Recover. Prior to authorizing a change to an Information Resource, procedures to back out or reverse a change or implementation are documented. Previous baseline configurations are retained to assist in a rollback if needed.

Configuration and change management processes incorporate applicable industry best practices, which support Information Resource availability, integrity, and confidentiality. Practices include:

* Use of standardized and documented methods, processes, and procedures
* Making informed risk-based decisions
* Tracking and communicating to relevant parties changes to Information Resources

A Configuration Management Database has been implemented and maintained with relevant information about the Information Resource including a description, Resource Owner, attributes, baselines, relationships, changes, and other important information.

C. Configuration Management Change Control

Changes to systems and application programs are managed to protect the systems and programs from failure as well as security breaches. System change control processes have been implemented and maintained.

The Committee ensures the following preparation activities are performed:

* Develop and enforce formal change control procedures
* Changes to Information Resources are analyzed to determine potential security and privacy implications
* Information Resources are safeguarded during change and emergency change
* Proposed changes to Information Resources are reviewed and approved
* Information Resource updates are tested prior to moving changes/updates into production
* Only authorized personnel are permitted to implement changes

The Committee ensures the following activities are documented:

* Changes include the date, time, Information Resource involved, actions taken, success/failure, and other important items
* Records of changes to the Information Resource are retained for the life of the Information Resource

As needed, role-based training is provided to appropriate Staff and include new features, security implications, changes in business processes, documentation, and other relevant factors.

The CSO ensures physical and logical access restrictions are implemented to manage changes to Information Resources. See the Change Management Policy for more information.

D. Security/Privacy Impact Analysis

When there is a material change to an Information Resource, or a security/privacy implication has been identified, the Risk Management Officer (RMO) ensures a security/privacy impact analysis is conducted. Such impact analysis includes:

* Identification of applicable regulatory or compliance requirements (see the Compliance Policy for more information)
* Data classification (see the Data Classification Policy for more information)
* Risk management and risk mitigation considerations (see the Risk Management Policy for more information)
* Additional change management approvals required

E. Configuration Settings

Configuration settings are parameters that can be changed in Information Resource hardware, software, or firmware. The CSO ensures that controls manage changes to configuration settings:

* A standard set of mandatory configuration settings has been established, maintained, and documented
* Configuration settings reflect the most restrictive mode possible while ensuring the Information Resource meets operational requirements

The CSO ensures each Information Resource provides only the essential features/capabilities needed and specifically prohibits or restricts services not required. For more information on networks, see the Network Configuration Policy.

Information Resource configurations are compared against approved security configurations defined for each device. If any deviations are encountered, an alert is issued and appropriate action is taken.

F. Configuration Management Plan

The CSO ensures a Configuration Management Plan (Plan) has been developed and maintained. The Plan documents and informs project stakeholders about configuration items, baseline configurations, change requests, configuration management database, configuration status accounting, and configuration management audits.

# V. Enforcement

Any Staff found to have violated this procedure may be subject to disciplinary action, up to and including termination.

# VI. Distribution

This procedure is to be distributed to ABC Company’s Risk Management Officer, Chief Security Officer, and Director of IT.

**Procedure History**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | 1/1/20XX | Initial procedure release |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**References:**

COBIT APO12.02, APO13.07, BAI05-03, BAI05-08, BAI06-06, BAI07-06, MEA03-01

GDPR Article 25, 32

HIPAA 164.308(a)(1)(ii)(A), 164.308(a)(8)

ISO 27001:2013 A.12.1.2, A.14.2.2-4

NIST SP 800-37 3.3, 3.4, 3.7

NIST SP 800-53 CM-1, CM-2, CM-3, CM-4, CM-5, CM-6, CM-7

NIST Cybersecurity Framework ID.BE-4, ID.RA-4, PR.AC-4, PR.DS-3, PR.IP-1, PR.IP-3, DE.AE-1

PCI 6.4.6, 12.11, A3.2.2.1