Configuration Management Policy

|  |  |
| --- | --- |
| 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

ABC Company’s Information Resources provide our organization with the tools needed to accomplish our objectives and meet our obligations. Information Resource configurations must be planned and managed to optimize resources, mitigate risk, and maximize return on investment.

# II. Purpose

The purpose of this policy is to establish a configuration management program that identifies responsibilities and requirements for a configuration management process designed to safeguard ABC Company’s Information Resources.

# III. Scope

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

# IV. Policy

A. Risk Management

Executive Management shall be involved in risk management and mitigation decisions including how security processes are communicated throughout the organization. ABC Company’s Risk Management Officer (RMO) shall ensure 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

A Configuration Management Committee (Committee) shall consist of ABC Company’s Risk Management Officer, Chief Security Officer, and IT Director. The Committee shall develop, implement and maintain configuration management processes.

Configuration management processes shall ensure:

* Baselines. Information Resources configuration baselines shall identify specifications that have been formally reviewed and agreed upon. Baselines shall only be changed through change control procedures. Examples of baseline configurations include logical placement within the organization, network topography, model, version, connectivity and interactions, etc.
* Changes. Changes and updates (including patches) to Information Resources shall be implemented only with approval of the appropriate Resource Owner.
* Recover. Prior to authorizing a change to an Information Resource, processes to back out or reverse a change or implementation shall be identified. Previous baseline configurations shall be retained to assist in a rollback.

Configuration and change management processes shall incorporate applicable industry best practices, which support Information Resource availability, integrity, and confidentiality. Recommended 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
* Systems shall employ the principle of least functionality by configuring systems to provide only essential capabilities
* Systems shall restrict, disable, or prevent the use of non-essential programs, functions, ports, protocols, and services
* Systems shall deny-by-exception (blacklisting) to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software

A Configuration Management Database shall be 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 shall be managed to protect the systems and programs from failure as well as security breaches. System change control processes shall be implemented and maintained.

The Committee shall ensure the following preparation activities are performed:

* Develop and enforce formal change control procedures
* Analyze changes to Information Resources to determine potential security and privacy implications
* Ensure Information Resources are safeguarded during change and emergency change
* Review and approve proposed changes to Information Resources
* Test Information Resource updates prior to moving changes/updates into production
* Ensure only authorized personnel are permitted to implement changes

The Committee shall ensure the following documentation activities are performed:

* Document change including date, time, Information Resource involved, actions taken, success/failure, and other important items
* Retain records of changes to the Information Resource for the life of the Information Resource

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

The Chief Security Officer (CSO) shall ensure 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) shall ensure a security/privacy impact analysis is conducted. Such impact analysis to include:

* 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 shall ensure that controls manage changes to configuration settings:

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

The CSO shall ensure 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 shall be compared against approved security configurations defined for each device. If any deviations are encountered, an alert shall be issued and appropriate action taken.

The CSO shall ensure Staff document, for each internal and external connection, the interface characteristics, security and privacy requirements, and the nature of the information communicated. Internal and external connections shall be terminated per policy. On a periodic basis, the continued need for each internal and external connection shall be reviewed.

F. Configuration Management Plan

The CSO shall ensure a Configuration Management Plan (Plan) is developed and maintained. The Plan shall document and inform project stakeholders about configuration items, baseline configurations, change requests, configuration management database, configuration status accounting, and configuration management audits.

The Configuration Management Plan shall

* Address roles, responsibilities, and configuration management processes and procedures
* Establish a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items
* Define the configuration items for the system and places the configuration items under configuration management

The CSO shall ensure the Configuration Management Plan is reviewed and updated in a timely manner. The Configuration Management Plan shall be protected from unauthorized disclosure and modification.

# V. Enforcement

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

# VI. Distribution

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

**Policy History**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | 1/1/20XX | Initial policy 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 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 6.2.1, 12.4.2, A1.1.3