January 1, 20XX

ABC Company

123 Main Street

Los Angeles, CA 90744

(800) ABC-COMP

[www.ABCCompany.com](http://www.ABCCompany.com)

Table of Contents

[I. Introduction 3](#_Toc37747638)

[II. Purpose of the Configuration Management Plan 3](#_Toc37747639)

[III. Roles and Responsibilities 4](#_Toc37747640)

[IV. Configuration Control 5](#_Toc37747641)

[V. Configuration Management 6](#_Toc37747642)

[VI. Configuration Management Audits 7](#_Toc37747643)

[Appendix A – Distribution List 9](#_Toc37747644)

[Appendix B – Receipt and Acknowledgement 10](#_Toc37747645)

# I. Introduction

Configuration management is an on-process of identifying and managing changes to Information Resources. Configuration Items are Information Resources that are to be placed under configuration control. This Configuration Management Plan:

* Provides information on the requirements and procedures necessary for configuration management activities
* Establishes the methodology for configuration identification and changes to Configuration Items
* Describes the process for maintaining status and verifying the completeness and correctness of Configuration Items

# II. Purpose of the Configuration Management Plan

This Configuration Management Plan (Plan) describes how configuration management is conducted throughout a lifecycle. This includes the responsibilities, procedures, activities, and oversight necessary to provide configuration identification, change control, status accounting and configuration audits.

This Plan documents and informs project stakeholders about configuration management, tools used, and how they will be applied by the project to promote success. The Plan defines methods for:

* Identifying baseline configurations
* Controlling modifications and releases
* Reporting and recording status of requested changes
* Ensuring completeness, consistency, and correctness
* Controlling storage, handling, and delivery

The intended audience of this Plan is ABC Executive Management, Chief Risk Officer, and Chief Security Officer.

# III. Roles and Responsibilities

A. Introduction

ABC Company cannot protect the confidentiality, integrity, and availability of information without ensuring that all Staff involved in changes to Information Resources:

* Understand risks related to changes to Information Resources
* Understand Staff roles and responsibilities
* Understand ABC Company’s security policies and procedures designed to manage and mitigate risks to Information Resources

B. Configuration Management Committee

A Configuration Management Committee (Committee) consists of ABC Company’s Risk Management Officer, Chief Security Officer, and IT Director. The Committee:

* Receives change requests
* Seeks clarification on any change request (if needed)
* Reviews and approves/rejects configuration change requests
* Ensures that approved changes are added to a Configuration Management Database

C. Configuration Items

The Committee identifies specific Configuration Items from the list below:

* Communications – cell phones, voice mail, e-mail, Fax, Internet, etc.
* Facilities – access controls, alarms, etc.
* information – collected, transmitted, and stored, databases, etc.
* Information systems (hardware) – workstations, servers, networking equipment (routers, switches, hubs, access points, etc.), load balancers, important peripherals, backups, etc.
* Information systems (software) – operating systems, software applications, utilities, etc.

D. Baseline Configurations

The Committee ensures that each Configuration Item is added to the Configuration Management Database. The Configuration Management Database includes relevant information about the Configuration Item including a description, Resource Owner, attributes, baselines, relationships, changes, and other important information.

A baseline configuration is established for each Configuration Item. A baseline is a collection of information describing the technical characteristics of each Configuration Item. Baselines serve as technical control points in a resource life cycle for the evaluation of proposed changes to the Configuration Item. The baseline and the approved changes or modifications provide a current description of the system. Major baseline configuration elements can include:

* Configuration Item name
* Functional purpose
* Resources needed
* Interfaces between internal and external resources
* Documentation – technical, operational, design, users, maintenance, etc.
* Change history

# IV. Configuration Control

A. Process Overview

Configuration Control involves systematically controlling and managing configurations throughout an Information Resource lifecycle. Configuration Item change requests are initially sent to the Resource Owner for review and authorization. If authorized, the Resource Owner sends the change request to the Committee.

When reviewing change requests, the Committee considers the risk to the organization, cost, timing, and impact of the change. Only necessary changes are approved by the Committee. This configuration control process ensures that Configuration Items are handled in a consistent manner.

B. Approved Change Requests

Once approved by the Committee, approved change requests are entered into a Configuration Management Database with a “Requested” status. The change request is then sent to the appropriate department for implementation and resolution. The department that implemented the change will send status (i.e. “Completed” or “Fail”) notification to the requestor, Resource Owner, and the Committee. The Configuration Management Database is then updated with the current status of the change.

Once notified that the change is in place, the Resource Owner arranges for appropriate:

* Testing of the change to ensure the Information Resource operates as desired
* Changes to documentation (if needed)
* Training of Staff (if needed)

It is important that the Risk Management Officer, Chief Security Officer, Director of IT, and Resource Owners have the ability to review configuration status at any given time. The Configuration Management Database ensures that Staff are working off of the same information and have access to the latest updates. Access to the Configuration Management Database is controlled:

* The Committee determines who has read and write access to the Configuration Management Database
* The Resource Owner determines Staff that have read access to the Configuration Management Database

# V. Configuration Management

A, Overview

The Configuration Management Database is a central repository of Configuration Items. As Configuration Items go through various stages of collection, processing, and reporting, the Configuration Management Database has the most current information available.

B. Configuration Management Database

The Configuration Management Database may include information on approved configuration documents, software, version numbers, data, relationships, status of submitted change requests, and configuration audits. The Configuration Management Database provides information on:

* Change requests. When request was initially submitted, department submitting request, and Information Resources involved.
* Versions. Information Resource current and prior versions.
* Relationships. Resources required, Configuration Item relationships.
* Configuration Management Audits. The information in the Configuration Management Database is accurate and complete.

C. Configuration Status Accounting

Configuration management processes ensure the proper recording and reporting of Configuration Items. This includes the status of Configuration Items, proposed changes, the implementation status of approved changes.

Configuration status accounting identifies a Configuration Item’s current status and lifecycle. A Configuration Status Report may include:

* Specifications that describe each Configuration Item
* A list of Configuration Items that comprise a baseline
* Configuration Item dates when each version was baselined
* History of baseline changes including rationales for change
* Configuration Item status with approved change requests
* A list of open change requests by Configuration Item
* Configuration audit list of deficiencies and non-conformities

# VI. Configuration Management Audits

A. Audit Process

Configuration management audits (Audits) help ensure the integrity of the Configuration Management Database is maintained. Audits ensure:

* Configuration management processes are being followed
* Recorded changes/updates were properly approved
* Configuration Items have been properly identified
* Information in the Configuration Management Database is accurate and complete

Audits are performed by independent Staff that not part of production operations. The audits are performed on an annual basis and after a major change or update to Information Resources. Deficiencies and non-conformities are identified in the Configuration Management Audit Report (Audit Report).

**Processes**

The Audit includes an evaluation of configuration management processes to ensure they are followed as specified in configuration management policies and plans. Such processes include:

* Change request – initiation, approval or rejection, modifications, and completion
* Configuration Item – additions, changes, and modifications

**Approvals**

The Audit verifies Resource Owners have approved each change request, the Committee has performed a risk assessment of the change request and approved each change, and the status of each change request is noted in the Database.

Also included in the Audit is a review of installed software against the Database to identify unlicensed or unauthorized software.

**Accuracy**

The Audit reviews information in the Database to verify it is complete and error free. The Audit reviews:

* Configuration Items to ensure the Database is complete and agrees with an inventory of Information Resources
* Baselines to verify they agree with actual Information Resource configurations
* Documentation is complete and includes maintenance requirements, licenses, warranties
* Configuration Item history, versions, timestamps, and change control integrity
* Configuration Item data is accurate and complete
* Adherence to requirements, standards, and service level agreements
* Changes were tested prior to moving changes/updates into production
* Safeguards during change
* Processes to back out or reverse a change or implementation
* Notification after change

C. Audit Report

Any deficiencies and non-conformities from configuration management policies, plans, and procedures are identified in the Audit Report. The Audit Report is distributed to the Committee so that appropriate action can be taken.

The Committee will identify the corrective actions necessary to resolve the deviations and assign responsibility for each corrective action to a person/department. As actions are taken, notes are added to the Configuration Management Database so a full history is available.

# Appendix A – Distribution List

Risk Management Officer

Chief Security Officer

IT Director

All Resource Owners

# Appendix B – Receipt and Acknowledgement

I have read ABC Company’s (Company’s) Configuration Management Plan and agree to abide by it as consideration for my continued employment by Company. I understand that violation of the enclosed policies and guidelines may result in disciplinary action including, but not limited to, termination.

This document supersedes all prior electronic equipment policies, guidelines, understandings and representations. I understand that if any of the provisions of this manual are found null, void, or inoperative for any reason, the remaining policies and guidelines will remain in full force and effect.

If I am uncertain about any policy or procedure, I will check with my immediate supervisor or Company management.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_

Employee Signature Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Employee Name (Printed)