**Table of Contents**

[1. Introduction to Configuration Management 3](#_Toc77942806)

[2. Purpose 3](#_Toc77942807)

[3. Scope 3](#_Toc77942808)

[4. Configuration Management Process Stages 3](#_Toc77942809)

[5. Policy Statements 4](#_Toc77942810)

**Document Control**

**Document Version History**

This table shows a record of significant changes to the document.

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Description of Change** |
| 1.0 | <Date> | <Name> | Original Version |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Approvals**

This table shows the approvals on this document for circulation, use and withdrawal

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Date** | **Approver** | **Title/Authority** | **Approval Remarks** |
| 1.0 | <Date> | <Name> | <Title> | <Remarks> |
| 1.1 |  |  |  |  |

# Introduction to Configuration Management

Consider Configuration Management as the support structure of the other Service Management processes. This policy’s purpose is to ensure each Service Management process can use – and have confidence in – the Configuration Management data.

Configuration Management is foundational to the Service Management organization. It ensures that all Configuration Items (CIs) within IT systems and infrastructure are accurately identified, and relationships recorded, the status of the CIs and modifications are effectively recorded, tracked, and reported, and changes to CIs are controlled.

Configuration Items (CIs) are any assets that need to be managed to deliver a service. CIs that should be under the control of Configuration Management include hardware, software, systems, services, applications, their relationships, and associated or related documentation, (e.g., Service Level Agreements). Configuration Management establishes and maintains the integrity of services and their configuration information, enabling effective control and uptime of the services.

If we know that the configuration information is correct, then it improves the evaluation of changes and improves the resolution times of incidents.

Configuration Management roles and responsibilities can be broad given the breadth of CIs in the enterprise. There should be one accountable party (i.e., Process Owner), one or more responsible parties (i.e., Process Managers), and many users and consumers of the Configuration Management Database (CMDB). The corresponding RACI document will reflect these roles in a more granular manner.

# Purpose

The purpose of Configuration Management is to control, identify, record, and report IT components, including versions (where appropriate), constituent components, states and most importantly, relationships to other technology components and services.

A policy is used to fulfill this purpose.

*<Change the wording of this policy template to reflect the needs of your organization>*

# Scope

The scope of Configuration Management includes all activities encompassing the management of Configuration Items throughout their respective lifecycles:

* Owned and operated by the organization
* Owned and operated by third-parties (or external service providers) where technology services are supported

# Configuration Management Process Stages

This policy governs each Configuration through the five stages of the Configuration Management lifecycle:

1. **Configuration Management Planning** – Understanding the scope (CI Classes and attributes) of what should be included in the CMDB and the roadmap for the future
2. **Configuration Identification** – Establishing naming convention to be used in the CMDB and how CIs will be reflected in the CMDB
3. **Configuration Control** – The intersection of Configuration Management and Change Management, Control ensures the accuracy of the CMDB data.
4. **Configuration Status Reporting** – Usually performed inside the ITSM (CMDB) tool, this stage includes understanding the CI Status (e.g., whether it is live or retired) and its relationship to other CIs.
5. **Configuration Verification and Audit** – An Annual audit of the CMDB to ensure the accuracy of the data for all consumers.

All external service providers that support or contribute to the design, build, transition, or operation of technology services must adhere to this policy. Further, these partners are expected to help mature and improve the Configuration Management as applicable.

# Policy Statements

The policy statements listed below are just an example and support the stated goal to manage the lifecycle of CIs and consequently provide a logical model of services for use by the other Service Management processes.

*<Change as needed to reflect your organization>*

| **ID** | **Policy Statement** | **Detail** | **Purpose** |
| --- | --- | --- | --- |
|  | There is one enterprise-wide Configuration Management Process in which all organization members and service providers, whether internal or external, will participate in and adhere to. | The process develops and maintains the single logical model of technology services. | For a process to achieve its full effectiveness, efficiency, and adaptability, it must be the sole process used for its intended purpose, and it must be used by all entities involved throughout the course of the defined process cycle. |
|  | Changes to CIs and their corresponding CI records must be approved changes going through the Change Management process. | Any change to a CI must have an approved RFC related to the CI before any change to the CI. | To ensure that all changes to CI records are properly documented and approved by Change Management. |
|  | All CI records will be updated in the ITSM tool suite. | The CMDB must reflect all changes to baselines and new functionality. | To ensure the accuracy of service models at all times.  For example, if a CI fails as the result of a change, the Incident Management process must have accurate and current information about the CI’s identity and location. |
|  | All Configuration Management process documentation will be subject to an annual review cycle by the Process Owner and results briefed to the Service Management Office (SMO). | The review includes but is not limited to process flows, Critical Success Factors, Key Performance Indicators, benefits, policies, and reports. | This Process Review Cycle is to determine if the process, as it is implemented and documented, is still relevant or requires updates and/or improvements. |
|  | All activities related to the Configuration Management Process are logged and communicated in the ITSM tool suite. | The key physical record in the CMDB contains all of the information for CIs supporting a service. | For a process to achieve its full effectiveness, efficiency, and adaptability, there must be one trusted dataset that captures all relevant information throughout the lifecycle of the activity. |