

**Configuration Management**

Policy Template

Customer Name

Author Name: Gouri Mahendru

Version: 2.1

Document History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Date | Summary of Changes | Author | Approved By |
| 1.0 | 10-Apr-14 | Initial Document | Sujatha | Sekar T |
| 1.01 | 1-May-17 | Change GAVS logo | Emmanuel F | Sekar T |
| 2.0 | 20-Jan-23 | Revised Policy Statements (section 5.0) | Gouri Mahendru | Sekar T |
| 2.1 | 16-Mar-23 | Updated as per new GS Lab | GAVS document format | Gouri Mahendru | Sekar T |

|  |
| --- |
| Statement of Confidentiality |
| This GS Lab (Great Software Laboratory) and/or GAVS (GAVS Technologies) artefact and/or document and/or presentation is strictly confidential. It contains proprietary information intended only for recipients.  The recipient acknowledges and agrees that: (i) this artefact and/or document is not intended to be distributed ii) the recipient does not have the right to implement, copy, reproduce, fax, publicly divulge, or further distribute it, in whole or in part in any form, without seeking the express written permission from GS Lab and GAVS.  Any unauthorized use of the contents of this artefact and/or document and/or presentation in any manner whatsoever, is strictly prohibited. The artefact and/or document and/or presentation represents GS Lab’s and/ or GAVS’s current product offerings and best practices which are subject to change without notice. Please note that GS Lab and GAVS collaborate in relation to some of its offerings.  All third-party trademarks used herein belong to their respective owners and may be protected by law. This artefact and/or document and/or presentation only refers to such trademarks under the doctrines of nominative and descriptive fair usage to illustrate and explain concepts without implying violation of any legal constraints. If improper activity is suspected, all available information may be used by GS Lab and /or GAVS for any remedy or for lawful purpose. |

Table of Contents

[**1.** **Purpose** 4](#_Toc130469336)

[**2.** **Scope** 4](#_Toc130469337)

[**3.** **Definitions** 4](#_Toc130469338)

[**4.** **Applicable Laws, Regulations, and Industry Standards** 4](#_Toc130469339)

[**5.** **Policy Statements** 4](#_Toc130469340)

[**6.** **Exceptions** 6](#_Toc130469341)

[**7.** **Non-compliance** 6](#_Toc130469342)

## **Purpose**

Describe the factors or circumstances that mandate the existence of the policy. Also state the policy’s basic objectives and what the policy is meant to achieve.

The purpose of this policy is to establish a Configuration Management practice at [Organization]. The desired goals of configuration management are:

* Optimize the use of IT assets.
* Enable proactive planning within IT
* Better manage IT risk

## **Scope**

Define to whom and to what systems this policy applies. List the employees required to comply or simply indicate “all” if all must comply. Also indicate any exclusions or exceptions that are out of scope, i.e. those people, elements, or situations that are not covered by this policy or where special consideration may be made.

All business-critical IT services are within scope of the CM project.

## **Definitions**

Define any key terms, acronyms, or concepts that will be used in the policy or accompanying procedures. A standard glossary approach is sufficient. An example definition:

* CM: Configuration management
* CMDB: Configuration management database
* CMS: Configuration management system
* CCB: Configuration Control Board

## **Applicable Laws, Regulations, and Industry Standards**

If applicable, list any laws or regulations that govern the policy or with which the policy must comply. Confirm with the legal department that the list is full and accurate. If there are no applicable laws, regulations, or industry standards delete this section.

|  |  |
| --- | --- |
| Guidance | Section |
| ISO 20000-1:2018 | Section 8.2 (Service Portfolio – Configuration Management) |

## **Policy Statements**

Describe the rules that comprise the policy. This typically takes the form of a series of short prescriptive and proscriptive statements. Subdividing this section into subsections may be preferable, depending on the length or complexity of the policy.

The CIO will establish a CCB. The goal of the CCB is to ensure that the information within the CMS is accurate and up to date.

The CCB will develop a configuration management plan for each in-scope service. This plan will detail how the CCB will implement CM for that service.

The data and information contained within the CMS is private (including the information within the CMDB). All IT personnel and employees of [Organization] are allowed to view the content, but this content is not to be made publicly available.

* Certain data within the CMS may be classified with a higher security level due to the nature of the data (e.g. business-critical systems, systems containing trade secrets, systems containing personally identifiable data, SSNs).

The CCB will establish a “data model.” this data model will contain information about:

* The relationships between services and configuration items.
* Services.
* Configuration items.

The criteria for identifying an entity as a “configuration item” are:

* The entity is involved in the delivery of a service that is in scope for CM.
* There is value in being able to report on the entity’s attributes.
* The value in being able to report on the entity’s attributes outweighs the cost and effort of keeping the entity’s data up to date in the CMS.

The criteria for selecting attributes to collect regarding each configuration item are:

* Collecting the attribute will provide value.
* The attribute can be collected automatically.
* If the attribute must be collected manually, then the cost and effort of manually capturing that information is less than the benefit that is received by being able to generate reports on that attribute.

The CCB will establish a “configuration baseline” for each configuration item included in the CMS.

* This baseline stipulates the expected values for the attributes of that configuration item.
* When a configuration item’s attributes differ from the configuration baseline, one of the following options will occur:
  + The attribute of the CI will change to match the configuration baseline.
  + The person that caused the change in configuration will submit a change request to change the configuration baseline.

CM involves people, process, and technology.

* **Training:** To ensure that people can fulfill their CM responsibilities, everyone that has CM responsibilities and accountabilities will receive regular training on those items.
  + The CCB is accountable for ensuring that IT personnel receive the necessary training to ensure the usefulness of the CMDB.
* **Process Definitions:** The CCB Chair will identify a person to be the “configuration management process owner.” The CM process owner will develop and maintain a Configuration Management Standard Operating Procedures document.

The value of CM comes from the ability to generate knowledge based on the information stored in the CMDB.

* With input from IT and the business, the CCB will establish a set of standard reports.
* The CCB shall ensure that IT personnel have the necessary training for reading the standard reports and for performing ad hoc reporting.

Changes to either the data model or the configuration baseline must go through the established change management process and have approval from the CM stakeholders.

* Members of the CCB cannot be involved with evaluating these change requests. It is therefore a best practice for members of the CCB to not sit on the CAB.
* All system owners are responsible for ensuring that the data within the configuration management system is correct and up to date, as per the standards published by the CCB.

## **Exceptions**

Define any exceptions to the above policy statements.

Emergency changes that are approved by the Emergency Change Advisory Board may impact the configuration management system without being subjected to all of the necessary change assessment procedures, as per the Change Management Policy.

When necessary, the CIO may permit individuals to sit on both the CCB and the CAB.

## **Non-compliance**

Clearly describe consequences (legal and/or disciplinary) for employee noncompliance with the policy. It may be pertinent to describe the escalation process for repeated noncompliance.

Violations of this policy will be treated like other allegations of wrongdoing at [Client Name]. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for noncompliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable [Client Name] policies
2. Termination of employment
3. Legal action according to applicable laws and contractual agreements