

**Change 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](#_Toc130469548)

[**2.** **Scope** 4](#_Toc130469549)

[**3.** **Definitions** 4](#_Toc130469550)

[**4.** **Applicable Laws, Regulations, and Industry Standards** 4](#_Toc130469551)

[**5.** **Policy Statements** 4](#_Toc130469552)

[**6.** **Roles and Responsibilities** 5](#_Toc130469553)

[**7.** **Non-compliance** 6](#_Toc130469554)

## **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.

This policy supports the [Client Name] technical change procedure. A controlled and consistent change procedure is necessary to deliver reliable, on-time changes that provide business value, while mitigating change-related risks.

## **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.

This policy covers all changes to in-production IT systems within the enterprise. Excluded from the scope of this policy are changes to systems that are in the process of being implemented, which will be controlled by project-level change control processes.

## **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:

**Change Management:** The set of processes that allows changes to be introduced to the live environment in a controlled fashion that minimizes disruption and maximizes efficiency.

## **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 8.5 (Service Design, Build and Transition – Change 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.

**Foundational Policy Requirements:**

* Changes to the [Client Name] IT environment will be requested, prioritized, documented, and monitored.

**Derived Policy Requirements:**

*All Change Management Processes*

* All change management workflows will be stored in the Change Management Standard Operating Procedure (SOP) document. The SOP will be reviewed and updated every [time Interval – suggest one year].
* Separate workflows will be used for preapproved, standard, and emergency changes.
* All changes will be tracked in [Tool].
* User acceptance testing will be executed following change implementation.
* Operational documentation will be updated as required following change implementation.

*Normal Changes*

* Standard changes will be formally requested through a Request for Change (RFC).
* RFCs will be reviewed for completeness by a Change Manager.
* Complete RFCs will be forwarded to the Change Advisory Board (CAB). Changes must be approved by the CAB in order to proceed to implementation.
* The CAB will determine an appropriate course of action based on the urgency of the change and a risk assessment.
* A post-implementation review will evaluate the success of the implementation.

*Emergency Changes*

* Emergency change requests will be directed to the Emergency Change Advisory Board (E-CAB).
* Emergency changes will be minimally documented.
* The E-CAB will determine an appropriate course of action based on the urgency of the change and a risk assessment.
* A post-implementation review will evaluate the success of the implementation.

*Preapproved Changes*

* Preapproved changes will be outlined and submitted using a previously approved RFC.
* The CAB will make recommendations and the Change Manager will be required approve the change.
* The CAB and Change Manager will have the authority to revoke preapproved status if accuracy and repeatability of a change is lost.

## **Roles and Responsibilities**

Outline roles here *or* add roles and responsibilities to your Change Management SOP. Avoid duplicating this information by linking between the related documents.

|  |  |
| --- | --- |
| **Role** | **Responsibilities** |
| Originator | * Originate, populate, and present the request for change (RFC) * Create communication content for Service Desk * Responsible for testing, implementation, and rollback and/or delegation of testing, implementation, and rollback activities |
| Business System Owner | * Provide a downtime window and freeze period guidance * Advise on need for change * Validate implementation (through UAT, etc.) |
| Change Manager | * Accountable for the quality and integrity of the change process * Assess effort and cost requirements for changes |
| Technical Subject Matter Experts (SMEs) | * Advise on RFC creation and review draft RFC * Develop and assess required technical plan (testing, rollback, etc.) |
| Change Advisory Board (CAB) | * Assess change requests, accounting for business need, cost/benefit, viability, and potential impacts to existing systems or processes * Approve, defer, return, reject, or cancel changes. Assign a priority to changes. Also, the CAB will make recommendations related to change implementation. |
| Emergency Change Advisory Board (E-CAB) | * A subset of the CAB that is responsible for approving or rejecting emergency changes * Meet on short notice and authorize or reject emergency change requests |
| IT Management (Operations, Service Desk, Infrastructure, Applications) | * Review RFCs and assess the potential impact of the request on existing systems, infrastructure, and operational processes * Allocate resources from their team to RFC required tasks |

## **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