**Change Management and Control Policy**

# ***Version Control Table***

| Version | Date | Author | Description |
| --- | --- | --- | --- |
| 1.0 |  |  |  |
| 1.0 |  |  |  |
| 1.0 |  |  |  |
| **1.0** |  |  |  |
|  |  |  |  |

| **Date of Next Revision** |  |
| --- | --- |

This policy will be reviewed for continued completeness, relevance, and accuracy within 1 year of being granted “final” status, and at yearly intervals thereafter.

The version control table will show the published update date and provide a thumbnail of the major change. CAUTION: the thumbnail is not intended to summarise the change and not a substitute for reading the full text.

# ***Table of Contents***

[**Version Control Table**](#_1t3h5sf) **2**

[**Table of Contents**](#_4d34og8) **3**

[**Purpose**](#_8q3in51gc09r) **4**

[**Scope**](#_2vn6fxkvscet) **4**

[**Objectives**](#_vs7rvoak6l42) **4**

[**Policy**](#_8wm42y65xfsj) **4**

[**Change Request**](#_vioz2zn27mka) **4**

[**Change Review**](#_uxxng66elqpo) **5**

[**Change Approval**](#_dpdxy0s5prqt) **5**

[**Change Implementation**](#_45p1bjae0n6l) **5**

[**Change Testing**](#_i8fybfmqimy3) **5**

[**Version Control**](#_e4ac8kyo1w7u) **5**

[**Change, Review, and Update**](#_5gvei5yt6zoy) **6**

[**Disciplinary Action**](#_cmhctdr2g6ok) **6**

[**Responsibility**](#_z0lmne9fwh3i) **6**

[**Related Documents**](#_v6z7e8uoe1xk) **6**

[**Risk Management Policy**](#_bl1oyyesf030) **6**

# 

# **Purpose**

The purpose of this policy is to establish management direction and high-level objectives for change management and control. In addition, this policy will ensure the implementation of change management and control strategies to mitigate associated risks such as:

* Information being corrupted and destroyed;
* Computer performance being disrupted and degraded;
* Productivity losses being incurred; and
* Exposure to reputational risk.

# **Scope**

This policy applies to all parties operating within [Company]’s customer-facing production environment and internal business systems.

# **Objectives**

The objectives of these policies are:

* The control of implementing and deploying infrastructure and software changes to the production environment with minimal disruption to the customers and business.
* Giving appropriate attention to those changes to prevent unintended consequences.
* Facilitating a high level of communication among stakeholders by ensuring that requests for changes are recorded, evaluated, authorized, prioritized, planned, tested, implemented, documented, and reviewed.

# **Policy**

## **Change Request**

* All changes to the production environment must have a Change Request.
* The Change Manager assesses and classifies Change Requests as depending on their effect on the customer.
* To be considered for implementation, Change Requests must include:
  + Information on products/services affected and the potential impact;
  + Documentation for completed risk and impact assessments, methods of procedure, back-out procedure, pre-and post-validation test plan;
  + Approvals/signoff for engineering peer review and release signoff.

## **Change Review**

* The Change Manager gathers information from Change Initiator necessary to complete the change and develop a plan on how to implement this change.
* The Change Manager develops the change requirements that will be attached to the Change Request for consideration in the analysis portion of the process.
* Procedures for aborting and recovering from unsuccessful changes should be documented.

## **Change Approval**

* For most important changes the approval from the Table of Authority is required.
* After planning, each Change Request gets reviewed to evaluate impact, technical aspects, process methodologies, and implementation.
* For Emergency Changes, approval from multiple team members is not required and can be performed by the senior management or another responsible person.

## **Change Implementation**

* The Change gets implemented.
* Failure of implementation at this level will typically require the Change Implementer to follow the back-out plan to ensure normal system operations.

## **Change Testing**

* In case of a major change, once it has been implemented, the Change Manager will conduct testing with the documenting the results and any failed cases.
* Fall back procedures should be in place to ensure systems can revert to what they were before implementing changes.

## **Version Control**

* Any software change and/or update should be controlled with version control. Older versions shall be retained in accordance with corporate retention and storage management policies.

# **Change, Review, and Update**

This policy shall be reviewed once every year unless the owner considers an earlier review necessary to ensure that the policy remains current. IT Manager shall exclusively perform changes to this policy.

# **Disciplinary Action**

Employees who violate this policy may face disciplinary consequences in proportion to their violation. Our management will determine how severe an employee’s offense is and take the appropriate action.

# **Responsibility**

The IT Manager is responsible for ensuring this policy is followed.

This policy shall be reviewed yearly or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

# Reference

* *[SOC 2 or ISO 27001 controls]*

# **Related Documents**

* Risk Management Policy