**[Company]**

**Change Management 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 after that.

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

#

# ***Table of Contents***

[**Version Control Table**](#_waib18pnmr6f) **2**

[**Table of Contents**](#_ukruovgntws6) **3**

[**Purpose**](#_rtao5kax1w39) **4**

[**Scope**](#_167msnbg1e7l) **4**

[**Policy**](#_ojhok29bz9oz) **4**

[Operational Procedures](#_4npgfaptvk74) 4

[Risk Management](#_x0jjb0myenk7) 5

[Testing](#_15qp3ix0zgzf) 5

[Approval](#_qhz1015mhhi9) 5

[Communicating changes](#_gtuacoasf7lv) 5

[Implementation](#_6b9uz1j178in) 5

[Fall back](#_cfgsjxd70agc) 5

[Documentation](#_adriq1gyybqm) 5

[Emergency Changes](#_cfsqw9t2cgrz) 6

[**Disciplinary actions**](#_oo4pebgvtuk2) **6**

[**Change, Review, and Update**](#_6cu0cv3y3y7n) **6**

[**Responsibility**](#_fxvzxllev4xj) **6**

[**Reference**](#_hhx0u7glv0fd) **6**

[**Related Documents**](#_xixdvq2ap8qn) **6**

#

# Purpose

The purpose of the Change Management Policy is to manage changes to [company] information systems, assets, and resources rationally and predictably so that all related stakeholders can plan accordingly. Applying a repeatable process to control change will improve the effectiveness of changes and improve cross-functional communication.

# Scope

This policy applies to all [company] employees, contractors, third parties who access internal information and business processes.

# Policy

Changes to information resources shall be managed and executed according to a formal change control process. The control process will ensure that changes proposed are reviewed, authorized, tested, implemented, and released in a controlled manner; and that the status of each proposed change is monitored.

## Operational Procedures

A change control process shall be in place to control changes to all critical company information resources (such as hardware, software, system documentation, and operating procedures). Wherever practicable, operational and application change control procedures should be integrated.

At a minimum, the change control process should include the following phases:

* Logged Change Requests;
* Identification, prioritization, and initiation of change;
* Proper authorization of change;
* Requirements analysis;
* Inter-dependency and compliance analysis;
* Impact Assessment;
* Change approach;
* Change testing;
* User acceptance testing and approval;
* Implementation and release planning;
* Documentation;
* Change monitoring;
* Defined responsibilities and authorities of all users and IT personnel;
* Emergency change classification parameters.

## Risk Management

A risk assessment shall be performed for all changes, and depending on the outcome, an impact assessment should be performed. This assessment shall include the potential effect on other information resources and possible cost implications and consider compliance with legislative requirements and standards.

## Testing

Before implementation, changes shall be tested in an isolated, controlled, and representative environment (where such an environment is possible) to minimize the effect on the relevant business process, assess its impact on operations and security, and verify that only intended and approved changes were made.

## Approval

All changes shall be approved before implementation. Approval of changes shall be based on formal acceptance criteria, i.e., the change request was made by an authorized user, the impact assessment was performed, and proposed changes were tested.

## Communicating changes

All users significantly affected by a change shall be notified of the change. Users shall be required to make submissions and comments before the acceptance of the change.

## Implementation

Implementation will only be undertaken after appropriate testing and approval by stakeholders. All significant changes shall be treated as new system implementation and shall be established as a project. Significant changes will be classified according to the effort required to develop and implement changes.

## Fall back

Procedures for aborting and recovering from unsuccessful changes shall be documented. Should the outcome of a difference be different from the expected result (as identified in the testing of the change), procedures and responsibilities shall be noted for the recovery and continuity of the affected areas. Fall back procedures will be in place to ensure systems can revert to before implementing changes.

## Documentation

Information resources documentation shall be updated on the completion of each change, and old documentation shall be archived or disposed of as per the Data Retention And Disposal Policy.

Information resources documentation is used for reference purposes in various scenarios, i.e., further development of existing information resources and ensuring adequate knowledge transfer in the original developer and development house being unavailable. Therefore, it is imperative that information resources documentation is complete, accurate, and updated with the latest changes. Policies and procedures affected by software changes shall be updated on the completion of each change.

## Emergency Changes

Specific procedures to ensure the proper control, authorization, and documentation of emergency changes shall be in place.

# Disciplinary actions

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

# 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. Changes to this policy shall be exclusively performed by the ISMS Manager and approved by the ISMS Committee.

# Responsibility

This is the responsibility of the ISMS Manager to maintain and make sure everyone is aware of this policy.

# Reference

* ISO 27001 A.12.1.2 Change Management
* ISO 27001 A.12.1.4 Separation of Development, Testing & Operational Environments

# Related Documents