**<Your Company Logo>**

**Change Management Policy**

# ***Version Control Table***

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Author | Description |
| 1.0 | <Date> | <Author> | Issued |
| 1.0 | <Date> | <Author> | Reviewed |
| 1.0 | <Date> | <Author> | Approved |
| **1.0** | <Date> | <Author> | **Granted “FINAL” status** |

|  |  |
| --- | --- |
| **Date of Next Revision** | **<date>** |

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 summarize the difference and is not a substitute for reading the full text.

# 

# Table of Contents

[**The Path to Compliance 2**](#_htrkie77tuhx)

[**We'll guide you through, ensuring a smooth path to compliance: 2**](#_bor2nqthjwhg)

[**Need Expert Assistance? 2**](#_j1ad4z2lk78s)

[**Version Control Table 4**](#_waib18pnmr6f)

[**Table of Contents 5**](#_ukruovgntws6)

[**Purpose 6**](#_gqluetr6usqy)

[**Scope 6**](#_167msnbg1e7l)

[**Policy 6**](#_ojhok29bz9oz)

[1. Definitions 6](#_ncvox7g00ywj)

[2. Change Process 7](#_wj4foj640oa9)

[2.1. Standard Change Management Procedure 7](#_jrp4yalp73a1)

[2.2. Change request 8](#_weflsg5ttypf)

[2.3. New system components configuration 8](#_1t8mfg4hipcb)

[2.4. Emergency Change Management Procedure 10](#_yhi3kh20qucq)

[**Disciplinary actions 10**](#_oqiw861lcdyd)

[**Change, Review, and Update 10**](#_6cu0cv3y3y7n)

[**Responsibility 10**](#_fxvzxllev4xj)

[**Reference 10**](#_hhx0u7glv0fd)

[**Related Documents 11**](#_xixdvq2ap8qn)

[Appendix 1.1 11](#_b5c7mcz10mwb)

[Appendix 1.2 11](#_5yez4o3x5td2)

# 

# 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 changes' effectiveness and cross-functional communication.

# Scope

This policy applies to all <Company> employees, contractors, and third parties who access internal information and business processes.

# Policy

Configuration changes will be reviewed, and approval of changes will be considered based on an analysis performed for any security and privacy impacts. Only approved changes will be implemented in the system. Configuration changes will be documented, and system changes will be communicated to authorized internal users. Changes will be monitored and reviewed.

## Definitions

*An “IT change”* is a planned or unplanned action taken to build, design, modify, improve, fix, and re-configure network devices and systems.

Two types of change management requests are to be used: emergency and standard. An emergency change occurs when an immediate change to systems is necessary due to operational issues or critical security issues. A standard change occurs as a part of normal maintenance operations.

The Change request must be created only for changes that are conducted on or influence on <Company> Critical Assets listed in the <Company> Critical Asset Registry.

*The “Change request scope”* is each <Company> Critical information system component subject to change. This component must be defined in the <Company> Critical Asset Registry or must influence any system components in the <Company> Critical Asset Registry.

The “Impact assessment” is a process to analyze the impact of a proposed organizational change on the company processes.

*The “Roll-back plan”* is a plan that let's get back to the exact state that was in before the change implementation started.

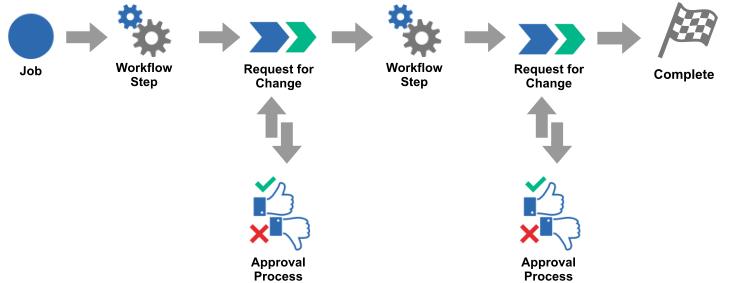
## Change Process

## Standard Change Management Procedure

1. <Company> what is scope change.
2. Develop a request in the mail for testing.
3. Identify the authorized party or parties to approve the request.
4. Obtain approval or disapproval from the authorized party for investigation and testing.
5. 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 and assess its impact on operations and security.
6. Determine the impact of incorporating the change. If implementing this change has a big impact (Low and higher, use Appendix 1.2. to define the impact) on infrastructure or employees, roll-back plans must be developed.
7. In the reply to the request for testing, develop a change request and attach an implantation change plan and potential impact of incorporating the change (How will the change impact the company budget? What about the timeline? How many departments and team members will be touched by the change request? How did the change impact security?). You need to use Appendix 1.1 as a change request template.

7.1. The individual in charge of the change must provide easy-to-understand links or other methods that allow overseeing the process, should any issues arise (short guidance on where to direct attention and what measures to take in case of any complications following the implementation of the modification).

1. Obtain approval or disapproval from the authorized party for implementation.
2. Implement the change.
3. Develop documentation and guidelines if needed.
4. Communicate the change to the necessary stakeholders (management, employees or clients). All users significantly affected by a change shall be notified of the change.



The flow of the change management process

## Change request

Change request shall contain the next information::

|  |  |
| --- | --- |
| **Name of the required section** | **Description** |
| *To:* | Define the all interested party in this change (e.g. CEO, CFO). |
| *Subject:* | Change request - Change Name/Title |
| **Change Description** | |
| *Description Of Change:* |  |
| *Reason for Change:* |  |
| *Type of Change:* | How urgent is the change (Standard or Emergency)? |
| *Impact on Deliverable:* | How will the change alter the schedule, budget, and quality of deliverables? |
| *Impact of Not Responding to Change (and Reason Why) (optional):* | Note the impact of not changing and the reasons why this course would be taken for a better sense of if this change is important. |
| *Date Needed:* | By what date must the change occur? |
| **Change Impact** | |
| *Task/Scope Affected:* | What tasks will be impacted to make this change? Estimate how the scope of “the project” (including security posture) will be impacted by the change. |
| *Cost Evaluation:* | Estimate how much money will be needed for the change. |
| *Quality Evaluation:* | How will the quality of the final product, service or process be improved or not by the change? |
| *Duration:* | Estimate the time it will take to implement the change. |
| *Additional Effort:* | What other things are needed to address this change, which are not already captured on the change request? |
| *Impact on Deadline:* | Will the change affect the deadline? Note that here. |
| *Comments:* | Further discussions that are not included above. |

## New system components configuration

The following actions should be performed by asset owner, IT Director, System Administrators, DevOps or Developers once a new active device was added or a new resource was created.

* Physical servers or Virtual resources:

1. Update Critical Asset Registry.
2. Update Network diagram.
3. Install <EDR> and Chef agents.
4. Security Group/Network ACL must be developed and applied to the new server/service.
5. Storage encryption must be enabled where applicable.
6. Configure a critical asset to send logs to <SIEM>.
7. Automated or manual backup should be configured according to critical assets.
8. Administrative access to the system should be provided according to the Access control policy.
9. New systems should be configured with the latest updates.
10. Vulnerability scanning must be performed according to the vulnerability management policy.

* Network equipment:

1. Update Critical Asset Registry.
2. Update Network diagram.
3. Update IP table.
4. Security Group/Network ACL must be developed and applied to the new device.
5. Configure a critical asset to send logs to the SIEM system.
6. Automated or manual backup should be configured for critical assets.
7. Administrative access to the device should be provided according to the Access control policy.
8. New systems should be configured with the latest updates.
9. Vulnerability scanning must be performed according to the vulnerability management policy.

The following actions should be performed by asset owner, IT Director, System Administrators, DevOps or Developers once a device or resource should be removed.

* Physical servers or Virtual resources:

1. Update Assets inventory.
2. Update Network diagram.
3. Asset should be removed from the <EDR> system.
4. Asset should be removed from the <SIEM> system.
5. Administrative access to the system should be revoked according to the Access control policy.

* Network equipment:

1. Update Assets inventory.
2. Update Network diagram.
3. Update IP table.
4. Device should be removed from the SIEM system.
5. Administrative access to the system should be revoked according to the Access control policy.

## Emergency Change Management Procedure

In certain situations, changes may need to be made faster than the change management process would allow. In these situations, an alternative path to change can be used.

1. Identify and define the situation that requires the emergency change.
2. Determine the impact of incorporating the change. If implementing this change has a big impact (Low and higher, use Appendix 1.2. to define the impact) on infrastructure or employees, roll-back plans must be developed.
3. Escalate concern to management and security.
4. Use change form to define the change request.
5. Send it to security for review.
6. Implement the change in test.
7. Provide emergency access to production (if necessary).
8. Promote the change to production.
9. Update change management request.
10. Develop documentation and guidelines (if necessary).
11. Communicate the change to the necessary stakeholders (management, employees or clients). All users significantly affected by a change shall be notified of the change.

# 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 or employee that was specifically appointed to perform such a task by 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

## Appendix 1.1

Change request template

*To:* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*Subject:* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Change Description**

*Description Of Change:* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*Reason for Change:* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*Type of Change:* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*Impact on Deliverable:* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*Impact of Not Responding to Change (and Reason Why) (optional):* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*Date Needed:* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Change Impact**

*Task/Scope Affected:* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*Cost Evaluation:* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*Quality Evaluation:* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*Duration:* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*Additional Effort:* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*Impact on Deadline:* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*Comments:* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## Appendix 1.2

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Value** | **Impact** | **Business Impact** | **Financial Impact** | **Legal Impact** | **Reputational damage** |
| **1** | Very Low | None, business operations continue as usual | No Financial Impact | None | None |
| **2** | Low | Additional workload in managing the asset | Minor financial impact | None | Staff aware, loss of morale, single client aware |
| **3** | Medium | The asset cannot be operated until the impact is mitigated | Some financial loss | Breach of laws, regulations or contract leading to litigation or prosecution & fines | Multiple clients and businesses aware, local media coverage |
| **4** | High | Core business functions are impacted | Significant financial loss | Breach of laws, regulations or contract leading to litigation or prosecution & significant fines | Widespread local or limited national media coverage |
| **5** | Very High | The whole company is impacted | Major financial loss/business threatening | Breach of laws or regulations leading to prosecution & possible imprisonment | Widespread national and international media coverage |