4.2.1 Change Management Policy

Contents

Version	Adjustment Date	Approved By	Approval Date
2.0	4/7/2024	Saud Alsulami	7/7/2024

1. Definitions

For purposes of this “Change Management Policy” the following definitions apply:

- **Cryptographic:** the practice of securing communication and data using mathematical techniques and algorithms to transform information into a format that is only intelligible to those authorized to access it.
- **Key Distribution:** the secure and reliable sharing of cryptographic keys between authorized parties. It ensures that cryptographic keys reach the intended recipients without interception or compromise, facilitating secure communication and data protection.
- **Digital Signatures:** cryptographic mechanisms used to verify the authenticity and integrity of a digital message or document.
- **Key Revocation:** the process of declaring a cryptographic key as no longer valid or trustworthy.
- **Confidentiality:** the protection of sensitive information from unauthorized access, disclosure, or use.
- **Integrity:** maintaining the accuracy, consistency, and reliability of data over its entire lifecycle. It ensures that data remains unchanged and unaltered by unauthorized or unintended means, such as errors or malicious activities.
- **Availability:** the accessibility and usability of systems, services, or data. It ensures that authorized users can access the information or resources they need when required, without experiencing undue delays or disruptions.

2. Purpose

The objective of this policy is to define and document the formal requirements to implement an approved change or add an information technology asset, and that includes Defining the change, classification of the change, reviewing the design, and controlling the implementation.

3. Scope

The scope of a change management policy outlines the controlled and systematic approach for implementing changes to IT systems, applications, and infrastructure, ensuring minimal disruption and maximizing the reliability and security of technology environments within Taqnyat.

4. Policy

4.1. Change request

A new change request must be following these steps:

- The change requester fills out a change request form. (Change Request Form)
- The change request must specify the functional and non-functional requirements as needed.
- Functional requirements define what the system needs to meet the change request and the behavior of the system or software in response to various inputs—including but not limited to business rules, administrative functions, data management, and authorization levels.
- Non-functional requirements describe how a system should perform. They are essential to ensure the system behaves optimally and provides a positive user experience. Non-functional requirements include but are not limited to performance, security, usability, and compatibility requirements.
- The change requester must specify the classification of the change (Major - Emergency).
- IT change requests must be submitted to CEO by e-mail to get the needed approval.

4.2. Change Classification

For any requested change, it is required to define the classification of the change by analyzing its impact as follows:

4.2.1. Minor Change:

A change that is low-risk and well understood, with a limited potential impact on production services, is sufficiently tested before implementation, and is easy to back out in the event of an issue.
This change needs limited resources and investment.
Example for minor changes:

- Adding a new printer to the network
- Upgrading the memory or storage capacity of a server
- add new rule on the firewall

4.2.2. Major Change:

A high-risk and complex change with a significant potential impact on production services and limited backup/recovery in the event of an issue.
This change needs to specify the resources and investment.
Example for major changes:

- Migrating to a new enterprise resource planning (ERP) system
- Moving to a cloud-based infrastructure

- Implementing a new security infrastructure or system
- Introducing a new virtualization technology or platform

A major change requires:

- Formal review, discussion, and approval with all impacted and involved parties, including business users and the technical advisor of the team performing the change.
- Testing (when possible).
- Notification of the change to affected clients.
- Post-implementation review.

4.2.3. Emergency Change:

A change that requires an immediate implementation to correct a critical issue, such as a disruption or outage of service, which could be discovered using monitoring and detection tools.

If any of the following conditions are met, then a change is deemed to be emergency:

- Threat to Business Operations.
- Threat to the health and safety of employees, customers, or other stakeholders.
- The change is time-sensitive and cannot wait for the major change process to be completed.

An emergency change requires:

- The person responsible for the emergency change must immediately notify the technical advisor and CEO to initiate the emergency change process.
- An assessment of the impact of the emergency.
- Communication with stakeholders must be implemented to expedite the change process as needed.
- Thorough review and testing may be reduced or not performed if necessary. However, it could be performed after the implementation of the changes.
- A change request submission within one business day after the issue has been resolved.
- A log of the implementation steps for review purposes.
- Post-implementation review must be performed by the NOC and stakeholders.

4.3. Implementation

After the Technical advisor's approval, all changes must be tested on the test environments or test server before the implementations.

4.4. Change approval

4.4.1. Minor changes:

- All standard changes must be approved by the System Owner.
- All standard changes are defined based on low impact.
- Standard changes include routine and scheduled low-impact changes (for example, adding a firewall role or new DNS entries).
- The system owner can make direct changes to systems under their ownership and is only required to inform the Information Management Manager.

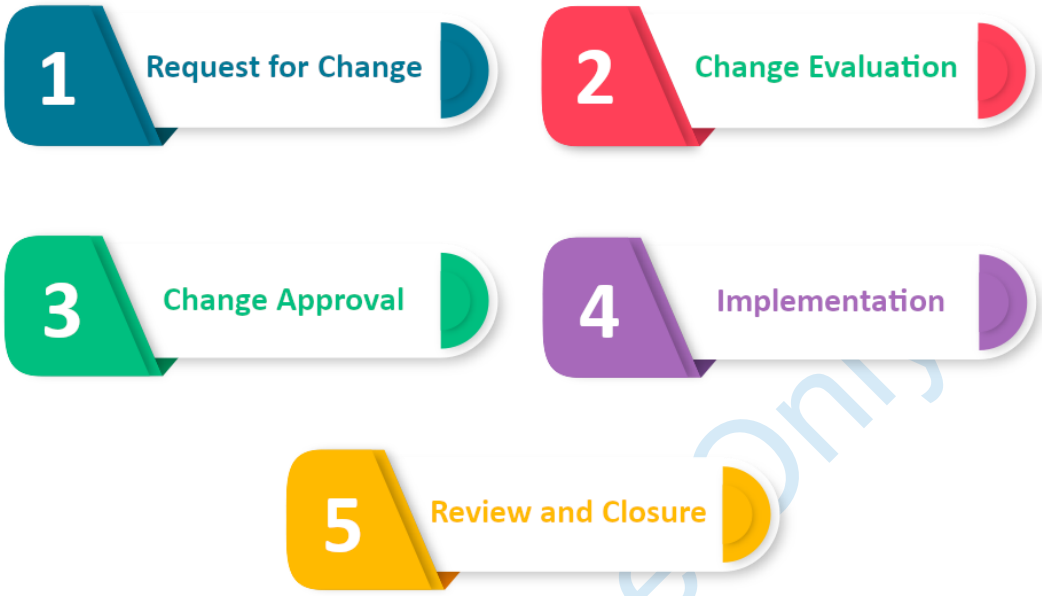
4.4.2. Major changes:

- Major changes are defined based on medium or above impact.
- Change requests must fulfill Information Security requirements.
- The CEO must approve the change request.
- If the Chief Security Officer submits the request, only Technical advisor approval needed.

4.4.3. Emergency changes:

- Emergency changes are defined based on the high impact on operations (for example, resolving an incident or problem).
- Requires approval from the CEO.
- A change request must be completed within 24 hours after the implementation of the emergency change.

5. Change Process



5.1. Request for Change (RFC):
The process begins with the submission of a Request for Change (RFC). An RFC is a formal proposal for a change to be made.

5.2. Change Evaluation:
The proposed change is evaluated to assess its feasibility, potential impact, risks, and benefits. This evaluation is crucial in determining whether the change should be approved, rejected, or deferred.

5.3. Change Approval:
Once the change is evaluated, it goes through a change approval process. This involves obtaining approval from the CEO.

5.4. Implementation:
The change is applied to a test environment before transitioning to the operational environment if the change is major. In the case of an emergency change, it has already been implemented.

5.5. Review and Closure:
Following implementation, a post-implementation review is conducted to assess the success of the change and gather lessons learned.

6. Non-compliance

Non-compliance with this policy may result in disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

7. References

- ISO 27002
- National Cybersecurity Authority's (NCA) ECC standards