Wishes

Change Management Policy and Procedure Template

Purpose

At its core, change management is the method and process of making changes to an organization's IT systems. The change management process is designed with the intent of reducing errors when changes are made to IT systems.

When disruptions occur, organizations are negatively impacted, which is why writing a Change Management Policy (CMP) is so important. For security-minded organizations, writing a CMP is a necessary piece of developing a thorough 'Information Security Policy'. You can ensure that your organization minimizes disruption and reduces risk through the implementation of a clear change management process.

Policy statement

The CMP will help to communicate the management's intent. This is to show that changes to Information and Communication Technology (ICT) supported business processes will be managed and implemented in a way that minimizes risk and impact to us and our operations. All changes to IT systems shall be required to follow an established change management process. This requires that changes to IT systems be subject to a formal change management process that ensures or provides for a managed and orderly method. This includes the way changes are requested, approved and communicated prior to implementation (if possible), and logged and tested.

Purpose

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

- information being corrupted and/or destroyed
- computer performance being disrupted and/or degraded
- productivity losses being incurred
- exposure to reputation risk

Scope

Employees

This policy applies to all parties operating within the organization’s network environment or utilizing information resources. No employee is exempt from this policy.

IT Assets

This policy covers the data networks, local servers and personal computers (stand-alone or network-enabled) located at offices and depots, where these systems are under the ownership of the organization. This includes any personal computers, laptops, mobile devices and servers authorized to access the organization’s data networks.

Documentation

The policy documentation will consist of CMP and related procedures and guidelines.

Records

Records being generated as part of the CMP shall be retained for a period of 2 years. Records shall be in hard copy or electronic media. The records shall be owned by the respective system administrators and shall be audited once a year.

Distribution and Maintenance

The CMP document shall be made available to all the employees covered in the scope. All the changes and new releases of this document shall be made available to the persons concerned. The maintenance responsibility of the document shall be with the CEO and system administrators.

Privacy

The CMP document shall be considered as ‘confidential’ and shall be made available to the concerned persons with proper access control. Subsequent changes and versions of this document shall be controlled.

Responsibility

The CEO is responsible for the proper implementation of the policy.

The CEO ensures that changes follow the change management process.

The CEO reviews the change management schedule monthly to ensure all changes follow the change management process.

The CEO reviews the change management schedule quarterly to ensure changes follow the change management process.

Policy

Changes to information resources will 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.

In order to fulfill this policy, the following statements shall be adhered to:

1.A current baseline configuration of the information system and its components shall be developed, documented and maintained.

2.A current inventory of the components of the information system along with the owner shall be developed, documented and maintained.

3.The baseline configuration of the information system shall be updated as an integral part of the information system component installation.

4.Changes to the information system shall be authorized, documented and controlled by the use of formal change control procedure.

5.Changes in the configuration of the information system shall be monitored through configuration verification and audit processes.

6.The information system shall be configured to provide only essential capabilities and shall prohibit and /or restrict the use of specific functions, ports, protocols, and/or services. A list of prohibited shall be defined and listed.

7.The inventory of the information system components shall be updated as an integral part of the component installation.

8. Automatic mechanisms/tools shall be employed to maintain an up-to-date, complete, reliable, accurate and readily available configuration of the information system.

9.Automatic mechanism/tools shall be employed to initiate changes/change requests. This is to notify the appropriate approval authority, and to record the approval and implementation details.

10.The information system shall be reviewed at a defined frequency to identify and eliminate unnecessary functions, ports, protocols, and/or services.

Change procedure

For compliance purposes all communications need to be in writing (by email, or within meeting minutes. This documentation will be retained by the CEO and filed with the change documentation relating to the change management. For this reason, verbal requests and authorisation are not acceptable.

Risk

If not properly controlled, changes could be made that negatively impact the business and prevent people from fulfilling their roles. Changes could be made by individuals who are not fully aware of the impact on other areas of the business. If change is not controlled the business could be exposed to fraudulent activities.

Submitting the change request form

1. Complete a Change Request Form. This form and information about how to complete it can be found on the Wishes Google Drive
2. Enter as much detail as possible in the ‘Request details’ section. If this change will affect other departments please enter the names of the department managers in the ‘Other departments affected’ section.
3. Once the form has been completed, email it to info@wishes.inc. They’ll log the form and pass it to the Change Management Controller, so that the change can be scheduled.

Review The Specification

The Change Request Form will be reviewed by the Change Management Controller who’ll:

- gather additional information
- add department managers deemed to be affected
- arrange meetings

Then the Change Management Controller creates a specification detailing exactly what's being changed, which is sent to all stakeholders. The specification should incorporate all the requirements:

1. The change stakeholders carefully review the specification to ensure that all the requirements and their particular interests are covered.
2. The change stakeholders will need to approve the specification by email.

The Change Management Controller will also discuss what the appropriate change rating should be with all the stakeholders. The change rating indicates the level of compliance required by the change and the priority that the change is being given.

The implementation plan

The implementation plan details all the stages that are required in order to successfully manage the change, and includes a Test Plan and Roll Back Strategy. In more complicated changes this may also include a project schedule and timeline:

1. Review the implementation plan.
2. Make the Change Management Controller aware of any amendments or changes.
3. Make a note of the timeline and any training or testing, plus how this will affect department staff.
4. Make a note of any dependent tasks. For example, if one department is unable to make a change until another has completed theirs.
5. Authorise the implementation plan by email.

Pre-change

Once the implementation plan has been approved, it's important that the staff in each department are made aware of what needs to happen, when and by whom.

The Department Manager:

- notifies affected Staff of the change and assigns actions and makes them aware of the Roll Back Strategy.
- ensures that Staff who have been allocated Test Actions have copies of the Test Plan and are aware that all test documentation is to be retained.
- leases with other Stakeholders and the Change Management Controller to ensure that all aspects of the change are progressing as planned.

Change

To minimize unnecessary disruption and ensure that the plan is followed as closely as possible, any issues are highlighted to the Change Management Controller, as soon as possible. The Change Management Controller will coordinate communications between the stakeholders, ensuring all staff follow the implementation plan.

Post-implementation review

Once a change has been implemented it's important that the situation is reviewed to identify any problems that could be prevented in the future, or improvements that could be made. The Stakeholders will carry out a post-implementation review one month after the change has been promoted to live. This is unless problems or issues present themselves soon thats this. Two months after the change has been implemented the stakeholders will conduct a further review.

The CEO will review the change documentation and follow up materials quarterly. The minutes and action points of these reviews are held on file with the change documentation. The internal and external auditors will examine the change management documentation on as needed basis and their comments and recommendations will be acted upon.

Exceptions

Exceptions to the guiding principles in this policy must be documented and formally approved by the CEO and Wishes.

Policy exceptions must describe:

- the nature of the exception
- a reasonable explanation for why the policy exception is required
- any risks created by the policy exception
- evidence of approval by all appropriate parties

Enforcement

Any employee found to have violated this policy may be subjected to disciplinary action in line with the HR policy.

Review of this policy will be: annually by the CEO.

Next review date: 01/01/2024.