

Change Management Policy

# Overview/Purpose

Change Management is a formal, systematic process for dealing with change, both from the perspective of the organization, and on an individual level. The intent of Change Management is to ensure that any hardware/software changes implemented are properly planned, tested, and implemented, so as to minimize any resulting disruption. It is the policy of **<Utility Name>** to follow a formal, documented process for implementing significant changes to systems, network, and applications, as documented in the *IT Change Request* Procedure.

# Scope

This policy applies to employees, contractors, and other individuals requesting changes to systems, networks, or applications. IT Manager and IT staff are responsible for following this Policy and related procedures.

# Policy

## Process

The Change Management process shall:

* Ensure that significant requests for changes to systems, networks, and applications are formally documented and submitted is accordance with the *IT Change Request* *Procedure*;
* Require that the IT Manager, and his/her designees, process change requests using the following steps:
  + Submission - only accepting change requests using a formal, documented process, excluding verbal or ad-hoc requests;
  + Impact Evaluation - careful consideration of the potential impact of the requested change to **<Utility Name>**'s operations.
  + Design and Planning - for an approved request, the preparation of an Implementation plan that is sufficiently detailed to ensure that the change is completed according to determinations made during the Impact Evaluation;
  + Implementation - carrying out the change in strict accordance with the details determined in the Design and Planning phase;
  + Results Evaluation - the careful review of the changed system, and all inter-related systems, following the Implementation to ensure that: a) the desired change was implemented successfully; b) there were no unanticipated impacts to other systems as a result of Implementation.

## Scope

The Change Management process includes, but it not limited to, the following requests:

* New hardware such as computer, mobile devices, printers, etc.;
* New software – server, desktop applications, and mobile applications might be included as well if the change requires server installation;
* Change in application or network permissions system;
* Change in the configuration or functionality of the network, including Internet connections, firewall functionality, etc. Note that for firewall, router, and switch modifications, the change should be requested using the Firewall Configuration Change Form;
* Changes to existing processes used by IT Department (policy, procedures, forms).

# Compliance

## Compliance Measurement

The <**person or group responsible for policy**> will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

## Exceptions

Any exception to the policy must be approved by the <**person or group responsible for policy**> in advance.

## Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action in accordance with **<Utility Name>** HR policies.

# Related Standards, Policies, and Processes

* PCI DSS Requirements   
  (<https://www.pcisecuritystandards.org/document_library>)

# Governance Responsibilities

The ISP uses the RACI model for assigning responsibility.

|  |  |  |  |
| --- | --- | --- | --- |
| Responsible | Accountable | Consulted | Informed |
| CIO | **CEO/GM** | **IT Department** | **All Employees** |

*[Explanatory Note: <Utility Name> should feel free to alter section to reflect the specific responsibility requirement determined by <Utility Name> management.]*

# Approval

\_

<**Insert title of approver**> Date

# Revision History

|  |  |  |
| --- | --- | --- |
| Date of Change(s) | Revised by | Summary of Change(s) |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |