CHANGE MANAGEMENT POLICY

POLICY# OTECH-POL2020-004

FRANK L.G. LUJAN, JR. – CHIEF TECHNOLOGY OFFICER
OFFICE OF TECHNOLOGY, GOVERNMENT OF GUAM
Otech.guam.gov

OFFICE OF TECHNOLOGY
GOVERNMENT OF GUAM

MARCH 4, 2020

Overview

Policy Number:	OTECH-POL2020-004
Title:	Change Management Policy
Purpose:	To define responsibilities, policies and procedures for changes to be made to the Government of Guam network.
Authority:	5 GCA Chapter 1 Article 12.105 (13), 12.106 (e)
Publication Date:	March 4, 2020
Policy Approval:	Frank LG Lujan, Jr Chief Technology Officer
Target Audience:	This management process applies to all GovGuam infrastructure devices and systems maintained and supported by OTECH.
Contact Details:	**Office of Technology** 211 Aspinall Avenue PO Box 884 Hagåtña, Guam 96910 O: 671.635.4500 F: 671.472.9508 otech.guam.gov

Revision History

Date of Change	Responsible	Summary of Change
August 2018	OTECH Systems Support	Draft policy
February, March, July, December 2019	OTECH Systems Support	Update policy and format
March 2020	OTECH CTO and Data Processing Manager	Review, approve and disseminate policy

Introduction

The Office of Technology (OTECH) recognizes the importance of providing and maintaining a secured and reliable information technology environment for the Government of Guam (GovGuam). OTECH understands that changes to the network are inevitable and this document provides guidelines in which changes to the information technology environment are requested, tested and approved prior to installation or implementation.

The purpose of this policy is to document the responsibilities, policies and procedures to be followed when any changes to the GovGuam computer network are to be made. This document is not to question the rationale of a change, but to ensure that all elements are in place, that there are no negative impact to the infrastructure, that all the necessary parties are notified in advance and that the schedule for implementation is coordinated with all other activities.

Definitions

Change – to transform, alter, or modify the operating environment or standard operating procedures that have a potential or significant impact on the stability and reliability of the infrastructure and impacts the conducting of normal business operation. A change includes any interruption in building environments (i.e. planned electrical outages) that may also cause disruption to the network infrastructure.

Event – any activity outside of normal operating procedures that will have a potential or significant impact on the stability and reliability of the infrastructure

Change Request – the official request for any change to the GovGuam computer network. All change requests should be submitted via email to the Chief Technology Officer (CTO) (cc Data Processing Manager). End user requests should be submitted via email to Help Desk where it can be routed to the CTO.

Policy

Change management provides a process to apply changes, upgrades or modifications to the environment. This covers any and all changes to hardware, software or applications. It also includes modifications or changes to the LAN/WAN, Network or Server hardware and software, or any other environmental components such as electrical or cooling systems. This policy is in place to ensure that any change that affects one or all of the environments that GovGuam relies on to conduct normal business operations are protected.

Changes to the environment arise from any circumstances, such as:

- User requests
- Hardware and/or software upgrades
- Firmware upgrades
- Acquisition of new hardware and/or software
- Environmental changes
- Business operational schedule changes
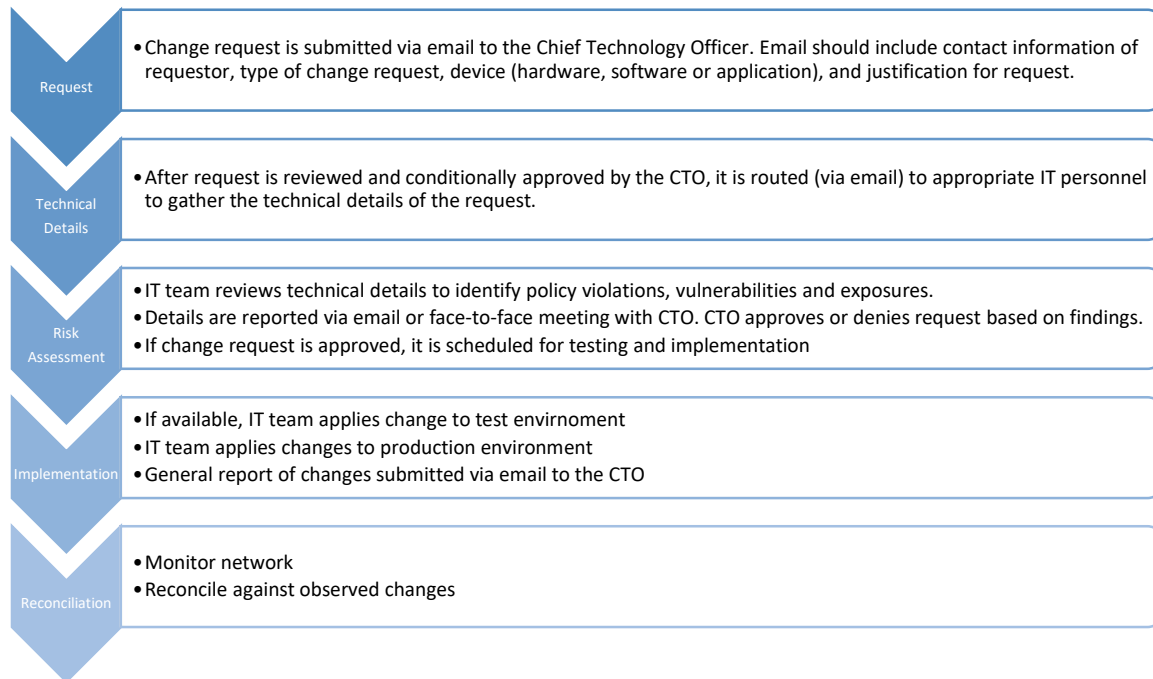- Unforeseen events

- Scheduled periodic maintenance

The above list is not all-inclusive; therefore, any questions on whether a change can be made should be directed to the OTECH CTO.

Change Management Process

The General Change Process is documented below.

Request	• Change request is submitted via email to the Chief Technology Officer. Email should include contact information of requestor, type of change request, device (hardware, software or application), and justification for request.
Technical Details	• After request is reviewed and conditionally approved by the CTO, it is routed (via email) to appropriate IT personnel to gather the technical details of the request.
Risk Assessment	• IT team reviews technical details to identify policy violations, vulnerabilities and exposures. • Details are reported via email or face-to-face meeting with CTO. CTO approves or denies request based on findings. • If change request is approved, it is scheduled for testing and implementation
Implementation	• If available, IT team applies change to test envirnoment • IT team applies changes to production environment • General report of changes submitted via email to the CTO
Reconciliation	• Monitor network • Reconcile against observed changes

In any case the General Change Policy cannot be maintained within an acceptable time limit, OTECH may make an executive decision to implement an Emergency/Crisis Change. An Emergency/Crisis Change is a change deemed necessary to provide network and technical support to resume normal business operations.

Emergencies may include:

- An office is completely out of service
- There is a server degradation of service needing immediate action
- A system/application/component is inoperable and the failure causes a negative impact
- A response to an emergency business need

Policy Compliance

Compliance Measurement

The Office of Technology will verify compliance to this policy through various methods, including but not limited to, periodic reviews and site inspections, video monitoring, business tool reports, internal and external audits and inspections, and feedback to the policy owner.

Exceptions

Any exception to this policy must be approved by the Chief Technology Officer (CTO) in advance and have a written record.

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

Non-Compliance

Any OTECH Staff, contractor, vendor, or end-user found to have violated this policy may have his/her privileges revoked and may be subject to disciplinary and/or legal action. At the discretion of the CTO the violator may be required to take compliance-based education in order to restore or maintain any access privileges associated with this incident.

OFFICE OF TECHNOLOGY
GOVERNMENT OF GUAM