IT SECURITY POLICY END USER PROTECTION

POLICY# OTECH-POL2019-007

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

OFFICE OF TECHNOLOGY
GOVERNMENT OF GUAM

JULY 26, 2019

Overview

Policy Number:	OTECH-POL2019-007
Title:	IT Security Policy – End User Protection
Purpose:	To establish a standard baseline for effective security measures enforced on all end user computing (EUC) hardware connected to the Government of Guam Wide Area Network (GGWAN), as well as any future security requirements for portable storage and mobile device management.
Authority:	5 GCA Chapter 1 Article 12.106 (a)
Publication Date:	July 26, 2019
Policy Approval:	Frank LG Lujan, Jr Chief Technology Officer
Target Audience:	**The intended recipients of this policy also include all entities under the authority of the Office of Technology, pursuant to 5 GCA Chapter 1 Office of the Governor § 12.102**, with EUC hardware connected to the GGWAN. This policy also applies to all vendors and third parties who connect, in any way, to the GGWAN.
Contact Details:	**Office of Technology** 211 Aspinall Avenue Hagåtña, Guam 96910 O: 671.635.4500 F: 671.472.9508 otech.guam.gov

Revision History

Date of Change	Responsible	Summary of Change
April 2019	OTECH Systems Support	Draft policy
April 2019	CTO, DPM	Review draft
July 2019	CTO	Approve and Disseminate Policy
February 2024	OTECH Systems Support	(a) Add Asset Management Section (b) Add Review & Internal Audit Section
March 2024	CTO CTO, *Frank LG. Lujan, Jr.* Date: March 1, 2024	Review, approve and disseminate policy

Introduction

End user computing (EUC) hardware (e.g. desktops, notebooks, workstations or tablets) are the primary gateway to the organization's sensitive information and business applications. Implementation of appropriate security controls for EUC hardware can mitigate the risk of exposures to Government of Guam (GovGuam) data and Information Technology (IT) systems. Consequently, end user protection is critical to ensuring a robust, reliable and secure IT environment.

The Office of Technology (OTECH) is committed to preserving the confidentiality, integrity, and availability of information technology resources within the Government of Guam and this document is intended to provide a baseline of effective security controls for all EUC hardware that connect to the Government of Guam Wide Area Network (GGWAN).

Baseline Requirements for EUC Hardware

1.0 Operating System Level Security

1.1 Centralized Endpoint Management

All Government of Guam EUC hardware connected to the GGWAN must be joined to the Government of Guam (guam.gov) Active Directory (AD) Domain to enforce effective and efficient access and security management.

1.2 Security Updates & Patches

Security updates and patches must be applied on a timely basis to harden EUC hardware from security vulnerabilities.

1.3 Anti-Virus Software

The corporate anti-virus solution must be installed and up-to-date on all GovGuam EUC hardware.

1.4 Firewall

The operating system software firewall must be disabled. In addition, all Microsoft Windows Defender software must also be uninstalled.

1.5 Remote Desktop Protocol

The remote desktop protocol must be enabled on all GovGuam EUC hardware.

1.6 File and Print Sharing

GovGuam EUC hardware must allow for file and print sharing

1.7 Asset Management

GovGuam EUC hardware must synced to GovGuam approved centralized management system to allow for asset management, network discovery, monitoring and software and license management and deployment.

2.0 Mobile/Portable Computing Security

- Users must be made aware of the need to secure unattended mobile and portable GovGuam EUC hardware (e.g. notebooks, portable hard drives, USB memory sticks, etc.) when not in use.

- Users who travel overseas must be made aware of the need to scan mobile (e.g. laptops) and portable (i.e. portable hard drives, USB memory sticks) GovGuam EUC hardware upon return before attaching to the GGWAN. Scans must be scheduled with OTECH.
- All GovGuam portable EUC hardware must be returned to Agency owners immediately upon employee termination.

Roles and Responsibilities

1.0 Agency

- Each Agency is responsible for appropriating funds for the purpose of upkeeping their information technology resources. This includes all hardware, software and services to be connected to the GGWAN in compliance with this policy.
- Each Agency is responsible for informing OTECH of any and all plans that will affect the IT infrastructure.
- Each Agency is responsible for scheduling IT services with OTECH via official email or footprints

2.0 OTECH

- OTECH is responsible for configuring, installing, deploying and servicing all GovGuam IT resources connected to the GGWAN.

Policy Compliance

Compliance Measure

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

Exceptions to the guiding principles in this policy must be documented and formally approved by the requestor's respective Agency Head and the OTECH CTO.

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 user found to have violated this policy will be disconnected from the GGWAN, without notice, and may be subject to disciplinary action.

Review and Internal Audit

This policy shall be reviewed and updated annually, on an as needed basis, or if there is a breach in protocol and procedures. OTECH shall initiate the review process on the first day of each Fiscal Year – 1st of October, or next business day. Policy review and updates shall be documented in the policy's Revision History section. The review process shall be completed before the end of the Fiscal Year's first quarter and the updated policy shall be disseminated (via OTECH website, Agency Memo or email) by December 31 of each year.