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

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
Sept. 2026	CTO Acting CTO, *Beatrice A. Santos* Date: September 1, 2026	(a) Update Standard Baseline Requirements

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).

Standard Baseline Requirements for EUC Hardware

1.0 Identity and Domain Management

1.0.1 Centralized Identity Management

All Government of Guam issued EUC hardware with access to GGWAN resources must be joined to the Enterprise Active Directory (AD) to ensure centralized management of user identities, permissions, and security policies.

1.0.2 Centralized Authentication

EUC local administrator accounts must be disabled. Authorized users must log in using their domain-issued credentials.

1.0.3 Account Lockout Policy

EUC devices shall be configured to automatically lock the workstation and require re-authentication after **15 minutes of inactivity**.

1.1 OS, Software and Patch Management

1.1.1 Operating System (OS) Standard

EUC devices must be configured with an OS Government Baseline supported version (e.g., Windows 11 Enterprise or Pro), to align with enterprise identity control management systems. Use of "Home" or unmanaged consumer editions are strictly prohibited.

1.1.2 Vulnerability Mitigation

EUC devices must be enrolled in the Enterprise Update Service to receive automated security updates and patches for the OS and enterprise applications.

1.1.3 Enterprise Anti-Virus (AV)

A mandated Enterprise Endpoint Detection and Response (EDR) and Anti-Virus (AV) solution must be installed, active, and reporting to the Enterprise console to provide real-time monitoring and behavioral analysis to detect cyber threats.

1.2 Local Network and Connectivity Configuration

1.2.1 Microsoft Defender Firewall

The native Microsoft Defender Firewall shall be disabled via GPO to ensure all traffic rules are managed via the Enterprise EDR/AV security solution.

1.2.2 Wireless Networking

All Wi-Fi/Wireless network adapters shall be disabled via GPO to maintain a secured environment and to prevent "bridging" (where a device is connected to a secure wired network

and an unsecured Wi-Fi simultaneously). Wi-Fi connectivity is restricted to authorized wireless networks only and must be explicitly approved by OTECH.

1.2.3 File and Print Sharing

File and Print Sharing shall be enabled to allow for connection to authorized network resources and centralized services.

1.2.4 Remote Desktop Protocol (RDP)

Remote Desktop must be enabled and restricted to "Network Level Authentication" (NLA) to allow IT administrators to provide remote support, troubleshoot issues, and perform routine maintenance.

1.3 Peripheral and Data Control

1.3.1 USB Port Restriction (Removable Storage)

All USB ports shall be restricted via GPO to block the reading and writing of data to any "Removable Storage" class device (thumb drives, external hard drives).

1.4 Asset Management and Visibility

1.4.1 Enterprise Asset Management Synchronization

All EUC hardware must be enrolled and visible to the Enterprise Asset Management solution. Devices must be connected to the GGWAN to ensure they "check-in" with the server at least once a week.

2.0 Mobile/Portable Computing Security

- Users must understand and acknowledge 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 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 Helpdesk.
- 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 and connect to the IT network infrastructure.
- Each Agency is responsible for scheduling IT services with the OTECH Helpdesk (helpdesk@otech.guam.gov).
- Each Agency is responsible for disseminating this policy and all related IT policies to their employees and contractors.

2.0 OTECH

- OTECH is responsible for configuring, installing, deploying and servicing all GovGuam EUC devices connected to the GGWAN.
- OTECH is responsible for managing and supporting the IT network and systems infrastructure.

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.