PERSONALLY OWNED DEVICE POLICY

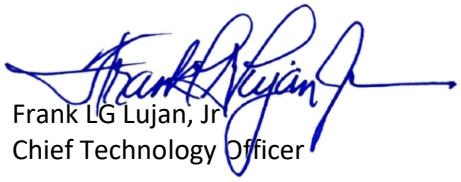
POLICY# OTECH-POL2019-008

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-POL2019-008
Title:	Personally Owned Device Policy
Purpose:	To define standards, procedures, and restrictions for end users connecting a personally-owned device to the Government of Guam Wide Area Network for business purposes.
Authority:	5 GCA Chapter 1 Article 12.106a
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** 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
July 2019	OTECH Systems Support	Draft policy
July 2019	CTO, DPM	Review draft, approve and disseminate

Introduction

A personally-owned device is any technology device that was purchased by an individual and was not issued by the Government of Guam. A personal device includes any portable technology like a camera, webcam, USB flash drive, USB thumb drive, DVD, CD, air card, mobile wireless devices such as Androids, Blackberry OS, Apple iOS, Windows Mobile, tablets, personal desktop computers, and in most cases, wireless access points.

If the appropriate security applications and procedures are not applied, personally-owned devices connected to the Government of Guam Wide Area Network (GGWAN) can be a conduit for unauthorized access to the Government's data and Information Technology (IT) infrastructure. This subsequently can lead to data leaks and system infections. The Table (1) below provides some examples of common attacks on wired and wireless environments:

Table 1 – Common Network Attacks

Threats	Description	Wired	Wireless
Data Leakage	Unauthorized transmission of data	Yes	Yes
Sniffing	Tapping or eavesdropping	Yes	Yes
Spam	Unsolicited email messages	Yes	Yes
Spoofing	Spoofing user email	Yes	Yes
Phishing	Fake emails that appear to be legitimate	Yes	Yes
Pharming	Redirection traffic to a nefarious website	Yes	Yes
Vishing	Leaving voice mail purporting to be a legitimate company	Yes	Yes
Denial of Service (DoS)	Disrupting the availability of network resources	Yes	Yes
Distributed DoS	Many external systems involved in a DoS Attack	Yes	Yes
Bluesnarfing	Stealing information via Bluetooth	No	Yes
SNIP	Unsolicited text messages	No	Yes
Jamming	Jamming a radio signal	No	Yes
Flooding	Text message flood	No	Yes
Exhausting	Running applications in the background to drain the battery	No	Yes
Blocking	Shutdown smartphone features	No	Yes

The Office of Technology (OTECH) must maintain management control and authorize the use of personally owned devices in order to preserve the integrity and availability of all IT resources within the Government of Guam. This document provides guidelines to define appropriate use of all personally owned devices connected to the GGWAN.

Policy

This policy shall:

- Define the appropriate use of personal devices by Government of Guam employees, vendors and third-parties;
- Set minimum standards and guidelines for their use; and,

- Clearly state that users of personal devices that are being used within the GGWAN must comply with local and federal laws and rules dealing with public records, records retention and confidentiality

It is the responsibility of each user who uses a personally owned device to connect to the GGWAN to ensure that all security protocols normally used in the management of data on conventional storage infrastructure are also applied. It is imperative that any mobile device that is used to conduct official Government business be utilized appropriately, responsibly and ethically in accordance with all relevant OTECH policies and user Agency policies. Failure to do so may result in immediate suspension of that user's account. Based on this requirement, the following rules must be observed:

Appropriate Use

1. OTECH defines acceptable business use as activities that directly or indirectly support the Government of Guam's mission, goals, functions and operations.
2. OTECH defines acceptable personal use on official time as reasonable and limited personal communication or recreations, such as reading or game playing
3. The following uses of personally-owned devices on the GGWAN are strictly prohibited:
    - To access, upload, download, or distribute pornographic, obscene, or sexually explicit material.
    - To transmit obscene, abusive, sexually explicit, or threatening language.
    - To violate any local or federal law.
    - To vandalize, damage, or disable the property of another individual or organization.
    - To access another individual's materials, information, or files without permission.
    - To violate copyright or use in an impermissible way the intellectual property of another individual or organization.
    - To promote, advertise or otherwise engage in a personal or private venture.
4. Mobile devices' cameras and video capabilities are to be disabled while on-site.
5. Users may use their personal mobile devices to access the following GovGuam resources: email, calendars, contacts, documents and website.

Access Control

6. OTECH reserves the right to refuse, decline or remove, by physical or non-physical means, the ability to connect personally owned devices to the GGWAN. OTECH will engage in such action if such equipment is being used in a way that directly or indirectly jeopardizes the Government's IT infrastructure and information systems or violates this policy.
7. Prior to initial use on the GGWAN or related infrastructure, **all personally-owned devices must be approved by OTECH**.

Security

Employees using personally-owned devices and related software for network and data access will, without exception, use secure data management procedures. Users are also responsible for complying with their respective Agency policies on data access and management.

8. All users of personally-owned devices **must employ reasonable physical security measures**. End users are expected to secure all such devices whether or not they are actually in use and/or being carried. This includes, but is not limited to, passwords, encryption, and physical control of such device whenever they contain enterprise data.

9. All personally-owned devices connected to the GGWAN must have installed **up-to-date anti-virus and anti-malware software**. In addition to this, all devices must be on a **supported Operating System with the latest patches** installed.

Help & Support

10. Users who use their personally-owned devices on the GGWAN will not be considered priority for support from OTECH.

Restrictions on Authorized Use

The following rules apply to ALL PERSONALLY-OWNED devices:

11. Users may connect their personally owned mobile devices to a GovGuam provided wireless network; however, users MAY NOT connect their personally owned mobile devices to a GovGuam workstation via USB cable.
12. Users are prohibited from connecting any personally owned Wireless Access Point (WAP), switch, router or HUB to the GGWAN
13. Personal devices that have camera, video or recording capabilities are restricted from using those functions to capture GovGuam proprietary data, communications or customer information, unless authorized in advanced by the OTECH CTO and Agency Head.
14. Personally-owned devices are strictly prohibited from accessing any information system containing Federal Tax Information (FTI), Personally Identifiable Information (PII), Social Security Numbers (SSN) and data protected under the Health Insurance Portability and Accountability (HIPPA) Act.

User Acceptance

The central concept of this policy is that the employee, or user, through an opt-in decision, trades some control over his or her personal device to access enterprise resources (such as network and email). It is important that the consequences and obligations of this arrangement are well-understood.

These obligations include, but are not limited to:

- User acceptance that a personal device may be remotely wiped (i.e., erasing state-only or, if needed, all data and applications) by OTECH as part of its data sanitization requirements (*OTECH's Data and Sanitization Policy)*
- User understanding that he or she is solely responsible for backing up any personal content on the device, as that information cannot be guaranteed to be protected by selective wipes
- User agreement to keep the device updated and in good working order
- User accepts that OTECH will set the standards for operating system and application version control and agrees to abide by those standards
- User acknowledgement that OTECH will in no way be responsible for damaged, lost or stolen personal devices while the user is performing official GovGuam business
- User agreement to allow OTECH to load a mobile device management software agent and any other software deemed necessary by the organization on personally owned devices
- User acceptance that enterprise work may be tracked to meet the legal and fiduciary responsibilities of the Government of Guam

- User understanding that utilizing his or her personally-owned device(s) is voluntary, and by no means constitutes a request by OTECH, direct or implied, to conduct enterprise business on the personal device outside of predetermined and regularly scheduled business hours.

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.