REMOTE ACCESS POLICY

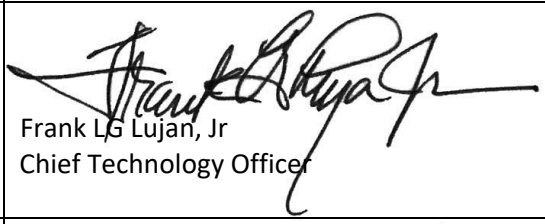
POLICY# OTECH-POL2020-003

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-POL2020-003
Title:	Remote Access Policy
Purpose:	To define rules and requirements for connecting to the Government of Guam's network from any host.
Authority:	5 GCA Chapter 1 Article 12.106 (a)
Publication Date:	March 4, 2020
Policy Approval:	 Frank LG Lujan, Jr Chief Technology Officer
Target Audience:	All OTECH employees, contractors, vendors and third parties. The intended recipients of this policy also include all entities under the authority of the Office of Technology, pursuant to the provisions of Public Law 34-076.
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
February 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
June 2022	OTECH Systems Support	• Update document to SSL-VPN MFA Requirements • Add Review & Internal Audit Section
July 2022	CTO OTECH CTO, *Frank LG Lujan, Jr.* Date: July 5, 2022	• Review and Approve policyupdates for dissemination.
February 2024	OTECH Systems Support	• Review policy – no updates
March 2024	CTO CTO, *Frank LG Lujan, Jr.* Date: March 1, 2024	• Review and Approve policy updates for dissemination.
May 2024	OTECH Systems Support	• Update requirements to enforce VPN geofencing to only allow US, US Territories, CNMI and FSM.
May 2024	CTO CTO, *Frank LG. Lujan, Jr.* Date: May 22, 2024	• Review and Approve policy updates for dissemination.

Introduction

The Office of Technology (OTECH) recognizes the importance of ensuring that access to information technology (IT) systems from remote locations is provided to users in a secure and effective manner. This policy defines a framework of implementation standards intended to protect the Government of Guam Network (GGWAN) and servers from the risks inherent in remote access. These standards are designed to minimize the potential exposure to the Government of Guam (GovGuam) from damages which may result from unauthorized use of GovGuam resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical GovGuam internal systems, and fines or other financial liabilities incurred as a result of those losses.

Policy

It is the responsibility of all GovGuam employees, contractors, vendors and agents with remote access privileges to the GGWAN to ensure that their remote access connection is given the same consideration as the user's on-site connection to the GGWAN. The trust is essential to this responsibility.

General access to the Internet for recreational use through the GGWAN network is strictly limited to GGWAN employees, contractors, vendors and agents (hereafter referred to as "Authorized Users"). When accessing the GGWAN from a personal computer, authorized users are responsible for preventing access to any GovGuam computer resources or data by non-authorized users. Performance of illegal activities through the GGWAN by any user (Authorized or otherwise) is prohibited. The authorized user bears responsibility for and consequences of misuse of the authorized User's access.

Remote access to information systems containing sensitive/secured date, to include Personally Identifiable Information (PII) and Medical or Health Information protected by HIPPA, is only considered for persons accessing within the United States and its territories. Remote access to sensitive/secured systems for persons located "off shore": outside of the United States or its territories, is strictly prohibited.

Requirements

- Secure remote access must be strictly controlled with encryption (i.e. Virtual Private Networks (VPNs)), strong pass-phrases, and multi-factor authentication (MFA))
- All remote connections into the GGWAN via VPN shall be established within the Continental United States (US), US Territories, the Commonwealth of the Northern Mariana Islands (CNMI) or the Federated States of Micronesia (FSM).
- Authorized Users shall protect their login, password and PIN, even from family members.
- While using a GovGuam-owned computer to remotely connect to the GGWAN, Authorized users shall ensure the remote host is not connected to any other network at the same time, with the exception of personal networks that are under their complete control or under the complete control of an Authorized User or Third Party.
- Use of external resources to conduct GovGuam business must be approved in advance by the Chief Technology Officer (CTO).
- All hosts that are connected to the GGWAN via remote access technologies must use the most up-to-date anti-virus software that is a named corporate standard, this includes personal computers.

- All hardware and software components that are connected to the GGWAN via remote access technologies must be operating on a supported Operation System (OS) and have the latest security patches installed.
- Authorized Users are prohibited from using such devices from recording, taking pictures of, or capturing screenshots of any GovGuam-owned data, applications, and systems obtained using remote access; including but not limited to: Cell Phones, Tables, Laptops, Video Cameras, Security Cameras, family members with access to workstations that can view GovGuam-owned resources.

Virtual Private Network (VPN)

Approved Government of Guam employees and authorized third parties (contractors, vendors, etc.) may utilize the benefits of a Virtual Private Network (VPN), which is a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees.

OTECH requires the use of multi-factor authentication (MFA) to establish remote connection into the GGWAN.

Additionally,

1. It is the responsibility of Authorized Users with VPN privileges to ensure that unauthorized users are not allowed access to the Government of Guam internal networks.
2. VPN use is to be controlled with using a one-time password authentication with a strong passphrase.
3. VPN gateways will be set up and managed by OTECH's Network and Systems Support Group.
4. VPN users will automatically disconnect from the GGWAN after a pre-defined period of inactivity. The user must logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.
5. Users of computers that are not GovGuam-owned equipment must configure the equipment to comply with all applicable OTECH policies.
6. SSL-VPN with MFA is the only approved method of remote access to the GGWAN. To bind VPN accounts via MFA, **OTECH has approved the following Time-Based One-Time Password (TOTP) Authenticator Apps**:
    a. Microsoft Authenticator
    b. Google Authenticator

    All other Authenticator Apps are strictly prohibited and may result in account revocation.
7. Request for VPN account must be submitted to the Chief Technology Officer to be reviewed for considerations. Approved VPN accounts will be created and managed by OTECH's Network and Systems Support Group.
    a. OTECH Form: **OTECH-19-003 (Remote Access Request)** - https://otech.guam.gov/resources/
8. By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of the Government of Guam network, and as such are subject to the same rules and regulations that apply to GovGuam-owned equipment.

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 user found to have violated this policy may have his/her privileges revoked and may be subject to disciplinary and/or legal action. The unauthorized use of any form of hacking programs or tools within the confines of the GGWAN or any GovGuam networked device is strictly prohibited. Any violations will be considered a cyber incident or cyber breach and will be prosecuted to the fullest extent of the laws of the territory of Guam. 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.

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.