

ISP-PROVIDED WIRELESS SECURITY POLICY

POLICY# OTECH-POL2026-001

FRANK LG LUJAN JR - CTO
OFFICE OF TECHNOLOGY, GOVERNMENT OF GUAM
<https://otech.guam.gov>



OCTOBER 1, 2026



Overview

Policy Number:	OTECH-POL2026-001
Title:	ISP-Provided Wireless Security Policy
Purpose:	The purpose of this policy is to define the minimum technical and security requirements for all wireless broadband services delivered via Internet Service Providers (ISP).
Authority:	5 GCA Chapter 1 Article 12.105 (a)(3), (b)(3), 12.109, 12.110
Publication Date:	October 1, 2026
Policy Approval:	 Beatrice A Santos, Acting Chief Technology Officer for Frank LG Lujan, Jr Chief Technology Officer
Target Audience:	The intended recipient of this policy includes all entities under the authority of the Office of Technology, pursuant to 5GCA Ch 1, Article 12.102. This shall apply to all Government facilities, personnel, temporary sites, and Guest Wi-Fi services utilizing ISP-provided wireless access.
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
September 2026	OTech System Team	Draft policy
September 2026	OTech ITSA & CTO	Review and update policy
October 2026	OTech CTO	Approve policy for dissemination



Introduction

The purpose of this policy is to define the technical and security requirements for the design, procurement, operation, and maintenance of all wireless broadband services delivered via Internet Service Providers (ISP). This policy mandates the strict physical and logical separation of all ISP-provided wireless networks from the internal Government of Guam Wide Area Network (GGWAN).

These guidelines are intended to mitigate risks associated with unauthorized access, lateral movement, and unencrypted traffic within the trusted GGWAN. *All ISP-provided wireless services must be reviewed and approved by OTECH.*

Roles & Responsibilities

OTECH Governance, Risk, Cybersecurity & Compliance	• Develop, maintain, disseminate and assess compliance with this policy. • Assist agencies and personnel with understanding and implementing this policy and related standards and procedures.
Agency Directors	• Ensure budget and funding aligns with all policy guidelines. • Define Wi-Fi acceptable use policy for their department, systems and personnel. • Ensure the acquisition, implementation and maintenance of ISP-provided wireless services align with this policy and all other applicable IT policies.
System Administrators	• Implement and maintain security and control mechanisms. • Continuously monitor GGWAN for rogue networks and update security policies, as needed.
GovGuam Employees, Contractors and Third-party vendors	• Comply with all applicable terms of this policy.

1. General Policy Statements

1.1 Complete Perimeter Isolation

- All ISP-supplied Wi-Fi infrastructure (including modems, routers, and Access Points) must be deployed completely separate from the GGWAN. Direct connection, bridging, or multi-homing of ISP Wi-Fi equipment into the trusted GGWAN is strictly prohibited. All ISP-provided wireless traffic must be terminated on a dedicated external segment.

1.2 Mandated MTSP Firewall Inspection

- All incoming and outgoing ISP Wi-Fi traffic must pass through an inline firewall monitored and managed by a certified Managed Threat Service Provider (MTSP). The MTSP firewall must, at minimum, enforce:
 - 24/7/365 continuous threat monitoring and automated Intrusion Prevention Systems (IPS).
 - Deep Packet Inspection (DPI) and malicious IP/domain filtering.
 - Granular egress filtering to block unauthorized protocols and outbound data exfiltration attempts.



1.3 Access to Internal Resources

- ISP-provided Wi-Fi networks are treated as untrusted public networks. Access to internal government intranet, databases, or restricted systems over ISP Wi-Fi is strictly forbidden unless routed through an OTECH approved, encrypted Virtual Private Network (VPN) with Multi-Factor Authentication (MFA) enabled.

2 Compliance, Enforcement & Auditing

2.1 Mandatory Compliance

- Full compliance with this policy is mandatory for all personnel and third-part vendors operating within government facilities or utilizing government networks.
- Relevant policies and resources: *All public OTECH policies and resources are posted on the OTECH website, otech.guam.gov.*
 - OTECH-POL2020-001, IT Hardware and Software Acquisition Policy
 - OTECH-POL2019-008, Personally Owned Device Policy
 - OTECH 20-010, Technology Acquisition Review

1.2 Rogue Wireless Detection & Security Audits

- Wireless Intrusion Prevention Systems (WIPS) and continuous network scanning will monitor facilities to detect unauthorized ISP connections or rogue access points. Any unapproved ISP Wi-Fi Access Point (AP) connected directly to internal GGWAN infrastructure will be automatically isolated and disconnected.
- Third-party vulnerability scans of the MTSP firewall interface may be conducted or requested at any time.
- Independent penetration tests may be conducted or requested at any time to verify zero route leakage between the external ISP Wi-Fi and the internal GGWAN zones.

1.3 Violations & Disciplinary Action

- Non-compliance, intentional bypass of the MTSP firewall, or unauthorized deployment of internal wireless access points constitutes a critical security breach. Violations may result in:
 - Revocation of network and system access privileges.
 - Formal disciplinary action.
 - Referral to law enforcement or federal authorities if non-compliance involves illegal activity or willful breach of classified/sensitive data per applicable federal and local guidelines.

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 from any and all other sources.

Exceptions

Exceptions to the guiding principles in this policy must be documented and formally approved by the



requestor's respective Supervisor, Agency Head and the Chief Technology Officer (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 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.

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.