I MINA'TRENTAI OCHO NA LIHESLATURAN GUÅHAN

RESOLUTIONS

Resolution No.	Sponsor	Title	Date Intro	Date of Presentation	Date Adopted	Date Referred	Referred to	PUBLIC HEARING DATE	DATE AUTHORS REPORT FILED	NOTES
152-38 (COR)	Committee on Rules	Relative to adopting I Liheslaturan Guåhan Comprehensive IT Policy Manual for I Liheslaturan Guåhan by adding a new Part I, Rule XXII, of I Mina'trentai Ocho Na Liheslaturan Guåhan Oten Areklamento (the 38th Guam Legislature Standing Rules).	3/16/26 1:59 p.m.							Appendix 1

I MINA'TRENTAI OCHO NA LIHESLATURAN GUÅHAN
2026 (SECOND) Regular Session

Resolution No. 152-38 (COR)

Introduced by: Committee on Rules

Relative to adopting *I Liheslaturan Guåhan Comprehensive IT Policy Manual* for *I Liheslaturan Guåhan* by adding a new Part I, Rule XXII, of *I Mina'trentai Ocho Na Liheslaturan Guåhan Otden Areklamento* (the 38th Guam Legislature Standing Rules).

BE IT RESOLVED BY THE COMMITTEE ON RULES OF *I MINA'TRENTAI OCHO NA LIHESLATURAN GUÅHAN*:

WHEREAS, *I Mina'trentai Ocho Na Liheslaturan Guåhan Otden Areklamento* (the 38th Guam Legislature Standing Rules) establishes the rules and procedures of *I Mina'trentai Ocho Na Liheslaturan Guåhan*, and were duly adopted on January 2025; and

WHEREAS, *I Liheslaturan Guåhan Comprehensive IT Policy Manual* has been developed to establish clear standards, responsibilities, and procedures governing information security, acceptable use, data protection, data handling, data classification, digital communications, and technology asset management; and

WHEREAS, the Committee on Rules of *I Mina'trentai Ocho Na Liheslaturan Guåhan* recognizes that secure, efficient, and modern information technology systems are essential to the effective operation of *I Liheslatura* and the protection of government information; and

WHEREAS, the increasing complexity of cybersecurity threats, data management requirements, and digital governance standards necessitates the adoption of a comprehensive and uniform IT policy framework; and

WHEREAS, the adoption of this manual will promote consistency, accountability, and best practices across all legislative offices and personnel; and

WHEREAS, it is necessary to incorporate the manual into the Standing Rules of *I Liheslaturan Guåhan* to ensure its continued authority, implementation, and periodic review; and

WHEREAS, *I Liheslaturan Guåhan* Comprehensive IT Policy Manual as the official governing document for all information technology operations, security protocols, and digital resource management within *I Liheslaturan Guåhan*; now therefore, be it

RESOLVED, that the Committee on Rules of *I Mina'trentai Ocho Na Liheslaturan Guahan* does hereby adopt *I Liheslaturan Guåhan* Comprehensive IT Policy Manual and adds a new Part I, Rule XXII, of *I Mina'trentai Ocho Na Liheslaturan Guåhan Otden Areklamento* (the 38th Guam Legislature Standing Rules);

"**PART H**

***I LIHESLATURAN GUÅHAN* COMPREHENSIVE IT POLICY MANUAL**

RULE XXII

Section 22. *I Liheslaturan Guåhan* Comprehensive IT Policy Manual. *I Liheslaturan Guåhan* Comprehensive IT Policy Manual to be adopted.

I Liheslaturan Guåhan Comprehensive IT Policy Manual to be adopted. appended to these Standing Rules as "Appendix 1" is hereby adopted.

I Liheslaturan Guåhan Comprehensive IT Policy Manual (the Manual) is the official information technology governance document of *I Liheslaturan Guåhan*. The Manual shall apply to all Members, employees, contractors, interns, and any

individuals granted access to the Legislature's information systems, networks, or digital resources.

All individuals subject to this Rule shall comply with the policies, standards, and procedures contained in the Manual.

The Committee on Rules, the Legislative Secretary, and the Clerk of the Legislature, in coordination with the Legislature's Management Information System Department, shall oversee implementation, updates, and enforcement of the Manual.

Revisions to the Manual may be amended by a resolution adopted by the Committee on Rules; and be it further

RESOLVED, that the Speaker and the Chairperson of the Committee on Rules certify, and the Legislative Secretary attest to, the adoption hereof, and that copies of the same be thereafter transmitted to all Members of *I Mina'trentai Ocho Na Liheslaturan Guåhan*; to Joann G. Camacho, Executive Director of *I Mina'trentai Ocho Na Liheslaturan Guåhan*; to Rennae V. C. Meno, Clerk of the Legislature; and to Attorney Darleen E. H. Phillips, Legislative Counsel.

DULY AND REGULARLY ADOPTED BY THE COMMITTEE ON RULES OF *I MINA'TRENTAI OCHO NA LIHESLATURAN GUÅHAN* ON THE DAY OF 2026.

Frank F. Blas, Jr.
Speaker

V. Anthony Ada
Chairperson, Committee on Rules

Sabrina Salas Matanane
Legislative Secretary

2026

APPENDIX 1

THE GUAM LEGISLATURE

COMPREHENSIVE IT POLICY MANUAL

Contents

Acceptable Use of Information Systems Policy

Definitions

- **Information Systems:**
All electronic means used to create, store, access, transmit, and use data, information, or communications in the conduct of legislative, administrative, constituent-related, research, or support activities. This includes the procedures, equipment, facilities, software, and data designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

- **Authorized User:**
Any individual—such as a senator, staff member, contractor, intern, volunteer, or an automated application or process—granted access to a system or resource by the system owner or Administrator of the Guam Legislature's Management Information Systems (MIS) Office in accordance with the Legislature's procedures, rules, and access control policies.

- **Extranet:**
An intranet system that is partially accessible to authorized individuals outside the Guam Legislature, such as government partners or approved third-party vendors, for specific and controlled purposes.

OVERVIEW

Data, electronic file content, information systems, and technology resources within the Guam Legislature must be managed as valuable Government of Guam assets.

The Guam Legislature Management Information Systems (MIS) Office does not seek to impose restrictions contrary to the Guam Legislature's established culture of transparency, professionalism, and public service. MIS is committed to protecting all authorized users, partners, and the Legislature itself from illegal, inappropriate, or damaging actions by individuals, whether intentional or accidental.

All Internet, Intranet, and Extranet-related systems—including but not limited to computer equipment, software, operating systems, email systems, servers, storage media, network accounts, Wi-Fi access, and online services—are the property of the Guam Legislature.

These systems are to be used strictly for official legislative business in service of the Senators, its committees, and the People of Guam.

Effective security is a collective responsibility involving the participation and support of every senator, employee, contractor, volunteer, and affiliate who uses or interacts with Guam Legislature information systems.

Every authorized user must know these guidelines and conduct themselves accordingly.

Purpose

The purpose of this policy is to outline acceptable use of computer equipment, electronic resources, and information systems at the Guam Legislature. These rules exist to protect authorized users and the Legislature. Inappropriate use exposes the Legislature to risks including malware, data breaches, interruption of network services, reputational harm, and legal liabilities.

Scope

This policy applies to all uses of information, electronic and computing devices, and network resources used to conduct legislative business or interact with internal networks and systems—whether such resources are owned or leased by the Guam Legislature, owned personally by an employee, or provided by a third party.

All senators, employees, contractors, interns, volunteers, consultants, and third-party affiliates are responsible for exercising good judgment regarding proper use of information systems, in accordance with Guam Legislature policies, Government of Guam regulations, and all applicable local and federal laws.

Policy Detail

Ownership of Electronic Files

All electronic files created, sent, received, or stored on Guam Legislature–owned, leased, or administered equipment—or otherwise under the custody of the Guam Legislature—are the property of the Guam Legislature.

Privacy

Electronic files created, transmitted, or stored on Guam Legislature systems are not private and may be accessed by Legislative IT personnel at any time, without notice to the user, sender, or recipient.

File content may be accessed by authorized personnel at the direction of the Speaker, the Legislative Executive Director, Human Resources, or in compliance with an official investigation or public records request under Guam law.

General Use and Ownership

• All access requests must be authorized and submitted through departmental supervisors or chiefs of staff.
• Authorized users are accountable for all activity occurring under their credentials.
• All data and files created on Guam Legislature systems become the property of the Guam Legislature.
• There is **no guarantee of privacy** for any information stored on Legislature-owned devices or accounts.
• Authorized MIS personnel may monitor equipment, systems, and network traffic at any time.
• The Guam Legislature MIS Office reserves the right to audit networks and systems periodically to ensure compliance.
• MIS may remove any non-business-related software or files from any system. Examples include games, personal music, personal video collections, unauthorized instant messengers, freeware, shareware, and unapproved cloud storage clients.

Security and Proprietary Information

All devices connected to the Legislature's network must comply with this policy and the Comprehensive IT Policy, including but not limited to:

- Acceptable Use of Information Systems Policy
- Data Classification & Handling Policy
- Email Use Policy
- Password Policy
- Mobil Device/BYOD Policy
- Wireless Network / Wifi Security Policy

Additional Requirements:

• Passwords must comply with the Legislative Password Policy.
• Users must not share login credentials, PINs, authentication tokens, or devices.
• Providing access to unauthorized individuals—intentionally or through negligence—is prohibited.
• Users may access or share Legislature proprietary information only as needed for their assigned duties.
• Workstations must be secured with password-protected screensavers set to 10 minutes or less.
• Users must lock their devices when left unattended.
• Users must log off or restart computers at the end of their shift unless instructed otherwise.
• All proprietary information stored on any device—whether owned by the Legislature or the user—is the sole property of the Guam Legislature and must be protected.
• All theft, loss, or unauthorized disclosure of proprietary information must be reported immediately to supervisors and Management Information Systems(MIS).
• Users must report security weaknesses, suspicious activity, and misuse to their supervisor or Management Information Systems(MIS).
• Users must not share dial-up, VPN, or other remote-access numbers or configurations without Management Information Systems(MIS) approval.
• Extreme caution must be used when opening attachments from unknown or unverified senders.

Unacceptable Use

Users must not intentionally access, create, store, or transmit material deemed offensive, indecent, obscene, or inappropriate for a professional legislative environment.

Under no circumstances may anyone engage in illegal activity using Legislature-owned systems.

System and Network Activities — Prohibited Actions

The following activities are prohibited, with no exceptions:

- Copyright violations, including installation of unlicensed or pirated software.
- Unauthorized copying or distribution of copyrighted materials.
- Introduction of viruses, malware, or malicious programs.
- Sharing passwords or allowing others to access your account.
- Using devices to transmit material that violates workplace conduct standards.
- Attempting to access systems or data without authorization.
- Installing software, patches, or updates without MIS approval.
- Using non-approved freeware or shareware.
- Moving, altering, or installing Legislature-owned equipment without MIS approval.
- Purchasing hardware or software without MIS compatibility review.
- Activities that degrade system performance, deny service, bypass security, or obtain unauthorized resources.
- Running security tools, network scanners, sniffers, password crackers, or similar utilities.
- Circumventing authentication or security controls.
- Interfering with other users' access or sessions.

Personal use of Legislature-owned computers from home must follow all the same rules. Family members and non-authorized persons may **not** use Legislature systems.

Legislature information systems may not be used for personal financial gain or personal political campaign activity.

Incidental Use

Incidental personal use of Legislature systems is permitted, with restrictions:

- Users must apply good judgment and may not abuse system access.
- Incidental personal use applies only to the authorized user—not family or acquaintances.
- Such use must not generate additional cost to the Legislature without prior approval.
- It must not interfere with the user's job performance.
- Users must not send or receive files that could cause legal, ethical, or reputational issues.
- Storage of personal files must be minimal.
- All messages, files, and documents—including personal ones—stored on Legislature

systems may be accessed in accordance with this policy and may be subject to Guam FOIA/Open Government laws.

Review and Acceptance

All Guam Legislature staff must review and accept this Acceptable Use Policy upon starting employment, service, or contractual engagement (see Exhibit A).

New employee onboarding will include this policy along with all other required IT security and administrative training. Signed acceptance forms will be retained by the Legislative IT Office.

Exhibit A

Receipt of Acceptable Use of Information Systems

Please sign and return this form to the Guam Legislature Management Information Systems(MIS) Office.

I have received a copy of the **Guam Legislature Acceptable Use of Information Systems Policy**.

I understand that the policy summary I have received is not exhaustive and that it is my responsibility to review and become familiar with the full **Comprehensive IT Policy**.

I understand that the most up-to-date policies will be maintained on the Legislature's Intranet and that I am responsible for reviewing policy updates as they occur.

I understand that the Comprehensive IT Policy supersedes all previously issued policies, and that the Guam Legislature may modify, replace, or rescind any policy at any time.

My signature below confirms that I have received my personal copy of the Acceptable Use Policy and accept responsibility for adhering to the Comprehensive IT Policies as updated.

User Signature: _____
User Name (Printed): _____
Date: _____

Retain one copy for your records and return the other to The Guam Legislature Management Information Systems (MIS).

Data Classification & Handling Policy

1. Purpose

The purpose of this Data Classification & Handling Policy is to ensure that all information created, stored, processed, or transmitted by the Guam Legislature is:

- Appropriately classified
- Properly protected according to its sensitivity
- Handled in compliance with Guam law
- Managed in a way that safeguards confidentiality, integrity, and availability

This policy supports compliance with:

- **5 GCA Chapter 8 – Open Government Law**
- **5 GCA Chapter 10 – Sunshine Reform Act of 1999**
- **2 GCA Chapter 1 – Guam Legislature Act**
- **4 GCA Chapter 13 – Public Official Disclosure Act**
- **18 GCA Chapter 91 – Uniform Electronic Transactions Act**
- **Government of Guam cybersecurity mandates**

2. Scope

This policy applies to all:

- Senators
- Attachés
- Legislative employees
- Contractors
- Consultants
- Interns and volunteers
- Authorized users of Guam Legislature information systems

It applies to all information formats, including:

- Electronic documents
- Email and messages
- Printed materials
- Mobile device data
- Databases and application data
- Audio, video, and multimedia
- Physical records and constituent case files
- Cloud-stored information
- Removable media (USB, external drives)

---

3. Data Classification Levels

All legislative data must be classified into one of the following four categories:

3.1 Level 1 — Public Information (No Restriction)

Information intended for public release or required by law to be publicly accessible.

Examples:

- Press releases
- Published legislation
- Public committee reports
- Official statements
- Information posted to the Legislature's public website
- Material subject to automatic disclosure under 5 GCA Ch. 10

Handling Requirements:

- No special restrictions
- May be freely distributed

- Must still be accurate and official

3.2 Level 2 — Internal Use Only

Information intended solely for internal operations, but not harmful if disclosed.

Examples:

- Internal memos
- Meeting agendas (non-confidential)
- Departmental procedures
- Non-sensitive administrative records
- Scheduling information
- Draft documents not yet approved for public release

Handling Requirements:

- Store on Legislature-approved systems
- Do not share outside the Legislature without approval
- Email only through official @guamlegislature.gov accounts

3.3 Level 3 — Confidential Information

Sensitive information that could cause administrative, operational, or reputational harm if disclosed.

Examples:

- Staff records
- Internal investigation materials
- Non-public constituent correspondence
- Draft legislation under embargo
- Procurement or vendor evaluations
- MIS network diagrams or security data

- Legal review documents
- Budget planning materials (pre-publication)

Handling Requirements:

- No transmission to personal email accounts
- Store only on secure MIS-approved systems
- Encrypt when transferring electronically
- Shred paper copies when disposed
- Do not discuss in public or unsecured areas
- Sharing requires supervisor authorization

3.4 Level 4 — Restricted / Sensitive Information

Information that requires the highest level of protection due to legal obligations or potential harm.

Examples:

- Personally Identifiable Information (PII)
- Personnel files covered under 4 GCA
- Sensitive constituent case files
- Security incident logs
- Passwords, authentication tokens, or cryptographic keys
- Financial or payroll data
- Data protected by privilege (attorney-client, legislative privilege)
- Law enforcement-sensitive information shared with the Legislature
- System configuration files or administrative credentials

Handling Requirements:

- Must be encrypted at rest and in transit
- Access restricted to authorized personnel only

- Must not be emailed without encryption
- Must not be stored on personal devices or cloud accounts
- Must not be copied to USB drives unless MIS-approved
- Printed copies must be locked in secure storage
- Disposal requires cross-cut shredding
- Transfer requires MIS oversight

---

4. Data Handling Requirements

4.1 Storage Requirements

- All data must be stored on MIS-managed servers, cloud environments, or approved devices.
- Personal cloud storage (Google Drive, Dropbox, iCloud, etc.) is prohibited for Levels 3 and 4 data.
- Mobile devices accessing Sensitive or Confidential data must use MIS-approved security configurations.

4.2 Transmission Requirements

Email

- Level 3 and 4 data requires encryption or secure transmission.
- Do not auto-forward emails to non-Legislature accounts.

Removable Media

- USB drives are prohibited unless MIS-provisioned and encrypted.
- No personal USB drives may be used.

Printing

- Do not leave sensitive printouts unattended.
- Retrieve printed materials immediately.

Remote Access

- Requires MFA
- Restricted to approved devices
- Prohibited for certain Level 4 materials without MIS approval

---

4.3 Access Control

- Access is granted based on the **Principle of Least Privilege**.
- Users may not access data outside their job responsibilities.
- Shared accounts may not be used for sensitive data unless strictly controlled.
- All access requests must follow the Account Management Policy.

4.4 Data Dissemination

Users must ensure:

- Data is shared only with authorized individuals
- Records are transmitted securely
- Disclosures comply with Guam law and Legislative Rules
- Confidential or Restricted data is never released to the public without authorization

Unapproved disclosure is strictly prohibited.

---

5. Data Retention and Disposal

MIS and the Legislative Clerks Office manage retention requirements.

5.1 Retention

- Follow MIS retention schedules, Legislative Rules, and 5 GCA requirements.
- Users must not delete records subject to retention.

5.2 Disposal

- Level 1 and 2 data: Recycle or delete normally.
- Level 3 data: Shred or use MIS-approved deletion methods.

- Level 4 data: Must be cross-cut shredded or digitally wiped using MIS-approved tools.

Improper disposal may constitute a violation of Guam law.

---

6. Reporting Obligations

Users must report the following immediately:

- Security breaches
- Unauthorized access or disclosure
- Loss or theft of devices
- Suspected phishing or social engineering
- Mishandling of sensitive data
- Misuse of Legislature records

Reports must be made to a supervisor **and** MIS.

---

7. Enforcement

Violations may result in:

- Removal of system access
- Mandatory retraining
- Disciplinary action in accordance with Legislative personnel policies
- Contract termination (for contractors)
- Civil liability under 4 GCA or 5 GCA
- Criminal referral if required by law

Unauthorized disclosure of Level 4 data is considered a serious offense.

---

8. Roles and Responsibilities

Management Information Systems (MIS)

- Define data classification guidelines
- Provide secure storage and transmission tools
- Monitor compliance
- Investigate data incidents
- Train users on proper data handling

Supervisors & Chiefs of Staff

- Ensure staff follow classification rules
- Approve access rights
- Notify MIS of personnel changes
- Enforce compliance within their offices

All Users

- Classify data correctly
- Handle data according to this policy
- Report incidents immediately
- Protect all Legislature information in their custody

---

9. Annual Review

MIS will review and update this policy **annually**, or more frequently if required by:

- Legislative rule changes
- New Guam statutes
- Cybersecurity developments
- Operational needs

---

10. Acknowledgment

All personnel must sign **Acceptable Use of Information Systems Policy Receipt Form** confirming:

- They understand the data classification levels
- They agree to handle information according to the corresponding requirements
- They understand penalties for improper handling

Password Policy

1. Purpose

The purpose of this Password Policy is to establish standards for the creation, protection, use, and management of passwords within the Guam Legislature. Strong password hygiene is essential for safeguarding legislative information systems, preventing unauthorized access, and ensuring compliance with Guam law, including:

- **5 GCA Chapter 8 – Open Government Law**
- **5 GCA Chapter 10 – Sunshine Reform Act of 1999**
- **18 GCA Chapter 91 – Uniform Electronic Transactions Act**
- **Applicable Government of Guam cybersecurity directives**

2. Scope

This policy applies to:

- All **Senators**, **employees**, **contractors**, **consultants**, **interns**, **volunteers**, and any authorized individuals with access to Guam Legislature information systems.
- All accounts used to access Guam Legislature resources, including but not limited to:
    - Network logins
    - Email accounts
    - Legislative applications
    - Remote access (VPN)
    - Mobile device access
    - Administrative or privileged accounts

This policy applies regardless of device ownership—Legislature-owned, personally owned, or third-party devices accessing Legislature systems.

3. Policy Requirements

3.1 Password Creation Standards

All passwords must meet the following minimum requirements:

- **Minimum length:** 12 characters
- Must contain at least **three** of the following:
    - Uppercase letters (A–Z)
    - Lowercase letters (a–z)
    - Numbers (0–9)
    - Special characters (!@#$%^&*_-+=)
- Must **not** contain:
    - User's first or last name
    - Usernames or email addresses
    - Easily guessable words, simple patterns, or predictable strings (e.g., "Password123," "Legislature2024")

Passphrases (long, memorable sentences) are encouraged.

3.2 Password Confidentiality

Users **must not**:

- Share passwords with anyone, including supervisors, MIS staff, coworkers, interns, or family members.
- Write passwords down in visible locations.
- Store passwords in unencrypted files or unsecured mobile apps.
- Reuse Guam Legislature passwords for personal accounts or outside services.

Passwords may only be stored in an **MIS-approved password manager**.

3.3 Password Expiration & Rotation

- Passwords must be changed **every 90 days**.
- Privileged or administrative accounts must rotate passwords **every 45 days**.
- Passwords **must not** be reused for at least **16** previous password generations.
- Users must immediately change passwords if:
    - They suspect compromise
    - MIS notifies them of a threat
    - There is a security incident
    - They inadvertently shared the password

3.4 Multi-Factor Authentication (MFA)

Where applicable, MFA is required for:

- Email access
- VPN/remote access
- Administrator accounts
- Access to secure or sensitive legislative data
- Any system designated by MIS as requiring additional protection

Authentication methods may include hardware tokens, authenticator apps, or SMS (SMS allowed only as fallback).

3.5 System Locking and Device Security

To prevent unauthorized access:

- Devices must lock after **10 minutes** of inactivity.
- Users must manually lock their workstation (Ctrl+Alt+Delete) when stepping away.
- Mobile devices must use a PIN, password, biometrics, or approved MFA method.

3.6 Password Reset Procedures

- Users must present valid identity verification to MIS before receiving a reset.
- MIS will never ask for a user's existing password.
- Temporary reset passwords will:
    - Expire immediately upon first login
    - Require the user to create a new password meeting policy standards

---

4. Privileged Accounts

Privileged or administrative accounts require additional controls:

- Must use **unique** passwords not shared with standard accounts.
- Must be stored only in the MIS-approved secure password vault.
- Administrators may not use admin credentials for general browsing or email.
- Privileged session actions may be logged and reviewed by MIS.

---

5. Enforcement

Violation of this policy may result in:

- Revocation of system access
- Retraining requirements
- Administrative or disciplinary action under Guam Legislature personnel rules
- Possible legal liability under Guam statutes (including 4 GCA § 1305 and 5 GCA transparency laws)
- Reporting to appropriate authorities in cases of suspected criminal activity

Intentional password misuse, sharing, or unauthorized access attempts may be treated as a security incident and escalated accordingly.

---

6. Roles & Responsibilities

Users

- Follow all password creation and protection requirements.
- Report suspected compromise immediately to MIS.

Management Information Systems (MIS)

- Enforce this policy.
- Manage authentication systems and password resets.
- Conduct periodic audits.
- Ensure compliance with government cybersecurity standards.

Supervisors & Chiefs of Staff

- Ensure their staff adhere to this policy.
- Notify MIS immediately when a user separates from service or changes roles.

---

7. Review Cycle

This policy shall be reviewed **annually** by MIS and updated as needed to:

- Maintain compliance with evolving cybersecurity best practices
- Meet new Government of Guam legal requirements
- Reflect changes in legislative operations and technology

---

8. Acceptance & Acknowledgment

All Guam Legislature personnel must sign the **Acceptable Use of Information Systems Policy Receipt Form** acknowledging that they have read, understood, and agree to comply with this policy.

Email Use Policy

1. Purpose

The purpose of this Email Use Policy is to establish the proper, secure, and lawful use of email systems within the Guam Legislature. This policy ensures:

- Protection of official legislative communications
- Prevention of misuse or unauthorized disclosure
- Compliance with Guam's transparency and public records requirements
- Preservation of the Legislature's integrity, security, and professionalism

This policy supports and aligns with:

- **5 GCA Chapter 8 – Open Government Law**
- **5 GCA Chapter 10 – Sunshine Reform Act of 1999**
- **2 GCA Chapter 1 – Guam Legislature Act**
- **18 GCA Chapter 91 – Uniform Electronic Transactions Act**
- Government of Guam cybersecurity mandates
- The Guam Legislature Acceptable Use Policy, Password Policy,

2. Scope

This policy applies to:

- All **Senators**, **staff**, **contractors**, **consultants**, **interns**, **volunteers**, and authorized users with Legislature-provided email accounts.
- All email systems provided or administered by the Guam Legislature, including:
    - @guamlegislature.gov email accounts
    - Shared mailboxes
    - Committee mailboxes
    - Automated/notification email accounts

- MIS-approved mobile email applications

This policy applies to both Legislature-owned and personally owned devices accessing legislative email.

---

3. Policy Statements

3.1 Official Use of Email

Email systems are provided primarily for **official legislative business**, including:

- Communication with constituents
- Work with government agencies
- Committee operations
- Legislative research
- Inter-office coordination
- Administrative and operational communication

Limited incidental personal use is permitted only in accordance with the Acceptable Use Policy.

3.2 Prohibited Uses

Users **must not** use Guam Legislature email systems for:

- Personal business ventures, profit-making activities, or campaign purposes
- Sending offensive, obscene, defamatory, discriminatory, or harassing content
- Political campaign solicitations (per local ethics statutes and 4 GCA)
- Mass forwarding chain letters or spam
- Unauthorized distribution of confidential or proprietary information

- Personal social media accounts (non-business use)
- Storage of personal files, photos, or non-work-related media
- Streaming services, subscription sign-ups, or promotional content
- Registering for personal websites or accounts using a Legislature email

Email may **not** be used for lobbying or private political advocacy outside official legislative functions.

3.3 Public Records and Transparency

Under Guam law:

- Most email communications may be subject to public disclosure under the **Sunshine Reform Act of 1999 (5 GCA Ch. 10)**.
- Users must maintain professionalism, accuracy, and appropriateness in all email communications.
- Emails may be archived and retained according to MIS and Legislative Rules for records retention.

Users must assume that **any email they send on a Legislature account could be made public**.

3.4 Email Security Requirements

To safeguard legislative information:

- Email accounts require passwords meeting the Legislature's Password Policy.
- Multi-Factor Authentication (MFA) must be used when required by MIS.
- Users must not forward Legislature email to personal email accounts.
- Users must not configure automatic email forwarding without MIS approval.
- Email access on mobile devices must use MIS-approved security settings.

All suspicious emails or attachments must be reported immediately to MIS.

3.5 Attachments and Downloads

Users must exercise caution when:

- Opening attachments from unknown or unexpected sources
- Clicking links within unsolicited or suspicious emails
- Downloading files to Legislature systems or devices

Potential phishing, malware, spoofing, or attempted credential theft must be reported immediately to MIS.

3.6 Email Retention and Archiving

- MIS may archive all email messages for institutional recordkeeping.
- Users must not attempt to circumvent, delete, or alter email records required for retention.
- Deletion of messages does not guarantee permanent removal due to automated backups.
- Records requests under 5 GCA may require MIS retrieval of archived email content.

3.7 Use of Shared Mailboxes

Shared or committee mailboxes:

- Must be approved and created by MIS
- Must have documented authorized users
- Must use least-privilege access
- Must not be used for personal communication
- Must follow the same security and retention rules as individual mailboxes

Users accessing shared mailboxes remain fully accountable for all actions performed under those permissions.

3.8 Restricted Information

Email **must not** be used to transmit:

- Unencrypted Personally Identifiable Information (PII)
- Sensitive constituent data without authorization
- Passwords or authentication tokens
- Internal MIS network information
- Security configuration files
- Legislative legal strategy or confidential caucus material (unless approved channels exist)

Encrypted email tools must be used when required by MIS.

---

4. Account Creation, Changes, and Termination

Email account management follows the Account Management Policy:

- Creation requires supervisor authorization
- Access changes must be formally submitted to MIS
- Email accounts must be disabled immediately upon separation from service
- Mailboxes may be archived upon user departure for retention compliance

No personal or non-authorized individuals may access legislative email.

---

5. Monitoring and Logging

Users acknowledge:

- MIS may monitor email usage, headers, logs, and metadata
- Content may be inspected as required by law, internal investigation, or HR directive
- The Legislature reserves full rights to email data stored on its systems

- Monitoring aligns with 5 GCA transparency requirements and internal security needs

There is **no expectation of privacy** when using Legislature email systems.

---

6. Enforcement

Violations of this policy may result in:

- Revocation of email access
- Removal of network access
- Mandatory retraining
- Disciplinary action up to and including termination
- Civil penalties under Guam law
- Possible criminal referral if conduct violates cybersecurity or government ethics statutes

Intentional misuse, unauthorized disclosure, or breach of sensitive information will be treated as a security incident.

---

7. Roles and Responsibilities

Management Information Systems (MIS)

- Provision and administration of email accounts
- Security enforcement and incident response
- Logging and retention of email records
- Approving email access for devices and systems

Supervisors, Chiefs of Staff, and Senators

- Ensure compliance within their offices
- Report staff changes to MIS immediately
- Review and manage shared mailbox access regularly

All Users

- Use email responsibly, ethically, and legally
- Follow all password and security protocols
- Report suspicious activity or incidents immediately

---

8. Policy Review

MIS will review this policy **annually** or as needed based on:

- New technology
- Updated Guam statutes
- Cybersecurity threats
- Legislative operational needs

---

9. Acceptance & Acknowledgment

All Guam Legislature personnel must sign the **Acceptable Use of Information Systems Policy Receipt Form** acknowledging that they have read, understood, and agree to comply with this policy.

Mobil Device / BYOD Policy

1. Purpose

The purpose of this Mobile Device / BYOD Policy is to define acceptable use, security requirements, and responsibilities for mobile devices accessing Guam Legislature information systems. This policy ensures:

- Security and protection of legislative data
- Compliance with Guam laws and cybersecurity standards
- Proper management of devices, both Legislature-issued and personally owned

This policy supports compliance with:

- **5 GCA Chapter 8 – Open Government Law**
- **5 GCA Chapter 10 – Sunshine Reform Act of 1999**
- **18 GCA Chapter 91 – Uniform Electronic Transactions Act**
- **2 GCA Chapter 1 – Guam Legislature Act**
- Government of Guam cybersecurity mandates

2. Scope

This policy applies to all:

- Senators
- Attachés
- Legislative employees
- Contractors
- Consultants
- Interns and volunteers
- Authorized users accessing Guam Legislature information systems via mobile devices

It applies to all mobile device types, including:

- Smartphones
- Tablets
- Laptops
- Smartwatches or wearable devices
- Mobile hotspots
- Any personal device used to access Legislature email, applications, networks, or data

---

3. Policy Statements

3.1 Device Authorization

- **Legislature-issued devices:** Only devices issued and configured by MIS may be used for official business unless otherwise approved.
- **BYOD devices:** Personally owned devices may be used only with MIS approval. Users must enroll their device in MIS-approved Mobile Device Management (MDM) or security platform.

MIS reserves the right to deny access to non-compliant devices.

3.2 Acceptable Use

Mobile devices may be used for:

- Official legislative communications and email
- Accessing approved applications and databases
- Legislative research and constituent management

Prohibited uses include:

- Storing unapproved personal applications containing sensitive data
- Using mobile devices to circumvent IT security policies
- Sharing Legislature accounts or credentials

- Remote access to internal networks
- Connecting unapproved devices to Legislature networks
- Accessing social media for personal purposes using Legislature email credentials

All users must comply with the Acceptable Use Policy and Email Use Policy when using mobile devices.

3.3 Security Requirements

All devices must comply with MIS-approved security standards:

- Password or PIN protected (minimum 6–16 characters; alphanumeric + symbols recommended)
- Biometric authentication encouraged (fingerprint, face ID)
- Device encryption enabled
- Automatic lock after 10 minutes of inactivity
- Anti-malware or approved security applications installed
- Regular OS and app updates installed

3.4 Network Access

- Only MIS-approved Wi-Fi, VPN, and network connections are allowed.
- Public Wi-Fi usage for accessing legislative data must occur only through VPN.
- Mobile hotspots may be used only with MIS approval.

3.5 Data Protection and Handling

- Users must follow the **Data Classification & Handling Policy**.
- Level 3 (Confidential) and Level 4 (Restricted) data must **never** be stored unencrypted on personal devices.
- Loss or theft of a device must be reported immediately to MIS. MIS may remotely wipe sensitive data from lost or stolen devices.

- Backup of legislative data on personal devices is prohibited unless approved by MIS.

3.6 Application Management

- Only MIS-approved applications may be used for legislative purposes.
- Personal applications may not be used to store or transmit legislative information.
- Jailbroken or rooted devices are strictly prohibited.

3.7 Email and Communication

- Legislature email may only be accessed through MIS-approved applications.
- Incidental personal email use on Legislature devices is permitted within the limits defined by the Email Use Policy.
- Sharing sensitive information via personal apps or messaging platforms is prohibited.

3.8 Compliance and Monitoring

- MIS may monitor, audit, and manage enrolled devices to ensure compliance with security policies.
- Users acknowledge that legislative data on personal devices may be subject to monitoring and retrieval.
- Users must allow MIS to remove access or wipe data if security risks are detected or upon termination of employment/contract.

---

4. Lost, Stolen, or Compromised Devices

- Users must report lost, stolen, or compromised devices **immediately** to MIS.
- MIS may remotely wipe devices containing legislative data.
- Users are responsible for ensuring sensitive data is not stored outside approved storage solutions.

---

5. Device Termination

Upon separation from the Legislature:

- All Legislature-issued devices must be returned.
- Personal devices with access to legislative accounts must have all data and accounts removed.
- MIS will remove all email, VPN, and application access.

---

6. Roles and Responsibilities

6.1 Management Information Systems (MIS)

- Approve and provision devices
- Enforce device security policies
- Audit device compliance
- Provide technical support and training
- Execute remote wipe and security enforcement

6.2 Supervisors & Chiefs of Staff

- Ensure team compliance with the policy
- Notify MIS of personnel departures or role changes
- Support MIS audits and security enforcement

6.3 Users

- Comply with all security requirements
- Report lost or compromised devices immediately
- Maintain devices according to MIS guidance
- Follow all relevant legislative IT policies

---

7. Enforcement

Violations may result in:

- Suspension or revocation of network/device access
- Disciplinary action or termination
- Contract termination for contractors or consultants
- Civil or criminal liability under Guam law (4 GCA, 5 GCA)

---

8. Policy Review

MIS will review this policy **annually** or as needed based on:

- Emerging mobile threats
- Technology changes
- Guam legislative and cybersecurity law updates
- Legislative operational needs

---

9. Acknowledgment

All personnel must sign an acknowledgment form confirming:

- They have read and understand the Mobile Device / BYOD Policy
- They agree to follow all device security and handling requirements
- They understand the potential consequences for violations

Wireless Network / WI-FI Security Policy

1. Purpose

The purpose of this Wireless Network / Wi-Fi Security Policy is to define requirements for the secure deployment, management, and use of wireless networks at the Guam Legislature. This policy ensures that:

- Legislative data and systems are protected against unauthorized access
- Wireless networks are used in compliance with Guam laws and cybersecurity standards
- Risks associated with wireless communications, including interference, eavesdropping, and misuse, are minimized

This policy supports compliance with:

- **5 GCA Chapter 8 – Open Government Law**
- **5 GCA Chapter 10 – Sunshine Reform Act of 1999**
- **2 GCA Chapter 1 – Guam Legislature Act**
- **18 GCA Chapter 91 – Uniform Electronic Transactions Act**
- Government of Guam cybersecurity mandates

2. Scope

This policy applies to all:

- Senators
- Legislative employees
- Contractors
- Consultants
- Interns and volunteers
- Authorized users accessing Guam Legislature wireless networks

It applies to:

- All wireless networks owned, managed, or provisioned by the Guam Legislature
- Wi-Fi access points, routers, and network controllers
- Personal and mobile devices connecting to Legislature networks

Note: Use of public Wi-Fi networks for connecting to legislative systems is **strictly prohibited**. No legislative data or credentials may be accessed over unsecured or public networks.

---

3. Wireless Network Usage

3.1 Authorized Access

- Only MIS-approved devices and users may connect to Guam Legislature Wi-Fi networks.
- BYOD devices must be enrolled in MIS-approved Mobile Device Management (MDM) before connecting.
- Guest access to public Wi-Fi is **not permitted under any circumstances**. Visitors must coordinate with MIS for any temporary access using secure, internal networks.

3.2 Network Segmentation

- Legislature Wi-Fi networks are segmented according to user roles and data classification:

Network	Authorized Users	Allowed Data Level
Legislature Secure Wi-Fi	Senators, staff, contractors	Levels 2–4 (Internal, Confidential, Restricted)
MIS Management Wi-Fi	MIS administrators	Levels 3–4 (Confidential, Restricted)

Public Wi-Fi networks are strictly prohibited, and no legislative data may be accessed via unsecured Wi-Fi.

---

4. Security Requirements

All wireless networks must adhere to MIS-approved security standards:

4.1 Encryption

- WPA3 Enterprise is the minimum standard for all secure networks.
- WPA2 Enterprise may be used temporarily with MIS approval.

4.2 Authentication

- Users must authenticate with MIS-managed credentials.
- BYOD devices must use multi-factor authentication (MFA) where required.

4.3 Access Control

- Only authorized devices are allowed to connect.
- MIS maintains an up-to-date device inventory.
- Unrecognized devices will be automatically blocked.

4.4 Monitoring

- MIS will monitor wireless traffic for anomalies, unauthorized access attempts, and performance issues.
- Logs are retained according to IT retention policies.

4.5 Physical Security

- Access points must be physically secured to prevent tampering.
- Wireless networks are designed to minimize coverage outside legislative buildings.

---

5. Device Requirements

Devices connecting to wireless networks must comply with:

- Mobile Device / BYOD Policy
- Data Classification & Handling Policy

Additional requirements:

- Antivirus or endpoint protection active and updated

- Latest OS and app security updates installed
- Jailbroken or rooted devices are prohibited
- Level 3 and Level 4 data must use MIS-approved encryption
- Loss or theft of devices must be reported immediately

---

6. Prohibited Activities

Users must not:

- Connect to public Wi-Fi networks while accessing legislative data (**strictly prohibited**)
- Bypass MIS security controls, including firewalls, VPNs, or network segmentation
- Share network credentials with unauthorized individuals
- Use personal hotspots to bypass Legislature network controls
- Install rogue access points, Wi-Fi extenders, or repeaters without MIS approval
- Use wireless networks for illegal, offensive, or non-legislative activities

---

7. Incident Reporting

Users must immediately report:

- Suspicious Wi-Fi activity
- Unauthorized network access attempts
- Lost, stolen, or compromised devices
- Security alerts or anomalies

MIS will investigate and may temporarily block or remotely wipe devices if needed.

---

8. Roles and Responsibilities

8.1 Management Information Systems (MIS)

- Deploy, configure, and secure wireless networks

- Approve device access and manage BYOD enrollment
- Monitor network traffic and security
- Respond to security incidents and breaches

8.2 Supervisors & Chiefs of Staff

- Ensure compliance with wireless network policies
- Report unauthorized access or incidents to MIS

8.3 Users

- Connect only authorized devices
- Protect credentials and access codes
- Comply with encryption, authentication, and usage policies
- Report issues immediately

---

9. Enforcement

Violations may result in:

- Loss of network access
- Disciplinary action or termination
- Contract termination for contractors or consultants
- Civil or criminal liability under Guam law (4 GCA, 5 GCA)

---

10. Policy Review

MIS will review this policy **annually** or as needed due to:

- Technology changes
- Security threats
- Legislative operational requirements
- Changes to Guam statutes

---

11. Acknowledgment

All personnel must sign an acknowledgment confirming:

- They have read and understand the Wireless Network / Wi-Fi Security Policy
- They agree to comply with all security requirements, including prohibition of public Wi-Fi
- They understand the consequences of violations