PERSONALLY IDENTIFIABLE INFORMATION (PII) POLICY

POLICY# OTECH-POL2020-005

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-POL2020-005
Title:	Personally Identifiable Information (PII Policy
Purpose:	To establish adequate controls to Government of Guam Information Technology (IT) systems and devices maintained by the Office of Technology (OTECH). As part of daily operational activities, GovGuam staff may have access to citizen or staff PII. This information is generally found in personnel files, citizen data sets, performance reports, program evaluations, grant and contract files, or other sources. Federal law and federal policies require that PII and other sensitive information be secured and protected at all times.
Authority:	5 GCA Chapter 1 Article 12.106 (e)
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
October 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
February 2024	OTECH Systems Support	(a) Add review & internal audit section
March 2024	CTO  CTO, *Frank LG. Lujan, Jr.* Date: March 1, 2024	Review, approve and disseminate policy

Introduction

Information security is the protection of information against accidental or malicious disclosure, modification or destruction. Information is an important, valuable asset of the Government of Guam's Information Technology systems which must be managed with care.

The Office of Technology (OTECH) is committed to ensuring the security and confidentiality of the information it processes on behalf of the Government of Guam (GovGuam). Poor management of access controls to sensitive information processed and stored within GovGuam facilities can lead to the illicit act of disclosure of information, fraud, and possible lawsuits.

This policy is intended to define the appropriate use and management of Personally Identifiable Information (PII) across GovGuam Applications, Systems and Devices managed and maintained by OTECH, as well as to harden and mature our collective efforts in improving our overall cybersecurity posture.

Definitions

OTECH defines "**Personally Identifiable Information**" (PII) as information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.

"**Sensitive Information**": Any unclassified information whose loss, misuse, or unauthorized access to or modification of could adversely affect the interest or the conduct of Federal programs or the privacy to which individuals are entitled under the Privacy Act.

The Department of Labor has defined two types of PII, "**protected PII**" and "**non-sensitive PII.**" The differences between protected PII and non-sensitive PII are primarily based on an analysis regarding the "risk of harm" that could result from the release of the PII.

"**Protected PII**" is information that if disclosed could result in harm to the individual whose name or identity is linked to that information. Examples of protected PII include, but are not limited to, social security numbers (SSNs), credit card numbers, bank account numbers, home telephone numbers, ages, birthdates, marital status, spouse names, educational history, biometric identifiers (fingerprints, voiceprints, iris scans, etc.), medical history, financial information, and computer passwords.

"**Non-sensitive PII**" is information that if disclosed, by itself, could not reasonably be expected to result in personal harm. It is standalone information that is not linked or closely associated with any protected or unprotected PII. Examples of non-sensitive PII include information such as first and last names, e-mail addresses, business addresses, business telephone numbers, general education credentials, gender, or race. However, depending on the circumstances, a combination of these items could potentially be categorized as protected or sensitive PII.

To illustrate the connection between non-sensitive PII and protected PII, the disclosure of a name, business e-mail address, or business address most likely will not result in a high degree of harm to an individual. However, a name linked to a social security number, a date of birth, and mother's maiden name could result in identity theft. This demonstrates why protecting the information of our citizens and employees is so important.

Policy

All parties must ensure the privacy of all PII obtained from citizens and to protect such information from unauthorized disclosure. All parties must ensure that PII has been obtained in conformity with applicable Federal and state laws and policies governing the confidentiality of information.

All PII transmitted via e-mail or stored on external drives must be encrypted and or password protected. All PII stored onsite must be kept safe from unauthorized individuals at all times and must be managed with appropriate information technology (IT) services. Accessing, processing, and storing of PII data on personally owned equipment at off-site locations (e.g. employee's home, and non-grantee managed IT services, e.g. Yahoo mail, Gmail, etc.) is strictly prohibited.

All parties who will have access to sensitive/confidential/proprietary/private data must be advised of the confidential nature of the information, the safeguards with which they must comply to protect the information, and that they may be liable to civil and criminal sanctions for improper disclosure.

Access to any PII obtained must be restricted to only those employees of the respective line agency who need it in their official capacity to perform duties.

All PII data must be processed in a manner that will protect the confidentiality of the records/documents and is designed to prevent unauthorized persons from retrieving such records by computer, remote terminal, or any other means.

Agencies must permit the Office of Technology (OTECH) to make onsite inspections during regular business hours for the purpose of conducting audits and/or conducting other investigations to assure that the agency is complying with the confidentiality requirements described above. In accordance with this responsibility, agencies must make records applicable to this agreement available to authorized persons for the purpose of inspection, review and/or audit.

Agencies must retain data received only for the period of time required to use it for assessment and other purposes, or to satisfy applicable Federal and GovGuam records retention requirements, if any. Thereafter, the agency agrees that all data will be destroyed, including deletion of electronic data.

Additional Requirements:

1. Before collecting PII or sensitive information, have individual sign releases acknowledging the use of PII for government authorized purposes only.

2. Whenever possible, use unique identifiers for participant tracking instead of SSNs. While SSNs may initially be required for performance tracking purposes, a unique identifier could be linked to each individual record. Once the SSN is entered for performance tracking, the unique identifier would be used in place of the SSN for tracking purposes. If SSNs are to be used for tracking purposes, they must be stored or displayed in a way that is not attributable to a particular individual, such as using a truncated SSN.

3. Use appropriate methods for destroying sensitive PII in paper files (i.e. shredding) and securely deleting sensitive electronic PII.

4. Do not leave records containing PII open and unattended.

5. Store documents containing PII in locked cabinets when not in use.

6. Immediately report any breach or suspected breach of PII.

Roles & Responsibilities

Role	Responsibility
OTECH Chief Technology Officer (CTO)	• Overall responsibility for the security, functionality and support of all GovGuam information systems, resources and applications supported and maintained by OTECH • Overall responsibility for reviewing and updating this policy on an annual or as needed basis • Monitor and review compliance to the requirements of this policy
Agency Heads	• Overall responsibility to ensure that all their employees, third party vendors and contractors comply with this policy • Ensure this policy is updated on an annual or as needed basis • Support the OTECH CTO with new security implementations and protocols pertaining to this policy • Review and explicitly approve or disapprove any exceptions to the requirements of this policy
IT Administrator	The IT Administrator for each Agency may vary, is appointed by the OTECH CTO and is responsible for: • Complying with the terms of this policy and all other relevant OTECH policies, procedures, regulations and applicable legislations • Taking prompt and proper action on any reported compliance issues in accordance with this policy. • Notifying CTO promptly on any reported compliance issues. • Recommending security enhancements to the OTECH CTO
Application Administrator	The Application Administrator for each Agency and Application may vary: • Complying with the terms of this policy and all other relevant OTECH policies, procedures, regulations and applicable legislations • Taking prompt and proper action in accordance with this policy • Recommending security enhancements to the IT Administrator and OTECH CTO
IT Help Desk	The IT Help Desk is operated by the Office of Technology and is responsible for:

	• Complying with the terms of this policy and all other relevant OTECH and GovGuam policies, procedures, regulations and applicable legislations • Supporting the IT Administrator and CTO on their duties and responsibilities in accordance with the terms of this policy
Agency Branch/Division /Bureau Administrators	• Disseminate and implement this policy within their respective division/branch/bureau • Ensure that all personnel who report to them are notified and instructed to comply with this policy • Comply to the terms of this policy
Employees	• Comply with the terms of this policy • Report all non-compliance instances with this policy (observer or suspected) to their Supervisor or Administrator as soon as possible.

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 transmission of PII not consistent with this policy 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.