SECURITY AWARENESS TRAINING POLICY

POLICY# OTECH-POL2021-006

FRANK L.G. LUJAN, JR.
OFFICE OF TECHNOLOGY, GOVERNMENT OF GUAM
Otech.guam.gov

OFFICE OF TECHNOLOGY
GOVERNMENT OF GUAM

AUGUST 30, 2021

Overview

Policy Number:	OTECH-POL2021-006
Title:	Security Awareness Training Policy
Purpose:	To bring awareness of security risks associated with information systems and of the applicable federal and agency requirements related to the security of strategic information systems.
Authority:	5 GCA Chapter 1 Article 12.106 (e)
Publication Date:	August 30, 2021
Policy Approval:	Frank LG. Lujan, Jr. OTECH, Chief Technology Officer (CTO)
Target Audience:	All OTECH employees and contractors.
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
August 2021	OTECH Systems Support	Draft policy
August 2021	CTO, DPM	Review draft, approve and disseminate
January 2022 March 2022	OTECH System Support	• Add Retention Policy Requirement under Management Commitment • Add Review & Internal Audit section • Include Cybersecurity Awareness Course Outline
March 2022	CTO OTECH CTO, *Frank LG Lujan, Jr.* Date: March 30, 2022	Review and Approve policy updates for dissemination.
February 2024	OTECH System Support	(a) Review policy – no updates required
March 2024	CTO CTO, *Frank LG. Lujan, Jr.* Date: March 1, 2024	Review and Approve policy updates for dissemination.

Introduction

Security and privacy awareness and training is an important aspect in protecting the confidentiality, integrity, and availability of sensitive information. Employees are the first line of defense and must be made aware of the security risks associated with the work performed within the Government of Guam. Those with significant security responsibilities must be adequately trained to carry out their assigned information security-related duties and responsibilities.

Scope

This policy applies to all OTECH employees and contractors and anyone else needing access to the Government of Guam information systems and network resources.

Policy and Procedures

OTECH will ensure that all employees and contractors are given security and privacy awareness training during the new hire process and before accessing any Government of Guam systems. This training reflects common security and privacy awareness specific to the Government of Guam's environment including, but not limited to, physical access, restricted areas, potential incidents, how to report incidents, laptop best practices, and how to spot a phishing scam.

In addition to the initial security training, all employees must attend the Identifying and Safeguarding Personally Identifiable Information (PII), *Version 2.0*[i] interactive on-line training course provided by the Center for Development of Security Excellence (CDSE), Security Awareness Hub[ii] within 30 days of hire.

OTECH will conduct annual refresher training for all employees and anytime there are significant changes to the environment based on assigned security roles and responsibilities

Management Commitment

OTECH Management will commit to the development of a security and privacy awareness program by allocating staff and resources. The Security Officer will have access to OTECH resources to assist with the completion and update of training materials and tracking of results.

OTECH shall retain copies of all training certifications, acknowledgements and agreements for a minimum of seven (7) years from date signed.

Coordination among Organization Units

OTECH will work with Government of Guam Line Agencies and contractors to ensure that required security controls are in place, are maintained, and comply with the policy described in this document. Security concerns, security incidents, or suspected/confirmed vulnerabilities will be shared with appropriate personnel in the organization so that the vulnerability can be remediated (or mitigated with compensating security controls) and we can ensure that similar vulnerabilities in other systems or processes can be addressed.

Compliance

Compliance with the policy defined in this document is mandatory. Failure to comply with OTECH Information Security Policies may result in disciplinary actions up to and including termination of employment. Employees may also be held personally liable for any violations of this policy. Failure to comply with OTECH Information Security Policies may result in termination of contracts for contractors. Legal actions may also be taken for violations of applicable regulations and laws. Systems that do not satisfy OTECH Information Security Policy requirements may be prevented from being allowed to operate as a production system.

Acknowledgement Forms and Training Outline

OTECH Rules of Behavior for Government of Guam Computer Network Users
OTECH Privacy and Security Training Acknowledgement
StaySafeOnline Security Awareness Training Videos
OTECH Cyber Awareness Quiz

Roles & Responsibilities

Role	Responsibility
OTECH Chief Technology Officer (CTO)	• Overall responsibility for the implementation of this policy • Overall responsibility for reviewing and updating this policy on an annual or as needed basis • Overall responsibility to ensure that all OTECH employees and contractors comply with this policy • Assign an OTECH Resource to act as the Security Officer
Security Officer	The Security Officer is appointed by the OTECH CTO and is responsible for: • Updating annual security training materials • Conducting Security and Privacy Awareness Training for all new hires based on assigned security roles and responsibilities • Ensuring that all OTECH employees attend the *Safeguarding Personally Identifiable Information (PII)* On-line training • Developing and documenting procedures to facilitate the implementation of the security awareness and training policy and associated awareness and training controls, and maintain documentation for 7 years. • Disseminating the Security Awareness Training policy to OTECH staff and contractors
Employees	• Understand and comply with all security related policies and procedures • Attend Security and Privacy Awareness Training and *Safeguarding Personally Identifiable Information (PII)* On-line training • Comply with established OTECH Rules of Behavior

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.

OTECH Privacy and Security Training Acknowledgement

I,_____, acknowledge that I have
(Full Name – Print Legibly)
read and Understand the Office of Technology (OTECH) Security Awareness Training Policy. I also acknowledge that I have completed and understand the material outlined in the Identifying and Safeguarding Personally Identifiable Information (PII) Security Training. I agree to comply with the terms and requirements contained therein regarding the privacy and security safeguards of PII and agree not to disclose any information acquired in the course of my assigned duties to authorized persons. I understand that violation of these requirements may result in disciplinary action, up to and including termination of employment or contract, as well as civil and criminal liability.

By my signature I acknowledge that I have read and will abide by this agreement.

Employer	Official Title/Position
Signature	Date
Security Officer Signature	Date

Safeguarding PII Training Outline

Overview

The Office of Technology (OTECH) has adopted the *Identifying and Safeguarding Personally Identifiable Information (PII) Version 2.0*[i] interactive on-line training course provided by the Center for Development of Security Excellence (CDSE), Security Awareness Hub[ii].

As noted on the CDSE website, the site is the premier destination for accessing security awareness courses for DoD and other U.S. Government and defense industry personnel who do not require transcripts to fulfill training requirements for their specialty. In addition, the *Identifying and Safeguarding Personally Identifiable Information (PII) Version 2.0* interactive training provides an overview of Personally Identifiable Information (PII), protected health information (PHI), as well as the laws and policy that govern the maintenance and protection of PII and PHI.

Module 1 - Course Overview

Course Introduction

- Identify course objectives
- Identify personally identifiable information (PII) and why it is important to protect it
- Identify both the organization's and individual's responsibilities for safeguarding PII
- Recognize the policy and procedures related to the use and disclosure of PII

Module 2 - Overview of PII

PII and PHI

- Identify course objectives
- Recognize PII and PHI
- Identify the information that identifies as PII and PHI
- Identify how PII and PHI is stored
- Identify who and how one can use PII and PHI

Safeguarding PII

- Identify the risks associated with the use and disclosure of PII

Regulations and Guidance

- Identify the legal, Federal regulatory, and DoD guidance on safeguarding PII
- Understand PII Legal Requirements
- Privacy Act of 1974
- Freedom of Information Act (FOIA)
- E-Government Act of 2002
- Federal Information Security Controls (FISMA)
- OMB Guidance for Implementing Privacy Provisions of the E-Government Act of 2002
- OBM Memorandum 07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information
- DoD 5400.11-R "Department of Defense Privacy Program"
- DoD Directive 5400.11 "DoD Privacy Program"
- Understand PHI Legal Requirements

- Privacy and Security Rules issued under the Health Insurance portability and Accountability Act (HIPPA)
- Health Information Technology for Economic and Clinical Act (HITEC)
- DoD 6025.18-R "DoD Health Information privacy Regulation," January 2003
- DoD 8580.02-2 "DoD Health Information Security Regulation," July 12, 2007

Module 3 - Safeguarding PII

Organizational Responsibilities

- Identify organizational safeguards for PII
- Identify administrative, physical and technical safeguards that organizations can employ to protect PII

Individual Responsibilities

- Identify individual safeguards for PII
- Understand personal responsibilities to safeguard the confidentiality, availability, and integrity of their organization's PII
- Identify administrative, physical and technical safeguards that individuals can exercise to protect their organization's PII

Protecting PHI

- Identify the purpose and role of risk assessments in safeguarding PII
- Understand covered and non-covered entities

Module 4 - Use and Disclosure of PII and PHI

Authorized Use and Disclosure

- Identify the procedures associated with the use and disclosure of PII and PHI
- Identify the penalties for failing to comply with the safeguarding requirements that apply to PII and PHI

Failure to Safeguard PII and PHI

- Identify the penalties for failure to safeguard PII and PHI
- Identify the penalties for non-compliance with the requirements governing use and disclosure of PII and PHI

Module 5 - Course Conclusion

Summary and Conclusion

- Completion Certificate

---

[i] Security Awareness Hub, *Identifying and Safeguarding Personally Identifiable Information (PII) Version 2.0* Course Launch - https://securityawareness.usalearning.gov/piiv2/index.htm

[ii] Center for Development of Security Excellence (CDSE), Security Awareness Hub - https://securityawareness.usalearning.gov/

Cyber Security Awareness Course Outline

Overview

With guidance from the Cybersecurity & Infrastructure Security Agency (CISA) and the National Cybersecurity Alliance, the Office of Technology (OTECH) has created a Cybersecurity Awareness Training Program that includes training videos, information flyers and awareness/prevention of the 10 most common cyber attacks.

The following training and informational resources are posted on the OTECH website (https://otech.guam.gov/cybersecurity/):

1. Cybersecurity Awareness Training Videos:
    a. Password Security
    b. Data Handling
    c. Removable Media
    d. Computer Theft
    e. Phishing and Ransomeware
    f. Vishing
    g. Internet Downloads
    h. Wifi
2. Cybersecurity Informational Flyers
    a. Protect Your Smartphone
    b. What is Multi-Factor Authentication
    c. How to Spot a Phishing Email
    d. Phishing: What You Need to Know
3. Top 10 Most Common Cyber Attacks
    a. Ransomeware
    b. Phishing and Spear Phishing Attack
    c. Man-in-the-middle (MitM) Attack
    d. Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS)
    e. Drive-by Attack
    f. Password Attack
    g. SQL Injection Attack
    h. Cross-site scripting (XSS) Attack
    i. Eavesdropping Attack
    j. Malware Attack

After reviewing the provided training and information, users are encouraged to take the OTECH Cyber Awareness Quiz.