RISK ASSESSMENT POLICY & PROCEDURES

POLICY# OTECH-POL2021-003

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

OFFICE OF TECHNOLOGY
GOVERNMENT OF GUAM

AUGUST 27, 2021

Overview

Policy Number:	OTECH-POL2021-003
Title:	Risk Assessment Policy & Procedures
Purpose:	To provide guidelines for assessing and addressing security risks on Government of Guam (GovGuam) Information Systems.
Authority:	5 GCA Chapter 1 Article 12.105 (a)(3), (a)(9), 12.109, 12.110
Publication Date:	August 27, 2021
Policy Approval:	 Frank LG Lujan, Jr Chief Technology Officer
Target Audience:	The intended recipients of this policy includes all entities under the authority of the Office of Technology, pursuant to 5GCA Ch 1, Article 12.102.
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
June 2021	OTECH Systems Support	Update policy
August 2021	CTO, DPM	Review draft, approve and disseminate
February 2024	OTECH Systems Support	(a) Add Review & Internal Audit Section
March 2024	CTO CTO, *Frank LG. Lujan, Jr.* Date: March 1, 2024	Review and approve policy updates for dissemination.

Introduction

The purpose of this document is to provide an overview of the process involved in performing a threat and risk assessment. The outcome or objective of a threat or risk assessment is to provide recommendations that maximize the protection of confidentiality, integrity and availability while still providing functionality and usability.

Roles and Responsibilities

Role	Responsibility
Agency Business Partner	• In collaboration with the Office of Technology (OTECH), holds all third-party vendors/contractors for Externally-hosted Information Assets accountable to this policy, within the vendor/contractor's span-of-control. • Develops and implements agency-level policy and procedures to meet any additional federal statutory requirements pertinent to agency risk management controls. • Collaborates with Agency and OTECH on User Acceptance Testing for the remediation of legitimate vulnerabilities.
Office of Technology (OTECH)	• Overall responsibility to execute, enforce and disseminate this policy and procedures. • Review and update policy on an as needed basis, or annually • Conduct risk assessments to determine mitigation priorities and articulate dangers to Government of Guam (GovGuam) IT Systems. • For OTECH-hosted Infrastructure and OTECH-hosted Applications, executes the vulnerability scans. • For Externally-hosted Information Assets, either executes the vulnerability scans, or collects vulnerability scans from vendors or third-party auditors. • Interprets all vulnerability scans: filters out the false-positives and false-negatives, and reports the legitimate vulnerabilities. • Determines the remediation schedule for legitimate vulnerabilities • The Chief Technology Officer (CTO) reviews and approves security categorization decisions. • Liaises with horizontal Industry Partners on a need-to-know basis to help contain similar vulnerabilities in the wild. Include MSISAC and U.S. Department of Homeland Security.
Agency Heads	• Overall responsibility for ensuring that IT system business partners are well informed of these guidelines • Collaborate with OTECH to ensure that all potential threats and risks are mitigated within the remediation • Ensure that Agency budget accommodates for any potential fee/cost for monitoring and vulnerability tools and remediation efforts.

Coordination Among Agency Entities

It is important that risks assessment be a collaborative process, without the involvement of the various organizational levels the assessment can lead to a costly and ineffective security measures. The Agency Heads, as well as the Agency Business Partners, will cooperate with OTECH in executing this

document. OTECH coordinates with horizontal Industry partners and vendors on a need-to-know basis to help contain similar vulnerabilities in the wild.

Policy

The following serves as the baseline procedures that are implemented to meet risk assessment requirements.

RA-2: Security Categorization

1. Categorizes information, and the information assets, in accordance with applicable state and federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.
    a. OTECH categorizes applications and servers, based on the data it received, processes, and stored. Information security controls are applied to systems that receive, process, and stored particular data types (e.g. Federal Tax, Social Security, Protected Health, Credit Card Information).
    b. Vendor-supported information assets that receive, process, and store particular data types are required to demonstrate information security compliance requirements, as outlined in the following policies:
        - OTECH-POL2020-001 IT Hardware and Software Acquisition Policy
        - OTECH-POL2021-002 IT System Development Requirement & Security Assessment Standards
2. Documents the security categorization results (including supporting rationale) in the security plan for the information system.
    a. OTECH has adopted common classification scheme for data, communications, and environments.
    b. For purposes of this classification, Personally Identifiable Information (PII) is any data that could potentially identify a specific individual.
    c. PII confidentiality impact levels are determined to indicate the potential harm that could result to the subject individuals and/or the organization, if PII were to be inappropriately accessed, used, or disclosed. The following confidentiality impact levels are used, as outlined in the NIST Guide to Protecting the Confidentiality of PII, NIST SP 800-122:

Not Applicable	Does not need to have its confidentiality protected, such as information that the organization has permission or authority to release publicly.
Low	The loss of Confidentiality, Integrity, or Availability (CIA) could be expected to have a Limited Adverse Effect on organizational operations, organizational assets, or individuals.
Moderate/ Medium	The loss of CIA could be expected to have a Serious Adverse Effect on organizational operations, organizational assets, or individuals.
High	The loss of CIA could be expected to have Severe or Catastrophic Adverse Effect on organizational operations, organizational assets, or individuals.

3. Agencies should determine the PII confidentiality impact levels of their data as outlined in NIST SP 800-122, based on six factors:

Identifiability	How easily PII can be used to identify specific individuals
Quality of PII	How many individuals are identified in the information
Data Field Sensitivity	The sensitivity of each individual PII data fields, as well as the sensitivity of the PII data fields together

Context of Use	The purpose for which PII is collected, stored, used, processed, disclosed, or disseminated
Access to and Location of PII	The nature of authorized access to PII. Questions that help determine this include: • How often will it be accessed, and by how many different persons and/or system? When PII is accessed more frequently, and more widely, there exists more opportunities for compromise of confidentiality. • Is it being stored on, or accessed from, remote workers' devices, or other systems, such as web applications, outside the direct control of the organization?

4. OTECH subscribes to the Cybersecurity and Infrastructure Security Agency (CISA) Traffic Light Protocol (TLP). OTECH's four classification levels are as follows:

Public (TLP: White)	Non-sensitive, suitable for public consumption. Examples include: • PII with no impact level (i.e. Not Applicable) • Public announcements or other publicly suitable information • Resource exposed to the Internet
Internal (TLP: Green)	Suitable for State Employees and contractors only, but not sensitive. Examples include: • PII with no impact level (i.e. Not Applicable) • Employee newsletters or announcements, etc. • Internal memorandums not classified as "sensitive" • Subnets containing OTECH Intranet servers.
Sensitive (TLP: Amber)	Suitable for State Employees and select contractors only. Examples include: • PII of a low or moderate confidentiality impact level • Infrastructure information (PII addresses, server names, etc.) • Information that would be embarrassing to the agency or the State if released. • OTECH File-servers, file-shares, and their associated subnets.
Restricted (TLP: Red)	Suitable for select State Employees and contractors only, access granted only on a need-to-know basis. Data must be encrypted at rest and in flight. Examples include: • PII of a high confidentiality impact level • Federally protected data to include Federal Tax, Social Security, Protected Health, Credit Card Information

5. As a security categorization decision, PII confidentiality impact levels and TLP determinations must be reviewed and approved by the CTO.

RA-3: Risk Assessment

1. Based on the data that reside on information assets, and the regulatory regime they are subjected to, risk levels are routinely audited.
2. OTECH may hire third party vendors to conduct independent risk assessments. These vendors are required to produce reports to include the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the in-scope information system, and the information it processes, stored, or transmits. These reports will be maintained by OTECH. OTECH will share risk assessment results to affected stakeholders on a need-to-know basis.

3. The sum-total of all such assessments lead to applicable security plans. The results of information security vulnerabilities are documented for remediation or mitigation based on available resources. The priorities for these efforts are also established.

RA-5: Vulnerability Scanning

OTECH shall perform vulnerability scans on all information assets. OTECH shall collaborate with third-party vendors to perform vulnerability scans, as needed. Scan reports, which are provided to the responsible parties, note patches that are missing, settings that expose possible vulnerabilities, and third-party software issues. If a specific threat is announced at any time, OTECH may schedule scans to assess the vulnerability risk.

Policy Compliance

Compliance Measure

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 the agency that procured the product.

Exceptions

Exceptions to the guiding principles in this policy must be documented and formally approved by the requestor's respective Agency Head and the OTECH 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 agency found to have violated this policy may be subject to disciplinary action at the discretion of OTECH.

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.