IT SYSTEM DEVELOPMENT REQUIREMENTS & SECURITY ASSESSMENT STANDARDS

POLICY# OTECH-POL2021-002

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-POL2021-002
Title:	IT System Development Requirements & Security Assessment Standards
Purpose:	To provide security control standards for all Government of Guam (GovGuam) Information Systems, to include all GovGuam information systems hosted outside of the GovGuam Network (GGWAN).
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	ValidUSA	Draft Template
June 2021	OTECH Systems Support	Update policy
August 2021	CTO, DPM	Review draft, approve and disseminate

Introduction

The Office of Technology (OTECH) is responsible for safeguarding all GovGuam Information Systems. Security has to be considered at all stages of life cycle of an information system (i.e. feasibility, planning, development, implementation, maintenance, and retirement) in order to:

a. Ensure conformance with all appropriate security requirements,
b. Protect sensitive information throughout its life cycle,
c. Facilitate efficient implementation of security controls,
d. Prevent the introduction of new risks when the system is modified, and
e. Ensure proper removal of data when the system is retired.

This policy provides guidance to ensure that systems security is considered during the acquisition, development and maintenance and testing stages of an information system's life cycle.

Third-Party Security Control Requirements

The intention of this guideline is to provide security control requirements for all GovGuam Third-Party vendors and contractors who provide external information system services to GovGuam Agencies. These standards not only cover network services, but should also extend to the people, processes, and technology required by the hosted information system.

All providers of external information system services are required to comply with the following organizational information security requirements, and organization-defined security controls in accordance with applicable state and federal laws, Executive Orders, directives, polices, regulations, standards, and guidance.

Third-Party vendors and/or contractors, hereafter referred to as "Contractor", are required to submit quarterly security audit reports to ensure continued security control compliance as detailed in the requirements below.

1. The Solution should be hosted in a data center with a redundant data center not within the same geographic location or Availability Zone as that term is defined by Amazon Web Services.

2. Contractor's Solution shall provide standard audit log requirements as defined by NIST 800-53 and IRS 1075. These include but are not limited to logging the following actions:

    a. Start and Stop of a user session.
    b. User Login and Log out
    c. Session Timeout
    d. Account Lockout (and failed access attempts)
    e. Event Scheduling and Execution
    f. Data Queries
    g. Any authentication failure, node, user, or otherwise

10. Contractor will be responsible for ensuring:

    a. scheduled backups occur
    b. the integrity of the data backed up

c. restoration of the data, should it be needed
d. recovery from a disaster meets the specifications of the disaster recovery plan
e. retention of all system data and images for the life of this contract

11. Implementation of any enhancements, maintenance or updates, will occur first through the Development or QA environments, and once testing has cleared, promotion to production can occur. These item(s) and initial testing will be conducted by the Contractor. Once initial testing is complete, the Contractor will notify the appropriate IT Administrators/System Owners and the item(s) can be tested and verified by respective GovGuam Agency.
12. The system shall perform both syntactical and semantic input validations on all API calls and methods.
13. Contractor's validation code will whitelist only acceptable characters. The code will also limit the size of input to reasonable values for a respective field and convert it to a standard encoding scheme before filters are applied.
14. The system will protect against Open Web Application Security Project common web application vulnerabilities.
15. Contractor's applications will encrypt data at rest and in transit.
16. Contractor's application will log all authentication attempts including date/time, user-id and IP address; the log will include attempts/failures.
17. Contractor will require employees at time of hire and on an annual basis to sign a computer use policy. This policy reviews unauthorized, modification, destruction and disclosure of data.
18. Contractor will conduct quarterly internal network vulnerability scans and after changes to network configuration including but not limited to:
    a. installation of new equipment such as switches, routers and other network appliances
    b. firewall adjustments and upgrades
    c. Contractor will provide the results of the scans to OTECH within 14 business days of receiving the report of the scan and not more frequently than once quarterly, take immediate action to remediate any findings considered Critical or High and, within 10 business days of request provide OTECH with a Plan of Action and Milestones (POAM) to remediate or mitigate any remaining findings.
    d. Contractor will conduct internal penetration testing quarterly, provide the results to OTECH within 5 business days of receiving the report, and, within 10 business days of receipt of such report, provide OTECH with a Plan of Action and Milestones (POAM) to remediate or mitigate any findings.
    e. Contractor will test its incident response plan concurrently with its Business Continuity Test on an annual basis. All documentation will be updated at that time and approved by the executive committee. Upon request, the Contractor will supply the documentation to OTECH within 5 business days.

f. Contractor continuously monitors its network and applications using a combination of tools such as Intrusion Prevention Systems (IPS), Intrusion Detection Systems (IDS), as well as log aggregator's, indexers and reporting tools.

g. Contractor's system Solution will be meet the 99.9% uptime requirement, 24 x 7 x 365, except for agreed upon maintenance windows.

h. Contractor's Solution shall include backup functions for databases.

i. Contractor's Solution shall be guaranteed to be virus-, malware-, and backdoor-free at the time of delivery to the DMV. The Contractor will maintain the production, QA and development hosted environments.

j. Firewall in external connections

k. Anytime a network with confidential information is connected to the Internet or an un-trusted 3rd party, the network shall be protected by a firewall.

l. If critical information or service is stored or run on a file server, any web server used to provide an interface for accessing this information must be secure and separated from the file server by a firewall.

Secure Development Requirements & Security Assessment Standards

The scope of this requirement applies to all GovGuam development processes, internally or externally developed to include the application, as well as the supporting platform, and the infrastructure.

The security assessment will cover people, process, and technology as well as:

- security controls and control enhancements under assessment
- assessment procedures to be used to determine security control effectiveness
- assessment environment

Assessment Roles & Responsibilities

- Security assessment results are to be provided to the following individuals:
  - OTECH Chief Technology Officer (CTO)
  - System Owner
  - Respective IT Administrator

System/Software Development Life Cycle

This section defines the process(es) for the development, verification and validation of all software for the project.

The system/software development life cycle shall comprise of the following phases:

- System requirements analysis (software aspects only)
- System design Software requirements analysis
- Security requirements analysis

- Software design (Preliminary design and Detailed design)
- Implementation and Unit testing
- Integration and testing; CSCI testing.
- Security testing
- Integration testing
- System integration and testing (software aspects only).

Purpose

To define and analyze a complete set of functional, operational, performance, interface, quality factors, design, criticality, security configuration and test requirements for each software contained within an information system.

Documents

The following documentation shall be prepared

- Unit Test Report.
- Source code listing *(unless written exemption approved)*
- Software Test Procedure (preliminary)
- Security testing plan and results

The developer shall test the code using industry defined principles and methods. Test shall be performed according to the requirements contained in the 'Unit Test Description' and according to the 'Software Test Plan'.

A record of the unit testing shall be recorded in the Unit Test Report.

Documents to be prepared:

- Source Code listings *(unless written exemption approved)*
- Unit Test Report
- Software Test Procedure
- Code Walkthrough Report
- Internal evaluation to be performed:

Integration & Testing

During the Integration and testing phase, Software units of the software code shall be integrated and informal tests on aggregates of integrated Units shall be performed activities.

The developer shall integrate the software units into components and test them.

Test teams shall perform the testing and provide 'Problem/change reports' in accordance with the Software Testing Plan.

System Development Requirements

Software development processes are based upon industry standards, with security an integral part of the life cycle process.

1. Software components for each system must be documented, with a description of the functionality provided.
2. Software releases must be documented, with quality assurance testing of the code and appropriate testing prior to release.
3. Development and production environments must be kept separate.
4. Production data must not be used for testing or development.
5. Access to software source code is restricted to authorized personnel.
6. Software transferred from development and testing to production must be accomplished under dual control.
7. Prior to implementation into production, the developed software must be installed and quality tested in a test environment.
8. Testing should be conducted based upon both functionality and security impacts. These criteria must also be incorporated within the release process.
9. All discrepancies noted during functionality and security testing must be resolved and signed off by management prior to implementation/installation into the production system.
10. Software will restrict user access to those specific activities for which they have a need and are authorized to perform.
11. Security testing of internally or externally developed software must include verification that temporary code, hard-coded keys, and any suspicious code are removed.
12. Strict process and code review must be conducted to ensure that development keys or passwords used during audits, user acceptance tests or code reviews are not transferred to production.
13. For all computers and/or components utilized in the Data Transmission System, a comprehensive, documented inventory is maintained by device or machine.
14. Approval must be secured from the IT director if software beyond the standard desktop configuration is to be installed and/or used. All software installed on the network must be approved by the IT director.
15. Code changes must follow a documented change procedure.
    a. Submission of change requests only by authorized users
    b. Reviews to ensure controls and integrity procedures are not compromised by change
    c. Identification of all software, information, database entities and hardware involved in or impacted by change
16. Security review to minimize likelihood of known security weaknesses

17. System documentation updates
18. Version control for all software updates
19. Audit trail of all change requests
20. Operating documentation and user procedures changed as needed to remain current
21. Timing of change to prevent or minimize business impact
22. Layered security mechanisms must be in place to increase security as a whole

Technical review of application after operating platform changes

When operating platforms including operating systems, databases and middleware platforms are changed, business critical applications should be reviewed and tested to ensure there is no adverse impact on organizational operations or security. The following should also be considered:

- Notification of change with enough lead time to allow appropriate tests and reviews

Development environment

A secure development environment includes people, processes and technology associated with system development and integration. Risks associated with individual system development efforts should be assessed and secure development environments established with the following considerations:

- Sensitivity of data to be processed, stored and transmitted by the system
- Applicable external and internal requirements, e.g., from regulations or policies
- Security controls already implemented by Valid that support system development
- Trustworthiness of personnel working in the environment
- Need for development testing environments and the need for segregation between different development environments
- Strict control of access to development environment
- Monitoring of change to the environment and code stored therein
- Storage of backups, high availability and failover
- Control over movement of data to and from environments
- Non-repudiation

System security testing

Security functionality should be tested throughout the development process and should include a detailed schedule of activities and expected results under a range of conditions.

Application security testing must be completed before the application is exposed to the internet to include:

- Supporting platform security controls

- Infrastructure controls must align with NIST SP8800-53
- All applications are tested and validated against the OWASP Secure Coding Practices including but not limited to static code analysis tools (SAST)
- Automated systems can be used to test systems.
- Completed Security Assessment Report and plan of action for remediation

System acceptance testing

Acceptance testing and criteria should be established for new information systems, upgrades and new versions. The following should be considered:

- Testing of information security requirements
- Testing of received components and integrated systems
- Use of code analysis tools and vulnerability scans to verify remediation of security-related defects
- Use of test environment which ensures realistic approximation of the production environment without introducing vulnerabilities into the production environment

Software Security Risks

All security issues that are discovered during testing must be mitigated based upon the following risk levels. The Risk Levels are based on the OWASP Risk Rating Methodology. Remediation validation testing will be required to validate fix and/or mitigation strategies for any discovered issues of Medium risk level or greater:

- **High**: Any high-risk issue must be fixed immediately, or other mitigation strategies must be put in place to limit exposure before deployment. Applications with high-risk issues are subject to being taken off-line or denied release into the live environment.
- **Medium**: Medium risk issues should be reviewed to determine what is required to mitigate and scheduled accordingly. Applications with medium risk issues may be taken off-line or denied release into the live environment based on the number of issues and if multiple issues increase the risk to an unacceptable level. Issues should be fixed in a patch/point release unless other mitigation strategies will limit exposure.
- **Low**: Issue should be reviewed to determine what is required to correct the issue and scheduled accordingly.

Software Security Assessment Levels

- **Full**: A full assessment is comprised of tests for all known web application vulnerabilities using both automated and manual tools based on the OWASP Testing Guide. A full assessment will use manual penetration testing techniques to validate discovered vulnerabilities to determine the overall risk of any and all discovered.
- **Quick**: A quick assessment will consist of a (typically) automated scan of an application for the OWASP Top Ten web application security risks at a minimum.

- **Targeted**: A targeted assessment is performed to verify vulnerability remediation changes or new application functionality

Data Encryption

The following guidelines are provided to ensure proper and effective use of cryptography to protect the confidentiality, and integrity of information.

Policy on the use of encryption

Cryptography or the encryption of data communications, is an important tool for information security. All security controls take some commitment and effort to implement, and encryption is no exception. Media and transport encryption technologies exist to help facilitate employee compliance, along with all other applicable IT policies, procedures and guidance.

The Agency shall adhere to OTECH's Information Security Standards for the protection (which includes encryption) and handling of information in storage and transit.

When data is transmitted outside the boundary of the physically secure location, the data shall be immediately protected via encryption that complies with OTECH Security Standards.

Encryption shall not be required if the transmission media meets all of the following requirements:

1. The Agency owns, operates, manages, or protects the medium.
2. Medium terminates within physically secure locations at both ends with no interconnections between.
3. Physical access to the medium is solely controlled by the Agency.
4. Protection includes safeguards (e.g. acoustic, electric, electromagnetic, and physical) and if feasible countermeasures (e.g. alarms, notifications) to permit its use for the transmission of unencrypted information through an area of lesser classification or control.

All systems that store information with Medium/Moderate confidentiality impact level or higher, must be configured to use full-disk encryption technologies. (Refer to OTECH-POL-2021-003 Risk Assessment Policy and Procedures for more information regarding OTECH's confidentiality impact matrix.)

Key Management

The management of cryptographic keys is essential to the effective use of encryption. In all cases where encryption is used, cryptography and key management will comply with OTECH Security Standards. Secret and private keys require protection against unauthorized use as well as disclosure. Equipment used to generate, store and archive keys will be physically protected. Key management or escrow processes must be used when using a key-based data encryption system. In addition, encryption keys suspected of having been compromised must be replaced immediately.

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.