IT AUDIT & ACCOUNTABILITY POLICY

POLICY# OTECH-POL2021-001

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

OFFICE OF TECHNOLOGY
GOVERNMENT OF GUAM

AUGUST 27, 2021

Overview

Policy Number:	OTECH-POL2021-001
Title:	IT Audit and Accountability Policy
Purpose:	To provide guidance for the Audit and Accountability (AU) security controls 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 include 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
May 2021	OTECH Systems Support	Draft policy
Aug 2021	CTO, DPM	Review draft, approve and disseminate
January 2022 March 2022	OTECH System Support	Update AU-6 List of Inappropriate Activities Add Review & Internal Audit section
March 2022	CTO OTECH CTO, *Frank LG Lujan, Jr.* Date: March 30, 2022	Review and Approve policy updates for dissemination.
February 2024	OTECH Systems 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

The Office of Technology (OTECH) Information Technology (IT) Audit and Accountability (AU) policy services to be consistent with best practices associated with organizational Information Security management. It is the intention of this policy to establish audit and accountability guidelines to help the organization implement security best practices in regards to event and transaction logging.

Audit trails maintain a record of system activity both by system and application processes and provides a means to help accomplish several security-related objectives, including but not limited to: (1) establishing individual accountability; (2) detecting security violations and intrusions; (3) identifying flaws in system and applications; (4) performing problem analysis; and (5) assisting in incidentreconstruction.

OTECH encourages all Government of Guam (GovGuam) information systems to follow the guidelines in this AU policy.

Policy

OTECH has chosen to adopt the Audit and Accountability (AU) principles established in NIST SP 800-53 "Audit and Accountability Control Family guidelines." The following subsections outline the AU standards that constitute OTECH's policy.

AU-1: Audit and Accountability Policy and Procedures

OTECH develops, disseminates (via official posting on OTECH's website), and periodically reviews/updates formal, documented procedures to facilitate the implementation of audit and accountability policy and associated audit and accountability controls.

The OTECH Chief Technology Officer (CTO), in accordance with information system owners, must develop, document, and disseminate controls addressing the Audit and Accountability of information resources.

The CTO must review and update these controls as necessary.

AU-2: Audit Events

Information systems must provide the means whereby authorized personnel have the ability to audit and establish individual accountability for any action that can potentially cause access to, generation of, modification of, or affect the release of confidential information.

Appropriate audit trails must be maintained to provide accountability for updates to mission critical information, hardware and software for all changes to automated security or access rules.

Audit logs must be monitored and/or reviewed as risk management decision warrant. Audit reports must be reviewed for indications of intrusive activity.

Whenever technically possible, information systems should generate audit records for the following information system events:

a) User account management activities;
b) System shutdown/reboot/error(s);
c) Application shutdown/restart/error(s);
d) File creation/deletion/modification;
e) Failed and successful log-on(s);
f) Security policy modifications; and
g) Use of administrator privileges.

AU-3: Content of Audit Records

Audit records must contain sufficient information to, at a minimum, establish:

a) The type of event occurred;
b) The date and time the event occurred;
c) The location or device where the event occurred;
d) The source of the event;
e) The outcome (success or failure) of the event; and
f) The identity of any user/subject associated with the event.

AU-4: Audit Storage Capacity

Audit storage locations must be allocated in sufficient capacity and monitored to reduce the likelihood of such capacity being exceeded. It is important that relevant documents, records and events not be lost due to insufficient allocation of storage capacity.

AU-5: Response to Audit Processing

The information system should alert appropriate organizational officials in the event of an audit processing failure.

Information System Administrators should ensure that information resources are configured to automate alerts in the event of an audit failure, automate alerts once maximum storage capacity for audit lots is reached, and configure audit logs to overwrite the oldest logs first in cases of reaching capacity, if necessary.

The system owner must define the action to be taken upon log failure and must coordinate any Enterprise system alerting with OTECH and System Administrators.

AU-6: Audit Review, Analysis and Reporting

The System Owner and System Administrators maintain the responsibility of reviewing information audit logs on their systems for unusual activity on a periodic bases defined on a system by system basis, and should keep a log that such a review has taken place. System audit reviews should analyze records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, report findings to appropriate officials, and take necessary actions.

Type of auditable activity reports shall include, but are not limited to, the following:

1. Authentication and Authorization Reports – provides a main means of controlling access to systems and data. Login failures and successes, including attempts to disabled/service/non-existing/default/guest/suspended accounts can help identify a possible security breach.

    a. Multiple login failures
    b. Multiple login failures followed by success by same account
    c. Privileged account access (success, failure) including administrator accounts, root, su use, Run As use, or other system and platform relevant equivalents
    d. VPN authentication and other remote access logins (success, failure) including source IP address

2. Change Reports – identify critical security changes to systems and networked assets – configuration files, accounts, regulated and sensitive data or other components of system or application.
    a. Additions/changes/deletions to users, groups
    b. Additions of accounts to administrator/privileged groups
    c. Additions/changes/deletions to network services
    d. Changes to system files – binaries, configurations
    e. Changes to other key files
    f. Application installs, updates (success/failure) by system, application, or user

3. Network Activity Reports – can identify suspicious system or network activity.

    a. Outbound connections from internal and DMV systems by source and destination
    b. Internal systems listening on non-required ports such as deviation from baseline and least privilege
    c. VPN network activity by username, count of sessions
    d. Wireless network activity, including rogue Access Point (AP) detection and rogue AP association logs

4. Resource Access Reports – identify system, application and database resource access patterns and can be used for activity audit, trending, incident detection, reveal insider abuse/attack, or be useful for capacity planning.

    a. Top internal clients blocked by proxy from accessing prohibited sites, malware sources, etc.
    b. File, network share or resource access (success, failure)
    c. Top database users (to be useful for security activity it should exclude known application access to the database and ideally, a production database should have no direct access from users or developers)
    d. Privileged database user access and activity

e. Internal systems sending mail excluding known mail servers

5. Malware Activity Reports – identify malicious software and events.

   a. Malware detection trends with outcomes (cleaned or not)
   b. Detect-only events from anti-virus tools (not cleaned)
   c. Anti-virus protection failures
   d. Internal connection to known malware IP addresses (firewall or other detection against a public blacklist)

Auditable events and reporting needs may change as business needs or regulatory requirements change, as well as, when addressing improvements for incident identification and response procedures.

AU-7: Audit Reduction and Report Generation

The information system audit and reporting tools must not alter original audit records or log data. Original audit records must be protected from unauthorized access, modification, and deletion.

AU-8: Time Stamps

Whenever technically possible, information systems should provide time stamps for use in audit record generation. GovGuam systems should synchronize internal information system clocks, at least daily at system boot, to ensure that time stamps are accurate.

AU-9: Protection of Audit Information

The information system should protect audit information and audit tools from unauthorized access, modification, and deletion. Access must be restricted against unauthorized access and tampering. Access must be minimized to necessary to System Administrators and information security personnel.

AU-10: Non-Repudiation

The System Owner, in conjunction with the System Administrators, is responsible for ensuring that logging and audit settings are configured per system and program requirements. This ensures an audit trail for non-repudiation purposes.

AU-11: Audit Record Retention

The System Owner, in conjunction with the System Administrators, is responsible for ensuring that audit records are retained for a minimum of 180 days or if exceeded, as defined by the System Owner Retention Policy. Logs and records for known incidents and legal actions must be retained until the incident is closed.

AU-12: Audit Generation

The Information system should be capable of generating audit records from the list of auditable events specified in AU-2 for all information system components. These records must be available to authorized personnel for configuration of auditable events, as well as being capable of generating that required audit content as defined in AU-3 of this guide.

Roles & Responsibilities

Role	Responsibility
OTECH Chief Technology Officer (CTO)	• Overall responsibility in developing and maintaining an Enterprise Security Program. • Ensuring all GovGuam Agencies effectively implement and maintain information security policies and guidelines. • Overall responsibility for reviewing and updating this policy on an annual or as needed basis.
System Owners (Agency Heads)	• Overall responsibility to ensure that their system meets the base AU security control requirements. • Ensuring necessary AU security controls are in place and operating as intended. • Ensuring budget is defined to effectively implement the AU controls required. • Ensuring budget is defined to accommodate system retention policies.
System Administrators	• Ensuring the appropriate AU security requirements are implemented consistent with OTECH security policies and hardening guidelines. • Coordinate the establishment of auditing and monitoring procedures • Managing auditing and monitoring processes.

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.