1. Purpose

Establish policy for effectively managing and monitoring audit and accountability controls to ensure there are sufficient information system logs of actions performed to determine accountability.

2. Applicability

This policy is applicable to all State of Rhode Island Executive Branch Departments (including agencies, boards and commissions), and their employees (including permanent, non-permanent, full-time, and part-time) and interns, consultants, contractors, vendors, contracted individuals, and any entity having access to state information systems and data, whether operated or maintained by the state or on behalf of the state. For this policy, the term "agency" is used to refer to any department, agency, division, or unit of the Executive branch of the State of Rhode Island.

3. Definitions

**Auditable Event**
An observable occurrence identified for its significance and relevance to the security of the information system and environment in which it operates (e.g. user logins/logoffs, system administrator activities).

**Audit Reduction**
A process that manipulates and organizes audit record data to provide analysts with more useful and meaningful information within audit reports during reviews.

**Non-Repudiation**
Ensuring that a user or process cannot falsely deny having performed an action.

---

1 State of Rhode Island Executive Branch Departments does not include the University of Rhode Island, the State Colleges, the General Treasurer, the Attorney General, or the Secretary of State.
4. Procedures for Compliance

Security controls in this policy will be implemented in accordance with the security categorization of the information system. The security categorization is based on the Information Assurance Level (IAL) requirements of the information system.

**Low Risk Systems (IAL1)**
Information systems that only contain data that is public by law or directly available to the public via mechanisms such as the internet. In addition, desktops, laptops, and supporting systems used by agencies are Low Risk unless they store, process, transfer, or communicate private or sensitive data.

**Moderate Risk Systems (IAL2)**
Information systems that store, process, transfer, or communicate private or sensitive data or have a direct dependency on a Moderate system. At a minimum, any information system that stores, processes, transfers, or communicates PII or other sensitive data types is classified as a Moderate system.

4.1. **[IAL1, IAL2] Audit and Accountability Policy and Procedures (AU-1).** The agency will develop, document, disseminate, review, and annually update an audit and accountability policy and procedures.

4.2. **[IAL1, IAL2] Audit Events (AU-2).** The agency will audit audited events on an ongoing basis and coordinate the security audit function with other agencies, as appropriate, to enhance the audit function, improve system security, and reduce overall enterprise risk. The agency will determine that the information system is configured to audit the following events:

- Successful and failed authentication attempts.
- Logons and logoffs.
- Activities of privileged users (e.g. system and network administrators).
- Changes to user accounts, access permissions, and system/application configurations (i.e. create, modify, delete).
- Changes to security functions (e.g. disabling logging, password criteria).
- Changes to network configurations (e.g. routers, firewalls, switches, proxies, servers).
- System and application startups, shutdowns, restarts, reboots, and errors.
- Any event determined by the agency [after reviewing its business processes, compliance requirements, and information system capabilities] to be relevant to the security of the information system and required by its regulatory environment.

4.2.1. **[IAL2] Reviews and Updates (AU-2.3).** The agency will review and update the list of auditable events annually.

4.3. **[IAL1, IAL2] Content of Audit Records (AU-3).** The information system will generate audit records containing the following information:
Division of Information Technology

- Event type and description.
- Date and time the event occurred (time stamp).
- Source, destination, and outcome of the event.
- Identity of the user associated with the event.

4.3.1. [IAL2] Additional Audit Information (AU-3.1). The information system will generate audit records containing additional detailed information the agency has identified as requiring additional auditing and deems critical to reconstructing the chronological order of activities leading to the event (e.g. provide non-repudiation of all actions performed or full text of privileged commands entered on the information system).

4.4. [IAL1, IAL2] Audit Storage Capacity (AU-4). The agency will allocate adequate audit record storage capacity necessary to maintain the logs of all auditable records.

4.5. [IAL1, IAL2] Response to Audit Processing Failures (AU-5). The agency will develop procedures for handling audit processing failures that are appropriate for the information system and its business process. The information system will automatically alert designated personnel (e.g. system administrators) in the event of an audit processing failure. Alerts will be distributed via a method that ensures designated personnel receive the alerts both on and off hours (e.g. phone call, text message, email). At a minimum, alerts will be sent to designated personnel when the following audit processing failures occur:
- Auditable events are not being logged.
- Audit records are being overwritten.
- Audit record storage capacity utilization reaches 75%, 90%, and 100%. The information system will overwrite the oldest audit records or shut down, as appropriate, when maximum audit record storage capacity is reached.

4.6. [IAL1, IAL2] Audit Review, Analysis, and Reporting (AU-6). The agency should review applicable federal and state laws, regulations, mandates, and compliance requirements to determine an appropriate audit record review timeframe. In the absence of a formal requirement, the agency will review audit records for indications of inappropriate, unusual, or suspicious activity:
- As close to real-time as possible, for system and application errors and alerts. Errors and alerts for IAL2 moderate risk information systems take precedence over IAL1 low risk information systems.
- Weekly, for FTI related audit records.
- Monthly, for IAL2 moderate risk information systems.
- Quarterly, for IAL1 low risk information systems.

Actual or suspected security incidents will be promptly reported to appropriate personnel and handled in accordance with ETSS Policy 10-12 (Incident Handling and Response).
4.6.1. [IAL2] Process Integration (AU-6.1). The agency will employ automated mechanisms to integrate the audit review, analysis, and reporting processes into incident response, continuous monitoring, and contingency planning activities to support agency processes for investigation and response to suspicious activities.

4.6.2. [IAL2] Correlate Audit Repositories (AU-6.3). The agency will analyze and correlate audit records across different log repositories to gain insight into agency and enterprise-wide risk management and situational awareness. The agency should contact DoIT to leverage, where possible, the Enterprise Security Incident and Event Management (SIEM) solution to assist in correlating and analyzing audit repositories.

4.7. [IAL2] Audit Reduction and Report Generation (AU-7). Audit reduction is a process that manipulates collected audit information and organizes this information in a summary format that is more meaningful to analysts. Audit reduction capabilities include modern data mining techniques with advanced filters to identify anomalous behavior within audit records. The information system will provide an audit reduction and report generation capability that supports on-demand audit review, analysis, reporting, and after-the-fact investigations of security incidents and does not alter the contents or time ordering of audit records.

4.7.1. [IAL2] Automatic Processing (AU-7.1). The information system provides the capability to automatically process audit records for events of interest based on audit fields within audit records.

4.8. [IAL1, IAL2] Time Stamps (AU-8). The information system will use synchronized internal system clocks to generate audit record time stamps expressed in local time with an offset from Coordinated Universal Time (UTC). If possible, information systems should synchronize internal system clocks to a centralized Enterprise Network Time Protocol (NTP) time server.

4.8.1. [IAL2] Synchronization with Authoritative Time Source (AU-8.1). The information system will compare internal system clocks to a National Institute of Standards and Technology (NIST) NTP time server and synchronize with the NIST NTP time server when the difference is greater than 100 milliseconds.

4.9. [IAL1, IAL2] Protection of Audit Information (AU-9). The information system will protect audit information (e.g. audit records, settings, reports) and audit tools from unauthorized modification, access, and destruction. Cryptographic mechanisms are implemented to protect the integrity of audit information and audit tools. Audit records will be read-only and not modified or deleted at any time prior to the end of the retention period. Audit records will be backed up on a system other than the one being audited. Audit records that contain sensitive or confidential data, including FTI, will be encrypted in accordance with ETSS Data Encryption Policy 05-03.
4.9.1. [IAL2] Access by Subset of Privileged Users (AU-9.4). The agency will authorize access to manage audit functionality only to designated privileged users (e.g. security administrators). System and network administrators will not have the ability to modify or delete log entries. Separation of duties will be enforced such that personnel who administer the access control function are different than those who administer or have access to audit record data. Audit record repositories and backup log archives will be accessible only to authorized personnel and be protected from breaches of confidentiality or integrity.

4.10. [IAL1, IAL2] Audit Record Retention (AU-11). The agency will retain audit records in accordance with all applicable federal and state laws, regulations, mandates, and compliance requirements. FTI related audit records will be retained for seven (7) years. In the absence of any documented retention requirements, audit records will be retained for a minimum of six (6) months. For information regarding information system record retention schedules, see State of Rhode Island Department of State General Record Schedule GRS7 (http://www.sos.ri.gov/assets/downloads/documents/GSR7-information-management-records.pdf).

4.11. [IAL1, IAL2] Audit Generation (AU-12). The information system will generate audit records for the auditable events defined in section 4.2 (AU-2) of this policy that contain the content defined in section 4.3 (AU-3) of this policy for all relevant information system components including, but not limited to, desktops and laptops (end-users), network devices (e.g. routers, switches, firewalls, intrusion detection), and servers (e.g. file, print, web, terminal).

5. Approval / Review Signature:

Brian Tardiff
Digitally signed by Brian Tardiff
Date: 2020.09.14 08:57:57 -04'00'

Chief Information Security Officer