DEPARTMENT OF ADMINISTRATION
Enterprise Policy

DOIT-10-13-2014

DIVISION OF INFORMATION TECHNOLOGY

Audit and Accountability Policy

Date of Last Revision 07/31/2014

Bijay Kumar
(401) 574-9220
bijay.kumar@doit.ri.gov

1. **Background**
   a. Organizations require a means of examining the actions of users with legitimate access authorization to IT system resources, assessing individual accountability, reconstructing events, detecting system intrusions, and identifying problems that do not trigger alerts. Various State and Federal laws, regulations, executive orders, and mandates require that organizations establish and maintain an effective audit function, especially with regard to sensitive information systems and confidential data. The ability to assess system actions and assign accountability to specific users is critical to maintain overall information system security.
2. **Purpose**
   a. To determine user accountability and maintain system security by ensuring there is adequate tracking of all logical access and system configuration changes to State of Rhode Island information resources.
3. **Scope**
   a. This policy covers all State Executive Branch Departments 1 (including agencies, boards and commissions), and its and their employees, whether permanent, non-permanent, full or part-time, and interns as well as all individuals including, but not limited to, employees, whether permanent, non-permanent, full or part-time, interns, and all consultants, contractors, vendors, contracted individuals, and any entity with access to State data or computers and systems operated by the State or maintained on behalf of the State.
4. **Authority**
   a. Executive Order 04-06 established the Division of Information Technology (DoIT) within the Department of Administration to improve the efficiency, effectiveness, and security of IT management and operations within the Executive branch of the State of Rhode Island. The Do IT Chief Information Officer (CIO) is authorized, directed, and responsible for the oversight, coordination, and development of all IT resources within the Executive branch. DoIT will define, maintain, and enforce State-wide IT related policies, standards, and procedures for the effective use and security of these resources.
5. **Definitions**

a. **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).

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

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

6. **Standards**

a. **Auditable Events.** Auditable events should be relevant to the security of information systems and the environments in which they operate. A balance must be struck between business needs, compliance requirements, and information system performance capabilities.

(i.) At a minimum, information system audit logs will capture the following auditable events:

1. Successful and failed authentication attempts.
2. Logons and logoffs.
3. Activities of privileged users (e.g. system and network administrators).
4. Changes (i.e. creation/modification/deletion) to user accounts, access permissions, and system/application configurations.
5. Modifications to security functions (e.g. disabling logging, password criteria).
6. System/ Application startups, shutdowns, restarts, reboots, and errors.
7. Network configuration changes (e.g. routers, firewalls, switches, proxies, servers).

(ii.) In addition to those listed above, Agencies that process FTI will log the following events:

1. Any changes with the potential to compromise the integrity of audit policy configurations and audit trail generation services.
2. Command line changes, batch file changes, and system queries.

(iii.) Auditable events will be logged for the following information system components:

1. Desktops and laptops (end-users).
2. Network devices (e.g. routers, switches, firewalls, intrusion detection).
3. Servers (e.g. file, print, web, terminal).

(iv.) Any event not specifically specified here, but that is required by federal or State law, regulation, or other mandate, must be logged in accordance with the federal or State law, regulation, or other mandate. Agency management is responsible for identifying these events and ensuring they're properly logged.

(v.) Monitoring devices will be employed strategically to collect pre-determined essential information and to record specific types of transactions of interest to the Agency. In case there is an indication of an increased risk to State of Rhode Island assets, operations and/or environment, the level of monitoring activity will be increased.

b. Audit Records. Adequate controls should be in place to assure, with a high level of confidence, the non-repudiation of actions performed on the system. Audit records should provide sufficient information to enable the creation of the chronological order of activities leading to an auditable event. Meeting this requirement may differ depending on a number of variables, such as the audit logging capability of the information system, business processing requirements, security, costs, and compliance requirements. At a minimum, however, all audit records will contain the following information:

(i.) Event type and description

(ii.) Time stamp (date and time) indicating when the event occurred.

(iii.) Event source, destination, and outcome.

(iv.) Identity of user generating the event.

(v.) Any other information that is deemed critical to reconstructing the chronological order of activities leading to the event (e.g. software/hardware, process, filename).

c. Audit Storage Capacity. Information system audit record repositories will have sufficient storage capacity to ensure that all auditable events are logged. Determining audit storage capacity depends on various factors, such as business processing and compliance requirements, the types of events being logged, costs, user base, the sensitivity of the information system/data, etc. System owners are responsible for allocating sufficient disk space for proper audit log retention.

d. Audit Processing Failures. In the event of an audit processing failure, information systems could, for example, shutdown, stop generating audit records, or overwrite the oldest records. System and data owners are responsible for developing procedures for handling audit processing failures that are appropriate for their information systems and data.

(i.) Information systems will automatically send an alert to designated personnel when:

1. Auditable events are not being logged.

2. The generation of audit reports has stopped.

3. Audit records are being overwritten.

4. Audit storage capacity utilization is at 75%, 90%, and 100%.

(ii.) Alerts will be distributed via a mechanism(s) that ensures designated personnel receive them, both on and off hours (e.g. email, text message).

(iii.) When audit storage capacity is reached and no other storage media is available, the oldest audit records will be overwritten to ensure the most current audit

records are saved. Information systems will immediately alert designated personnel whenever this occurs.

e. **Reviews.** Audit logs should be analyzed for to assess indications of inappropriate and unusual activity and to provide assurance that the logging function is performing properly. In order to be able to identify unusual activity, reviewers must first understand and recognize normal activity. Reviews should correlate logs between different systems to obtain a more granular view of the interactions between Agency information systems and network devices.

   (i.) Audit logs will be periodically reviewed for indications of inappropriate or suspicious activity in accordance with all applicable Federal and State laws, regulations, Executive Orders, compliance mandates, and any other requirements. The timeframe between reviews depends on the sensitivity of the system, data, applicable compliance requirements, and a number of other factors specific to the Agency or unique business process. The Agency is responsible for determining this timeframe. In the absence of any applicable and/or documented requirements, audit logs will be reviewed:

   1. At least quarterly for critical or sensitive information systems.

   2. At least semiannually (every 6 months) for non-sensitive or non-critical information systems.

   3. System and application alerts and errors will be reviewed as close to real-time as possible. Alerts and errors for sensitive information systems take precedent over non-sensitive systems.

   (ii.) Any actual/suspected incident or suspicious activity resulting from the review or continuous monitoring activities will be handled in accordance with DoIT's Incident Handling and Response Policy for more information. Follow-up reviews may be necessary depending on the type of security incident.

   (iii.) Reviews will be formally documented to ensure there is a record of the review being performed.

f. **Audit Reduction and Report Generation.** Audit logs should be reduced to save storage space and provide useful information within the audit report and for the review process.

   (i.) Information systems will have the capability of generating audit reports based on selectable criteria (i.e. ad hoc) for near real-time or after-the-fact analysis.

   (ii.) Reviews will be easier if automated tools and information system audit reduction and report generation capabilities are used that support on-demand, ad hoc, customizable, and after-the-fact analysis of security incidents. Automated audit analysis tools improve the effectiveness of audit log reviews and increase the likelihood that they are performed on a timely and periodic basis. Automated tools should be used whenever possible to:

   1. Detect intrusions based attack signatures, variance techniques, audit reduction methodologies, etc.

2. Generate audit reports by distilling relevant information from raw data contained within audit logs.

g. **Time Stamps.** Information systems will use synchronized internal system clocks to generate audit record time stamps. If possible, information systems should use a centralized timeserver for network time protocol (NTP) time synchronization.

h. **Securing Audit Information.** Audit information, including audit tools, records, settings, and reports, will be protected from unauthorized access, modification, and deletion.

(i.) Separation of duties will be enforced such that personnel who administer the access control function are not the same as those who administer or have access to the audit log data.

(ii.) Audit logs that contain federal tax information and other sensitive or confidential data will be encrypted at all times.

(iii.) Audit logs will be read-only and not be modified or. deleted by anyone at any time prior to the end of the retention period.

(iv.) The audit log repository and backup log archives will be accessible only to authorized personnel and be protected from breaches of confidentiality and integrity.

i. **Retention.** Audit logs will be retained in accordance with all applicable Federal and State laws, regulations, Executive Orders, mandates, and compliance requirements. If the absence of documented retention requirements, audit logs will be retained for a minimum of six (6) months.

j. **Standards Reviews.** These standards will be reviewed annually and updated as required.

k. **Noncompliance.** Any employee who willfully violates these standards shall be subject to disciplinary action up to and including termination of employment.

l. **Waivers.** The Agency may request a waiver from these standards by formally submitting justification for the waiver and demonstrating that compensating controls are in place to mitigate the risk. If approved, the Agency Director must accept in writing all risk to IT system resources and data associated with the waiver. Waivers require approval from and are granted solely by the DoIT Chief Information Officer. Waivers expire one year from date of issue, whereupon they must be renewed.

7. **Roles and Responsibility**

a. Enterprise Information Security Office

(i.) Periodically review and update these standards, as required.

(ii.) Periodically perform audit and accountability security assessments of Agency information systems to ensure compliance with these standards.

(iii.) Identify and document auditable events required by every Agency information system.

b. Agency

(i.) Comply with provisions documented in these standards.

(ii.) Develop procedures for handling audit processing failures appropriate for the information system.

(iii.) Identify and document auditable events specific to the information system and not identified by the Enterprise Information Security Office but that are required by Federal or State laws, regulations, Executive Orders, compliance mandates, or other requirements.

(iv.) Periodically review audit records.

8. Signatures

Chief Information Officer, DoIT	7/31/14 Date
Chief Information Security Officer, DoIT	7/30/14 Date