Audit & Accountability Policy

Approved Date – 02/22/2021
Published Date – 02/22/2021
Review Date – 03/01/2024

1. Purpose

Specify the requirements for establishing event logging and transaction monitoring controls on all the District of Columbia Government (District) owned information systems.

2. Authority

DC Official Code § 1-1401 et seq., provides the Office of the Chief Technology Officer (OCTO) with the authority to provide information technology (IT) services, write and enforce IT policies, and secure the network and IT systems for the District government. This document can be found at: *https://code.dccouncil.us/dc/council/code/sections/1-1402*.

3. Applicability

This policy applies to all District workforce members (including contractors, vendors, consultants, temporary staff, interns, and volunteers) performing official functions on behalf of the District, and/or any District agency or entity (e.g. subordinate and independent agencies, Council of the District of Columbia, D.C. Charter Schools, etc.) who receive enterprise services from OCTO. In addition, this policy applies to any provider or third-party entity with access to District information, networks, and applications.

4. Policy

District agencies and departments must develop or adhere to a strategy which demonstrates compliance with this policy and its related standards. The following outlines the requirements for this policy. The District's agencies must develop and review or update annually and after changes to the policy, a procedure in support of this policy with the following requirements.

4.1. Event Logging

District Agencies must:

4.1.1. Determine that the information system can log the following events for ease of system audit annually or as needed:

- Server startup and shutdown
- Starting and stopping of audit functions
- Loading and unloading of services
- Installation and removal of software
- System alerts and error messages

- Application alerts and error messages
- Modifications to the application
- User logon and logoff
- System administration activities, such as the Windows “Run As” or Linux “su” or “sudo” usage
- Accesses to information, files, and systems
- Account creation, modification, or deletion
- Password changes
- Modifications of access controls, such as change of file or user permissions or privileges (e.g., use of suid/guid, chown, su)
- Additional security-related events, as required by the system owner or to support the nature of the supported business and applications
- Clearing of the audit log file
- Remote access outside of the agency network communication channels (e.g., modems, dedicated VPN) and all dial-in access to the system
- Changes made to an application or database by a batch file
- Application-critical record changes
- Changes to database or application records, where the application has been bypassed to produce the change (via a file or other database utility)
- All system and data interactions concerning the District sensitive data

4.1.2. Coordinate the event logging function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection criteria for events to be logged.

4.1.3. Provide a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents.

4.1.4. Conduct annual review and update of the event types selected for logging.

4.2. Content of Audit Records

The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

4.3. Content of Audit Records | Additional Audit Information

The information system generates audit records containing the following additional information:

4.3.1. Date and time when the event occurred.

4.3.2. Software/hardware component of the information system where the event occurred.

4.3.3. Source and destination network addresses

4.3.4. Source and destination port or protocol identifiers

4.3.5. Type of event that occurred

4.3.6. Subject identity (e.g., user, device, process context)

4.3.7. The outcome (i.e., success or failure) of the event

4.3.8. Security-relevant actions associated with processing.

4.4. Content of Audit Records | Limit Personally Identifiable Information Elements

The information system-generated audit records must only include PII that is needed for operational purposes only.

4.5. Audit Log Storage Capacity

District agencies must allocate a minimum audit record storage capacity retention period of at least one year for non-critical systems. Agencies may elect to lengthen this retention period as determined appropriate, in order to support after-the-fact investigations of security incidents and to meet any regulatory or system-specific retention schedule requirements.

4.6. Response to Audit Logging Process Failures

District Agencies must:

4.6.1. Alert the agency CIO in the event of an audit processing failure.

4.6.2. Take the following additional actions:

- Overwrite oldest audit logs once maximum capacity is reached
- Automatically shut down information systems to eliminate the chance of an incident
- Must implement secondary audit record duplication mechanism to prevent loss of logs

4.7. Audit Record Review, Analysis, and Reporting

District agencies must:

4.7.1. Review and analyze information system audit records weekly for indications of abnormalities or discrepancies.

4.7.2. Report findings to agency management and escalate to OCTO City-Wide Information Technology Security (CWITS) if the issue cannot be resolved at the agency level.

4.8. Time Stamps

District agencies must:

4.8.1. Use internal system clocks to generate timestamps for audit records.

4.8.2. Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT).

4.9. Protection of Audit Information

District agencies protect audit information and audit tools from unauthorized access, modification, and deletion.

4.10. Protection of Audit Information | Access by Subset of Privileged Users

District agencies must authorize access to management of audit functionality to only agency defined subset of privileged users. Individuals with privileged access to an information system and who are also the subject of an audit by that system may affect the reliability of audit information by inhibiting audit activities or modifying audit records.

District agencies must authorize access to manage audit functionality only to designated security administrator(s) or staff other than the system and network administrator. System and network administrators must not have the ability to modify or delete audit log entries.

4.11. Audit Record Retention

District agencies shall retain audit records for seven (7) years to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

4.12. Audit Generation

District agencies must:

4.12.1. Provides audit record generation capability for the auditable events for the following information systems components:

- Servers, laptops, and desktops.
- Network Components (e.g., Switches, Routers)

4.12.2. Allow the designated security administrator(s) or staff to select which auditable events are to be audited by specific components of the information system.

5. Exemptions

Exceptions to this policy shall be requested in writing to the Agency's CIO and the request will be escalated to the Chief Information Security Officer (CISO).

6. Definitions

The definition of the terms used in this document can be found on the *Policy Definitions website*.