Audit Log Management Standard

Purpose

Audit log management includes generating, storing, and analyzing logs files in order to identify and respond to suspicious or anomalous events occurring within the District, prioritizing, and remediating vulnerabilities in District systems and software. The *Audit Log Management Standard* provides the processes and procedures for ensuring logs are created and properly analyzed. This standard applies to all departments and all assets connected to the District network.

Responsibility

The Information Technology (IT) business unit is responsible for all log management functions. Specifically, administrators are responsible for configuring the correct devices to generate, store, and transmit logs. IT is responsible for informing all users of their responsibilities in the use of any assets assigned to them, such as applying updates in a regular manner or restarting their systems. All District technology assets are required to comply with the audit logging procedures.

Exceptions

Exceptions to this policy are likely to occur. Requests for exception must be made in writing and must contain:

- The reason for the request,
- Risk to the District of not following the written policy,
- Specific mitigations that will not be implemented,
- Technical and other difficulties, and
- Date of review.

Policy

Generation

1. A District-wide strategy must be developed to establish and maintain an audit log process.
    a. This strategy must be documented.
    b. Documentation must be updated annually, or when significant changes have occurred.
    c. The contents of logs must be specified within the Secure Configuration Standard.
2. Audit logging must be enabled on all District assets, as is practical.
3. Audit logs must not be disabled on District assets.

Transmission

1. Procedures must be developed to move logs from District assets to an audit log datastore.
    a. This may be done manually or via electronic means.
2. Access controls must be used to prevent audit logs from being modified in an unauthorized manner.

Storage

1. Procedures must be developed to collect audit logs from District assets.

2. Sufficient storage space must be allocated for audit logs for the period of time required for analysis and retention.
    a. Sufficient space must be allocated to store audit logs on all District assets.
    b. Sufficient space must be allocated to store audit logs on any centralized audit log datastore.
3. Retention timeframes for audit logs should be in accordance with the District data management process.

Review and Analysis

1. All high severity events must be acted upon in accordance with the audit log management process.

Disposal

1. All audit logs must be stored for a period of time specified by the audit log management process.
2. Archived logs must be available for analysis.
3. Disposal of audit logs should be in accordance with the District data management process.

Alert

There are no IG1 safeguards that support this portion of the audit log management process.

Revision History

Each time this document is updated, this table should be updated.
.

Version	Revision Date	Revision Description	Name
V1.0	01/02/2023	Initial Written Standard	Scott Tisinger