Information Security Audit Trail Monitoring and Reporting Policy

Policy Number:	Creation Date/Revisions:	Effective Date:
OCTO003.310	11/01/04 Rev 3.0	02/02/04

1. Purpose

This document is intended to outline the minimum requirements necessary to accurately track, record, and report computer system access and usage throughout the District of Columbia's computer network. This standard ensures systems access and data use is sufficient for the following purposes:

- Proper system functionality
- District system user accountability
- Aid investigation into improper transactions or impropriety that may lead to personnel or legal actions
- Monitoring District agency compliance in meeting regulatory requirements

2. Details

All District government computer systems must use auditing systems to monitor usage and to detect security breaches. This applies to all computer systems and applicable components such as mainframes, distributed systems, LAN/WAN, routers, firewalls, applications, etc.

The monitoring of events, usage, output, and the management of activity records must be consistent across platforms in order to mitigate threats associated with authorized access and unauthorized intrusions. Data must be collected in a common format. Analysis of the data must be able to reconstruct transactions and processing. This includes recording data to trace changes to the access rules and attributes of the audit system itself.

To ensure the integrity of the audit trails, all audit trail files must be protected, controlled, and backed up on a bi-weekly basis. Audit trail logs will be maintained for a period of 90 days, or longer if the situation warrants, i.e., for investigations, and legal proceedings. Passwords used to control access to information systems must be encrypted within the audit trail.

2.1 Audit Security Measures

The following security measures must be implemented and maintained for all District government Information Systems:

2.1.1 Audit Controls

- Enable audit and event logging of data to provide a traceable basis for tracking the overall effectiveness of processes.
- All systems will generate an electronic audit trail that records access to the system and relevant security events as defined in section 2.1.2. Major applications will provide a

mechanism to trace transactions from start to finish, including all critical processing actions.

- Audit trails will be regularly (at least bi-weekly) backed up and retained for at least 90 days. If circumstances dictate, i.e., for investigations or legal proceedings, the retention period may be extended indefinitely.

2.1.2 Data Recording

Systems will cause a record to be written to the security audit trail for each of the following events:

- Successful logons
- Failed user authentication attempts
- Resource access attempts that are denied by the resource access control mechanism
- Attempts, both successful and unsuccessful, to obtain privilege
- Activities that require privilege (particularly deleting and altering)
- Access (read, write, and/or delete) to highly sensitive data, as defined in the Office of the Chief Technology Officer (OCTO) Data Sensitivity Standard
- Access to security-critical resources
- Changes to user's security information
- Changes to the set of privileges associated with a user
- Changes to access rights to resources
- Changes to the system security configuration
- Modifications of system supplied software, where applicable

2.1.3 Data Reporting and Evaluation

- The system will provide a mechanism for reporting security events and alarms.
- Metrics data will be recorded and made available to Citywide Information Technology Security (CWITS) personnel for evaluation in order to validate the effectiveness of security controls as well as identify weaknesses.
- Data in the form of daily reports will be generated from Mainframe, LAN, WAN and distributed systems audit logs for analysis of risks.
- Audit trail data will be evaluated at least on a weekly basis to identify anomalies and possible incidents.

2.1.4 Escalation

- When a probable security incident is identified through the audit trail review/evaluation, the person discovering the incident must notify an appropriate

supervisor, or other appropriate authority, including the District Computer Emergency Response Team (DCERT). This reporting responsibility includes OCTO and the Office of the Inspector General.

- An emergency response process will be invoked by the DCERT Team and other authorities for security incidents that appear suspicious, or have a high probability of impacting multiple areas or causing a critical outage.

3. Statutory Authority

- District Law 5-168, Section 4, 32 DCR 721
- District Law 11-259, Section 305(a), 44 DCR 1423
- District Code Section 1-1135, b, (6)
- District Law 12-175. Act 12-239

4. Scope

This standard applies to all agency employees, contractors and volunteers of the District of Columbia government, including the following users:

- Full or part-time employees
- Contractors who are authorized to use District government-owned equipment or facilities
- Volunteers who are authorized to use District government resources and who have been provided with a user account

The District government reserves the right to use all its authority to identify and discipline persons who misuse District government information systems.

5. Exemptions

None. OCTO will consider granting exceptions on a case-by-case basis if requested in writing by the head of an agency.

6. Roles and Responsibilities

6.1 Office of the Chief Technology Officer

- Interpretation, implementation, publication and enforcement of this standard

6.2 Director of Citywide Information Technology Security Program

- Establish and enforce the guidelines of this standard
- Assist agencies with implementing this standard

- Evaluate agency compliance with this standard
- Monitor, analyze and respond to reported incidents

6.3 Agency Directors

- Ensure agency compliance with provisions of this standard
- Establish local procedures to satisfy the requirements of this standard
- Ensure all incidents are reported to appropriate authorities

7. Related Policies and Supporting Documentation

- OCTO Information Security Policy, 07/31/01
- Government Accounting Office (GAO), Executive Guide, Information Security Management, May 1998 (GAO/AIMD-98-68)