

DHHS POLICIES AND PROCEDURES

Section VIII:	Privacy and Security
Title:	Security Manual
Chapter:	Information Systems Review and Auditing Policy
Current Effective Date:	6/15/05
Revision History:	
Original Effective Date:	

Purpose

To establish review and audit requirements for all the Department of Health and Human Services (DHHS) critical and sensitive systems/applications and to ensure compliance with DHHS policies, and federal and state regulations.

Policy

DHHS shall ensure that all critical and sensitive systems/applications and the related infrastructure shall be evaluated as an ongoing process to improve the quality of its operations. This policy shall apply to all DHHS Divisions/Offices.

Roles and Responsibilities

The DHHS Divisions/Offices are responsible for ensuring that business is conducted in a safe, secure manner. Program managers and their Information Technology Services (ITS) Security/ITS counterparts share in the responsibilities of determining the controls necessary to protect information in the workflow.

DHHS is the owner of all information technology resources, including data. The system owner is the manager or agent responsible for the business use of the information, i.e., the individual or individuals upon whom the responsibility rests for carrying out the program that uses the resources. Ownership may be shared by division directors, deputy/assistant directors, and/or managers of various sections or offices within a division/office, as appropriate.

System owners are responsible for determining the sensitivity of data and ensuring that adequate controls are implemented to protect the data. Typically, the security controls used shall be determined in consultation with technical support staff, the DHHS Privacy and Security Office (PSO), and the DHHS Division/Office Information Security Official. Individuals that typically are part of the determination are application owners, system administrators, data processing function managers, and computer security managers. For some divisions/offices, such technical expertise may be provided in association or affiliation with or through written agreement or contract with other DHHS Divisions/Offices or vendors.

The DHHS PSO shall provide security audit guidelines and self-assessment checklists for the DHHS Divisions/Offices.

Implementation

The Information Systems (IS) review and auditing process can be performed at several levels within an organization. Application/system administrators may perform self-assessments or checks on a regularly scheduled basis. This type of review typically focuses on a specific system or application and may employ audit functionality. Another level of review is the IS review which is typically broad enough to include network and IT operations activities. This review should follow the DHHS security audit guidelines provided by the DHHS PSO. The independent audit is typically a formal audit conducted by the DHHS Office of Internal Audit, the DHHS Office of the State Auditor or a contracted vendor.

The implementation of this policy shall be based upon and guided by the use of management-approved security standards and best practices provided by the DHHS PSO. The following paragraphs specify the information systems auditing policy requirements:

1. **Self-Assessments**
The DHHS PSO shall develop and maintain a set of security auditing tools for the DHHS Divisions/Offices. These tools will enable the DHHS Divisions/Offices to conduct periodic security self-assessments.
2. **Information System Activity Reviews**
In addition to application or system-level audits, information system activity reviews shall be conducted or facilitated by the DHHS PSO on a periodic basis.
3. **IS Review or Audit Process**
An IS review or audit process shall be implemented to evaluate information systems. These audits or reviews may address physical security, ITS operations security, network security, and Business Continuity and Disaster Recovery. Audit findings shall be documented, properly communicated to the organization, and retained for future reference.

Formal or independent audits may identify problems. The audit findings shall be presented to the responsible DHHS Division/Office manager. The DHHS PSO shall be given a copy of all audit findings. A written response (from the DHHS Division/Office Manager) to the audit findings will be required within 30 days from the report issue date or by the date specified by the auditor, whichever is less. The PSO shall provide assistance in formulating a response. This response shall describe the activities planned by the division/office to rectify problems identified in the audit findings report. The PSO may validate the successful implementation of the corrective action outlined in the response plan.

4. Audit/Review Frequency

All DHHS critical applications and systems shall be audited/reviewed after being placed into production. The audit frequency shall be on a periodic basis. Assessment and operational reviews shall be conducted based upon the criticality and risk level of the application.

5. Automated Audit Control Functionality

All systems that process sensitive information or which are considered critical to DHHS shall provide for automated audit control functionality. The audit control mechanism shall include the following functionality:

- A. Provide the ability to record the start-up and shutdown of each audit;
- B. Capture within each audit record the date and time of the event, type of event, subject identity, objective identity, and the outcome (success or failure) of the event;
- C. Apply a set of rules in monitoring the audited events and, based upon these rules, indicate a potential violation;
- D. Prohibit access to the audit records by all unauthorized users, and to prevent unauthorized deletion or modification of the records;
- E. Create the audit records in a manner suitable for a user to interpret the information;
- F. Provide the ability to perform searches of audit databases on criteria with logical relationships;
- G. Include or exclude auditable events from a set of defined audited events;
- H. Ensure that audit records will be maintained when audit storage is full or an attack has occurred; and
- I. Ensure that those privileged users who have a role as administrator of a network device, operating system, or security software such as a firewall, Intrusion Detection System, etc., will have all events logged.

6. System Audit Logging

The automated audit process shall produce audit logs. All log data must be classified as sensitive and handled accordingly. These logs must be retrievable through clearly defined procedures and must be maintained for time periods prescribed for audit, legal, and recovery purposes. Logging shall occur at the network, operating system and application level.

System administrators and database administrators must review audit logs to the extent necessary to detect potential security incidents and security breaches.

7. Fault Logging

Faults should be reported and corrective action taken. All hardware or software problems should be logged in order to assist maintenance personnel. If problems persist, a review should also be conducted to ensure that controls have not been bypassed and the system compromised, i.e., unauthorized access to information.

8. Audit Trail Documentation

The audit trail shall include sufficient information to establish what events occurred and who (or what) caused them. Defining the scope and contents of the audit trail information captured will be done carefully to balance security needs with possible performance, privacy, or other costs. In general, an activity event record specification will include: event type, time of event occurrence, user ID associated with the event, program or command used to initiate the event, sensitive data accessed and/or modified, and additional data necessary to investigate and mitigate the event.

9. Access to Audit Logs and Audit Trail Data

Audit logs shall be protected from unauthorized access, modification, or destruction and shall be reviewed periodically for action. Access to logs shall be restricted to those responsible for auditing, those performing assigned maintenance tasks, (e.g., system administrators, firewall administrators, database administrators, etc.) and other approved reviewers.

Access to online audit logs shall be strictly controlled to ensure the integrity of audit trail data against modification. Audit trail records shall be protected by strong access controls to help prevent unauthorized access. IT operations supporting the DHHS Divisions/Offices shall ensure the correct setting of computer clocks for audit log analysis.

Audit trail software shall also be protected. Controlled access to the event recording mechanism shall be provided.

10. Retention of Audit Logs

Audit logs shall be retained for a period specified by the system owner (typically one (1) year) unless otherwise specified by federal or state regulations. Audit logs shall be backed up and stored off-site, as required, along with the data. Exceptions to this rule are where federal or state regulations require that audit logs be kept for a longer period. In the event of an investigation, audit logs will be kept for an extended period if they are used as evidence in an ongoing investigation.

11. Testing

IS audits shall evaluate security program compliance with the agency's policies and procedures and/or test the effectiveness and the integrity of an information processing system.

Enforcement

For enforcement questions or clarification on any of the information contained in this policy, please contact DHHS Security Officer (DHHS.Security@ncmail.net). For general questions about department-wide policies and procedures, contact the [DHHS Policy Coordinator](#)

Exceptions

Any exceptions to this policy will require written authorization. Exceptions granted will be issued a policy waiver for a defined period of time. Requests for exceptions to this policy should be addressed to the Director of the Division of Information Resource Management (DIRM). The waiver request will be processed in accordance with the DHHS [*ITS Waiver and Appeals Policy*](#).