

DHHS POLICIES AND PROCEDURES

Section VIII:	Privacy and Security
Title:	Security Manual
Chapter:	ITS Operations Security Policy
Current Effective Date:	6/15/05
Revision History:	
Original Effective Date:	

Purpose

To establish the Department of Health and Human Services (DHHS) security requirements for the Information Technology Services (ITS) operations environment. This policy applies to the management and operation of the extended information processing infrastructure environment in the DHHS Divisions/Offices.

Policy

DHHS Divisions/Offices shall establish administrative, physical, and technical controls in the production environment to ensure an adequate level of security. This policy defines the security requirements necessary for protecting the production environment.

Roles and Responsibilities

The information processing needs of the DHHS Divisions/Offices vary considerably and likewise ITS Operations support may differ. The Division of Information Resources Management (DIRM) provides ITS oversight for all DHHS Divisions/Offices and various levels of direct ITS support for some. All DHHS Divisions/Offices, either through the relationship with DIRM, their own ITS staff, or through other third party contractor vendors, must provide a minimum level of security to support their programs and ITS operations.

The policy requirements specified below address the minimum DHHS security requirements:

1. The DHHS Privacy and Security Office (PSO) will provide guidance to the DHHS Divisions/Offices in the form of policy, standards, enterprise-wide procedures and guidelines.
2. If the DIRM is used to maintain ITS Operations for a DHHS Division/Office, it shall be responsible for ensuring the security of that environment. DIRM shall provide to the division/office a service level agreement outlining the responsibilities to meet the security requirements.
3. If a DHHS Division/Office maintains its own applications and systems, its staff shall be responsible for implementing the security of those operations through adherence of the DHHS PSO policies and standards.

4. If the DHHS Divisions/Offices have ITS operations that are being handled by a contractor/vendor, the division or office shall provide contract management oversight to ensure that adequate security is being provided. New and renegotiated contracts shall outline the security requirements to be met.

Implementation

Policy implementation shall comply with the referenced standards and best practices. The following paragraphs specify the operations security requirements: ITS governance – all DHHS operations management shall follow an approved ITS governance methodology. Control Objectives for Information and related Technology (COBIT) is a recommended standard. The DHHS PSO will provide guidance to the DHHS Divisions/Offices regarding the meaning and practical application of this standard.

1. ITS governance ensures there is a top-down management approach with auditable control objectives to ensure compliance.
2. ITS operations staff – IT operations shall be adequately staffed and resourced to ensure the availability of applications and systems as well as protect the confidentiality and integrity of the data being processed. Staffing requirements include:
 - A. Skill Level – The skill level of each individual in the production environment shall be adequate so that tasks can be performed efficiently and disruptions in service will not occur as a result of inexperience.
 - B. Cross-Training Staff – Cross-training is necessary to ensure availability. In the workflow, management needs to ensure that duties are assigned so that there is no conflict of interest (e.g., where an individual is reviewing their own work).
 - C. Job Descriptions – Clearly documented job descriptions indicating role and level of access to systems and applications.
3. ITS – All ITS systems and applications in the production environment shall be adequately supported and maintained. All technology shall be evaluated to ensure that it can provide the level of security required. Some legacy platforms may require additional controls to bring risk to an acceptable level. Technology that can no longer provide the level of security required should be replaced in accordance with the department’s schedule and in line with state adopted architecture requirements.
4. ITS processes and procedures – All ITS processes and procedures shall be documented and maintained using an approved document control system. IT processes and procedures shall include but not be limited to the following:
 - A. Configuration Management
 - B. Inventory Control

- C. Change Control
 - D. Patch Management
 - E. Backup and Restoration
 - F. Viruses and Malicious Code Protection
 - G. Object Reuse
 - H. System and Application Access
5. Operations Documentation and Escalation – Vendor documentation and operations procedures shall be available to all support personnel. Escalation procedures and contact lists shall be posted in the operations area and properly maintained. Helpdesk operations shall be implemented wherever possible to minimize downtime.
 6. Data Classification – All operations data shall be reviewed to determine the level of sensitivity and criticality. Classified data shall be properly labeled and controls implemented to protect the data against unauthorized access.
 7. Physical and Environmental Security – Physical and environmental security controls shall be implemented to adequately protect the operations environment.
 8. User Access and Auditing – Access to DHHS Information Resources should be based upon a “need to know” or a “need to use”. All DHHS Divisions/Offices shall adopt access methodology as approved by the DHHS PSO.
 - A. Assigning user privileges – A formal authorization process shall establish the privileges each user is granted and determine what information resources can be accessed. Data access shall be based upon the data classification and level of user access granted or similar approach which may be dependent upon the specific technology implemented by the vendor. This process will be controlled and require the approval of management.
 - B. Establishing Information Systems (IS) User Accountability – Each DHHS information processing system shall be configured to provide individual user accountability.
 - C. IS Auditing – All DHHS sensitive and critical information processing systems shall audited on a periodic basis. IS auditing priorities shall be scheduled on the basis of incident history, application criticality and the sensitivity of the information.
 9. Security Risk Management – Security risk in the operations environment shall be kept to a level that is considered “acceptable risk”.
 - A. Security Plans – Security plans shall be developed and maintained for all DHHS applications, systems and the corresponding ITS Infrastructure.
 - B. Controls – Administrative processes and procedures, physical access controls and technical controls shall be implemented to ensure the confidentiality, availability and integrity of information in the production environment.

- C. Incident Management, Alerts and Notifications – Security alerts and notification mechanisms shall be implemented to improve the response time of operations personnel. Comprehensive incident management and reporting mechanisms must be implemented in the operations environment and in accordance to the DHHS Incident Management Policy and Standard.
- 10. Contingency Planning – Contingency plans shall be written and maintained to ensure the availability of business critical ITS operations in the event of loss of service and in accordance to the BCP/DR policy. Alternative site operations shall be developed as part of a disaster recovery plan, as needed for business continuity based on a formal risk assessment. Not all systems require alternative recovery sites.
- 11. Security Certification of DHHS Information Processing Systems – All DHHS information processing systems shall be evaluated against security certification criteria to determine the level of security implemented in the operations environment.

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](#).