

## **DHHS POLICIES AND PROCEDURES**

---

<b>Section VIII:</b>	<b>Privacy and Security</b>
<b>Title:</b>	<b>Security Manual</b>
<b>Chapter:</b>	<b>ITS Inventory Management and Control</b>
<b>Current Effective Date:</b>	<b>6/15/05</b>
<b>Revision History:</b>	
<b>Original Effective Date:</b>	

---

### **Purpose**

The purpose of this document is to ensure that the Department of Health and Human Services (DHHS) establishes an inventory of data and information resources. The centrally-managed inventory will assist in strategic planning, budget projections and investment management, management of technical infrastructure, continuity planning, disaster recovery, and risk management.

### **Policy**

DHHS shall establish and maintain an Information Technology Services (ITS) inventory. The ITS Inventory Management and Control System shall serve as a tool to assist each DHHS Division/Office to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities and maintain day-to-day functions.

### **Roles and Responsibilities**

The DHHS Division of Information Resource Management (DIRM), shall establish, manage and maintain an inventory of all ITS resources for the department. DIRM shall accomplish this by working directly with the DHHS Divisions/Offices. These procedures shall also include monitoring and the updating of the inventory as well as validating the information collected.

DHHS Divisions/Offices shall be responsible for implementing data classification, labeling, and control procedures. They shall also be responsible for reviewing and updating the inventory and for submitting updated information in a timely manner.

The DHHS Privacy and Security Office (PSO) shall have access to the ITS Inventory Management and Control Database and receive reports of any discrepancies found.

### **Implementation**

Policy implementation shall comply with best practices and include the following requirements:

1. DIRM, including seat managed resources, shall establish and maintain for each division/office an inventory of information resources. The ITS inventory management and control process shall be implemented in a manner that reduces the duplication of reporting and focuses on capturing the reporting requirements of legislative, state and federal mandates. Divisions/Offices shall supply the information for the inventory and provide updates as needed.

The following inventories shall be maintained centrally:

- A. Software, including application software, system software, development tools and licensure status.
  - B. Hardware and equipment, including computer equipment and communication equipment.
2. Each division/office or affiliate division/office shall maintain databases and data files, system documentation, user manuals, training material, operational or support procedures, disaster recovery and business continuity plans, and archived information in order to meet the requirements of DHHS Security policies and procedures. Critical files must be backed up and stored in a safe location.
  3. The IT Inventory shall be updated no less frequently than annually and as needed to ensure accurate reporting to requesting authorities. Due to requests from other state agencies, more frequent updates may be required.
  4. DIRM will circulate a pre-populated inventory list along with instructions to designated division coordinators at least annually or as inventory reports are required.
  5. DIRM will report all inventory discrepancies (e.g., missing equipment) and work with the DHHS PSO and the Division/Office to resolve security incidents that involve the IT Inventory. Incident management procedures may be activated depending on the types or magnitude of discrepancies revealed.
  6. Types of information required on an ongoing basis include but are not limited to:

Software

- Name of system/application
- Version number of application/system
- Description or purpose of application/system
- Application/system status (i.e., active, retired, etc.)
- Test dates/schedule for disaster recovery plans
- Current system support, business and technical contact information
- Minimum security requirements to maintain the confidentiality, integrity and availability of information contained in a business application system in accordance with the DHHS Data Classification, Labeling and Access Control Policy
- Licensure

## Equipment, Devices or Hardware

- Asset type
- Identifying information such as make, model, serial number
- Fixed asset number if applicable
- Cost
- Age/date of purchase
- Upgrade or modification schedule
- Location
- Operating system and platform

## Enforcement

*For enforcement questions or clarification on any of the information contained in this policy, please contact DHHS Security Officer ([DHHS.Security@ncmail.net](mailto: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](#).