DHHS POLICIES AND PROCEDURES

Section X:	**Information Technology**
Title:	**DHHS Information Technology Asset Management and Inventory Control**
Current Effective Date:	**11/1/09**
Revision History:	
Original Effective Date:	**11/1/09**

Purpose

To ensure that the Department of Health and Human Services (DHHS) establishes an enterprise-wide asset management and inventory control system to track and compile statistics of all information technology (IT) hardware and software assets.

Policy

The development and utilization of an enterprise-wide IT asset management and inventory control system will assist DHHS in strategic planning, budget projections and investment management, management of technical infrastructure, continuity planning, disaster recovery and risk management.

Implementation

Roles and Responsibilities

On behalf of DHHS, the Division of Information Resource Management (DIRM) shall research, review and select an IT asset management and inventory control system. The system shall be used to provide a basis for enterprise-wide decision making by senior DHHS leaders, and assist each DHHS division and office in accomplishing its assigned mission, protect its assets and fulfill its legal responsibilities while maintaining day-to-day functions.

The DIRM shall:

- Establish, manage and maintain the enterprise-wide asset management and inventory control system chosen for the department
- Establish and maintain an enterprise-wide inventory record regarding the acquisition, disposal, and transfer of all IT assets by working in conjunction with the DHHS divisions and offices
- Monitor the inventory and validate the information collected
- Ensure that approved, licensed versions of software are maintained and used on all workstations, servers and other information technology platforms
- Periodically review appropriate change logs and confirm changes made.

- Acquire and deploy patches/changes for applications, services and hardware to the enterprise-wide asset management and inventory control system
- Ensure appropriate data controls are in place and employees are vetted where appropriate or required
- Develop enterprise-wide procedures for the management of the DHHS enterprise-wide asset management and inventory control system including but not limited to; the provisioning of roles and scopes, and the labeling of IT assets
- Maintain appropriate documentation of changes made to applications, systems and hardware devices
- Report to the DHHS Privacy and Security Office (PSO) on a monthly basis the implementation of security patches, service packs or security related changes to DIRM managed IT assets

DHHS divisions and offices shall[1]:

- Implement patches to locally managed IT assets
- Classify internal data
- Label IT assets
- Comply with local inventory reporting and control procedures in accordance with the DHHS IT Asset Inventory and Reporting Standard
- Ensure all IT assets are connected to the network at a minimum of once a month in order to receive patches and update inventory status
- Maintain and safeguard all IT property entrusted to their care
- Maintain appropriate documentation of changes made to applications, systems and hardware devices
- Report to the DHHS Privacy and Security Office (PSO) on a monthly basis the implementation of security patches, service packs or security related changes to locally managed IT assets

The DHHS PSO shall have access to the IT asset management and inventory control system expressly for the purposes of audit, validation and incident response.

The DHHS PSO shall be segregated from the DIRM managed DHHS Information Technology Asset Management and Inventory Control system to provide integrity of audit, validation and incident response processes and to ensure segregation of duties. To assist DIRM in the maintenance of an enterprise-wide inventory record the PSO's instance of the DHHS Information Technology Asset Management and Inventory Control system shall report inventory to the enterprise system.

Nothing in this policy shall preclude divisions or offices from using the IT asset management and inventory control system for their own purposes.

[1]. In cases where DIRM provides IT support to a Division or Office it shall be the responsibility of DIRM to provide the functions listed below.

Guidelines

In order to meet the requirements of DHHS security policies and procedures, each division and 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. Critical files must be backed up and stored in a safe location.

The IT asset inventory shall be updated no less frequently than annually and/or as needed to ensure accurate reporting to requesting authorities. Due to requests from other state agencies, more frequent updates may be required.

The IT asset management and inventory 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.

All IT inventory discrepancies shall be reported to the Division of Information Resource Management and appropriate division or office for resolution.

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 DHHS Privacy and Security Office. The waiver request will be processed in accordance with the DHHS ITS Waiver and Appeals Policy.

Enforcement

The DHHS Privacy and Security Officer shall be the point of contact for issues or questions regarding the ongoing implementation of this policy. However, it is the responsibility of division/office/facility/school management to ensure compliance with the provisions of this policy. Violations may subject a division/office/facility/school to corrective action as identified through audit processes conducted by the DHHS Privacy and Security Office on behalf of the DHHS Office of the Internal Auditor (OIA).

Reference:

- North Carolina General Statute
  - N.C.G.S. §§132 “North Carolina Public Records Act” Public records defined

- NC Statewide Information Security Manual
  - Chapter 1 – Classifying Information and Data, Section 01: Setting Classification Standards
    - Standard 010101 – Defining Information
    - Standard 010103 – Storing and Handling Classified Information

    - Chapter 3 – Processing Information and Documents, Section 02 System Operation and Administration Upgrade
        - Standard 030206 – Managing System Operations and System Administration
        - Standard 030218 – System Utilities; Segregation of Duties
        - Chapter 4 – Purchasing and Maintaining Commercial Software, Section 02 Software Maintenance and Upgrade
        - Standard 040201 – Applying Patches to Software
    - Chapter 5 – Securing Software, Peripherals and Other Equipment, Section 06 Documenting Hardware
        - Standard 050601 – Managing and Using Hardware Documentation
        - Standard 050602 – Maintaining a Hardware Inventory or Register
    - Chapter 8 – Developing and Maintaining In-House Software, Section 02 Software Development
        - Standard 080206 – Separating System Development and Operations
    - Chapter 9 – Dealing with Premises Related Considerations, Section 01 Premises Security
        - Standard 090102 – Securing Physical Protection of Computer Premises
    - Chapter 13 – Detecting and Responding to IS Incidents, Section 04 Other Information Security Incident Issues
        - Standard 130404 – Establishing Dual Control/Segregation of Duties

- NC DHHS Security Standards
    - Administrative Security
        - Data Stewardship Security Standard
        - Asset and Inventory Control Standard

- Office of State Controller
    - Administrative Policies and Procedures Manual

- NC DHHS Policies and Procedures Manual, Section VIII – Privacy and Security, Privacy Manual
    - Administrative Policies, Privacy Safeguards

For questions or clarification on any of the information contained in this policy, please contact the DHHS Privacy and Security Officer. For general questions about department-wide policies and procedures, contact the DHHS Policy Coordinator.