

DHHS POLICIES AND PROCEDURES

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

Purpose

To establish a set of requirements that defines the minimum level of physical and environmental security for all the Department of Health and Human Services (DHHS) facilities to safeguard information resources.

Policy

DHHS Divisions/Offices, assisted by the DHHS Privacy and Security Office (PSO) and in collaboration with the DHHS Office of Property and Construction and the DHHS Safety Director, shall implement adequate physical and environmental security controls at their facilities to protect people, property and information resources.

Roles and Responsibilities

The responsibility for physical and environmental security will vary among the DHHS Divisions/Offices depending upon organization structure and facility arrangements (i.e., owned, leased or shared). These responsibilities may cross divisions/offices authorities and be assigned through written agreement or contract. Key roles that affect the implementation of this policy are:

Facility Managers – All DHHS Divisions/Offices shall have facility management. This function may be outsourced (e.g., with leased buildings) or there may be a DHHS representative assigned to one (1) or more buildings.

Visitor Control Personnel – All DHHS buildings shall have visitor control procedures.

Safety Officers – Each DHHS facility shall have designated emergency evacuation personnel that will ensure that emergency evacuation routes are clearly posted, emergency response procedures documented, tested are distributed to all building personnel.

Network and Computer Operations Management - All network and computer operations managers/administrators shall be responsible for the physical security of the hardware and software assets assigned to them.

Managers and Supervisors – All DHHS Division/Office Managers and Supervisors responsible for operations shall ensure that adequate physical security is provided to protect assets.

Contracts Administration – Contracts administration shall ensure that third party agreements provide the level of security defined in DHHS policies. DHHS contracts and

interagency agreements shall contain the necessary physical security provisions to protect sensitive and critical information in the work stream.

Employees/Contractors/Volunteers – All DHHS employees/contractors/volunteers have an obligation to protect DHHS physical assets.

Implementation

Policy implementation shall be based upon the use of management-approved security standards and in coordination with the DHHS Office of Property and Construction and DHHS Safety Director. The following paragraphs specify the physical and environmental policy requirements in order to address Information Technology Services (ITS) security.

1. Facility Security (Building, Parking Lots)
Facility security shall be provided at all DHHS Divisions/Offices. This will include facility management, site perimeter protection, and parking lot security. Facilities may utilize guards and/or surveillance monitoring when necessary. DHHS Divisions/Offices shall ensure that its facilities have implemented adequate physical and environmental security necessary to protect its information resources within budgetary resources.

The DHHS PSO, in collaboration with the DHHS Office of Property and Construction, shall assist the DHHS Divisions/Offices in preparing and maintaining a facility security plan. This document shall include building records, vendor contact lists, physical security contract information, and key control procedures. This information shall be included as appropriate in the division/office business continuity plan.

2. Physical Access Control (Internal/External)
DHHS Divisions/Offices are responsible for providing adequate physical security in the workplace. DHHS shall implement physical access control procedures at designated points where personnel access needs to be limited. The DHHS workforce (employees/contractors/volunteers) shall receive badges and display them properly, so they are clearly visible, at the DHHS Divisions/Offices.
3. Visitor Control
DHHS Divisions/Offices shall implement visitor control procedures that may include any or all of the following features:
 - A. Visitor log maintained.
 - B. Sign-in/sign-out procedures with time recorded.
 - C. Temporary badge with tracking number properly displayed.
 - D. Visitor escorted at all times in accordance to procedures developed in accordance with the [DHHS Privacy Manual, Administrative Policies, Privacy Safeguards](#).

4. **Closed-Circuit TV (CCTV) Surveillance Monitoring**
Monitoring at the DHHS Divisions/Offices shall be performed, as DHHS funding permits and appropriate to the facility, to ensure workforce safety and prevent property loss. Surveillance monitoring shall be limited to areas perceived as high risk unless otherwise required (e.g., JCAHO accredited facilities).
5. **Protecting the Technical Infrastructure**
DHHS Divisions/Offices shall provide the level of physical and environmental protection of its technical infrastructure as specified by the DHHS PSO to minimize the risk of unauthorized access or environmental hazards. The DHHS PSO shall collaborate with the requesting of funding of and remediation of the physical and environmental factors as required.
6. **Work Area Security**
The employee/contractor work area shall be properly secured to protect both sensitive and critical information and ensure privacy. Workstations shall be placed in a location that protects the confidentiality of data. Documents and media shall be stored in a secure manner.
7. **Physical Inventory Control**
The Division of Information Resource Management (DIRM) shall maintain a formal inventory of ITS assets (hardware, software and applications) for the DHHS Divisions/Offices. Asset inventory shall be performed at regularly scheduled intervals or when a significant change has occurred. Refer to the DHHS ITS Inventory Policy for more specific details.
8. **Power Protection**
DHHS Divisions/Offices shall provide power protection to support both personnel safety and ensure the availability of its information systems. All sensitive and critical information processing systems shall be protected by an uninterruptible power supply. All critical applications shall be configured to switchover to an alternate power source immediately upon loss of power.
9. **Physical Security of Telecommunications Resources**
The telecommunications lines and equipment of DHHS Divisions/Offices shall be adequately protected to ensure both availability and the confidentiality of this resource. Sensitive information shall only be sent over secure lines. The DHHS Division of Information Resource Management (DIRM) and the Office of Property and Construction shall ensure that adequate safeguards are in place.
10. **Physical and Environmental Security of Off-Site Storage Facilities**
The off-site storage facilities for DHHS Divisions/Offices shall be afforded the same level of protection as the main processing site. Adequate physical security and environmental controls shall be implemented to protect the data.

11. **Controls for Environmental Exposures in the Workplace**
DHHS Divisions/Offices shall protect both personnel and assets by implementing controls that will protect the environment from environmental hazards. These controls may include but are not limited to: Temperature and humidity controls, smoke detectors and fire suppression systems.
12. **Mobile Computing Devices Security (Laptops, PDAs, etc)**
Laptop computers shall be issued only to authorize division/office personnel who shall be responsible for both the physical security and the information stored on the device. All laptops shall be inventoried with a property tag or barcode shall be password protected to limit access to its authorized user, and meet the [ITS Desktop and Laptop Security Standard](#) and DHHS Acceptable Use to DHHS Information Systems Policy. The DHHS PSO shall develop and maintain enterprise-wide standards and procedures for implementing laptop security.

Any use of PDAs and other mobile computing devices must meet the required security standards and be approved by the supervisor. The use of PDAs or smart phones, etc. to access and log personally-identifiable information at DHHS is restricted and access should be granted only under approved circumstances. Documentation of authorization shall be retained by the supervisor. The user is responsible for seeking authorization from the supervisor and notifying the supervisor of any changes in use of or type of equipment. The DHHS PSO, in consultation with the DHHS Division/Offices, shall develop and maintain enterprise-wide procedures for implementing PDA security. Any authorized use must also be in compliance with the DHHS Acceptable Use to DHHS Information Systems Policy.

Wireless access to the state network and its related equipment and components shall meet standards and policies established by ITS and DHHS. The DHHS PSO shall be responsible for the development and revisions of policy and standards as technology advances and shall consult in with the DHHS Divisions/Offices, regarding proposed revisions to wireless policy and standards.

13. **Property Control**
Any movement of information, software media, hardware or other physical assets shall be strictly controlled. Only authorized personnel shall be permitted to take DHHS Division/Office property off the premises and they shall be responsible for protecting the property and controlling its use. The DHHS PSO shall develop and maintain enterprise-wide procedures for ITS property control, in consultation with the DHHS Divisions/Offices.
14. **Removable Storage Devices**
The use of removable storage devices or external devices (e.g.; USB Flash Drives) shall be restricted to authorized personnel in order to safeguard and protect confidential data and information technology assets. Authorization for the use of removable storage devices must be granted by the user's supervisor in writing and

specify the intended use of the device. Documentation must be maintained according to division/office procedures and minimally include: Identification of staff, identification of job functions requiring the use of a removable storage device, type of device utilized, knowledge of standards and policies, and signatures of authorized staff and supervisor signifying acceptance of conditions. Any use must meet DHHS security policies and standards, specifically the DHHS Acceptable Use for DHHS Information Systems Policy.

The DHHS PSO shall be responsible for the development and revisions of policy and standards as technology advances, in consultation with the DHHS Divisions/Offices.

15. **Safety and Emergency Procedures**
DHHS Divisions/Offices shall regard personnel safety as a high priority and take the necessary steps to ensure a safe workplace. The DHHS PSO shall develop, in collaboration with other responsible division/offices and the DHHS Safety Director, enterprise-wide emergency procedures for handling a variety of threats. Emergency procedures shall be written, maintained and tested periodically at each facility for each significant threat.
16. **Emergency Equipment**
All DHHS facilities shall contain emergency equipment (e.g., emergency lighting, fire extinguishers) to establish an adequate level of safety for those working within a facility. This equipment shall be inspected annually to ensure its operational capabilities.
17. **Incident Management**
Incidents shall be managed and reported as required in the DHHS Security Incident Management Policy.
18. **Disposal of Sensitive Documents, Media and Equipment**
DHHS sensitive documents, media and equipment must be disposed of in an approved manner that protects the confidentiality of the information printed or stored. The DHHS PSO, in collaboration with responsible division/offices and ITS ([Standards for Clearing or Destroying Media](#)) shall develop enterprise-wide procedures for the following:
 - A. Disposal of sensitive documents.
 - B. Destruction of computer equipment that may contain sensitive information
 - C. Sanitization (i.e., object reuse) of equipment that might be sold or transferred to other organizations.
 - D. Destruction of various types of media.
19. **Physical Site Inspections**
A physical security inspection shall be performed periodically by the DHHS PSO to ensure policy compliance. The inspection process, including but not limited to the

schedule, tools used and results of the inspection shall be coordinated with the DHHS Office of Property and Construction and the DHHS Safety Director. The DHHS PSO shall notify the DHHS Division/Office Security Official of the results of physical security inspections for the purpose of remediation of deficiencies.

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](#).