

DHHS POLICIES AND PROCEDURES

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

Purpose

This policy defines the Department of Health and Human Services (DHHS) security training and awareness program and establishes the security training requirements for each of the DHHS Divisions/Offices.

Policy

DHHS workforce shall receive security training needed to support DHHS security policies and procedures in the course of their normal work. The DHHS security training and awareness program shall consist of security awareness presentations, security reminders, general security training, system-specific security training, security management training and professional security education for members of the workforce.

Definitions

Term	Definition
Security Awareness Presentations	Addresses security issues to show the importance of security and the adverse consequences of security failures.
Security Reminders	Workplace aids that continually remind individuals of the importance of having adequate security.
General Security Training	Teaches the basic security skills that enable users to perform their jobs more effectively and relates to general understanding of information systems.
System-Specific Security Training	Role-based training that is mapped to job functions with specific performance-based training requirements of a system.
Security Management Training	Risk management training with an emphasis on due diligence in the workplace.
Professional Security Education	Targets Information Technology Services (ITS) security professionals and focuses on developing the ability to perform complex activities using best practices.

Roles and Responsibilities

The DHHS Privacy and Security Office (PSO)

The PSO shall develop a comprehensive security training and awareness program for the divisions/offices. This effort shall be in coordination with the divisions/offices taking into account their division/office specific requirements.

- Ensure that the general and system-specific security training is provided to DHHS divisions/office staff.
- Develop and maintain the summary of enterprise wide policy, standards, and procedures for distribution to DHHS workforce.

DHHS Divisions/Offices Information Security Officials

The DHHS Division/Office Information Security Officials shall work with the DHHS PSO to implement the DHHS training requirements. Responsibilities include:

- Facilitate the completion of the initial assessment of division/office workforce member's security training needs.
- Periodically evaluate information security training needs.
- Ensure that security awareness presentations are developed to meet division/office specific requirements.
- Ensure that security awareness and training is provided throughout the organization.
- Distribute the summary of enterprise wide policies, standards, procedures and division/office specific security policies, procedures and standards to the workforce.
- Develop and implement non-enterprise level, system-specific training to supplement general security training, in consultation with and assisted by the DHHS PSO, as required.

Implementation

Implementation of the policy shall comply with the referenced standards and best practices. The following paragraphs specify the Security Training and Awareness requirements.

Security Training and Awareness Program

1. The DHHS PSO shall develop and implement an enterprise-wide security training and awareness program. This program shall include training plans to develop, implement, and deliver the training to DHHS workforce members (see #3 below). The purpose of the program is to assure that the DHHS workforce and third parties who receive process or store DHHS information are aware of their security responsibilities and know how to fulfill them. See the National Institute of Standards and Technology

publication, Building an Information Technology Security Awareness and Training Program for additional guidance ([NIST 800-50](#)).

2. In addition to reflecting the security requirements required by DHHS and state and federal regulations, the security training requirements shall reflect the business requirements of DHHS and provide flexibility for extension to accommodate future technologies and related risk management decisions. The National Institute of Standards and Technology publication, Information Technology Security Training Requirements: A Role-and Performance-Based Model, may serve as a reference ([NIST 800-16](#)).
3. The DHHS PSO shall develop Security Training plans for General Security Training, System-Specific Security training, and Professional Security Education. These plans shall be reviewed by the divisions/offices on an annual basis to take into consideration new technology and risk management decisions. These plans shall include the following elements if applicable:
 - A. Goal
 - B. Scope
 - C. Training participants; e.g., training, support, business
 - D. Approach (i.e., train the trainer or train the end users)
 - E. Methodology (i.e., face-to-face vs. audio vs. self-study)
 - F. Deliverables (i.e., training plan, reference manual, video track, etc.)
 - G. Training Objectives
 - H. Schedule
 - I. Registration
 - J. Review and Evaluation
4. DHHS Divisions/Offices shall document all security training other than security awareness for division/office workforce members. Security training documentation shall be maintained in accordance with the DHHS Records Management policy and Human Resources policies. Proof of security training shall be maintained in accordance with the division/office policy.

Security Awareness Presentations and Reminders

1. DHHS PSO and DHHS Divisions/Offices, in conjunction with the DHHS Public Affairs Office (PAO), shall develop and maintain a communications process to communicate new computer security program information, security bulletin information, and security items of interest.
2. The DHHS Division/Office Information Security Officials shall provide for or collaborate with DIRM on the scheduling of security awareness presentations within their organization using material developed by ITS and the DHHS PSO.

3. Security awareness presentations or messages may be delivered through e-mail, posters, pop-up messages, web-based sessions, “brown-bag” seminars or other media depending on the complexity of the message. These messages may also be delivered through “sign-on warning banners” that address information privacy and security issues to all logon/access points to computer information systems where technically practical.
4. All workforce members shall receive continuing information security awareness updates that focus attention on security issues.

General Security Training

1. The DHHS PSO shall develop or coordinate the development of material for general security training as part of their information security training program. General security training will be sponsored or approved by the Division of Information Resources Management (DIRM).
2. All DHHS workforce members shall receive general security training and regular updates in organizational policies and procedures before being granted access to DHHS information resources.
3. General security training shall include acceptable use of information system resources, legal responsibilities and business controls, as well as training in the correct use of information processing facilities, e.g., log-on procedure, procedures for guarding against malicious software, password management, and recognizing and reporting security incidents.
4. A summary of the DHHS Information Security policies must be delivered to all DHHS workforce members including employees, contractors, or volunteer staff, either in paper format or electronically, prior to being granted access to DHHS information resources.

System Specific Security Training

1. DHHS Division/Office managers/supervisors must ensure that workforce members have training and supporting reference materials sufficient to allow them to protect DHHS information resources.
2. Divisions/Offices in consultation with affiliate division/vendor shall provide system-specific security training. DIRM will serve as the lead division, in collaboration with effected divisions/offices, in providing system specific security training for enterprise systems.
3. When workforce members’ job responsibilities change, their information security needs must be re-assessed by the immediate supervisor. New security training must

be provided as necessary for the change in job responsibility.

Security Management Training

1. The DHHS PSO shall provide security management training for the designated DHHS Information Security Officials and Division/Office management.
2. The DHHS PSO shall assist the DHHS Division/Offices in identifying training needs for the Information Security Officials. The DHHS PSO shall recommend yearly, professional security training courses and seminars necessary to ensure that ISO skills are at an adequate level.

Professional Security Training

1. Provisions for division/office ITS staff training shall include training in information security threats and safeguards, with the extent of technical training to reflect the job holder's individual responsibility for configuring and maintaining information security safeguards. Where ITS staff change jobs, their information security needs must be re-assessed and any new training provided as a priority.

Training Evaluation

1. The DHHS PSO shall work with each DHHS Division/Office to monitor training requirements, compliance and effectiveness. Key information to be captured shall include courses, dates, audience members, costs and sources in order to provide enterprise wide analysis and reporting regarding awareness, training, and education initiatives. Captured information shall also include test scores, audience commentary, and suggestions for improving the provided training.
2. All security training and awareness presentations shall provide formal evaluation and feedback mechanisms to address objectives initially established for the training program. Methods for evaluation and feedback may include but are not limited to evaluation forms/questionnaires, focus groups, selective interviews, independent observations, and formal status reports. The DHHS PSO shall work with the Division/Office security official in evaluating the adequacy and effectiveness of the information security program and seek ways of improving upon the quality of this program.

Enforcement

All DHHS disciplinary actions, up to dismissal for DHHS employees, and/or termination procedures for contractors shall be in compliance with relevant personnel and contract policies.

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](#).