

DHHS POLICIES AND PROCEDURES

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

Purpose

Much of the information provided by the Department of Health and Human Services (DHHS) is accessible to the public. However, some of the information is sensitive and must be protected (e.g., personally-identifiable health information) in a manner defined by both federal and state regulations. This policy establishes personnel security requirements for those staff who access or are responsible for handling sensitive information. The personnel requirements are based upon the classification of data and tasks performed on the related information systems. This policy is intended to ensure that security responsibilities are clearly defined in job descriptions for each member in the DHHS workforce and that management has considered security in staffing each position.

Policy

DHHS shall establish personnel security requirements to protect sensitive information:

1. Define job roles and responsibilities within the organization that are subject to the security requirements.
2. Specify the level of security requirements associated with designated job roles and responsibilities.
3. Monitor job classification changes.
4. Provide sanctions for non-compliance.
5. Implement personnel termination procedures that ensure that adequate security is provided.

Roles and Responsibilities

The following roles and responsibilities are impacted by this policy:

1. The DHHS Privacy and Security Office (PSO) will establish enterprise-wide procedures for determining job security levels and provide technical assistance and training to division staff responsible for classifying staff and contractors.

2. Utilizing the DHHS PSO enterprise-wide procedures, DHHS Divisions/Offices will determine the level of data sensitivity and criticality of the systems that process this data.
3. DHHS Division/Offices will map personnel positions with the classification levels and monitor all changes to the job positions. Likewise, DHHS contracts shall be reviewed according to DHHS *Security for Information Systems Contracts* policy to ensure the proper security classification levels and access have been met in accordance with DHHS security policies.
4. DHHS Division/Offices shall ensure that job descriptions are completed per State Personnel Policy and address relevant security requirements and tasks. Completed job descriptions shall be maintained in personnel folders.

Implementation

The following sections specify requirements for implementing the framework for personnel security.

1. Defining security responsibilities within the organization. DHHS security roles and responsibilities shall be included in job descriptions. These roles and responsibilities shall include:
 - A. Any general responsibilities for implementing or maintaining security policy, and
 - B. Any specific responsibilities for the protection of particular assets or the execution of particular security processes or activities.
2. Security roles and responsibilities shall be addressed:
 - A. During the recruitment (where job responsibilities are defined to the prospective employee),
 - B. In contracts (specified in a service-level agreement/contract), and
 - C. Monitored (by management) during the individual's employment.

All DHHS job descriptions shall be classified according to security level (high-medium-low). Utilizing the established DHHS criteria, this determination shall be made by the division/office supervisors in consultation with their user staff and the assigned information security official and approved by the appropriate management official.

3. Classifying job positions (job positions shall be classified according to the following security levels):
 - A. **Low Sensitivity:** This classification level implies there is the potential for limited impact resulting in data compromise or damage caused to an

information system or operations. These positions are typically non-critical or have some importance in the data workflow or operations environment.

- B. **Moderate Sensitivity:** This classification level means there is the potential for moderate to serious impact resulting in data compromise or damage caused to an information system or operations. These positions typically have considerable importance in the data workflow or operations environment.
- C. **High Sensitivity:** This classification level has the potential for serious impact resulting in data compromise or damage caused to an information system or operations. These positions are typically key positions that affect managing the data workflow, influence the development of information systems, manage the operations or network environment, involve life-critical or mission-critical systems, or have significant fiduciary responsibility.

4. Monitoring Job Classification Changes:

- A. Position changes to all DHHS workforce members, such as promotions and transfers, shall require a validation to ensure the proper security level classification has been reviewed. These security procedures shall be reviewed with the appropriate workforce members when there are changes to terms of employment or contract, particularly when workforce members are entering or changing positions within the organization. The DHHS PSO shall provide enterprise wide procedures and guidelines on how DHHS Divisions/Offices should review these positions.
- B. Revising and maintaining current job classifications will help reduce the incidence of security incidents occurring in the workplace. However, any incident, whether the result of the failure to maintain current job descriptions or not, should be reported immediately to management and to the assigned information security official, in accordance to the DHHS Incident Reporting policy and procedures.

5. Disciplinary Action and Termination Procedures:

- A. 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.

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*](#).