

DHHS POLICIES AND PROCEDURES

Section VIII:	Privacy and Security
Title:	Security Manual
Chapter:	DHHS Security Organization
Current Effective Date:	6/15/05
Revision History:	This policy replaces two (2) existing chapters of the DHHS Security Manual: “Development of Security Policies,” and “Security Official.”
Original Effective Date:	5/01/04

Purpose

The purpose of this policy is to establish the structure of the Department of Health and Human Services (DHHS) security organization. This policy specifically addresses the security roles and responsibilities of the DHHS Privacy and Security Office (PSO), Division/Offices and staff within the department. In addition, this policy defines the process for developing, reviewing and communicating security policies, standards, procedures and guidelines for the department.

Policy

DHHS shall ensure that security is implemented properly by establishing the DHHS PSO and a security organization structure within each of the DHHS Divisions/Offices. Under the auspices of DHHS Directive, II-12, The DHHS PSO shall be the DHHS lead office for the enterprise-wide security program. Each DHHS Division/Office shall implement their own information security program, following the directives, procedures, and guidelines from the DHHS PSO, which will be managed by an information security official.

Security policies, standards, and procedures shall be developed at both the enterprise-wide level and at the implementation level by the DHHS PSO and supplemented as necessary by the DHHS Divisions/Offices for their specific use. The DHHS PSO shall be responsible for the development of enterprise-wide security policies, standards, procedures, and guidelines. The Division/Office Information Security Officials shall be responsible for the implementation of those policies, standards and procedures, with the assistance of the DHHS PSO, as needed.

Definitions

For purposes of clarification, the following definitions shall be used in establishing security program:

- Security policy is the governing principle that establishes the security requirements for the DHHS Divisions/Offices.

- A standard is a specification that establishes an approved methodology or technology that is to be implemented.
- A procedure is a series of interrelated steps taken to implement the policy and standard.
- A guideline is a recommended approach.

Roles and Responsibilities

1. DHHS PSO

The DHHS PSO shall be managed by the DHHS Security Officer. The DHHS PSO shall be responsible for implementing the enterprise wide-security program. In addition, the office shall be responsible for the development, coordination, enforcement, and monitoring of the enterprise-wide security policies, standards, guidelines and procedures. The responsibilities of the DHHS PSO are:

- Providing security consulting and guidance for the department.
- Developing and implementing an information security program.
- Developing enterprise-wide security policies for the department.
- Developing security standards for the department.
- Developing enterprise-wide security procedures for the department.
- Developing security implementation guidelines for the department.
- Developing an enterprise-wide risk management implementation methodology for the department.
- Conducting security risk assessments for the department.
- Facilitating audits conducted by state and federal agencies external to DHHS.
- Participating in departmental disaster recovery planning team to develop, continually review, and update as necessary information technology business continuity and disaster recovery plans.
- Providing guidance in the implementation of information technology security policies and procedures.
- Providing consultation and direction regarding the security of information technology to divisions/offices within the department.
- Coordinating security activities within the department.
- Developing the enterprise-wide security training program for the DHHS Division/Offices.
- Providing security training to the DHHS Information Security Officials.
- Providing security awareness training for the DHHS Divisions/Offices.
- Monitoring state and federal security legislation for applicability to state enterprise-wide security policies and standards.
- Monitoring DHHS Division/Office compliance with the DHHS enterprise-wide security policies.
- Conducting investigations of security incidents within the department.

- Communicating all department expectations for security to division/office Information Security Officials.
- Developing security metrics on the level of security implemented within the department.
- Providing support to the DHHS Security Work Group.

2. DHHS Security Officer

The responsibilities of the DHHS Security Officer shall include, but not be limited to the following:

- Managing the DHHS PSO.
- Acting as the department expert for issues related to information technology security.
- Serving as DHHS liaison in the information technology area to coordinate with the State Chief Information Officer and State Chief Information Security Officials.
- Serving as liaison to the NC Office of the Attorney General in the analysis and application of state and federal security laws.
- Reporting security compliance status to Divisional, DIRM, and Department management.
- Escalating security issues to DIRM management, DHHS management, and State CIO, as appropriate.
- Working directly with the DHHS Privacy Officer to address privacy issues that require security interventions.
- Reviewing and approving all security corrective action plans submitted as a result of audits and compliance monitoring.
- Reviewing and approving security solutions within the department that address both the implementation of technology and their related processes.
- Coordinating with DHHS Division/Offices' Directors and Division/Office Security Officials regarding non-ITS related security incidents.
- Establishing and implementing a policy waiver review process.

3. DHHS Information Security Work Group (SWG)

The DHHS PSO will establish a DHHS Security Work Group (SWG). The workgroup will consist of representatives assigned by each DHHS Division/Office. The SWG, in an advisory capacity to the DHHS PSO, will assist the DHHS PSO in formulating policies, standards, guidelines, and procedures. These policies, standards, guidelines and procedures shall be: reasonable, based on industry best practices, consistent with federal and state laws, and consistent with current DHHS standards.

Members will assure that the appropriate personnel within the divisions/offices have

the opportunity to review the security policies, standards, procedures and guidelines. Members also serve as a clearinghouse to and from the DHHS Divisions/Offices regarding the DHHS Security Program.

4. The DHHS Security Work Group membership shall include:

- DHHS Security Officer
- DHHS Security Project Manager
- DHHS Division Office representatives and/or Division/Office Security Officers as determined and selected by the Division or Office
- DIRM Business Application Subject Matter Expert(s) as applicable to the topic area
- DIRM Computing Services Subject Matter Expert(s) as applicable to the topic area
- NC ITS Representative(s) as applicable to the topic area

5. DHHS Division/Offices

DHHS Divisions/Offices shall be responsible for policies and procedures developed by the DHHS PSO and development of division/offices-specific policies and procedures which may be necessary to supplement those developed by the DHHS PSO. These policies and procedures must be in compliance with the DHHS enterprise-wide security policies, standards and procedures developed by the DHHS PSO.

6. Each DHHS Division or Office shall:

- Assign a division/office representative to the SWG. This representative shall attend SWG meetings and review the security policies, standards, procedures and guidelines developed and adopted by the DHHS PSO.
- Designate a DHHS Division/Office Information Security Officials or provide contractual oversight in order to implement the division/office security program.
- Facilitate or develop, maintain and implement plans, policies, and procedures to ensure the security of information technology within the division/office.
- Implement division/office security requirements by incorporating new security technology and practices into existing information technology environments and business operations, respectively.
- Ensure that division/office staff and workforce participate in enterprise-wide training provided by the DHHS PSO and supplement the enterprise-wide training with division/office-specific training as needed.
- Implement a risk management program within the DHHS Division/Office following specific guidelines and procedures created by the DHHS PSO.

- Ensure that the physical security is appropriate at the DHHS Division or Office.
- Partner with the DHHS PSO to ensure the information security of the division/office.

7. DHHS Division/Office Information Security Officials

DHHS Division/Office Information Security Officials shall guide all division or office activities related to adherence to DHHS Security Policies regarding the prevention, detection, containment, and correction of security violations for information technology, in accordance with state and federal laws or rules and as delegated to the DHHS Security Officer.

The DHHS Division/Office Information Security Officials responsibilities shall also include, but are not limited to, the following:

- Serving as the division/office liaison to the DHHS Security Office and as the single point of contact for security related questions and issues.
- Ensuring the implementation, management and enforcement of division/office information security policies, standards and procedures.
- Working directly with Division/Office Privacy Official to address privacy issues that require security interventions.
- Reporting security incidents and issues directly to the DHHS Security Officer.
- Coordinating security incident response activities with the DHHS Security Official to contain, investigate, and prevent future security breaches.
- Developing supplemental procedures, as necessary, to those developed by the DHHS PSO, based on departmental policies, to ensure the security of information technology within the division/office.
- Receiving all division/office information security vulnerability and alert reports and disseminating this information to the appropriate staff for resolution.
- Ensuring division/office compliance with the enterprise-wide DHHS Security Policies, standards and procedures developed by the DHHS Security Office.
- Ensuring the ongoing integration of information security with the Division/Office's business strategies and requirements.
- Ensuring physical safeguards for information systems assets.
- Participating on DHHS Security Office work groups, committees or task forces as established.
- Serving as the lead DHHS Security Official if the division or office designates assistant Security Officials or security representatives for individual sites or offices. The lead DHHS Security Official will serve as the single point of contact for information flowing from and to the DHHS Security Officer. The lead DHHS Security Official will be responsible for the duties outlined within

and will coordinate the activities of the assistant DHHS Security Officials.

Implementation

Development of Security policies, standards, procedures and guidelines

The DHHS PSO shall be responsible for the development of enterprise-wide security policies, standards, and procedures. The DHHS PSO will research and develop drafts of enterprise-wide policies, standards, procedures and guidelines. These drafts will be presented to the members of the SWG for review. All comments will be addressed and discussed in SWG meetings. Upon acceptance, the revised draft of the policies will be sent to the DHHS Policy Coordinator for final approval and publication. All DHHS security policies will be maintained in the DHHS On-Line Publications, under Privacy and Security.

The DHHS PSO will collect and evaluate all requests for change. Any updates, modification or revisions to enterprise-wide security policies, procedures and standards shall be initiated by the DHHS PSO. The office shall utilize the SWG (see above process) to introduce and review documentation for all revisions.

Due to the sensitivity and confidentiality of security policies, standards and/or procedures there may be limitations placed upon the publication and availability of this documentation to the public. Limitations of access will be in compliance to GS 132 and GS 121.

Enforcement

For questions or clarification on any of the information contained in this policy, please contact [DHHS Security Office](#) general questions about department-wide policies and procedures; contact the [DHHS Policy Coordinator](#).

Chapter 126 employees who fail to comply with DHHS policies and/or agency procedures shall be subject to the DHHS Disciplinary Action guidelines and related personnel policies except that the sanctions for educators subject to Chapter 115C of the North Carolina General States shall be in accordance with NCGS 115C-325 or 115C-287.1. DHHS volunteers, guests, vendors, and contractors are expected to adhere to security policies, procedures, and standards. Termination procedures for contractors and vendors shall be in compliance with relevant contract policies.

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](#)

References

1. International Security Organization (ISO) 17799 “Information Technology-Code of Practice for Information Security Management” as mandated by NCGS 147-33.82 and other federal/state regulations as applicable.
2. 45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards; Final Rule.

The HIPAA Security Rule [§ 164.308(a)(2)] requires the designation of an individual who is responsible for the development and implementation within the covered entity of security policies and procedures that implement the HIPAA Security requirements.

DHHS Directive II-12 delegates authority to the Director of the Division of Information Resource Management (DIRM) to oversee and coordinate the establishment of a security policy and program for the department's information resources, including hardware, software, telecommunication network, and information. Additionally, the DIRM Director must monitor compliance with the established policies and program. To meet the requirements of DHHS Directive II-12, the DIRM Director has delegated these responsibilities to the DHHS Security Officer.

North Carolina General Statutes (NCGS), as listed below, dictate the direction of DHHS security activities.

- NCGS §147-33.82 states that the State Chief Information Officer (CIO) is given responsibility for the development of enterprise-wide information technology security policies and standards to be followed by all NC state government agencies, including DHHS, unless exempted by law.
- NCGS §147-33.82(f) (4) requires each NC State Government Division and Office to designate a liaison in the information technology area to coordinate security activities with the State CIO.
- NCGS §147-33.89 requires state agencies to establish a team to develop, implement, and update business continuity and disaster recovery plans for that division or office. NOTE: The requirement to develop and maintain disaster recovery plans is one of the HIPAA Security Rule standards that must be filled by the individual delegated responsibility for the covered entity’s security compliance.
- Additional references can be found in the DHHS Security Glossary and Reference Policy.