

DHHS POLICIES AND PROCEDURES

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

Purpose

To establish security requirements necessary to protect access of Department of Health and Human Services (DHHS) information utilizing data and telecommunications networks. These requirements will ensure compliance with federal, state, and departmental regulations. The scope of this policy includes network architecture, network security management, network technology, email security, third-party network connection security, telecommunications security, and wireless security.

Policy

DHHS shall implement the level of security necessary to protect DHHS network assets and information.

Roles and Responsibilities

While the DHHS Divisions/Offices are ultimately responsible for ensuring the security of their programs and information, the responsibility for providing an adequate level of network and telecommunications security within DHHS lies with the Office of Information Technology Services (ITS), the Division of Information Resources Management (DIRM) Networking Services, and the DHHS Privacy and Security Office (PSO).

ITS is responsible for managing and enforcing the North Carolina Integrated Information Network (NCIIN). Unless otherwise specified by contract or service level agreement, DIRM is responsible for managing, implementing and providing oversight of the network resources and data of the DHHS Divisions/Offices. The DHHS PSO is responsible for monitoring network security and enforcing the implementation of DHHS security policies, standards, and enterprise-wide procedures.

The following key roles and responsibilities have been identified for this policy:

1. The DHHS PSO provides development of enterprise-wide security policies, standards, procedures, and guidelines. This responsibility includes training and guidance for the DHHS Divisions/Offices as related the overall DHHS security program. The DHHS PSO is also responsible for the investigation of security related incidents.

2. DHHS Divisions/Offices and their assigned Division/Office Information Security Officials serve as the security point of contact. They are also responsible for providing implementation oversight of the security program and reporting security-related incidents.
3. All divisions/offices may not have individuals designated in the positions listed below. However, each division/office does have staff assigned to carry out the following functions either through assignment or agreement.
4. System owners/custodians are responsible for maintaining the data in accordance with the security data classification level.
5. Facilities managers are responsible for monitoring or maintaining the physical security of the environment.
6. Network managers/administrators are responsible for maintaining network operations and ensuring that an adequate level of security is provided.

Implementation

The DHHS PSO, in coordination with the relevant sections within DIRM and the divisions/offices, shall develop and publish enterprise-wide standards, procedures and guidelines to support the implementation of the following requirements:

1. Network Architecture – DHHS shall design, implement, and maintain its network architecture with the appropriate level of administrative and technical security controls. A layered architecture design should be provided as a form of defense to isolate external attacks and the overall damage to the network environment.
 - A. Network Addressing – All network names and addresses shall be managed and approved by a central addressing authority within DHHS. Internal network addresses shall be considered sensitive data and shall not be distributed to unauthorized personnel.
 - B. Network Services and Protocols – Only management-approved network services and protocols will be implemented. All non-authorized protocols and services will be removed and/or disabled.
 - C. Network Perimeter – A clearly-defined boundary shall be established to control traffic between DHHS information resources and external entities. All inbound and outbound network traffic shall pass through appropriate access control devices prior to reaching DHHS information resources. The DHHS network shall monitor for and disconnect any traffic not passing through the appropriate access control points.

- D. Network Availability and Redundancy – The DHHS network design shall provide adequate redundancies to reduce the likelihood of a single point of failure.
 - E. Network Integrity – The DHHS network shall establish a system of controls to safeguard the data traffic, detect and correct transmission line errors, and ensure message integrity throughout the system.
2. Network Security Management – All DHHS networks shall implement a security management function that includes network configuration management and continuity of operations, and provides an audit capability.
- A. Network Incidents – All network incidents shall be reported immediately using a DHHS-approved process.
 - B. Physical Security – DHHS Divisions/Offices shall protect all network equipment from unauthorized access.
3. Network Technology – The DHHS PSO shall establish standards to properly configure all network security technology to protect sensitive information flowing across the network.
- A. Network Switching Devices – Network management shall be responsible for approving the selection and configuration of all network devices such as routers, hubs, and switches deployed.
 - B. Network Servers – DHHS servers shall be protected commensurate with the level of sensitivity and criticality of the information and function that they perform.
 - C. Network Firewall – Only DHHS-approved traffic and services shall be permitted through the DHHS firewall(s).
 - D. Virtual Private Network (VPN) – All VPN solutions shall be designed to provide authentication, authorization, data protection, and accounting capabilities. All DHHS VPN solutions shall utilize approved software and contain an end-to-end security strategy.
 - E. Intrusion Detection Systems (IDSs) – Due to the significant risk of internal and external intrusion from unauthorized persons, intrusion detection systems shall be implemented. The DHHS PSO shall be responsible for the IDS design and implementation.
 - F. Content Filtering – The DHHS Network shall provide content filtering to minimize spam and the risk of damage occurring from receiving malicious email attachments or downloading viruses, worms, spyware or other malicious code.
4. Email Security – Electronic mail is critical to performing DHHS Operations and delivering needed services to its client base. DHHS shall implement security processes and solutions that protect:
- A. Mail Servers – Hosts that deliver, forward and store mail.

- B. Mail Clients – Software that allows users to read, compose, send and store email messages.

In general, all sensitive DHHS information transmitted over the external network must be protected. The DHHS privacy policy provides specific language regarding public records and emails that are exempt because of their privileged status. Individuals must not send, forward or receive confidential or sensitive DHHS information through non-DHHS email accounts. When transmitting confidential or sensitive information via NC Mail, the email should be password-protected. DHHS email shall be retained in accordance with the guidelines established by the state of North Carolina for retention and disposition.

- 5. Third Party Network Connection Security – All third-party connections shall be evaluated by considering access, administration, confidentiality, and monitoring requirements. Network Services provided over third-party connections shall be limited to those services necessary to perform the functions required. Third-party access shall be limited to those services and/or devices that are needed to perform the required business function. For most DHHS Divisions/Offices, this activity will be completed using standards developed by DIRM.
- 6. Telecommunications Security – All DHHS Division/Office telecommunications lines shall be secured in a manner that ensures availability and prevents tampering. DHHS Divisions/Offices or affiliated staff designated by agreement or assignment shall provide the following:
 - A. Intrusion Detection – All DHHS Divisions/Offices shall implement a method to detect intrusion activity on its telecommunications lines.
 - B. Line security – All DHHS Divisions/Offices telecommunications lines shall be secured in a manner that ensures availability and prevents tampering.
 - C. Telecommunications Equipment Security – All DHHS Divisions/Offices telecommunications equipment, terminal boxes, and access points shall reside in secure, controlled areas. Only authorized personnel shall be permitted access to this equipment.
 - D. Records – DHHS shall maintain current configuration records on all telephone systems, including outside and inside wiring, cabling, telephone and wiring closets, and equipment. DHHS shall classify all telephone lists and directories. These documents shall be shredded when no longer needed.
- 7. Wireless Security – Wireless solutions offer the benefits of portability, flexibility, increased productivity, and lower installation costs but require added security to protect data. If utilizing wireless security technology, DHHS shall implement approved wireless solutions designed to protect the confidentiality of information when using wireless networks and devices.

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](#).