DHHS POLICIES AND PROCEDURES

Section VIII:	**Security and Privacy**
Title:	**Security Manual**
Chapter:	**Acceptable Use for DHHS Information Systems**
Current Effective Date:	**June 15, 2005**
Revision History:	**This policy replaces DHHS Policies and Procedures, Computer Use Policy, Section IV: Communications, dated May 01, 2004.**
Original Effective Date:	**August 1, 2004**

Purpose

This policy defines the information system security responsibilities and acceptable use rights for employees, volunteers, guests, vendors and contractors (hereinafter, "**Users**") of North Carolina Department of Health and Human Services ("**DHHS**", or alternatively, the "**Department"**) information system resources.

Information systems include all platforms (operating systems), all computer sizes (personal digital assistants through mainframes), and equipment, and all applications and data (whether developed in-house or acquired from third parties) contained on those systems.

This policy document includes an agreement form that once signed, certifies the User's understanding and affirmation of the policy.

Policy

Each DHHS Division/Office shall be responsible for ensuring that every individual seeking access to DHHS network and/or information systems reviews this policy and signs an acceptable use agreement based upon the terms specified in this policy. Users must sign the agreement form included herein before permission is granted to use the DHHS systems.

Implementation

1. User Access Responsibilities

All information and data processing systems to which users are given access are to be used only to conduct the activities authorized by the Department. The use of these resources must be conducted according to the policies, standards, and procedures instituted by the Department or on its behalf. The unauthorized use or disclosure of information provided by these data processing systems may constitute a violation of Department, State, and/or Federal laws which will result in disciplinary action consistent with the policies and procedures of the Department (see **Enforcement** section below).

DHHS Divisions/Offices may require additional agreements regarding the confidentiality of specific types of information; for example, medical records, client case files, personnel records, financial records, etc. This policy may augment such Division/Office policies, but is not intended to replace such policies, which remain in effect.

2. Rights of Information Ownership

The Department and its Divisions/Offices retain the rights of ownership to all IS resources including hardware, software, functionality, data, and related documentation developed by the Department's information systems users on behalf of the Department. All Department IS resources remain the exclusive property of the State of North Carolina and/or the Department, unless otherwise prescribed by other contractual agreements.

3. Use of NC Integrated Information Network ("NCIIN") and the Internet

The Internet is a world-wide collection of interconnected computer networks. The State's wide area network, NCIIN, is the NC controlled network connected to the Internet.

Following is a list of policies regarding the use of NCIIN and the Internet:

A. While in performance of work-related functions, while on the job, or while using publicly owned or provided information processing resources, DHHS users are expected to use the NCIIN and Internet responsibly and professionally. Users shall make no intentional use of these services in an illegal, malicious, or obscene manner as described in NC General Statute (GS) 14-190.1. Users may make reasonable personal use of publicly owned or provided NCIIN or Internet resources as long as:

1. The direct measurable cost to the public is none, is negligible, or access supports the mission of the agency;
2. There is no negative impact on user's performance of public duties;
3. The policy is applied equitably among all personnel of the agency;
4. Users may be required to reimburse the agency if costs are incurred that do not have prior approval by the Agency or Division/Office.

B. When sending or forwarding e-mail over the NCIIN or the Internet, Users shall identify themselves clearly and accurately. Anonymous or pseudonymous posting is expressly forbidden, unless otherwise allowed by law to make anonymous postings.

C. Users are responsible for protecting DHHS sensitive information by following the DHHS policies and DHHS Division/Office policies and procedures.

D. Users have a responsibility to ensure, to the best of their ability, that all public information disseminated via NCIIN and the Internet is accurate. Users shall

provide in association with such information the date at which it was current and an e-mail address allowing the recipient to contact the public staff responsible for making the information available in its current form.

E. Users shall avoid unnecessary network traffic and interference with other users, including but not limited to:

1. Unsolicited commercial advertising by DHHS Users. Such use is strictly forbidden. For the purpose of this Policy, "unsolicited commercial advertising" includes any transmission that describes goods, products, or services and that is initiated by a vendor, provider, retailer, or manufacturer of the described goods, products or services, or by a third party retained by, affiliated with, or related to the vendor, provider, retailer, or manufacturer. For purposes of this definition the vendor, provider, retailer, or manufacturer must be a non-governmental entity. This prohibition shall not include:

   a. Discussions of a product or service's relative advantages and disadvantages by users of those products or services (unless the user is also the vendor, retailer or manufacturer, or related or affiliated with the vendor, provider, retailer, or manufacturer),
   b. Responses to questions, but only if such responses are direct replies to those who inquired via e-mail, or
   c. Mailings to individuals or entities on a mailing list so long as the individual or entity voluntarily placed his/her name on the mailing list.

2. The use of computer resources, including e-mail, to conduct any activities already prohibited by the Office of State Personnel or other DHHS policies (such as private/personal fund raising, political activities, etc.) shall be prohibited.

3. Mass emailing by public employees and NCIIN users that do not pertain to governmental business is prohibited.

4. Users shall not use the Internet, the NCIIN, or any State information system to (i) allow the unauthorized dissemination of confidential information, or (ii) for any purpose that is not permitted by DHHS policies or would compromise public safety or public health.

5. Users shall not stalk others; post, transmit, or originate any unlawful, threatening, abusive, fraudulent, hateful, defamatory, obscene, or pornographic communication, or any communication where the message, or its transmission or distribution, would constitute a criminal offense, a civil liability, or violation of any applicable law.

6. Users shall not access or attempt to gain access to any computer account to which they are not authorized. They shall not access or attempt to access any portions of the NCIIN networks to which they are not authorized. Users also shall not intercept or attempt to intercept data transmissions of any kind to which they are not authorized.

7. Users given access to which they are not privileged or entitled, are required to report the circumstances immediately to their supervisor. Supervisors are responsible for determining the User's appropriate access rights. Supervisors must notify their Division/Office Information Security Official should they determine that access rights need to be modified.

4. **Workstation Security**

These requirements apply to office, home or other remote access locations if utilized for DHHS business.

A. As appropriate, sensitive paper and computer media shall be stored in suitable locked cabinets and/or other forms of security furniture when not in use, or behind locked doors, especially outside working hours.

B. Personal computers and computer terminals should not be left logged on when unattended or not in use. Personal computers or computer terminals shall be protected from unauthorized access by physical, technical, or administrative controls such as passwords, time driven screensavers, controlled workstation access, operational procedures, etc.

C. Classified or sensitive information should not be printed on a printer located in public areas. However, in the event that public printers must be used to print sensitive or classified information, such information shall be cleared from printers immediately.

D. Users shall adhere to the requirements of **ITS Desktop and Laptop Security Standard**.

5. **Media Storage**

A. Classified information stored on external media (e.g., diskettes or CDs) must be protected from theft and unauthorized access. Such media must be appropriately labeled so as to identify it as classified information.

B. 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. The Division/Office security official shall maintain an inventory of all authorizations and use of removable storage devices. Any use must meet DHHS security policies and standards.

Users shall request the use of state owned storage devices. Division/Offices shall strive to provide state owned-storage devices to staff and there by limit the use of any personal device used to conduct any state business. Any use of personal devices must be disclosed to the supervisor and be approved.

C. Mobile computing devices and removable storage devices (e.g., laptops, PDAs, USB flash drives, etc) must never be left in unsecured areas and their use must meet DHHS Security Standards. Any incidents of misuse, theft or loss of data must be reported to the supervisor and to the Division Security Official. The incident should be reviewed and reported in accordance with the DHHS Incident Management Policy.

D. DHHS sensitive or confidential information shall not be stored at home without appropriate authorization from the user's supervisor/manager, in consultation with the Division/Office Security Official. Users shall follow appropriate physical safeguards for offsite use. Documentation of authorization and storage of sensitive information in the home shall be maintained in accordance with the Division/Office's procedures.

6. **User Privacy**

All users of the Department's information systems are advised that their use of these systems may be subject to monitoring and filtering. DHHS reserves the right to monitor – randomly and/or systematically – the use of Internet and DHHS information systems connections and traffic. Any activity conducted using the State's information systems (including but not limited to computers, networks, e-mail, etc.) may be monitored, logged, recorded, filtered, archived, or used for any other purposes, pursuant to applicable Departmental policies and State and Federal laws or rules. The Department reserves the right to perform these actions with or without specific notice to the user.

7. **Software License Agreements**

A. The theft of computer resources, including computer software, is illegal. All computer software, including software obtained from sources outside the Department, is subject to license agreements that may restrict the User's right to copy and use the software. Software distributed on a trial basis, even

through the Internet, does not suggest that the software is free or that it may be distributed freely.

B. The Department does not require, request, or condone unauthorized use of computer software by its employees, volunteers, and contractors. The Department enforces Federal Public Law 102-561, which strictly prohibits any violation of copyright protection. Violation of copyright protection is considered a felony and is punishable by up to five years in prison and/or fines up to $250,000 for all parties involved.

8. **Computer Viruses: Malicious Code**

A. It is the responsibility of each User to help prevent the introduction and spread of computer viruses and other malicious code. All personal computers in the Department must have virus detection software running at all times. All files received from any unknown source external to the Department, including those on storage on media and electronically downloaded or received as e-mail attachments, except for attachments received via NCMail, must be scanned for computer viruses before opening or using the files. (Attachments received via NCMail are automatically scanned.)

B. Users should immediately contact their manager or supervisor, other appropriate designated staff or the Division/Office Security Official when a virus is suspected or detected, so that it may be confirmed and removed by the appropriate staff.

C. Users must report all information security violations to the Division/Office Security Official, who will notify the DHHS Privacy and Security Office in accordance with the Incident Management policy and procedures. The DHHS Security Officer shall be responsible for notification of the ITS Security Office.

9. **Installation of Hardware or Software**

A. DHHS information system hardware and software installations and alterations are handled by authorized DHHS employees or contractors only. Users shall not install new or make changes to existing information system hardware or software.

B. Users shall not download software from the Internet unless specifically approved by the user's supervisor and the designated IT personnel. Downloading audio or video stream for a work-related webinar or audio conference is permissible without prior authorization.

10. **Remote Access**

A. Authorized users of DHHS's computer systems, networks and data repositories may be permitted to remotely connect to those systems, networks and data repositories to conduct state-related business only. Users will only be granted remote access through secure, authenticated and managed access methods and in accordance with the ITS and DHHS Remote Access Security Policy and Standard.

B. Users shall not access agency networks via external connections from local or remote locations, including homes, hotel rooms, wireless devices, and off-site offices without knowledge of and compliance with the User Access Responsibilities section described above within this policy.

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{ XE "policies" } and procedures{ XE "procedures" }, contact the **Office of Policy & Planning.***

Exceptions

Any exceptions to this policy will require written authorization from the DHHS Security Officer. The DHHS Division or Office will be issued a policy waiver for a defined period of time for granted exceptions. Requests for exceptions to this policy should be addressed the DHHS Security Officer **(DHHS.Security@ncmail.net)**