# DHHS POLICIES AND PROCEDURES

| | |
|---|---|
| **Section VIII:** | **Privacy and Security** |
| **Title:** | **Privacy Manual** |
| **Chapter:** | **Acceptable Use for DHHS Resources** |
| **Current Effective Date:** | **6/1/16** |
| **Original Effective Date:** | **8/1/04** |

## 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"**) resources.

Resources include all platforms (i.e. operating systems), all digital devices (e.g. computers, smart phones, tablets, mainframes, switches, routers, etc.), equipment (e.g. faxes, copiers, phones, etc.), network connections, applications (both developed in-house and acquired from third parties) and the data used, created by or contained within them.

Communications include but are not limited to: faxes, printed documents, recordings, phone calls, social media (e.g. Facebook, Google+, Twitter, Blogs YouTube, Instagram, etc.) and email.

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.

DHHS Divisions/Offices may require additional agreements or policies regarding the confidentiality of specific types of information (e.g. medical records, client case files, personnel records, financial records, etc.). Such supplements may be more restrictive than this policy.

## Implementation

### Rights of Information Ownership

The Department and its Divisions/Offices retain the rights of ownership to all resources and communications including but not limited to data, and related documentation developed by Users on

behalf of the Department, regardless of location or resources used. All Department information resources remain the exclusive property of the State of North Carolina (NC) or the Department, unless otherwise prescribed by other contractual agreements.

## Your Role and Responsibilities

All information and data resources 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. All individuals with access to state-owned data are responsible for the protection and confidentiality of such data. The unauthorized use or disclosure of information provided by these data processing systems may constitute a violation of Department, state, or federal laws which will result in disciplinary action consistent with the policies and procedures of the Department.

Users have a responsibility to ensure, to the best of their ability, that all public information disseminated via Departmental resources and communications is accurate. Users shall provide in association with such information the date at which it was current and a method by which the recipient can contact the staff responsible for making the information available in its current form.

Users are responsible for:

- Safeguarding the information entrusted to the Department from unauthorized use, disclosure, modification, damage or loss
- Limiting the amount of information to the minimum required
- Ensuring that the recipient(s) of the information is/are legally authorized to receive the information
- Reporting weaknesses in computer security, misdirected information, breaches (suspected and confirmed) or incidents (including possible misuse or violation of this policy) immediately to the Division/Office Information Security Official (ISO), who will notify the DHHS Privacy and Security Office
- Reporting theft, loss, or unauthorized disclosure of information

## Rules of Acceptable Use

The resources provided by DHHS are to be utilized both responsibly and professionally; just because an action is technically possible does not mean that it is appropriate. Based on the following principles for acceptable use of Department resources, Users are:

- To protect the confidentiality, integrity and availability of departmental data by behaving in a manner consistent with DHHS's mission and complying with all applicable laws, regulations, policies, standards and guidelines
- To comply with the policies, processes and guidelines for the specific resources to which they have been granted access. When other policies are more restrictive than this policy, the more restrictive policy takes precedence
- To report any potential or identified privacy or security incident to the appropriate privacy or

security staff

- Allowed reasonable use (i.e. incidental personal use) of resources as long as:
    - Such use does not result in direct cost to the Department;
    - Such use does not cause embarrassment to the Department;
    - There is no negative impact on user's performance of their duties; and
    - The use is not prohibited (would not cause legal action against the Department)
- To respect the security and integrity of the department's resources.
- To be considerate of the needs of other Users by making every reasonable effort not to impede the ability of others to utilize resources and show restraint in the consumption of shared resources.
- To respect the rights and property of others, including but not limited to; privacy, confidentiality and intellectual property (e.g. copyright, trademarks, etc.).
- Bound by the department's respective contractual and license agreements when using third party resources.
- To cooperate appropriately during incident response and investigation of potential unauthorized or illegal use of resources.

**Prohibited Uses**

Users may not:

- Attempt to disguise their identity, the identity of their account or the resource that they are using. Users may not attempt to impersonate another person (i.e. use another individual's account) or organization. Likewise users shall not misuse or misrepresent the department's name, resource names, or network address spaces
- Attempt to intercept, monitor (i.e. read), forge, alter (i.e. change) or destroy (i.e. delete) another User's communications without express written permission from the Department CISO
- Use resources in a way that disrupts or adversely impacts (degrades performance of) their legitimate uses or creates interference with/for other users. Such conduct includes, but is not limited to: hacking; illegal peer-to-peer file sharing; unauthorized alteration of resources that are likely to result in the loss of work, resource downtime; or excessive consumption resulting in congestion that interferes with the work of others
- Use resources in an unlawful or illegal manner, including but not limited to; cyberstalking; threats of violence; obscenity (as described in NC General Statute (GS) 14-190.1.); child pornography; or any form that would constitute a criminal offense, a civil liability, or violation of any applicable law. In addition, users may not intentionally access, create, store or transmit material which may be deemed to be offensive, indecent or obscene. This provision applies to any digital communication distributed or sent with or while using Department resources
- Use resources for private business, commercial or political activities, fundraising, non-departmental advertising, or activity that is prohibited by the DHHS Division of Human Resources and Office of State Human Resources
- Download, install or run security software or utilities that reveals weaknesses in resources (e.g. vulnerability scanning, port mapping, network-mapping, etc..); monitors or intercept communications (e.g. packet sniffers, keystroke loggers, etc.); or allows for the attempting to bypass security controls (e.g. password crackers, etc.) without express written permission from

the Department CISO

- Download, install or distribute software to state-owned devices without express written permission from the Division or Office Director
- Knowingly take any action which has the likelihood of introducing any virus, Trojan, malware (spyware, bot, ransomware, etc.) or other harmful software onto Departmental resources; nor should action be taken to deliberately circumvent controls designed to prevent such threats.
- Attempt to access restricted resources or communications without authorization by the appropriate owner or administrator
- Engage in the unauthorized copying, distributing, altering or translating of copyrighted or State-owned materials, software, music or other media without the express permission of the copyright holder or as otherwise allowed by law[1]
- Use resources in a manner that allows for the unauthorized gathering, dissemination or disclosure of confidential data (social security numbers, Personally Identifiable Information (PII), credit card numbers, medical records, Federal Tax Information (FTI), etc.)
- Extend, modify or retransmit network resources beyond what has been configured accordingly by the state or department through the installation of software or hardware (e.g. switches, routers, wireless access points, etc.) without express written permission from the Division or Office Director
- Connect personal devices to the State Network without express written permission from the Division or Office Director (this requirement does not apply to state-supplied "guest" Wi-Fi networks)
- Connect personally-owned "smart" devices (thermostats, wearable tech, appliances) to the State Network
- Share their account(s), passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), or other similar information or devices used for identification and authorization purposes
- Download State data to personally owned devices without express written permission from the Division or Office Director
- Attempt to obtain extra resources beyond those allocated, or circumvent information security measures

## Requirements

- All devices connected to the State Network must have updated malware/antivirus protection
- Users must ensure all files downloaded from an external source to the State Network or any device connected to the State Network, including a diskette, compact disc (CD), USB flash drive, or any other electronic medium, is scanned for malicious software such as viruses, Trojan horses, worms or other malicious code
- Systems administrators and authorized users must not divulge remote connection information or other access points to information technology resources to anyone without proper authorization
- Users must ensure that the transmission or handling of personally identifiable information

[1] Information on the Digital Millennium Copyright Act can be found at: http://www.copyright.gov/legislation/dmca.pdf and the Copyright Act at: http://www.copyright.gov/title17/.

(PII) or other sensitive data is encrypted or has adequate protection
- Users accessing the State Network through a Local Area Network (LAN) must avoid unnecessary network traffic and interference with other users
- Access to the Internet from state-owned, home based, devices must adhere to all acceptable use policies. Employees must not allow family members or other non-employees to access nonpublic accessible information systems

**User Privacy**

All users of the department's information systems are advised that their use of these resources and certain communications may be subject to monitoring and filtering. DHHS reserves the right to monitor – randomly 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.

**Software License Agreements**

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

The theft of software is illegal. The department does not require, request, or condone unauthorized use of 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 (5) years in prison and/or fines up to $250,000 for all parties involved.

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 software 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, provided it is limited to the minimum amount of time necessary.

**Enforcement**

*For enforcement questions or clarification on any of the information contained in this policy, please contact the DHHS Privacy and Security Office. For general questions about department-wide policies and procedures, contact the DHHS Policy Coordinator.*

**USER CERTIFICATION OF NOTIFICATION AND AGREEMENT OF COMPUTER USE POLICY**

I certify that I am an employee, volunteer, guest, vendor or contractor working for or on behalf of the Department of Health and Human Services and that I have read this "Acceptable Use Policy" and understand my obligations as described herein. I understand that this policy was approved by the Secretary of the Department of Health and Human Services and these obligations are not specific to any individual division or office of the department, but are applicable to all employees, volunteers, and contractors of the department. I understand that failure to observe and abide by these obligations may result in disciplinary action, which may include dismissal and/or contract termination. I also understand that in some cases, failure to observe and abide by these obligations may result in criminal or other legal actions. Furthermore, I have been informed that the department will retain this signed agreement on file for future reference. A copy of this agreement shall be maintained in the personnel file and/or in the contract administration file.

_____

Print Name

_____ _____

Employee, Volunteer, Guest, Vendor or Contractor Signature Date

_____ _____

Supervisor's Signature Date