NC DEPARTMENT OF HEALTH AND HUMAN SERVICES

DEPARTMENT: NC DHHS Privacy and Security Office	**POLICY NAME:** Acceptable Use for DHHS Resources
PAGE: 1 of 9	**REPLACES POLICY DATED:** 6/1/16
CURRENT EFFECTIVE DATE: 4/22/2020	**ORIGINAL EFFECTIVE DATE:** 8/1/04
REVISED DATE: 1/31/2020, 4/22/2020, 6/2/2021, 9/24/2024 **REVIEW DATE:** 11/1/19, 4/22/2020,6/2/2021	**APPROVED DATE:** 8/1/04
APPROVED BY: Ray Yepes, CIRO; Pyreddy Reddy, CISO; 9/23/2024	

SCOPE:

This policy applies to NC DHHS Department Divisions/Offices and its employees.

PURPOSE

This Acceptable Use Policy (AUP) 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.) MS Teams 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.

Roles 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 policy, 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:

1. Safeguarding the information entrusted to the Department from unauthorized use, disclosure, modification, damage, or loss.

2. Limiting the amount of information to the minimum required.

3. Ensuring that the recipient(s) of the information is/are legally authorized to receive the information.

4. Reporting weaknesses in computer security, misdirected information, breaches (suspected and confirmed) or incidents (including possible misuse or violation of this policy) immediately to the DHHS Privacy and Security Office. This can be reported via the following website: https://security.ncdhhs.gov/

5. Reporting theft, loss, or unauthorized disclosure of information.

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.

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:

1. 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.

2. 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.

3. To report any potential or identified privacy or security incident to the appropriate privacy or security staff.

4. Allowed reasonable use (i.e. incidental personal use) of resources if:
    a. Such use does not result in direct cost to the Department,
    b. Such use does not cause embarrassment to the Department,
    c. There is no negative impact on user's performance of their duties, and
    d. The use is not prohibited (would not cause legal action against the Department)

5. To respect the security and integrity of the department's resources.

6. 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.

7. To respect the rights and property of others, including, but not limited to, privacy, confidentiality, and intellectual property (e.g. copyright, trademarks, etc.).

8. Bound by the department's respective contractual and license agreements when using third party resources.

9. To cooperate appropriately during incident response and investigation of potential unauthorized or illegal use of resources.

Requirements

1. Users may not connect personal devices to the DHHS or State's Network without prior approval from the Division or Offices Information Security Official (ISO). This requirement does not apply to users who connect to the DHHS Network through a Department-supplied "guest" Wi-Fi network.
2. Users may not connect **prohibited** personal devices on agency property for the purpose of conducting non-work-related activities and/or activities that have not been approved in advance by management. **Prohibited** personal devices include thumb drives, electronic notebooks, tablets, or laptops.
3. Personally owned "smart" devices may not be connected to the State Network. "Smart" devices, commonly referred to as the "Internet of Things," include smart thermostats, smart appliances, or wearable technologies.
4. All devices connected to the State Network must have updated malware/anti-virus protection.
5. Users must not attempt to access any data, documents, email correspondence, and programs contained on systems for which they do not have authorization.
6. Systems administrators and authorized users must not divulge remote connection information or other access points to information technology resources to anyone without proper authorization.
7. Users must not 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.
8. Users must not use their state credentials, e.g., .gov email addresses, for non-official tasks.
9. Users must not make unauthorized copies of copyrighted or state-owned software.
10. Users must not download, install, or distribute software to state-owned devices unless it has been approved by the agency head or the agency head's designee.
11. 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.
12. Users must ensure that the transmission or handling of personally identifiable information (PII) or other restricted or highly restricted data is authorized and encrypted.
13. Users must not download State data to personally owned devices unless approved by the agency head or the agency head's designee.
14. Users must comply with the State's Data Retention Guideline located at https://archives.ncdcr.gov/government/state-government-agencies/functional-schedule/information-technologytechnology. **Note**: Per the NC Department of Natural and Cultural Resources (DNCR), *OneDrive for Business: Best Practices and Usage, "*OneDrive for Business is not intended for permanent storage of public records."

    See: https://archives.ncdcr.gov/government/digital-records/digital-records-policies-and-guidelines/microsoft-365-best-practices-and-usage365-best-practices-and-usage. Long term

storage and collaboration efforts must utilize other available tools, e.g., Microsoft SharePoint.

15. Users must not purposely engage in activity that is illegal according to local, state or federal law, or activity that may harass, threaten or abuse others, or intentionally access, create, store or transmit material which may be deemed to be offensive, indecent or obscene such as racially or sexually explicit materials.
    a. This includes intentionally creating, viewing, storing or transmitting pornographic material using Departmentally managed networks or devices such as laptops, desktops, cell phones or any device capable of connecting to a network.
    b. Employees who have official duties that are in alignment with G.S. 143-805(d) are exempted from this provision while in performance of those job duties.
16. Users accessing the State Network through a Local Area Network (LAN) must avoid unnecessary network traffic and interference with other users. Specific prohibitions include, but are not limited to, the following:
    a. Unsolicited commercial advertising by public employees and State Network users. For the purpose of this policy, "unsolicited commercial advertising" includes any transmission initiated by a vendor, provider, retailer, or manufacturer of goods, products, or services, or by a third party retained by, affiliated with, or related to the vendor, provider, retailer, or manufacturer that describes goods, products, or services. This prohibition does not include the following:
        i. 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 to or affiliated with the vendor, provider, retailer, or manufacturer);
        ii. responses to questions, but only if such responses are direct replies to those who inquired via electronic mail, or (iii) 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.
    b. Any other type of mass mailing by employees and others accessing the State Network through the agency LAN that does not pertain to governmental business or a state-sponsored activity.
17. Users accessing the State Network through an agency LAN must only access Internet-streaming sites as consistent with the mission of the agency for the minimum amount of time necessary.
18. Users must not engage in activity that may degrade the performance of information resources, deprive an authorized user access to resources, obtain extra resources beyond those allocated, or circumvent information security measures.
19. Users must not download, install or run security programs or utilities such as password cracking programs, packet sniffers, or port scanners that reveal or exploit weaknesses in the security of information technology resources unless approved in writing by the agency head or the agency head's designee.

20. Users must not operate any utility, application, or service that would obfuscate or anonymize user or device identity (e.g., IP address, MAC address, user identity, geographic location, etc.). Such services include, but are not limited to, the following: personal or 3rd Party VPN, Private Relay, and Tor.
21. Information technology resources must not be used for personal benefit, e.g., gambling, political activity, unsolicited advertising, unauthorized fund raising, personal business ventures, or for the solicitation of performance of any activity that is prohibited by any local, state, or federal law.
22. 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 data classified as restricted or highly restricted.
23. Users must report any weaknesses in computer security to the appointed agency security liaison or designee for follow-up investigation. Reports shall be made within 24 hours of discovery by using the following website https://security.ncdhhs.gov/. For the purpose of this AUP, weaknesses in computer security include unexpected software or system behavior, which may indicate an unauthorized disclosure of information or exposure to security threats.
24. Users must report any incidents of possible misuse or violation of this policy.
25. Users have a responsibility to promptly report the theft, loss or unauthorized disclosure of information using the following link https://security.ncdhhs.gov/.
26. Users should not use unauthorized Cloud Services (e.g., file storage/sharing services like Dropbox, Google Drive, etc.) for sharing of state data.
27. Users must not send state data to non-authorized individuals or accounts or services via an auto-forwarding capability. Forwarding of state data must comply with the measures outlined within this policy.
28. Users wishing to use any type of audio of video recording devices or software must follow Divisions or Offices policies and procedures on their use.
29. Users shall not 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.
30. Attempt to access restricted resources or communications without authorization by the appropriate owner or administrator.
31. Users shall not 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.
32. Users shall not use resources in a manner that allows for the unauthorized gathering, dissemination, or disclosure of confidential data such as social security numbers, Personally Identifiable Information (PII), credit card numbers, medical records or Federal Tax Information (FTI).
33. Users will not 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.

34. Users wishing to gain approval to work while overseas must gain approval from their supervisor and ISO prior to traveling. Approval can be requested by filling out the "Attestation to Travel Abroad Request".
35. Any use of publicly available AI tools (Chat GPT, Copilot, Gemini etc) shall follow best practices. Further guidance on this can be found in the Related Documents section of the AUP.

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

Failure of the Department's Users to comply with this Acceptable Use Policy and Information Security Policies and Standards set forth by the State and the Department may result in disciplinary actions up to and including termination of employment. Any unauthorized intentional or as a result of negligence disclosure of information shall constitute grossly inefficient job performance. A violation of the Acceptable Use Policy that results in serious loss of or damage to state property or funds which adversely impacts the state, agency or the business unit constitutes grossly inefficient job performance.

Failure of the Department's contractors to comply with Acceptable Use Policy or other Security Policies and Standards may result in termination of their contract.

The Department may also pursue or may assist other parties in pursuing legal remedies for violations of law or for recovery of damages resulting from violation of information security policies and standards.

For questions or clarification on any of the information contained in this policy, for general questions about department-wide policies and procedures, contact the ***DHHS PSO Policy Writer.***

Related Documents

Users are responsible for reviewing and understanding the Statewide Information Security Manual and NC DHHS policies. Users are responsible for complying with these policies and standards and best practices.

- NCDIT Statewide Information Security Manual
- NCDIT Statewide Data Classification & Handling Policy
- NC DIT AI Corner
- Teleconferencing Security Tips | NCDIT
- NC DIT International Travel Policy
- NC DHHS Security Manual
- NC DHHS Privacy Manual

USER CERTIFICATION OF NOTIFICATION AND AGREEMENT TO THE NC DHHS ACCEPTABLE USE POLICY

I certify that I am an employee, volunteer, guest, vendor or contactor 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 actions, which may include dismissal and / or contract termination. I also understand that in some cases, failure to observe and abide by these obligations may results 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 Contract Signature Date

_____ _____

Supervisor's Signature Date