NC DEPARTMENT OF
HEALTH AND
HUMAN SERVICES

North Carolina Department of Health and Human Services

Acceptable Use Policy (AUP)

Department-wide IT Policy

September 2025

Document Information

Revision History

Date	Version	New or Revised Requirement	Description	Author
July 21, 2025	1	New	Updated with AI content	Jason Gilmore

Document Details

Department Name	NC DHHS Privacy and Security Office
Owner	DHHS Chief Information Security Officer
Title	Acceptable Use Policy (AUP)
Publication Date	September 8th 2025
Next Release	
Document Type	
Document Number	1
Version	1

Table of Contents

Purpose

Information resources are strategic assets of the State of North Carolina and must be treated and managed as valuable resources. The purpose of this policy is to do the following:

1. Establish minimum appropriate and acceptable requirements regarding the use of information resources connected to the State Network.
2. Comply with applicable Department requirements, state and/or federal law and other rules and regulations regarding the management of information resources.
3. Educate individuals who may use information resources with respect to their responsibilities associated with computer resource use.
4. Establish a process to ensure that users acknowledge and agree to abide by the rules of behavior before gaining access to information resources connected to the State Network

Owner

N.C. Department of Health and Human Services - Chief Information Security Officer

Scope

This policy applies to any employee, contractor or third party (hereinafter, "**Users**") of Department and/or State resources.

Policy

Section 1. Agency Policy Requirements and Exceptions

The Statewide Information Security Policies require DHHS to adopt an acceptable use policy that describes responsibilities and expected behavior for the use of the State Network, information, and information systems. (Security Planning Policy, PL-4 – Rules of Behavior, Personnel Security Policy, PS-6 – Access Agreements).

This Acceptable Use Policy sets out the minimum requirements for the use of DHHS or State resources.

Divisions or Offices who need any Exceptions to the minimum requirements identified in this must follow the DHHS process for obtaining an approved Security Exception by the DHHS Privacy and Security Office.

This Acceptable Use Policy shall be reviewed annually, at a minimum.

Section 2. Application

This policy applies to any state employee, contractor or third party who uses any device, whether state-owned, personal, or belonging to a third-party, to directly or indirectly connect to the State Network, or uses any other IT Resource. G.S. 143B 1370(a)(5) (g) defines the State Network as "any connectivity designed for the purpose of providing Internet Protocol transport of information for State agencies." State law also requires the N.C. Department of Information Technology (NCDIT) to manage the State Network. IT Resource include all platforms (i.e. operating systems), all electronic 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.

Each DHHS Division/Office shall be responsible for ensuring that every individual seeking access to the State network and/or information systems or other IT Resource 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 State systems and IT Resources that connect to the State Network and annually thereafter.

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, federal, or DHHS 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, access, use, and disclosure of information to the minimum required.

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

Rights of Information Ownership

The Department and its Divisions/Offices retain the rights of ownership to all IT 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 IT 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 or authorized. Based on the following principles for acceptable use of Department resources, users are:

1. To protect the confidentiality, integrity, and availability of state, federal, or 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 IT Resource 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 Officer or Information Security Official (see section titled "Reporting" below)

4. To respect and preserve the security and integrity of the Department's and its partner's IT Resources.

5. To be considerate of the needs of other Users by making every reasonable effort not to impede the ability of others to utilize IT Resources and show restraint in the consumption of shared resources.

6. To respect the rights and property of others, including, but not limited to, privacy, confidentiality, and intellectual property (e.g. copyright, trademarks, etc.). Users must not attempt to access restricted resources or communications without authorization by the appropriate owner or administrator.

7. To be bound by the department's respective contractual, license, or other agreements when using third party resources.

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

Section 3. Requirements

Use of Personal Devices

1. Users may not connect personal devices to the State Network without express written permission from the agency head or the agency head's designee. This requirement does not apply to users who connect to the State Network through a state-supplied "guest" Wi-Fi network.

2. Users may not connect prohibited personal devices on State Network 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 and other portable 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. Users are prohibited from downloading State data to personally owned devices unless approved by the agency head or the agency CIO. Access to State email, or M365 applications on a personally owned device must be authenticated leveraging Multi Factor Authentication (MFA) via the Microsoft Authenticator App, or another approved MFA method such as phone call or SMS message.

Access to the Network

1. All devices connected to the State Network must have updated malware/anti-virus protection. Users must accept software updates whenever provided, in accordance with statewide security update requirements. Users must not download or utilize independent malware/anti-virus protection not approved or authorized by the Agency.

2. Users must not attempt to access any data, documents, email correspondence, and programs contained on systems for which they do not have authorization.

3. Systems administrators and authorized users must not divulge remote connection information or other access points to information technology resources to anyone without proper authorization.

4. 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.

5. Users must not use their state credentials, e.g., .gov email addresses, for non-official tasks.

6. 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 VPN, Private Relay, and Tor.

7. 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.

8. 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 state-owned or issued devices or data classified as restricted or highly restricted.

9. Users should not use unauthorized Cloud Services (e.g., file storage/sharing services like DropBox, Google Drive, etc.) for sharing of state data.

Downloading and Copying

1. Users must not make unauthorized copies of copyrighted or state-owned software.

2. Users must not download State or federal data to personally owned devices unless approved by the agency head or the agency head’s designee.

3. 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.

4. 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.

5. 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 IT Resources

6. 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.

7. Users are prohibited from viewing or downloading pornography, as that term is defined under G.S 143-805, on government networks and devices owned, leased, maintained, or controlled by the agency.
    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

Performance

1. 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.

2. 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.

3. Users wishing to use any type of audio or video recording device or software must follow Division’s or Office’s policies and procedures on their use.

4. 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.

5. 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, Medicaid ID number, medical records (PHI and/or ePHI), or Federal Tax Information (FTI).

6. 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.

7. Employees who intend to work while traveling internationally must obtain prior approval from senior leadership within their Division or Office and at the Department level. To start the approval process, the user should contact their Information Security Official (ISO). The ISO will provide them with the NC DHHS Security Exception Form C. Once the form is submitted the review/approval process will take a minimum of 6 weeks. If permission is granted the user will be required to follow the Statewide International Travel Policy for the duration of their trip.

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, contractors, or third parties. 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 an 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.

Retention

1. Users must comply with the State's Data Retention Guideline located at https://archives.ncdcr.gov/government/state-government-agencies/functional-schedule/information-technology. **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."

2. **See:** https://archives.ncdcr.gov/government/digital-records/digital-records-policies-and-guidelines/microsoft-365-best-practices-and-usage. Long-term storage and collaboration efforts must utilize other available tools, e.g., Microsoft SharePoint.

3. Users are responsible for all data generated by publicly available AI tools and all data is subject to retention guidelines.

Transmission

1. Users must not purposely engage in activity that is illegal according to local, state or federal law, 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.

2. Users must ensure that the transmission or handling of personally identifiable information (PII) or other restricted or highly restricted data is authorized and encrypted.

3. 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.

4. 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.

Reporting

1. Users are obligated to report any weaknesses in computer and other IT Resource security, including unexpected software or system behavior that may indicate unauthorized disclosure of information or exposure to security threats. Additionally, any incidents of possible misuse or violation of the Acceptable Use Policy, as well as the theft, loss, or unauthorized disclosure of information and IT Resources, must be reported. All such reports should be submitted to the DHHS Privacy and Security Office at https://security.ncdhhs.gov for follow-up investigation.

2. Reports shall be made within 24 hours of initial discovery using the NC DHHS Incident Reporting form at: https://security.ncdhhs.gov/.

    a. If the report involves data classified as Federal Tax Information, **report must be made immediately but not more than 24 hours**; if it involves Social Security Administration or CMS data the **report must be made immediately but not more than 1 hour of discovery.**

Artificial Intelligence and Generative Artificial Intelligence, (collectively referred to here as "AI")

Artificial Intelligence is a broad term used to describe an engineered system where machines learn from experience, adjusting to new inputs, and potentially performing tasks previously done by humans. More specifically, it is a field of computer science dedicated to simulating intelligent behavior in computers. It may include automated decision-making (International Association of Privacy Professionals, Glossary, https://iapp.org/resources/glossary, 2024).

Generative AI (GenAI) is a field of Artificial Intelligence that uses deep learning trained on large datasets to create content, such as written text, code, images, music, simulations and videos, in response to user prompts (International Association of Privacy Professionals, Glossary, https://iapp.org/resources/glossary, 2024).

This policy does not apply to basic AI embedded within common commercial products, such as predictive text in word processors or dynamic route adjustment based on real-time traffic conditions in map navigation systems, while noting that government use of such products must nevertheless comply with applicable law and policies to assure the protection of security, privacy, rights, and state value.

No publicly available or free version of any AI tool may be installed on any State IT Resource without specific approval from the appropriate (Division or Office) DHHS Information Security Official.

The North Carolina Responsible Use of Artificial Intelligence Framework establishes guiding principles for the ethical, transparent, and effective use of AI tools in state agencies. To align with this framework, all users must adhere to these standards to ensure AI tools are deployed ethically and responsibly, protecting privacy, promoting equity, and minimizing risks. The following requirements outline the key actions users must take to comply with these principles and support the responsible use of AI, which includes GenAI:

1. Never enter personally identifiable (PII) or confidential information into publicly available AI tools.

2. Prior to entering any code into or using code generated by a publicly available AI tool, obtain agency CIO and Information Security Official approval, and only use an AI tool that has been deemed trustworthy by Enterprise Security Risk Management Office (ESRMO).

3. Review and independently fact check any output produced by publicly available AI tool.

4. Be transparent and identify when content was drafted using publicly available AI tools, and the tool that was used.

5. Users must disable chat history and opt-out of providing conversation history as data for training publicly available AI tool models prior to use.

6. Assess the risks of any use of publicly available AI tool and mitigate risks whenever possible.

Data Privacy

Across the U.S. and around the world, privacy laws have been enacted to govern the collection, maintenance, use and dissemination of information about individuals. The State of North Carolina has adopted the Fair Information Practice Principles (FIPPs) to guide privacy and security policy. Employees should consider the Fair Information Practice Principles as best practices.

Implementing these principles reduces the risk of unauthorized disclosure of information and supports the creation of reliable records to inform decision-making.

The eight guiding principles that are commonly accepted and form the Fair Information Practice Principles in the United States are:

- **Transparency:** The organization should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of personally identifiable information (PII).

- **Individual Participation:** Consent should be sought from the individual for the collection, use, dissemination, and maintenance of PII. A mechanism should also be provided for appropriate access, correction, and redress regarding the organization's use of PII.

- **Purpose Specification:** The organization should specifically articulate the authority that permits the collection of PII and the purpose(s) for which the PII is intended to be used.

- **Data Minimization:** The organization should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as it is necessary to fulfill those purpose(s).

- **Use Limitation:** The organization should use PII solely for the purpose(s) specified in the notice. Sharing PII outside of the organization should be for a purpose compatible with the purpose(s) for which the PII was collected.

- **Data Quality and Integrity:** The organization, to the extent practicable, should ensure that PII is accurate, relevant, timely and complete.

- **Security:** The organization should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

- **Accountability and Auditing:** The organization should be accountable for complying with these principles, providing training to all employees, contractors or third parties who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

DHHS 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 randomly or systematically monitor the use of Internet and DHHS information systems, connections, and traffic. Any activity conducted using the state’s IT Resources (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.

Section 4. Incidental Use

State systems are intended for primarily business purposes, but limited incidental and occasional personal use may be permissible when authorized by your management and it’s use complies with the following:

1. Such use does not result in direct cost to the Department,
2. Such use does not cause embarrassment to the Department,
3. There is no negative impact on the user’s performance of their duties, and the use is not prohibited by the resource owner and would not form the basis for legal action against the Department
4. Does not involve interests in personal or outside business and/or other non-authorized organizations and activities such as selling or soliciting personal property/items, promoting commercial ventures, charitable, religious, or political activities
5. Incidental personal use of electronic mail, Internet access, fax machines, printers, copiers, and any other IT resources is limited to employees only. This does not include family members.

Section 5. Violations

Failure of the Department employees to comply with this Acceptable Use Policy (and all Security and Privacy Policies and Procedures) set forth by the State and the Department may result in disciplinary action, termination, loss of IT Resources, or personal legal consequences. Any unauthorized disclosure of information (intentional or negligent) 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 that adversely impacts the state, Department, or a business unit constitutes grossly inefficient job performance.

Failure of Department contractors to comply with the Acceptable Use Policy (and all other Security and Privacy Policies and Procedures) 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, such as the Acceptable Use Policy.

Section 6. Acknowledgement of Policy

NCDHHS employees, contractors, or third parties must acknowledge in writing that they have received a copy of this policy. Written acknowledgement is also required annually on a date determined by Human Resources.

I have read, understand, and will abide by the above Acceptable Use Policy when using computer and other IT Resources owned, leased, or operated by the state. I further understand and will abide by the above Acceptable Use Policy when using personal computing devices not owned, leased, or operated by the state. I further understand that I have no expectation of privacy when connecting any device to the State Network and that a violation of the Acceptable Use Policy may be deemed by the Department to be unethical and may constitute a civil or criminal offense. Should I commit any violation of The Acceptable Use Policy my access privileges may be revoked, disciplinary action may be taken, and/or appropriate legal action may be initiated.

________________________________ ________________________
Name Date

____
User Signature

References

The following sections in the Statewide Information Security Manual provide additional guidance in the appropriate use of State information technology resources.

Access Control Policy, AC-2 – Account Management
Access Control Policy, AC-4 – Information Flow Enforcement
Access Control Policy, AC-17 – Remote Access
Access Control Policy, AC-18 – Wireless Access
Access Control Policy, AC-20 – Use of External Information Systems
Configuration Management Policy, CM-9 – Configuration Management Plan
Configuration Management Policy, CM-10 – Software Usage Restrictions
Configuration Management Policy, CM-11 – User Installed Software
Personnel Security Policy, PS-6 – Access Agreements
Security Planning Policy, PL-4 – Rules of Behavior
System and Information Integrity Policy, SI-3 – Malicious Code Protection
System and Information Integrity Policy, SI-8 – Spam Protection
System and Information Integrity Policy, SI-12 – Information Handling and Retention

The following Office of Privacy and Data Protection policies provide additional guidance in the appropriate use of State information technology resources.

State Adoption of Fair Information Practice Principles
Media Protection Policy
North Carolina State Government Responsible Use of Artificial Intelligence Framework
Principles for Responsible Use of AI
NCDIT Statewide Data Classification & Handling Policy
NC DIT AI Corner
NC DIT International Travel Policy
NC DHHS Security Manual
NC DHHS Privacy Manual