NCDIT NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

# State of North Carolina

## Acceptable Use Policy

**Statewide IT Policy**

January 2025

# Document Information

## Revision History

| Date | Version | New or Revised Requirement | Description | Author |
|---|---|---|---|---|
| Jan 28, 2025 | 1 | New | Updated with AI content | Chris Brittingham |

## Document Details

| | |
|---|---|
| **Department Name** | Enterprise Security and Risk Management Office |
| **Owner** | State Chief Risk Officer |
| **Title** | Acceptable Use Policy (AUP) |
| **Publication Date** | January 25, 2025 |
| **Next Release** | January 1, 2026 |
| **Document Type** | DRAFT |
| **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 state 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 Information Technology – State Chief Risk Officer

# Scope

This policy applies to state agencies, departments and other entities not specifically excluded from Article 15 of N.C. General Statute Chapter 143B.

# Policy

Use this section to create policy requirements.

## Section 1. Agency Policy Requirements and Exceptions

The Statewide Information Security Policies require agencies 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 development and use of individual agency use. Agencies may adopt more stringent policies.

Exceptions to the minimum requirements in this policy template must be approved in writing by the State Chief Information Officer. Agencies must use the Department of Information Technology (DIT) Exception Request Process and Form to request any exception(s) to this policy.

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

## Section 2. Agency Template

State agencies may use the following template for their acceptable use policies. Agencies that choose not to use the template must include all the elements of Sections 1-4 within the following Acceptable Use Policy for their agency use. If agencies choose to allow incidental personal use of information technology resources, they must include the minimum requirements of Section 3 – Incidental Use—of this policy (p. 6) within their own Acceptable Use Policy.

# Statewide Acceptable Use Policy

## Section 1. Application

This policy applies to any state employee, contractor or third party who uses any device, whether state-owned or personal, to connect to the State Network. 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 North Carolina Department of Information Technology (NCDIT) to manage the State Network.

## Section 2. 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. 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.
3. 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 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 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 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.
6. Users are prohibited from viewing or downloading pornography on government networks and devices owned, leased, maintained, or controlled by the agency.

### 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.

### 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."

   **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.
2. 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, 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.
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 must report any weaknesses in computer security to the appointed agency security liaison or designee for follow-up investigation. Weaknesses in computer security include unexpected software or system behavior, which may indicate an unauthorized disclosure of information or exposure to security threats.
2. Users must report any incidents of possible misuse or violation of the Acceptable Use Policy within a reasonable amount of time.
3. Users have a responsibility to promptly report the theft, loss or unauthorized disclosure of information within a reasonable amount of time.

**Artificial Intelligence (AI) and Generative Artificial Intelligence (GenAI)**

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 and GenAI tools are deployed ethically and responsibly, protecting privacy 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:

1. Never enter personally identifiable (PII) or confidential information into publicly available generative AI tools.
2. Prior to entering any code into, or using code generated by, a publicly available generative AI tool, seek agency CIO and security approval, as well as using 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 generative AI.
4. Be transparent and identify when content was drafted using publicly available generative AI.
5. Users must disable chat history and opt-out of providing conversation history as data for training publicly available generative AI models prior to use.
6. Assess the risks of any use of publicly available generative AI 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 and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

## Section 3. 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 does not do the following:

1. Interfere with the normal performance of an employee's work duties.
2. Result in direct costs to the agency, cause legal action against, or cause embarrassment to the agency. Agencies should restrict incidental personal use of electronic mail, Internet access, fax machines, printers, copiers, and any other information technology resources to employees. This does not include family members.

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.

## Section 4. Violations

Violation of this policy could result in disciplinary action, termination, loss of information resources and criminal prosecution.

## Section 5. Acknowledgement of Policy

DIT employees and contractors 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 electronic resources owned, leased, or operated by the state. I further understand that will abide by the above Acceptable Use Policy when using personal computing devices not owned, leased, or operated by the state agency. I further understand that I have no expectation of privacy when connecting any device to the State Network and that any violation of the regulations above is unethical and may constitute a criminal offense. Should I commit any violation of this 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