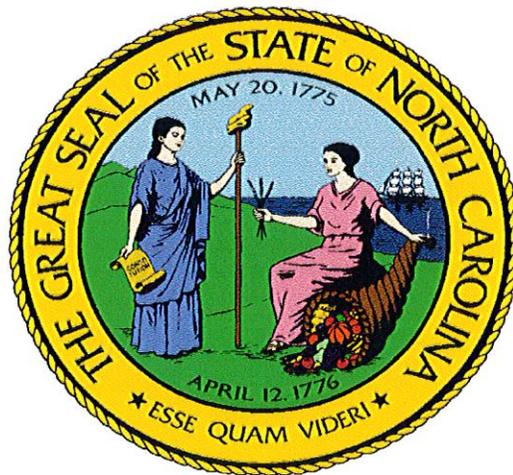


NORTH CAROLINA DEPARTMENT OF ADMINISTRATION

POLICIES AND PROCEDURES

ACCEPTABLE TECHNOLOGY USE POLICY



INTRODUCTION

It is the policy of the Department of Administration to conduct all business activities relating to the purchase and payment of goods and services in accordance with all applicable laws, rules, regulations and business standards.

PURPOSE

The Department of Administration (DOA) recognizes that for certain job functions it is critical that an employee have access to the State's Network.

References and Applicable Laws:

G.S. 143B—1336(a)(5)

SCOPE

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—1336(a)(5) 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 Department of Information Technology (DIT) to manage the State Network.

POLICY

025. **Requirements**

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 such devices as thermostats, wearable technologies, or appliances.
3. All devices connected to the State Network must have updated malware/anti-virus protection.
4. Users must not attempt to access any data, documents, email correspondence, and programs contained on systems for which they do not have authorization.
5. Systems administrators and authorized users must not divulge remote connection information or other access points to information technology resources to anyone without proper authorization.
6. 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.
7. Users must not make unauthorized copies of copyrighted or state-owned software.
8. 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.
9. Users must ensure that the transmission or handling of personally identifiable information (PII) or other sensitive data is encrypted or has adequate protection.
10. Users may 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 not download State data to personally owned devices unless approved by the agency head or the agency head's designee.
12. 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.

13. 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.
14. 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.
15. 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.
16. 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.
17. Information technology resources must not be used for personal benefit, 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.
18. 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.
19. Users must report any weaknesses in computer security to the Department of Administration's 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.
20. Users must report any incidents of possible misuse or violation of the Acceptable Use Policy.
21. Users have a responsibility to promptly report the theft, loss or unauthorized disclosure of information.

026. **Violations**

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

027. **Acknowledgement of Policy**

Department of Administration employees and contractors must acknowledge in writing or via LMS that they have received a copy of this policy. 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 Department of Administration. I further understand that I will abide by the above Acceptable Use Policy when using personal computing devices not owned leased, or operated by the Department of Administration. 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.

User Signature

Date

Approved by the Secretary of Department of Administration:	 Kathryn Johnston
Approval Date:	Version : ADM 025-027 (V.1) – 5/12/2016
Effective Date:	
Revision Date:	

THIS POLICY SUPERSEDES ALL ACCEPTABLE TECHNOLOGY POLICY