Office of the Governor
State Chief Information Officer

Security Policy

Title: Use of the North Carolina state Network and the Internet

Purpose: To establish a policy pertaining to the use of the state network and the global Internet by public staffs and other network users.

Scope: This policy applies to all public agencies, their agents or designees subject to Article 3D of Chapter 147, "State Information Technology Services." Use by local governments, LEAs, community colleges, constituent institutions of the University of North Carolina and other public agencies is encouraged to the extent allowed by general statutes.

BACKGROUND

The Internet is a worldwide collection of interconnected networks. The State's wide area network, the "state network", is one of many networks connected to the Internet. Electronic tools associated with Internet access, such as electronic mail (E-mail) and the World Wide Web (WWW), help public agencies streamline information access and conduct business. These tools are used with the state network to facilitate inter-agency communication and information processing. These same tools are used for communications between public agencies and entities on the Internet, such as other government organizations, educational institutions, private businesses, and citizens.
There are many parallels between the new electronic information tools and older technologies used for similar purposes (for example, telephones and written correspondence). As such, the same general concepts of professionalism and appropriate use of publicly owned or publicly provided information processing resources apply.
Increasing numbers of public staffs now access the Internet. Public use of publicly provided information on the state network is also growing. Public staffs have stewardship responsibilities for public information. The open connection afforded by Internet access underscores the need for heightened awareness among public employees regarding prudent behavior as it pertains to information dissemination and access.

POLICY STATEMENT

1. While in performance of work-related functions, while on the job, or while using publicly owned or publicly provided information processing resources, public employees and other state network users are expected to use the state network and the Internet responsibly and professionally and shall make no intentional use of these services in an illegal, malicious, or obscene manner. Public employees and state network users may make reasonable personal use of publicly owned or provided state network or Internet resources as long as:

   a. The direct measurable cost to the public is none or is negligible or access supports the mission of the agency;
   b. There is no negative impact on employee performance of public duties;

c. The policy is applied equitably among all employees of the agency;
d. Employees shall reimburse the agency if costs are incurred, provided that costs may be incurred only in critical situations.

2. When sending or forwarding E-mail over the state network or the Internet, public employees and other state network users shall identify themselves clearly and accurately. Anonymous or pseudonymous posting is expressly forbidden, unless otherwise allowed by law to make anonymous postings.

3. Public employees, to the best of their ability, have a responsibility to make sure that all public information disseminated via the state network and the Internet is accurate. Employees shall provide in association with such information the date at which it was current and an electronic mail address allowing the recipient to contact the public staff responsible for making the information available in its current form.

4. All files downloaded from a source external to the state network that might potentially harbor a virus, Trojan horse, worm or other destructive code must be scanned, if the technology permits, for such harmful contents. This includes files obtained as e-mail attachments and by any other file transfer mechanism. It is the responsibility of public employees and state network users to help prevent the introduction or propagation of computer viruses. All agencies will be held responsible for ensuring that they have current software on their network to prevent the introduction or propagation of computer viruses.

5. The Internet provides easy access to software distributed by companies on a trial basis. This free access does not indicate that the software is free or that it may be distributed freely. All applicable software copyright and licensing laws must be followed.

6. Public employees and other state network users shall avoid unnecessary network traffic and interference with other users including but not limited to:

6a. Unsolicited commercial advertising by public employees and other state network users is strictly forbidden. For the purpose of this Policy, "Unsolicited Commercial Advertising" includes any transmission that describes goods, products, or services and that is initiated by a vendor, provider, retailer, or manufacturer of the described goods, products, or services, or by a third party retained by, affiliated with, or related to the vendor, provider, retailer, or manufacturer. For purposes of this definition the vendor, provider, retailer or manufacturer must be a non-governmental entity. This prohibition shall not include either (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.
6b. Any other type of mass mailing by public employees and other state network users, which meets both conditions: 1. Does not pertain to governmental business and 2. Results in network spamming is strictly forbidden. Additionally, public employees and other state network users must access Internet “streaming” sites as consistent with the mission of the agency for the minimum amount of time necessary to obtain the information originally sought.
6c. Public employees and other state network users shall not stalk others, post, transmit, or originate any unlawful, threatening, abusive, fraudulent, hateful, defamatory, obscene, or pornographic communication, or any communication where the message, or its transmission or distribution, would constitute a criminal offense, give rise to civil liability, or otherwise violate any applicable law.

6d. Public employees and other state network users shall not access or attempt to gain access to any computer account to which they are not authorized. They shall not access or attempt to access any portions of the state networks to which they are not authorized. Public employees and other state network users also shall not intercept or attempt to intercept data transmissions of any kind to which they are not authorized.

7. Operators of email services must create an abuse@<*host domain name*> account and other additional internal procedures to manage their email complaints. Users who receive email that they consider to be unacceptable according to this policy can choose to forward the original email message (including all headers) to the appropriate email abuse@<*host domain name*> account.

8. Public agencies must ensure that each public employee and other state network user is provided with a copy of this policy (or an agency's more stringent policy, if applicable) before or at the same time the employee or other state network user is provided initial access to the state network.

ENFORCEMENT – DENR ADDENDUM

The Department of Environment and Natural Resources considers any violation of acceptable use principles or guidelines to be a serious offense and reserves the right to copy and examine any files or information residing on computer systems allegedly related to unacceptable use, and to protect its systems and networks from systems and events that threaten or degrade operations. Violators are subject to disciplinary action, up to and including termination of employment. Offenders also may be prosecuted under laws including but not limited to the Communications Act of 1934 (amended), the Family Educational Rights and Privacy Act of 1974, the Computer Fraud and Abuse Act of 1986, The Computer Virus Eradication Act of 1989, Interstate Transportation of Stolen Property, the Electronic Communications Privacy Act, and state conflicts of interest laws.