

NORTH CAROLINA DEPARTMENT OF COMMERCE	Policy # MIS-1 Title: Network Acceptable Use Policy
Effective Date: October 1, 1999	Administering Authority:
Revisions: February 18, 2009	Management Information Systems
Statutory Authority: N/A	

The NC Department of Commerce adopts the North Carolina Information Technology Services Office's policy as follows:

ITS POLICY 18.06

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 Internet by ITS staff and others who access the state network through the ITS LAN.

For more information contact: ITS Information Security.

Policy

1. While in performance of work-related functions, while on the job, or while using publicly owned or publicly provided information processing resources, ITS employees and others accessing the state network through the ITS LAN 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. ITS employees and others accessing the state network through the ITS LAN may make reasonable personal use of publicly owned or provided state network or Internet resources as long as:

- The direct measurable cost to the public is none or is negligible or access supports the mission of the agency;
- There is no negative impact on employee performance of public duties;
- The policy is applied equitably among all employees of the agency;
- 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, ITS employees and others accessing the state network through the ITS LAN shall identify themselves clearly and accurately. Anonymous or pseudonymous posting is expressly forbidden, unless otherwise allowed by law.

3. ITS employees and others accessing the state network through the ITS LAN, 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.

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 shall be scanned for such harmful contents. Scanning is required for files obtained as e-mail attachments and by any other file transfer mechanism. It is the responsibility of ITS employees and others accessing the state network through the ITS LAN to help 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. ITS employees and others accessing the state network through the ITS LAN shall avoid unnecessary network traffic and interference with other users including but not limited to:

- Unsolicited commercial advertising by public employees and 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.
- Any other type of mass mailing by ITS employees and others accessing the state network through the ITS LAN – which does not pertain to governmental business or results in network spamming – is strictly forbidden. Additionally, ITS employees and others accessing the state network through the ITS LAN 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.
- ITS employees and others accessing the state network through the ITS LAN 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.
- ITS employees and others accessing the state network through the ITS LAN 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 network networks to which they are not authorized. ITS employees and others accessing the state network through the ITS LAN also shall not intercept or attempt to intercept data transmissions of any kind to which they are not authorized.

7. ITS has set up the following mailboxes to receive comments or complaints. These mailboxes are:

- spam@ncmail.net Report spam to this address. Requires sending of complete email headers so the spam can be classified and blocked.
- abuse@ncmail.net Used to report other email abuse such as pornography, inappropriate usage of NCMail and other issues dealing with abuse of the NCMail Service.
- access.denied@ncmail.net To request whitelisting or blacklisting of specific email addresses.

- hostmaster@ncmail.net Request DNS changes.
- postmaster@ncmail.net Other requests including general questions, operations, service quality, hacking, denial of service (DOS) attacks and other issues.

ITS has also established additional internal procedures to manage 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 mailbox listed above.

8. ITS must ensure that each ITS employee and others accessing the state network through the ITS LAN are provided with a copy of this policy before or at the same time the employee or state network user is provided initial access to the state network.
9. Instant messaging, ICQ and any other real time communication protocol shall not be used by any ITS employee or other user accessing the state network through the ITS LAN, unless it is approved in advance and in writing by the State CIO.

Enforcement

The State CIO shall have authority to interpret and apply this policy. The State CIO may modify or amend this policy at any time.

Exceptions: All exceptions to this policy must be approved by the State CIO.
Contact ITS Information Security for comments, suggestions, or questions about this policy.

Approved: July 1, 1999

Effective: July 1, 1999

Revised: September 7, 1999; Revision Date: September 12, 2000; March 28, 2002; April 9, 2003; May 4, 2006