



Information Technology Services Policy Manual

18.07 **NCMail Policy**

Purpose: To establish policy and procedures for use of NCMail.

Reference: None.

For More Information: Contact the NCMail Administrator

The Office of Information Technology Services (ITS) operates the NCMail Service (NCMail), a system that provides e-mail to government employees through their subscribing agencies or departments. NCMail also includes a Central Message Store (CMS), which provides for backup and storage of the e-mail for the subscribing agencies and departments. As part of ITS responsibilities, ITS sets basic use policy to govern NCMail subscribers. ITS also reviews NCMail use for compliance with laws and regulations that apply to all agencies/departments using NCMail services. Final authority for the *NCMail and Central Message Store Policy* lies with the State Chief Information Officer.

Definitions

Administrator	A person responsible for administration of the NCMail Service for one or more domains or organizations that subscribe to the NCMail Service.
E-mail	Electronic mail (e-mail) is the electronic transfer of information typically in the form of electronic messages, memoranda, and attached documents from a sending party to one or more receiving parties via an intermediate telecommunications system. E-mail is a means of sending messages between computers using a computer network. E-mail is not a private communication. All information transmitted through NCMail travels over open networks. E-mail communications are best regarded as postcards rather than as sealed letters.

Custodian	A custodian of records for a government agency is the public official in charge of an office having public records.
CMS	CMS or the Central Message Store is the storage, retention and backup system for users of NCMail. It also includes methods of allowing different e-mail software products to communicate with each other. The agency or department owns the information transmitted by e-mail of its users, and CMS provides the storage service.
Domain	An administrative entity used within the NCMail system for providing span of control for Local Administrators. Most State agencies on the NCMail Service consist of one or more domains. The primary domain for NCMail is ncmail.net, but other domains may also be a part of the NCMail system, such as dot.state.nc.us or nclabor.com.
Local Administrator	A local or agency administrator of the NCMail Service. Local Administrators have agency level responsibility for submission of account adds and deletes, distribution list management and initial problem determination and resolution for E-mail problems.
MailDMZ	An SMTP mail relay service provided by NCMail for State and local governmental agencies that may or may not be part of the NCMail Central Mail Store (CMS) Service.
NCMail	E-mail services operated by ITS, as defined in this policy, including the internal use of NCMail and the sending and/or receiving e-mail from outside the NCMail internal system.
Spam	Any type of unsolicited commercial e-mail (UCE) or unsolicited bulk e-mail (UBE) for any purpose. Authorized agency and department wide communications to employees are not included in this definition.
Users	All persons whose access to or use of NCMail is funded by the state or is available through equipment owned or leased by the state.

The *NCMail and Central Message Store Policy* sets the rules and requirements for agency and department e-mail service through NCMail. Compliance with this policy is mandatory for continued use of NCMail.

The objectives of this policy are to:

- ensure that the use of NCMail is related to, or for the benefit of, state government;
- inform users that e-mail messages and documents are subject to the same laws, regulations, policies, and other requirements as information communicated in other written forms and formats; and,
- minimize disruptions to state government activities from inappropriate use of NCMail.

Policy Scope

This policy applies to all NCMail users.

Policy Hierarchy

Use of NCMail is governed by federal and state laws, policy and standards established by the State Chief Information Officer (CIO), and this ITS policy. Each agency and/or department may adopt additional policies for the individual users within the agency or department.

In considering the need for additional restrictions and guidelines, each agency may take into account its particular needs, mission, available technology, level of staff training, size, geographic diversity, and organizational culture.

Subscribing Agency/Department Responsibilities

By participating in the use of networks and systems provided by NCMail, agencies and departments agree to comply with federal and state laws, and State CIO and ITS policies. The *NCMail and Central Message Store Policy* is incorporated by reference to the NCMail Service Level Agreement. An agency's/department's signing of the Service Level Agreement evidences the agency's/department's agreement to abide by the ITS policy.

Each agency/department is responsible for the activity of its users and should familiarize each user with the *NCMail and Central Message Store Policy* and any additional restrictions or guidelines.

Unacceptable Use

Unacceptable use is defined as activity that does not conform to the purpose, goals, and mission of the agency and to the individual user's job duties and responsibilities. Any use of NCMail where the use is questionable should be avoided. When in doubt, seek policy clarification before pursuing the activity. Examples of unacceptable use are:

1. Private or personal for-profit activities. This includes personal use for marketing or business transactions, advertising of products or services, and any other activity intended to foster personal gain.
2. Unauthorized not-for-profit business activities.
3. Use for, or in support of, unlawful/prohibited activities as defined by

federal, state, and local laws or regulations. Illegal activities relating to Internet and network access include, but are not limited to:

- a. Tampering with computer hardware or software;
 - b. Knowingly vandalizing or destroying computer files;
 - c. Transmitting threatening, obscene, or harassing materials;
 - d. Attempting to penetrate a remote site/computer without proper authorization;
 - e. Using the Internet in an effort to access data that is protected and not intended for public access;
 - f. Violating federal and state laws dealing with copyrighted materials or materials protected by a trade secret; and,
 - g. Intentionally seeking information about, obtaining copies of, or modifying contents of files, other data, or passwords belonging to other users, unless explicitly authorized to do so by those users.
4. Attempts to subvert network security, to impair functionality of the network, or to bypass restrictions set by the network administrators. Assisting others in violating these rules by sharing information or passwords is also unacceptable behavior.
 5. Deliberate interference or disruption of another user's work or system. The user must not take actions that cause interference to the network or cause interference with the work of others on the network. Users are prohibited from performing any activity that will cause the loss or corruption of data, the abnormal use of computing resources (degradation of system/network performance), or the introduction of computer worms or viruses by any means.
 6. Seeking/exchanging information, software, etc. which is not related to one's job duties and responsibilities.
 7. Unauthorized distribution of state data and information.

Correspondence and Comments

NCMail service has set up the following mailboxes to receive comments. These mailboxes are:

- spam@ncmail.net Report spam to this address. Requires sending of complete e-mail headers so the spam can be classified and blocked.
- abuse@ncmail.net Used to report other e-mail 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 e-mail 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.

User comments, concerns, and/or complaints should be addressed to one of these mailboxes. The ITS Customer Support Center team reviews this correspondence, classifies it according to type, and takes appropriate action. For example, comments concerning operations, service quality, and spam are managed by the ITS Customer Support Center team, while comments concerning such subjects as hacking, cyberstalking, and denial of service attacks are handled as set forth in the ITS Security Incident Management Plan.

NCMail and CMS Security

Individual users should take all reasonable precautions to prevent the use of their e-mail account by unauthorized individuals. Transmission of e-mail to locations outside of the agency/department's local area network may require the use of the Internet for transport. Individual users should realize that the Internet adheres to open standards and is inherently insecure. Users also must assess risk before sending confidential information over an open network.

Disclosure may occur intentionally or inadvertently when an unauthorized user gains access to electronic messages. Disclosure may also occur when e-mail messages are forwarded to unauthorized users, directed to the wrong recipient, or printed in a common area where others can read them.

Although confidential information should not be included in e-mail communications unless proper, formalized security precautions have been established, certain e-mail communications may be confidential. It is the responsibility of each state agency to protect confidential information with clearly written policy where intentional, inappropriate, or accidental disclosure of the information might violate a legal or regulatory requirement.

Password Protection

NCMail users shall not save their NCMail password on hard drives, diskettes, or other electronic media and shall comply with the provisions of the Statewide Information Security Manual. To access NCMail, users shall enter their password each time they log-in.

Disclosure

All requests for e-mail information are managed by the custodian of the records; that is, the head of the agency and/or department or the custodian's designees. ITS shall forward all requests for e-mail records access or restoration to the custodian. The custodian shall determine whether to allow access or restoration of e-mail records. ITS is not permitted to release agency/department e-mail information to any source other than authorized agency/department personnel without prior written permission from the custodian or the custodian's designees. Requests to ITS for e-mail infrastructure support services, including access to and/or restoration of data, must come only from the agency/department.

Archival

ITS provides the computing infrastructure for receipt, storage, and transmission of electronic mail records.

As custodians of their own information, agencies and departments are responsible for e-mail records management, including access, distribution, classification, disposition and retention of their e-mail records, as required by the North Carolina Public Records Law and other applicable statutes. Agencies and departments may store and remove e-mail records on the Central Message Store in keeping with agency record retention schedules. ITS does not remove agency/department records from CMS without prior approval of the agency/department.

Backup and Restoration

As part of the e-mail infrastructure, ITS performs regular CMS e-mail backups in order to aid agencies and departments in the restoration of records to the message store and to provide business recovery capability. These backups are maintained to allow restoration of deleted agency e-mail records for a period not to exceed 30 days

Disaster Recovery/Business Recovery Planning

ITS provides backup, restoration, and disaster recovery services for CMS and directory information of users.

NCMail servers are backed up regularly on magnetic tape, and the tapes are stored off-site. ITS executes incremental backups during the week, Monday-Friday, and a full backup on Saturday and Sunday. ITS periodically tests the integrity of the backups. After 30 days, the tapes are cycled and re-used. *ITS does not keep and is not responsible for backups beyond 30 days.*

Sufficient server capacity is maintained on designated servers to handle movement of user accounts and data in the event of a non-recoverable failure to a server. Restoration time varies depending on the volume of data.

Unsolicited Bulk E-mail

Unsolicited Bulk E-mail (UBE) is commonly known as "spam". Spam is a huge problem; at the time of this writing approximately 1.5 million e-mail messages arrive at MailDMZ on a typical day, and over 900,000 are discarded as spam. During peak periods of spam or virus activity it is not uncommon for NCMail to discard over 2 million messages per day. These policies are intended to reduce the amount of spam traversing the NCMail system while ensuring that legitimate e-mail is delivered.

The following policies apply to the NCMail System with respect to spam.

1. The NCMail System will use all possible technical means to identify and block spam incoming from other e-mail systems as well as spam generated by NCMail accounts or accounts on State Government e-mail systems which utilize MailDMZ Relay Services.
2. Any NCMail User who sends unsolicited advertisements or solicitations, commercial or otherwise, may have their account disabled and be disallowed further service.
3. The Customer is responsible for ensuring that their End Users use the services obtained from NCMail in an appropriate manner. Therefore, the Customer must take steps to manage the use of the services obtained in such a way that network abuse is minimized. The Customer must also make contact information fully available and up-to-date for field administrators, and must respond in a timely manner to any complaints. NCMail shall consider any complaints regarding the Customer's End Users to apply to the Customer.
4. In extreme cases, NCMail operations personnel have the option to immediately disable or block any account in order to forestall further abuse or damage to e-mail systems. Should this occur, the Customer shall be notified as soon as possible.
5. Unsolicited advertisements or solicitations sent from other networks which reference e-mail accounts at NCMail shall be treated as if they originated from the account referenced, unless there is sufficient reason given for NCMail operations staff to believe that the message truly originated with some unrelated party.
6. Likewise, postings made to the Usenet newsgroups or other online forums which reference e-mail accounts at NCMail, and are deemed to be inappropriate according to the local ethical standards of that forum, may be treated in the same manner as unsolicited bulk e-mail above.

Enforcement

ITS takes security measures to protect the reliability, availability and integrity of the NCMail service. To accomplish this function, ITS uses appropriate measures to detect security breaches and other violations of system integrity. ITS reviews the security of all network activity, including all NCMail communications, to ensure that use does not violate federal and state laws, statewide policies and standards established by the State CIO and by this policy. By using NCMail, individual users agree to be subject to and abide by policies governing use. A violation of this policy may result in immediate suspension of NCMail services to the agency/department and/or individual users.

SELECTED LAWS RELATING TO NCMail USE

Federal:

United States Code, Title 18, Section 1030. “Fraud and related activity in connection with computers”

United States Code, Title 18, Section 2510, *et seq.* “Wire and electronic communications Interception and interception of oral communications”

United States Code, Title 18, Section 2701. “Unlawful access to stored communications”

North Carolina:

N.C.G.S. § 14-454. “Accessing computers.”

N.C.G.S. § 14-455. “Damaging computers, computer systems, computer networks, and resources.”

N.C.G.S. § 14-196. “Using profane, indecent or threatening language to any person over the telephone; annoying or harassing by repeated telephoning or making false statements over telephone.” The statute includes the making of any false electronic mail concerning death, injury, illness, disfigurement, indecent conduct or criminal conduct of the person receiving the e-mail or any close family member.

N.C.G.S. § 14-458. “Computer trespass; penalty.”

N.C.G.S. §114-15.1. “Misuse of state property.”

N.C.G.S. §14-196.3. “Cyberstalking”

N.C.G.S. §14-202.3 “Solicitation of child by computer to commit an unlawful sex act”

N.C.G.S. §14-277.1 “Communicating threats”

Latest Revision Approved: July 5, 2006