



<p>STATE OF NEW JERSEY IT CIRCULAR</p> <p>Title: 166 – Electronic Mail/ Messaging Content Policy and Standards</p>	NO: 14-17-NJOIT	SUPERSEDES: Email/Messaging Policy (ITPS09-01-1998)
	LAST REVIEWED: April 8, 2015	DATE PUBLISHED: April 2, 2014
	VERSION: 2.0	EFFECTIVE DATE: 45 Days From Signature
	FOR INFORMATION CONTACT: Office of Policy and Planning	

ATTN: Directors of Administration and Agency IT Managers

I. PURPOSE

The purpose of this policy is to define and govern proper utilization of the State of New Jersey’s Electronic Mail/Messaging systems. This policy has been established to 1) Prevent inappropriate use of the State network and the Internet; 2) Protect the State’s investment in networked technology; 3) Safeguard the information contained within State systems, and 4) Reduce business and legal risk.

II. AUTHORITY

This policy is established under the authority of the State of New Jersey [N.J.S.A. 52:18a-230 b](#). This policy defines New Jersey Office of Information Technology’s (NJOIT) role with regard to technology within the Executive Branch community of State Government.

The New Jersey Office of Information Technology (NJOIT) reserves the right to change or amend this circular.

III. SCOPE

This policy applies to all State Departments, Agencies, “in but not of” entities, their employees, contractors, consultants, temporary workers, and others who develop and administer information systems and resources for systems. This policy supersedes all existing statewide and agency email/messaging usage policies. Agencies may, with the review and approval of the Statewide Office of Information Security within OIT, supplement this policy with additional rules and regulations, if necessary to clarify how this policy applies to a specific agency’s operations. Any additions cannot conflict with the requirements established by this policy. Agencies can adopt more stringent standards if necessary to meet their own stricter privacy and security requirements. Such additions also must be reviewed and approved by

the Statewide Office of Information Security. No addition can compromise the security of statewide systems. Notwithstanding any of the foregoing, nothing in this policy supersedes existing collectively bargained agreements.

IV. DEFINITIONS

Please refer to the Statewide Policy Glossary at <http://www.nj.gov/it/ps/glossary/>.

V. STANDARDS

A. Purpose of electronic messaging systems

State-provided email/messaging systems are available, when appropriate, for authorized users to accomplish their job responsibilities.

B. Incidental Personal Use Permitted

The State offers employees access to its communications networks for business purposes. Limited personal usage is permitted if it does not 1) Interfere with work duties; 2) Consume significant resources, 3) Constitute any use prohibited by this policy, 4) Interfere with the activities of others, 5) Put State network and systems at risk or, 6) Violate State or agency policies.

C. No Expectation of Privacy

1. State-owned computers, software, networks and Internet access are the property of the State of New Jersey. As such, the State has the absolute right to monitor the use of such property, and the users have no rights to privacy. The State has the right to intercept, inspect, and log any aspects of its computer systems, including, but not limited to, email, instant messaging, text messaging and social media communications, and any attachments or links therein.
2. The State and authorized personnel or agents have the right to inspect any and all electronic communications and records of communications that were created or received using State equipment and resources. These records are open to inspection regardless of whether they are stored on a network, in a personal computer, or on an external storage device. Such communications may be subject to public disclosure. An employee's use of the State's network, Internet access and/or computers shall constitute an express consent to the rights of the State set forth in this section.

D. Retain Records as Required by Law

Records Management Services, part of the Division of Revenue and Enterprise Services in the Department of the Treasury, directs the proper retention and

destruction of State records. Agencies must follow Records Management's rules on preservation of electronic communications. State agencies shall adhere to any applicable law or regulation governing electronic communications and preserve records when there is a reasonable anticipation that producing them may be required as part of future or pending litigation.

E. Handling Suspicious or Unfamiliar Email From Outside State Systems

IT directors are responsible for proper handling of email sent to their agencies from outside networks (i.e., Google G-mail, Yahoo, etc.) and for ensuring that agency staff receives instruction on safe procedures for handling of email and attachments from outside sources. Non-network messages pose a risk to State computers and networked systems because of the possibility that they carry viruses and malware. In general, IT directors should instruct users not to open emails from unfamiliar senders or emails that appear suspicious, and inform users that they should not click on links or open attachments in email sent from outside state systems or via forwarded email. IT directors should identify all users whose work requires them to open emails and/or attachments or links from senders of unknown reliability, and provide these employees with appropriate safeguards and training to mitigate risks. IT directors can contact the Statewide Security Officer for guidance, risk management information, and instruction.

F. Use of Personal Email Accounts

Agency IT staff should caution all users about accessing personal email accounts (i.e., Google G-mail, Yahoo, etc.) via State computers due to the risks posed by malware and viruses. Those agencies allowing use of personal email accounts must work with OIT staff to develop and ensure the usage of standard safeguards designed to minimize risk. IT directors should know if staff members in their agency are permitted to use personal email accounts so IT staff can provide those staff members with appropriate instruction on how to mitigate risk.

G. Encryption of Confidential, Proprietary and Sensitive Information

Agencies shall develop and implement policies requiring encryption of email transmissions of confidential, proprietary and/or sensitive information. Each agency, relying primarily on applicable laws and regulations, should create policies that define what information handled by the agency is confidential, proprietary and/or sensitive. Examples of confidential, proprietary and/or sensitive information include, but are not limited to, medical records and health information, tax records, Social Security numbers, non-public details of confidential investigations, business records that include proprietary data, homeland security information, and any data deemed private by law and regulation. Each agency, working with OIT, should instruct employees on encryption procedures and the instruction laid out on the website that is at: <http://highpoint.state.nj.us/intranets/oit/services/infosecure/eesrcig/>.

H. Use Required Disclaimer:

System administrators and/or respective system owners shall ensure that messages and data sent via any State-provided email/messaging system include a disclaimer regarding accidental transmission to an unintended third party. The standard disclaimer language should be one of the following, 1) State of New Jersey or 2) agency specific:

1. State of New Jersey

CONFIDENTIALITY NOTICE: *This email message and all attachments transmitted with it may contain State of New Jersey legally privileged and confidential information intended solely for the use of the addressee only. If the reader of this message is not the intended recipient, you are hereby notified that any reading, dissemination, distribution, copying, or other use of this message or its attachment is prohibited. If you have received this message in error, please notify the sender immediately and delete this message.*

2. Agency Specific

CONFIDENTIALITY NOTICE: *The information contained in this communication from the (Insert Your Agency's Name) is privileged and confidential and is intended for the sole use of the persons or entities who are the addressees. If you are not an intended recipient of this email, the dissemination, distribution, copying or use of the information it contains is strictly prohibited. If you have received this communication in error, please immediately contact the (Insert Your Agency's Name) at (XXX) XXX-XXXX to arrange for the return of this information.*

I. No Waiver of Privilege or Confidentiality:

Nothing in this policy, and in subsequent standards, including those issued by state agencies or departments to implement this policy, shall be construed to waive any claim of privilege or confidentiality for the contents of electronic mail available to the state, or to require public disclosure of electronic communications.

VI. RESPONSIBILITIES

A. Department and Agencies Shall Endeavor To:

1. Authorize access to State-provided email/messaging for appropriate agency staff.
2. Ensure that only duly authorized persons use State-provided email/messaging systems.

3. Provide for proper training of all authorized personnel using State-provided email/messaging systems and, whenever possible, post a warning that appears on the computer screen when a user signs on to a State-owned network, computer or device. This warning screen should state that users have no expectation of privacy when using email and internet systems, and note that all usage of State-owned systems and networks is monitored for compliance with this policy. Contact the Statewide Office of Information Security within OIT for an example of a standard warning screen.
4. Establish internal controls, at the IT director level, for monitoring compliance with this policy.
5. Establish internal operating procedures to conduct audits of State-provided email/messaging systems by the IT director when deemed appropriate.
6. Establish internal operating procedures to ensure the disabling of an individual's electronic mail and network accounts when an individual is separated from State service or placed on a leave of absence.
7. Relay all email/messaging communications through the State's Enterprise Email Security Gateways and Content Inspection System (EESGCIS) to monitor, filter access and inspect traffic for all authorized users' email/messaging use. The EESGCIS is managed and operated by the Office of Information Technology.
8. Have authorized system administrators of all agencies, during the course of systems maintenance and testing for systems security, report to appropriate management and OIT staff, any unauthorized use or breaches in security discovered.

B. Users Shall:

1. Comply with all federal and State laws while accessing the network and/or Internet. Employees are expressly prohibited from downloading, storing, transmitting, displaying or printing any image, document, application, file or data on any computer, server, or storage medium or other peripheral that violates federal or State law or policy, including but not limited to, files that infringe upon copyright protections or those that involve pornography, gambling, workplace violence, or sexual harassment, or which tend to create a hostile work environment. All electronic mail/messaging use must conform to Equal Employment Opportunities (EEO) and Ethics policies. Investigative staff members, in the performance of their duties, are exempt. Please refer to policies available at: <http://www.state.nj.us/csc/about/divisions/eo/policies.html>.

Refer to Ethics at:

Plain Language Guide to New Jersey's Executive Branch Ethics Standards available at: <http://www.state.nj.us/ethics/docs/ethics/plainlanguage.pdf>.

New Jersey Conflicts of Interest Law available at: <http://www.state.nj.us/ethics/statutes/conflicts/>.

New Jersey State Ethics Commission's Guidelines available at <http://www.state.nj.us/ethics/statutes/guide/>.

2. Employees should be aware of email/messaging computer security and privacy to guard against email content with computer malware. Awareness consists of attending security awareness training that includes proper procedures for handling email from unknown or untrusted sources.
3. Employees are prohibited from using the State's email/messaging system to:
 - a) Communicate any non-work-related solicitations, e.g., whether for charitable, political, personal, religious or any non-State business. This includes, but is not limited to, chain letters or advertisements.
 - b) Make personal profit. State email/messaging systems cannot be used to purchase or sell non-work related goods or services or to conduct personal business. This includes, but is not limited to, buying, selling, trading or any activity that benefits any other secondary employment purpose.
 - c) Misrepresent oneself or the agency/department or the State of New Jersey.
 - d) Lobby elected officials, conduct political business, advocate for political causes, or participate in partisan political activities, except in such instances where such activity is required in order to perform an employee's job.
 - e) Conduct unlawful activities.
 - f) Disclose proprietary information or any other privileged, confidential, or sensitive client and/or employee information without authorization to any third party or to anyone who does not have authorization to access such information.
 - g) Pursue, obtain, exchange, or download any non-authorized and/or non-State information with the intent to cause congestion or disruption of electronic mail systems or networks.
 - h) Open, read or send email from another's email account deliberately, without proper authorization.

- i) Disable security systems such as a software firewall, intrusion prevention, anti-spyware, or virus detection system, employed to protect electronic communication and data.
- j) Broadcast or publish unsolicited views on social, political, religious or other non-business related matters not permitted pursuant to a collectively negotiated agreement applicable to the affected employee.
- k) Network or communicate peer-to-peer (instant messaging, social media, etc.) within the enterprise system with the intent to bypass monitoring or stated messaging policies.
- l) Alter and then forward or otherwise distribute a message, data display, or attachment that originated with another in order to deceive readers about the author's true intent.

C. Requirement to Report Inappropriate Use:

Users must notify their supervisor or the Agency's IT Director of any inappropriate use of State-provided email/messaging systems, as noted in this policy.

D. Policy Applies at All Times:

This policy in its entirety applies to use of the State's communications systems both during and outside of working hours and on and off the State's premises.

E. Violators Face Disciplinary Action, Civil or Criminal Liability:

Violations of this policy or departmental policies promulgated pursuant to this policy may result in revocation of access and/or disciplinary action, regardless of the user's intent. Such discipline shall be in accordance with applicable laws, regulations, agreements reached through collective negotiations, and agency discipline practices. In addition, violators may be subject to civil or criminal prosecution under federal and/or state law.

VII. EXCEPTIONS AND NON-COMPLIANCE

Departments and Agencies shall comply with this policy within 45 days of its effective date.

A compliance exception must be requested if there is an inability to comply with this policy because of a business reason or system constraint. Exceptions and non-compliance with this policy shall be managed in accordance with Policy [08-02-NJOIT](#), 111 – Information Security Managing Exceptions.

VIII. REFERENCES

- A. [New Jersey Division of Records Management Circular Letter 03-10-ST: Managing Electronic Mail: Guidelines and Best Practices.](#)
- B. [New Jersey IT Circular: Acceptable Internet Usage](#)
- C. [New Jersey Open Public Records Act.](#)

Singature of File

04/08/2015

E. STEVEN EMANUEL

DATE

**Chief Technology Officer-NJ Office of Information Technology
State Chief Information Officer**