

DEPARTMENT OF HUMAN SERVICES

EFFECTIVE DATE: November 23, 2015

ISSUE DATE: November 24, 2015

SUBJECT: COMPUTER USAGE AND ACCESS TO DHS NETWORK, INTERNET AND EMAIL

I. PURPOSE

The purpose of this Order is to set forth the uniform standards and guidelines for network, internet and email access, usage and control within the Department of Human Services (DHS). This policy has been established to: 1) Prevent inappropriate use of the state-issued computers, network, internet and email; 2) Minimize risks of network disruption; 3) Protect the State's investment; 4) Safeguard the information contained with the State systems and; 5) Reduce business and legal risk.

II. SCOPE

This order has Department-wide applicability and includes employees, contractors, consultants, temporary workers, and others who have access to Department information systems and resources.

III. AUTHORITY

State of New Jersey IT Circular, 14-30-NJOIT, "Acceptable Internet Usage"
State of New Jersey IT Circular, 14-17-NJOIT, "Electronic Mail/Messaging Content Policy and Standards."
State of New Jersey IT Circular, 15-06-NJOIT, "Internet Access Policy for New Jersey State Agencies."

IV. DEFINITIONS

Employee shall mean any individual working for an agency under the direct control of the Commissioner and, for the purpose of this policy, any person working in the Department from another State agency, temporary service provider, intern, contractor or consultant who utilizes the Department computer system or network.

Computer shall mean any state computer or peripheral including, but not limited to, desktop computers, notebook/laptops, handheld mobile devices and removable drives regardless of where and how they are connected.

Network or Computer Network shall mean any system that interconnects two or more computers in order to provide data communications either internally within our organization or with external individuals or agencies.

Internet Access shall include all available routes to the Internet, including but not limited to, State access lines, direct Internet Provider Service (ISP) accounts, wireless networks, and/or personal Modem/ISP/Wireless accounts.

PC/PII stands for Proprietary, Confidential and Personally Identifiable Information belonging and having value to DHS or the State of New Jersey.

Supervisor/Manager shall mean the person(s) responsible for completing an employee's performance review (PAR/PES) and/or responsible for managing the unit to which the employee is assigned.

Wireless Device may include but are not limited to tablets, personal digital assistants (PDA's), universal serial bus (USB) port devices, compact discs (CD's), digital versatile discs (DVD's), flash drives, modems, mobile phones, and any other existing or future mobile or portable storage device that may connect to, access and/or store information or data.

V. RESPONSIBILITY FOR COMPLIANCE

- A. Each Employee shall be responsible for complying with this Computer Usage and Access to DHS Network and Internet and Email Policy. Employees who violate this policy will be subject to disciplinary action.
- B. The Security Operations Manager and other designated staff members with access to the recording systems and data shall be responsible for recording internet activity and communicating known violations of this policy to the employee's manager as soon as they are discovered.
- C. Supervisor/Managers shall be responsible for taking appropriate action to correct violations of this policy including the imposition of disciplinary charges, up to and including removal from State service, as warranted by the nature of the violation.
- D. Any instances of employee misuse of the Internet for illegal or pornographic purposes or any other purposes that may be deemed offensive shall be referred to the Office of Employee Relations. The

Human Services Police shall be notified of all illegal uses of the internet, computer or network.

VI. POLICY

- A. The Department offers employees access to its computers and networks, including the internet, for business purposes only. However, as with the telephone, limited incidental person use of the computer, network, Internet system mobile devices is permitted if the usage does not: 1) Interfere with work duties; 2) Consume significant state resources; 3) Constitute any use prohibited by this policy or that of the State; or 4) Interfere with the activities of others.
- B. Except as provided by a general internet browser encryption (HTTPS encryption), employees should not use encryption technology or software for personal use.
- C. Employees must report any damaged, malfunctioning, lost, or stolen DHS wireless device (e.g. mobile device, laptop) to the Information Technology Office located in their respective divisions/offices. Procedures for lost, stolen, damaged and malfunctioning equipment is as follows:
1. If a device is lost or stolen, the employee is also responsible for contacting the appropriate local law enforcement authority as directed. If the employee fails to make notification, he or she will be held responsible for any unauthorized device usage.
 2. Complete "IT Damaged, Lost or Stolen" Form.
 3. If the equipment is damaged, bring the equipment and the Form to the Divisional IT office
 4. Divisional IT will examine the equipment, review the Form and take a photo of the damaged equipment. They will forward both the form and the photo to DHS-CO OIS Manager of Computer Operations located at Capital Place One, 222 S. Warren Street, 2nd floor, Trenton, NJ 08625.
 5. A panel consisting of CIO DHS-CO or designee, DHS-CO OIS Manager of Computer Operations, and the DHS Employee Relations Coordinator will review, on case by case basis, the circumstances of lost, stolen or damaged equipment and determine replacement cost.
 6. Employee will be notified via e-mail of Committee's findings by DHS-CO Manager of Computer Operations.
 7. If DHS assesses that the employee is at fault for the lost stolen or damaged equipment, DHS may charge a fee to replace any wireless device, computing device or damaged peripherals up to the full amount of the replacement cost. The employee must

provide a check in the amount of the replacement cost, payable to the Treasurer, State of New Jersey and forwarded to the Department's Office of the Chief of Operations and Financial Officer. No replacement will be issued until fee is paid.

8. If fee is not paid, corrective or disciplinary action may be initiated.
- D. The Department of Human Services shall adopt and incorporate the most recent New Jersey Office of Information Technology (NJOIT) policies, which address the proper utilization of the State's Communication Networks, Internet and Electronic E-mail. These policies are set forth in the following attachments:
1. A copy of the State of New Jersey IT Circular 14-17-NJOIT, "Electronic Mail/Messaging Content and Standards", Attachment B.
 2. A copy of the State of New Jersey IT Circular 14-30-NJOIT, "Acceptable Internet Usage", Attachment C.
 3. A copy of the State of New Jersey IT Circular 15-06-NJOIT, "Internet Access Policy for New Jersey State Agencies", Attachment D.
- E. All employees shall be provided a copy of this Administrative Order, which sets forth policy on the use of DHS computers, Network and Internet. Each employee shall sign an acknowledgement receipt, attesting that he or she has read and understands the guidelines of which they will be held accountable.

VII. ATTACHMENTS

Lost Stolen or Damaged Equipment Flow Process Chart

VIII. PROCEDURAL HISTORY

This Administrative Order revises and replaces the Administrative Order 4:15 which was issued and effective February 2, 2009. This Administrative Order 4:15 supersedes and replaces ISC #: 99-2, "Information Technology Email/Messaging Circular" and ISC #: 03-03, "Client/Customer/Patient Access to the Internet through the DHS Network."



Elizabeth Connolly, Acting Commissioner

IT DAMAGED, LOST OR STOLEN EQUIPMENT RECEIPT

Employee Name: _____ **Incident Date:** _____

The following equipment belonging to DHS Information Systems Department has been:

DAMAGED STOLEN LOST

Explain in Detail:

ITEM DESCRIPTION	MODEL	SERIAL NO.

Management Decision: (Select all that Apply)

Not Responsible

Responsible Payment Due Amount Due (Payment to "State of NJ"); \$ _____

Comments: _____

Employee Signature _____ **Date** _____

Supervisor Signature _____ **Date** _____

CIO Signature _____ **Date** _____



NJ OFFICE OF INFORMATION TECHNOLOGY
Chris Christie, Governor
E. Steven Emanuel, Chief Information Officer

P.O. Box 212 www.nj.gov/it/ps/
300 Riverview Plaza
Trenton, NJ 08625-0212

<h1>STATE OF NEW JERSEY IT CIRCULAR</h1> <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**



NJ OFFICE OF INFORMATION TECHNOLOGY
Chris Christie, Governor
E. Steven Emanuel, Chief Technology Officer

P.O. Box 212 www.nj.gov/it/ps/
300 Riverview Plaza
Trenton, NJ 08625-0212

STATE OF NEW JERSEY IT CIRCULAR Title: 1600 – Acceptable Internet Usage	NO: 14-30-NJOIT		SUPERSEDES: 09-07-NJOIT	
	LAST REVIEWED: September 5, 2014		DATE PUBLISHED: September 5, 2014	
	VERSION: 1.0		EFFECTIVE DATE: Date of Signature	
	FOR INFORMATION CONTACT: Office of Policy and Planning			

ATTN: Directors of Administration and Agency IT Leaders

I. PURPOSE

To establish a core policy for the use of State Data and Communications Networks and the Internet by Agency employees and other authorized users. Agencies may build upon this policy by adding requirements specific to their agencies as long as the additions neither weaken nor contradict the rules in this document. Agencies must submit additional rules and supplements to this circular letter to the Statewide Office of Information Security.

II. AUTHORITY

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

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

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. The policy set forth in this document is limited and qualified by the Federal Wire Tap Act, 18 U.S.C. §2710 et seq, and the New Jersey Wiretap Act, N.J.S.A. 2A:156A-1 et seq.

By accessing the State’s networks or Internet systems, a user agrees to adhere to the State’s policies, including agency-specific policies, regarding their use.

IV. POLICY

The Internet presents employees with opportunities for global communications and research but also creates risks, including security concerns and legal liability. In order for the State to maximize the benefits and minimize the risks associated with use of the Internet, this circular documents the policy for Internet access and use by all users.

The only people who may access the Internet through the State's information infrastructure or information technology are State employees and other persons for whom the State specifically authorizes access. The authorization should be supported by a banner displayed on the computer screen prior to login, and/or documentation, which includes, but is not limited to a signed agreement or a memo to a file. The banner language is provided in [14-04-S1-NJOIT 1703-01 Disclaimer Standard](#).

Employees are given State-provided access to the Internet to assist them in the performance of their jobs. The State will monitor Internet activity and users, therefore, should have no expectation of privacy. All records and logs created by Internet use are the property of the State and are subject to monitoring. Users are expected to conduct their electronic communications in a professional, responsible and courteous manner. Misuse of the State's information infrastructure, information technology and electronic communications media, including, but not limited to, the unauthorized transmission of confidential or proprietary information; the use of profane, harassing or other offensive language; or other inappropriate uses, including, but, not limited to, those listed in paragraph VIII below, may subject the user to discipline, including termination of employment, the initiation of civil action, or criminal prosecution.

V. NO PRIVACY EXPECTATIONS

The State reserves the right, without prior notice, to monitor, intercept, read, copy, or capture, and disclose, for any purpose, the content of any information sent to and from, or stored on the State's infrastructure, computing devices, and computer systems – including e-mail, attachments to e-mail, and World Wide Web pages and logs. All users, including State employees, using the State's infrastructure or Internet waive any right to privacy of the information, and consent to such information being accessed and disclosed by State personnel.

The State may disclose or use any information monitored, intercepted, read, copied or captured to authorized personnel or law enforcement so that the information can be used for disciplinary action, civil litigation or criminal prosecution.

The State may release or provide data or information if directed to do so by operation of law, pursuant to a lawfully issued subpoena, or pursuant to a ruling by a court or arbitrator of competent jurisdiction.

Nothing in this policy shall be taken to waive, relinquish or abrogate any privilege or confidentiality recognized by law or to authorize disclosure of any privileged, confidential or proprietary information except as provided by law.

VI. STATE SYSTEM SECURITY

While using the Internet, employees shall not engage in behaviors known to put at risk the security and integrity of the State's information infrastructure or information technology, networks, computer equipment and portable computing devices. These prohibited behaviors include accessing suspicious or unfamiliar content, or downloading emails from unknown users for non-work-related purposes. Workers who must access such content or emails in the performance of their duties shall do so only after contacting their agency's or department's CIO to ensure that security procedures are in place and followed. Agencies shall provide security training to workers assigned to roles requiring handling of unfamiliar emails or other content that presents risks to State systems.

Employees shall not use another employee's computer to gain access to the Internet without that employee's consent or supervisory approval. An agency may establish a specific policy regarding access to the Internet in the form of a supplement to this circular when such a supplement is necessary to address the duties and responsibilities of the agency.

Users should not use the same password for State accounts as they use for personal accounts. State account passwords should be unique to each account.

VII. ACCEPTABLE USE: PERMITTED PURPOSES

All State laws, regulations and policies prohibiting discrimination, harassment, hostile environments, violence, and sexual harassment in the workplace apply to an employee's access or use of State information infrastructure and technology. The State also requires adherence to the Conflict of Interest Law and the Uniform Code of Ethics (as may be supplemented by an agency code approved by the State Ethic Commission) when using the Internet. Users must comply with all State and federal laws and regulations applicable to the Internet. Users also must adhere to any conditions or restrictions on Internet access and use put in place by the agency where they work or where they are authorized to use an agency's equipment, systems or networks.

Software for browsing the Internet is provided to users for State-related business. Agencies may permit limited, incidental, personal use that does not interfere with work duties, consume significant State resources, constitute a use prohibited by this policy, and/or interfere with the activities of others. Personal use of State equipment shall not amount to more than *de minimis*, occasional use. More than limited incidental personal use may subject an employee to discipline or denial of Internet access. Except as

allowed by an agency's policy, personal use is permitted only during authorized break times or lunch periods, or before or after a worker's scheduled shift. No agency is obligated to make Internet access available to any employee for personal use, nor is any agency obligated to let workers come in early or stay late to facilitate personal use of State Internet connections.

Note: Users of State systems must not present personal communications as representing the views or official correspondence of an Agency or the State. This includes, but is not limited to, personal emails, social media postings, blogs, website postings and instant messages.

VIII. EXAMPLES OF IMPERMISSIBLE USES

The following are examples of impermissible uses of the State information infrastructure or information technology systems. This list is not intended to be exhaustive or exclusive. A user may not:

- A.** Violate or infringe on a recognized privilege or the right to privacy.
- B.** Violate agency or departmental regulations or policies prohibiting discrimination, harassment or hostile environments in the workplace.
- C.** Violate any local, state, or federal law.
- D.** Conduct personal, for-profit business activity.
- E.** Solicit for religious, political, charitable or other causes.
- F.** Perform any political campaign activities.
- G.** Conduct any non-governmental related fundraising or public relations activities or engage in such activities when they are not part of a user's State-authorized duties.
- H.** Perform illegal, unethical, or criminal activities.
- I.** Transmit or download, store, install, or display any kind of image or document on any agency system that violates agency and/or State policies prohibiting discrimination, violence, harassment or hostile environments in the workplace.
- J.** Download software in violation of licensing agreements or agency policies.
- K.** Transmit or post agency information without management approval.
- L.** Gain or attempt to gain unauthorized access to any computer, computer records, data, databases or electronically stored information.
- M.** Violate licensing, trademark or copyright laws.

- N. Knowingly cause the transmission of a program, information, code or command, and as a result of such conduct, intentionally cause damage to a computer, systems or network.
- O. Gamble or play games on the Internet.
- P. Engage in instant messaging, streaming media or streaming video for non-work related purposes.
- Q. Transmit defamatory, knowingly false or misleading, abusive, profane, pornographic, threatening, racially offensive, or otherwise biased, discriminatory or illegal material.
- R. Use State equipment or assets to access, transmit, copy, convey information in violation of an executed agency or department non-disclosure agreement.

Except to the extent required in conjunction with a bona fide, agency-approved project or assignment, or other agency-approved undertaking, no user shall utilize State-owned or leased information infrastructure or information technology to access, download, print or store any information infrastructure files or services containing sexually explicit content. Such agency approvals shall be given in writing by agency heads or their designees.

Encryption can be used only to protect sensitive data handled as part of an employee's job assignment. Users should not send encrypted data through or with State systems except when necessary for the performance of State-related duties. Personal use of encryption is prohibited on State systems.

IX. MONITORING OF SITE ACCESS AND SYSTEM USE

The State reserves the right to monitor and filter site access by users and to review data downloaded from the Internet. The State may also monitor access to the State information infrastructure and information technology system, including successful and failed log-in attempts and logouts, inbound and outbound file transfers, and sent and received e-mail messages. The State may monitor, intercept, read, copy, or capture any information placed on its computers or computer systems. The State may disclose such information to authorized personnel or law enforcement officials as well as to authorized personnel involved in any disciplinary action, civil litigation or criminal prosecution.

The State will use the State's Enterprise Internet Filtering and Content Inspection System (EIFCIS) to monitor, filter access and inspect traffic for all employees' Internet use. The EIFCIS will be managed and operated by the Office of Information Technology.

X. SOFTWARE

The agency IT Director must approve and have an inventory of all software used to access the Internet.

XI. MALWARE SCANNING AND SECURITY PROTECTION

A computing device issued by the State or configured for State usage must meet minimum security protection standards before it can be used to access the Internet. Among the steps that should be taken:

- A.** Select software products that can be configured to help prevent the introduction of spyware or malware and other intrusions.
- B.** Enable software needed to identify and locate portable devices and, if necessary, wipe the media remotely if lost or stolen.
- C.** Protect a portable device's stored data and applications by encrypting and password protecting the device.
- D.** Use supported operating system, software, and web browser with the ability to receive updates.
- E.** To reduce the possibility of installation of malicious code, ensure that the software browsers and add-ons run with a minimal set of permissions.
- F.** When possible, inspect traffic before it gets into the State's network to ensure that it does not contain malware and block any malware that is found.
- G.** Scan all downloaded files for malware and other malicious software, using security protection software approved by the agency in consultation with OIT.

XII. SOCIAL MEDIA AND NETWORKING

Social media and networking can help the State fulfill its mission and goals, and support professional development. However, usage comes with security and reputational risks. If social media and networking are permitted by a department or agency, users must adhere to the following acceptable use guidelines:

- A.** Allow social media site access only to users who are specifically authorized to have it.
- B.** When feasible, block or ban unnecessary functionality within social media web sites, such as instant messaging (IM) or file exchange, that allow unsecure transfer of data and links.

- C. Discourage users from accessing links within a social network, such as a “friends” site, that serve no work-related purpose, and ensure workers know that they are not to click unfamiliar or non-work related links on social media sites.
- D. Monitor social media using data loss prevention (DLP) technology designed to prevent loss of intellectual property.
- E. Monitor social media content for sexually harassing, racist or other inappropriate content.
- F. Archive and log all relevant content that might constitute a business record and/or that might need to be retained for legal purposes or as public records.
- G. Enable technical risk mitigation controls to the extent possible. These controls may include:
 - 1. Filtering and monitoring all Social Media website content posted and/or viewed.
 - 2. Scanning all files exchanged with other users of Social Media web sites.

XIII. REPRESENTING THE STATE

Employees and other users of State systems must exercise the same care in posting information to the Internet as they would with any external communication by the agency.

XIV. PROPRIETARY AND CONFIDENTIAL INFORMATION

Users shall maintain all proprietary and confidential information in confidence and shall not use the Internet or the State information infrastructure or technology to access, disclose or distribute such information in an unauthorized manner. Such information should not be distributed unless it is encrypted and password protected.

XV. COPYRIGHT

Users should not violate any of the copyright laws when accessing, printing or disseminating materials found on the Internet.

XVI. CONSENT

Access or use of State-furnished computers or Internet facilities constitutes consent to this policy on Acceptable Use of the Internet.

XVII. TECHNICAL

Users should schedule, wherever possible, communications-intensive operations such as large file transfers, video downloads, mass e-mailings and the like for off-peak times.

XVIII. RESPONSIBILITIES

A. Employee

Employees shall follow this policy and all agency Internet policies and procedures. Users should report any misuse or policy violations to their supervisor or Agency IT Director.

B. Agency

Develop agency guidelines, procedures, and internal controls for monitoring compliance in accordance with this policy.

Furnish employees and vendors granted access to agency systems with copies of this notice, and provide all new employees and other users with copies of this policy concurrent with authorizing them to use agency computers.

Discipline employees for violations of this policy or of any standards or guidelines referenced.

Promote awareness of acceptable use of the Internet by training employees in the use of tools to access the Internet.

XIX. EXCEPTIONS AND NON-COMPLIANCE

Agencies must request compliance exceptions if there is an inability to comply with this policy because of a business reason or system constraint. All requests for a compliance exception shall be made to the Statewide Information Security Officer (SISO) in writing. Agencies have the right to enforce disciplinary action when appropriate for policy violations.

XX. REFERENCES

[Title 7 of the Civil Rights Act of 1964](#) as amended

[Communications Decency Act of 1996](#)

[N.J.S.A. 10:5-1](#) et. seq.

[N.J.S.A. 11A:1-1](#) et. seq.

[N.J.A.C. 4A:7-3.1](#)

[Uniform Code of Ethics/New Jersey Conflicts of Interest Law](#)
[Executive Order 49 \(Issued April 17, 1996 – Governor Whitman\)](#)
[The Computer Fraud and Abuse Act](#)

Signature on File

E. STEVEN EMANUEL
Chief Technology Officer-NJ Office of Information Technology
State Chief Information Officer

9/5/2014

DATE



NJ Office of Information Technology
Chris Christie, Governor
E. Steven Emanuel, Chief Technology Officer

P.O. Box 212 www.nj.gov/it/ps/
300 Riverview Plaza
Trenton, NJ 08625-0212

<p>STATE OF NEW JERSEY IT CIRCULAR</p> <p>Title: Internet Access Policy for New Jersey State Agencies</p>	NO: 15-06-NJOIT	SUPERSEDES: 06-03-NJOIT
	LAST REVIEWED: April 8, 2015	DATE PUBLISHED: April 8, 2015
	VERSION: 1.0	EFFECTIVE DATE: Date of Signature
	FOR INFORMATION CONTACT: Office of Policy and Planning	

ATTN: Directors of Administration and Agency IT Managers

I. PURPOSE

To establish the overall policy for secure access to, and use of the Internet by State agencies.

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. DEFINITIONS

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

IV. POLICY AND PROCEDURES

The Office of Information Technology (OIT) and agencies will maintain a secure, coordinated and cost-effective approach to Internet access by State agencies. OIT has been given the authority to administer access to the Internet by users at New Jersey State agencies.

To encourage a secure, coordinated and cost-effective approach to Internet access, OIT will contract for an ISP and administer State agency Internet access. OIT must review and approve separate access contracts negotiated by individual agencies. Each such agency must show that a technical incompatibility or special functional requirement exists to justify approval of such contracts.

Agency access to the Internet through the designated ISP or OIT-approved agency ISP is offered as a tool for meeting the programmatic needs of the State. State-provided Internet access is State property and is intended for official business. The use of State-provided Internet access by State agencies and their employees constitutes the acceptance of responsibilities and obligations set by federal, State, and local laws and regulations.

In accordance with [14-30-NJOIT](#), 1600 – *Acceptable Internet Usage*, OIT and State agencies have the authority and responsibility to monitor Internet access. Any unauthorized access and use discovered during such monitoring may be reported to agency management for appropriate action.

V. FUNCTIONS

A. Agency

1. An agency shall provide for agency Internet access administration.
2. An agency may install and update necessary system-wide virus protection software in consultation with OIT.
3. An agency shall determine which employees shall be allowed access to and use of the Internet.
4. An agency may monitor agency staff access to and use of the Internet to ensure that it is appropriate and consistent with agency program goals.

B. Office of Information Technology

1. OIT shall administer and manage TCP/IP addressing.
2. OIT shall monitor the performance and capacity levels of its Internet-access infrastructure.
3. OIT shall upgrade the infrastructure as necessary to meet the programmatic needs of State agencies.
4. OIT shall ensure that security and firewall systems are sufficient and operational.
5. OIT shall provide agencies with access to monitoring information as requested.

Signature on File

E. STEVEN EMANUEL

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

4/8/2015

DATE