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:	SUPERSEDES:
14-30-NJOIT	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 | *9/5/2014*

E. STEVEN EMANUEL | **DATE**

Chief Technology Officer-NJ Office of Information Technology

State Chief Information Officer