STATE OF NEW HAMPSHIRE
DEPT OF INFORMATION TECHNOLOGY
INFORMATION TECHNOLOGY SECURITYGROUP

STATEWIDE COMPUTER USE POLICY

Standard #:	NHS0011.03.2019.V2
Impact:	Statewide
Effective Date:	04/28/2017
Created Date:	04/28/2017
Last Reviewed Date:	05/16/2023
Last Revised Date:	03/04/2019
Status:	FINAL
Owner:	ITSG

1. PURPOSE

The purpose of this policy is to specify the appropriate use of computers, computer equipment, software, systems, networks, files, electronic mail, and the Internet. This policy applies to all Authorized User(s) as defined in 3.1.

2. POLICY

State computing resources are provided for State business purposes only. This policy specifies the rules and requirements related to the acceptable use of State computing resources. Review and Signature (hardcopy or digital) by all Authorized User(s), as defined below, is required annually.

3. DEFINITIONS

3.1. "Authorized User(s)" shall mean any and all full or part-time classified, unclassified, and non-classified State employees; volunteers and interns authorized to use State computing resources; and contractors, vendors or individuals associated with the State and authorized to use State computing resources.

3.2. "Computer Use" means the use of a State computer and/or the State's electronic systems, including networks, software, electronic mail (e-mail), use of the Internet, assigned mobile devices such as cellular phones, laptops and tablets, and the storage of and access to files through such computers or systems.

3.3. "State" means the State of New Hampshire.

3.4. "Agency" means each Agency, Department, Commission or Board in the State Executive Branch.

3.5. "DoIT" means the New Hampshire Department of Information Technology.

3.6. "Supervisory personnel" means the employee's immediate supervisor or a person at a higher supervisory level within the employee's chain of management within the Agency.

3.7. "Litigation Hold" means the process of preserving information that may be required to comply with a request related to current or anticipated litigation.

3.8. "eDiscovery" means the process in which electronic data is sought, located, secured and searched for use as evidence in a legal case.

4. BACKGROUND

Improper Computer Use may present significant problems for an Agency and the State as a whole. Depending upon the circumstances, misuse might result in damage to the State's systems or equipment, might result in lost productivity or increased expense to the State or might be damaging in other ways. The use of the State's computer system to store personal files, music or videos, for example, utilizes storage space on the system, making that space unavailable for State business, while the use of the Internet for personal purposes utilizes bandwidth that is legitimately intended for conducting official activity. This policy has been adopted in order to address such concerns.

5. PRIVACY & BUSINESS USE

Each Agency may grant Computer Use to Authorized User(s) in order to facilitate communication and perform their assigned job duties. Computers, computer equipment including State owned mobile devices, files and e-mail are the property of the Agency. The Agency may monitor, or request the monitoring of, Computer Use for purposes including, but not limited to, lawful purposes, applicable regulatory compliance, checking system performance, ensuring appropriate system usage, and ascertaining bandwidth and storage capacity. Each Agency may access any of its employees' computer files and e-mail stored on State owned computers or computer equipment as needed in the course of its business. The Agency may deny or limit an employee's computer use in order to ensure compliance with this policy.

5.1. Authorized User(s) do not have a personal privacy right to material created, received, or sent via e-mail or the Internet, nor do they have a personal privacy right to information stored in computer files. Computer Use is a privilege not a right. An employee's Supervisory personnel, as well as others with appropriate authority, may curtail, limit, modify, or eliminate that privilege at any time. All employees are expected to be responsible and adhere to all acceptable use policies and procedures as defined by the State and Agency.

5.2. Computer Use is limited to State business or authorized use. This means, for example, that State e-mail systems may not be used for purely personal activities, such as communications not related to State business such as personal "blogging" or Internet use, accessing personal social media websites or checking non-work personal e-mail accounts. During work periods which do not interfere with the completion of other job assignments, employees may, however, access systems or websites which support Agency business functions (such as the NH FIRST Time Management System) or which are offered by or through the Agency to its employees.

5.3. Authorized User(s) who are granted Computer Use are expected to follow this policy. Improper Computer Use, including but not limited to failure to follow this policy, may result in the loss of some or all Computer Use privileges and may also result in disciplinary action as provided in the administrative rules of the Department of Administrative Services Division of Personnel or other applicable authority. Authorized User(s) are hereby alerted that state and federal laws establish criminal penalties for specific computer-related activities. See, among others, N.H. RSA 638:16 - 19. In cases of misuse resulting in financial loss to the State and/or the public, the employee might also be required to reimburse the State for damages, as well as any costs of collection and interest.

5.4. The State may use software to identify unauthorized, inappropriate or sexually explicit Internet sites. Authorized User(s) access to such sites may be blocked. In the event an Authorized User nonetheless encounters inappropriate or sexually explicit material

except as authorized by the Agency while browsing on the Internet, immediately disconnect from the site, regardless of whether the site was not subject to blocking software and report this immediately to your supervisor who will determine if further notification is required.

5.5. Authorized User(s) are advised that in the event the Authorized User(s) opens an e-mail and opens or downloads an e-mail attachment containing content directly related to State business to their Agency authorized personally owned or other approved non-State owned computer or device may be subject to Litigation Hold and Electronic Discovery.

6. SPECIFIC POLICIES

6.1. ***Account Usage and Access***

Receiving a State managed computer account is a privilege extended only to the Authorized User(s). Except as otherwise provided in this policy, only the Authorized User(s) to whom an account is registered is allowed to access the account. Authorized User(s) are required to take reasonable precautions to prevent unauthorized use of their account, including adherence to all policies related to password maintenance and file storage.

6.1.1. Authorized User(s) may not share their login ids, personal access codes or passwords with others. The automatic or manual forwarding/copying of state e-mail to an external destination is prohibited.

6.1.2. Authorized User(s) shall not store State business files on local computer hard drives or removable media devices unless authorized. If authorized, only equipment DoIT approved expressly for this usage can be utilized and files must be routinely copied to network storage for proper backup except otherwise authorized by the Agency. Note that DoIT will not attempt to recover files lost due to improper storage. The downloading, copying or storing of State data on unapproved and non-state owned devices is prohibited.

6.1.3. At no time shall an Authorized User(s) leave a computer without first ensuring that the computer is properly secured from unauthorized access by locking the computer, engaging a password protected screen saver or logging out from the computer.

6.1.4. Authorized User(s) shall store important information contained within e-mail according to Agency policies and retained in accordance with Agency approved retention policies. E-mail no longer needed shall be purged periodically unless the Authorized User(s) is subject to a Litigation Hold.

6.1.5. Authorized User(s) are responsible for all systems and information accessed by their assigned account except in cases where it was confirmed an account was maliciously obtained and used by others

6.1.6. Authorized User(s) shall never select, if provided, the ‘remember’ option to save or cache account credentials.

6.1.7. Authorized User(s) shall not intercept, disclose, or assist in intercepting or disclosing, any electronic communications except as authorized by this policy or as otherwise authorized by the Agency.

6.1.8. Authorized User(s) must follow appropriate federal and state laws and regulations as they apply to the collection, storage, distribution or exchange of regulated and protected information.

6.1.9. Authorized User(s) providing false or misleading information for the purposes of gaining Computer Use is prohibited under this policy.

6.1.10. Authorized User(s) must follow this computer use policy as well as agency-specific policies that provide additive guidance more specifically outlining agency policy.

6.2. ***Inappropriate Computer Use***

Authorized User(s) shall not intentionally or through neglect misuse or damage the State's computers, its systems or other users' information nor steal, abuse or damage resources, equipment or supplies belonging to the State or Agency. Authorized User(s) will not engage in computer-related illegal or unethical activities, personal activities such as recreational game-playing, vacation planning, other employment or self-owned businesses; shopping and the like on any State computer; or store personal electronic files on a State computer or network, including but not limited to documents, spreadsheets, pictures, videos, software, applications or music.

6.3. ***Examples of Unacceptable Computer Use***

The following is a non-exhaustive list of "unacceptable" Computer Use of state owned computers, computer equipment or devices. Employees shall not use the State's computers or its systems for the following purposes or in these manners.

6.3.1. Communicating or exchanging information not directly related to the business, mission or goals of the Agency or the State of New Hampshire or as approved in this policy.

6.3.2. Browsing, uploading, downloading or posting to the Internet for non-business purposes regardless of access provided by DoIT and Agency filtering policies.

6.3.3. Publishing information on the Internet without the approval of the appropriate Supervisory personnel.

6.3.4. Any purpose which violates federal or state law, or any Computer Use to access or distribute any illegal material, or for any illegal purpose.

6.3.5. Computer Use in a manner that intentionally interrupts or disrupts network users, services or equipment.

6.3.6. Intentionally seeking out information on, obtaining copies of, or modifying files and other data which is private, confidential or not open to public inspection, unless specifically authorized to do so legally by a person with appropriate authority.

6.3.7. Computer Use to intentionally copy software, electronic files, programs or data which may be prohibited from such copying, unless a determination has been made by a person with appropriate authority that such copying is in fact permissible. Efforts to obtain such permission should be documented.

6.3.8. Seeking passwords of others or the exchange/sharing of passwords with others, including supervisors.

6.3.9. Intentionally representing oneself electronically as another person, unless specifically authorized to do so.

6.4. ***Inappropriate Use of Software***

Only software owned by, licensed by, or approved for use by the State may be installed on State equipment.

6.4.1. State owned or licensed software may not be installed on personally owned equipment without prior Agency approval.

6.4.2. Software that has been licensed to the State must not be copied or moved to another site by the user. Users must exercise a high degree of care to protect software licenses from unauthorized access, misuse, theft, damage, destruction, or modification.

6.5. ***Annual Awareness Training***

All employees must complete Cybersecurity awareness training annually, including state required baseline mandatory modules as well as additional modules or other training as applicable and identified by the Agency based on their role within the Agency, the data classification and associated regulatory requirements.

6.6. ***Confidentiality and Nondisclosure***

Authorized User(s) should treat the information they possess or access as propriety and not subject to spontaneous disclosure.

6.7. ***Acknowledgement Requirements***

All employees are required to review and acknowledge this policy as well reflect on their adherence of the policy on an annual basis during their annual performance review and/or at another time as specified by the Agency**.**

6.8. ***Department of Information Technology Statewide Standards and Policies***

DoIT periodically issues policies, procedures and standards which are applicable statewide and with which all State employees should be familiar. DoIT statewide polices and standards are located on the Agencies Intranet accessible by Authorized User(s) connected to the State network.

6.9. ***Modified and Supplemental Requirements***

The Agency may create an addendum to this policy with more restrictive requirements or limitations imposed within particular divisions, units, bureaus and offices of their Agency. In the event of a conflict, the most restrictive will apply.

6.10. ***Failure to Abide by Policy***

Employees who do not comply with this policy, as from time to time amended, or who decline to execute the Employee Acknowledgement when requested to do so, may be

subject to disciplinary action as described in the Administrative Rules of the Division of Personnel or other applicable authority, up to and including dismissal from employment.

The State and its Agencies may reserve the right to monitor, to check system performance to ensure computers, systems, and networks are used properly and to restrict activity on the network as appropriate. Individual Authorized User(s) should have no personal expectation of privacy for any information they create or receive utilizing State's IT resources.

In the event there is a policy question, each Authorized User(s) shall check with supervisors, management or designees.

7. AUTHORITY/REFERENCES

RSA 21-R, XVIII
Department of Information Technology Statewide Standards:
http://www.nh.gov/doit/intranet/toolbox/standards/index.php

EMPLOYEE ACKNOWLEDGEMENT

I hereby acknowledge that I have read and understand the foregoing Statewide Computer Use Policy and have been given the opportunity to ask any questions that I may have in regard to this Policy. I agree to act in accordance with the Policy, as it may from time to time be amended, and understand that if I do not act in accordance with the Policy, as from time to time amended, I may be subject to disciplinary action as described in the Administrative Rules of the Division of Personnel or other applicable authority, up to and including dismissal from employment.

Employee's Printed Name	Agency
Employee's Signature	Date