OhioDAS

State of Ohio Administrative Policy

Use of Internet, E-mail and Other IT Resources

No:
Information Technology
IT-04

Effective:
September 14, 2017

Issued By:

Robert Blair, Director

1.0 Purpose

This state policy establishes controls on the use of state-provided information technology (IT) resources to ensure that they are appropriately used for the purposes for which they were acquired.

A glossary of terms found in this policy is located in Appendix A - Definitions. The first occurrence of a defined term is in ***bold italics***.

2.0 Policy

Agencies shall establish an ***Internet***, e-mail and ***IT resources*** use policy in compliance with this state policy and ensure that employees, contractors, temporary personnel and other agents of the state adhere to that policy. Agencies shall define and implement such a policy based on the business requirements of the agency. Agency policy shall describe the extent to which personal use is allowed. Agencies may adopt or endorse this state policy as agency policy or may further restrict the duration, frequency and nature of personal use.

2.1 **Use of State-Provided IT Resources:** The State of Ohio provides computers, services, software, supplies and other IT resources to employees, contractors, temporary personnel and other agents of the state for supporting the work and conducting the affairs of Ohio government. Personal use, if permitted by an agency, shall be strictly limited and can be restricted or revoked at an agency's discretion at any time.

2.1.1 **Use of State-Provided Telephones and Services:** Restrictions on the use of IT resources outlined in this policy apply to wired and ***wireless*** telephone devices and services, including facsimile machines connected to the state's ***telephone service***. Additional restrictions on the use of state telephones and services are covered by Ohio Administrative Policy IT-11, "Use of State Telephones."

2.1.2 **Use for Collective Bargaining Purposes:** In addition to this state policy, collective bargaining contract provisions control the use of state-provided IT resources for contract enforcement, interpretation and grievance processing.

2.2 **Unacceptable Personal Use:** Any personal use of IT resources that disrupts or interferes with government business, incurs an undue cost to the state, could potentially embarrass or harm the state, or has the appearance of impropriety is strictly prohibited. Personal use that is strictly prohibited includes, but is not limited to, the following:

2.2.1 **Violation of Law:** Violating or supporting and encouraging the violation of local, state or federal law is strictly prohibited.

2.2.2 **Illegal Copying:** Downloading, duplicating, disseminating, printing or otherwise using copyrighted materials, such as software, texts, music and graphics, in violation of copyright laws is strictly prohibited.

2.2.3 **Operating a Business:** Operating a business, directly or indirectly, for personal gain is strictly prohibited.

2.2.4 **Accessing Personals Services:** Accessing or participating in any type of personals advertisements or services, such as or similar to dating services, matchmaking services, companion finding services, pen pal services, escort services, or personals advertisements is strictly prohibited.

2.2.5 **Accessing Sexually Explicit Material:** Downloading, displaying, transmitting, duplicating, storing or printing sexually explicit material is strictly prohibited.

2.2.6 **Harassment:** Downloading, displaying, transmitting, duplicating, storing or printing material that is offensive, obscene, threatening or harassing is strictly prohibited.

2.2.7 **Gambling or Wagering:** Organizing, wagering on, participating in or observing any type of gambling event or activity is strictly prohibited.

2.2.8 **Mass E-mailing:** Sending unsolicited e-mails or facsimiles in bulk or forwarding electronic chain letters in bulk to recipients inside or outside of the state environment is strictly prohibited.

2.2.9 **Solicitation:** Except for agency-approved efforts, soliciting for money or support on behalf of charities, religious entities or political causes is strictly prohibited.

2.3 **Participation in Online Communities:** Any use of state-provided IT resources to operate, participate in, or contribute to an online community including, but not limited to, ***online forums***, ***chat rooms***, ***instant messaging***, ***listservs***, ***blogs***, ***wikis***, ***peer-to-peer file sharing***, and ***social networks***, is strictly prohibited unless organized or approved by the agency. If an individual is approved to participate in any of these forms of communication as part of state business, that person shall fulfill agency-defined security education and

awareness requirements for proper use before participating. The content of the education and awareness requirements shall include methods to avoid inadvertent disclosure of sensitive information and practices to avoid that could harm the security of state computer systems and networks.

2.4 **Use of *Cloud File Sharing Solutions***: Only state approved cloud file sharing solutions, Microsoft OneDrive for Business and SharePoint Online, shall be used to store, share and synchronize state ***data***. This requirement is not intended to limit the use of state approved cloud services and solutions. The purpose of the requirement is to prohibit the use of cloud file sharing solutions that are not authorized for state use, that may not be adequately secured and that may compromise the state's ability to preserve and access information and comply with public records laws.

When using state approved cloud file sharing solutions, the following restrictions apply:

2.4.1 **Cloud File Sharing and Data**: Only data related to state business shall be stored in state approved cloud file sharing solutions.

2.4.2 ***Sensitive Data* and Cloud File Sharing Solutions**: Sensitive data shall only be stored in Microsoft OneDrive for Business or SharePoint Online if an agency has approved the practice. If approved, agency procedures shall align with the requirements outlined in Ohio Administrative Policy IT-14, "Data Encryption and Securing Sensitive Data". Agencies shall ensure that users understand the procedures for handling and securing sensitive data.

2.4.2.1 Sensitive state data shall not be downloaded from cloud file sharing solutions onto personal devices unless explicitly authorized by the user's agency.

2.4.3 **Alternative Cloud File Sharing Solutions**: Any other cloud file sharing solutions shall be submitted to the Department of Administrative Services (DAS) Office of Information Security and Privacy for evaluation and approval prior to being used to share state data.

2.5 **Unauthorized Installation or Use of Software:** Installing or using software including, but not limited to, instant messaging clients and peer-to-peer file sharing software, or personally owned software, without proper agency approval is strictly prohibited. Installation and use of unlicensed software is strictly prohibited.

2.6 **Unauthorized Installation or Use of Hardware:** Installing, attaching, or physically or wirelessly connecting any kind of hardware device to any state-provided IT resource, including computers and network services, without prior authorization is strictly prohibited. Connecting or attempting to connect a wireless device to the state's wireless service without proper agency approval is strictly prohibited.

2.7 **No Expectation of Privacy:** This policy serves as notice to employees, contractors, temporary personnel and other agents of the state that they shall have no expectation

of privacy in conjunction with their use of state-provided IT resources. Contents of state computers may be subject to review, investigation and public disclosure. Access and use of the Internet, including communication by e-mail and instant messaging and the content thereof, are not confidential, except in certain limited cases recognized by state or federal law. The state reserves the right to view any files and electronic communications on state computers, monitor and log all electronic activities, and report findings to appropriate supervisors and authorities.

2.7.1 **Impeding Access:** Impeding the state's ability to access, inspect and monitor IT resources is strictly prohibited. Employees, contractors, temporary personnel and other agents of the state shall not encrypt or conceal the contents of any file or electronic communication on state computers without proper authorization. Employees, contractors, temporary personnel and other agents of the state shall not set or manipulate a password on any state computer, program, file or electronic communication without proper authorization.

2.8 **Public Records**: Employees, contractors, temporary personnel and other agents of the state shall understand that records created as a result of the use of state-provided IT resources may be subject to disclosure under Ohio's public records law and must be retained in accordance with state and agency record retention schedules. In addition, the records created may also be subject to ***eDiscovery***.

2.9 **Misrepresentation:** Concealing or misrepresenting one's name or affiliation to mask unauthorized, illegal, fraudulent, irresponsible or offensive behavior in electronic communications is strictly prohibited.

2.10 **Restrictions on the Use of State E-mail Addresses:** Employees, contractors, temporary personnel and other agents of the state shall avoid the appearance of impropriety and avoid the appearance of leveraging the stature of the state in the use of their assigned state e-mail address. State e-mail addresses, such as "firstname.lastname@ohio.gov" or "firstname.lastname@agency.state.oh.us," shall not be used for personal communication in public forums such as, or similar to, listservs, discussion boards, discussion threads, comment forums, or blogs.

2.11 **Violations of Systems Security Measures:** Any use of state-provided IT resources that interferes with or compromises the security or operations of any computer system, or compromises public trust, is strictly prohibited.

2.11.1 **Confidentiality Procedures:** Using IT resources to violate or attempt to circumvent ***confidentiality*** procedures is strictly prohibited.

2.11.2 **Accessing or Disseminating Sensitive Data or Personally Identifiable Information:** Accessing or disseminating sensitive data or ***personally identifiable information***, without authorization is strictly prohibited.

2.11.3 **Accessing Systems without Authorization:** Accessing networks, files or systems or an account of another person without proper authorization is strictly

prohibited. Employees, contractors, temporary personnel and other agents of the state are individually responsible for safeguarding their passwords.

2.11.4 **Duplicating Passwords**: Employees, contractors, temporary personnel, and other agents of the state who are assigned both user accounts and ***privileged user accounts*** shall not use the same password for multiple accounts. Users must maintain unique passwords for each account.

2.11.5 ***Save Password Option***: Employees, contractors, temporary personnel, and other agents of the state shall not leverage save password options.

2.11.6 **Distributing Malicious Code:** Distributing ***malicious code*** or circumventing malicious code security is strictly prohibited.

2.12 **Penalties:** Violation of this policy may result in disciplinary action or contractual penalties, and may be cause for termination. In addition, employees, contractors, temporary personnel and other agents of the state may be subject to a civil action or criminal prosecution as a result of inappropriate use or misuse of IT resources. The Ohio Revised Code (ORC) makes certain misuses of IT resources criminal offenses:

- ORC Section 2909.04 – knowingly using a computer system, network or the Internet to disrupt or impair a government operation.
- ORC Section 2909.05 – causing serious physical harm to property that is owned, leased, or controlled by a government entity.
- ORC Section 2913.04 – accessing without authorization any computer, computer system, or computer network without consent of the owner.
- ORC Section 2921.41 – using a public office to commit theft which includes fraud and unauthorized use of government computer systems.

2.13 **Contractual Agreements**: As of the effective date of this policy, any new contractual agreements for vendors and contractors shall include a requirement to comply with this policy as well as any associated agency policies prior to gaining access to statewide and agency IT resources.

2.14 **Compliance:** Agencies shall undertake measures to ensure that employees, contractors, temporary personnel and other agents of the state adhere to agency policy.

2.14.1 **Education and Awareness:** Agencies shall ensure that restrictions and controls on personal use of IT resources are addressed by education and awareness programs. Employees, contractors, temporary personnel and other agents of the state shall be made aware of their respective agency's use policy, this state policy, applicable local, state and federal laws, and any applicable collective bargaining agreement provisions. Agencies shall provide employees,

contractors, temporary personnel and other agents of the state under their employ a copy of the agency's Internet, e-mail and IT resources use policy.

2.15 **State Registry:** The DAS Office of Information Technology (OIT) Enterprise IT Architecture and Policy Program Area shall maintain a registry of the Internet, e-mail and IT resources use policies of state agencies.

2.15.1 Statewide IT Policy shall establish a procedure for the submission of agency Internet, e-mail and IT resources use policies and shall instruct agencies as to the requirements of the procedure. Agencies shall be notified of any relevant changes in the procedure.

2.15.2 Upon request, Enterprise IT Architecture and Policy shall make the registry available for inspection in a timely manner to any interested party.

2.16 **Procedures:** Agencies shall submit a copy of their Internet, e-mail and IT resources use policy to DAS OIT Enterprise IT Architecture and Policy.

2.16.1 If at any time an agency should make a change of substance in their Internet, e-mail and IT resource use policy, a copy of the revised policy shall be submitted to Enterprise IT Architecture and Policy.

2.16.2 Copies of policies shall be submitted using one of the following forms and methods.

- For hardcopy documents or for documents in .pdf or .doc formats on optical media, submit via interagency mail to DAS OIT, Enterprise IT Architecture and Policy, 30 East Broad Street, 39th Floor
- For documents in .pdf or .doc formats, submit as e-mail attachments to DAS.State.ITPolicy.Manager@das.ohio.gov
- For documents posted to an externally available website not requiring authentication, submit the applicable URL via e-mail to DAS.State.ITPolicy.Manager@das.ohio.gov

3.0 Authority

ORC 125.18, 2909.04, 2909.05, 2913.04, 2921.41

4.0 Revision History

Date	Description of Change
01/01/1996	Ohio IT Policy OPP-008 replaces PB-002 and all previously released memoranda regarding this topic.
03/20/2006	Revise policy requirements on acceptable and unacceptable personal use of IT resources by employees, contractors, temporary personnel and other agents of the state.
03/19/2008	Policy requirements concerning participation in online communities were moved from ITP-B.6, "Internet Security," into section 2.3 of this policy.
04/18/2011	References to Ohio IT Policies ITP-B.3, "Password and PIN Security," and ITP-B.4, "Malicious Code Security," were removed from the policy. These policies were rescinded due to the publication of Ohio IT Standard ITS-SEC-02, "Enterprise Security Controls Framework."
05/04/2015	Added requirements for the use of cloud storage solutions and eDiscovery as well as modified the public records and record retention section. Transferred policy content to a new State of Ohio Administrative Policy Template. Re-numbered policy to IT-04 to be consistent with new numbering format.
09/14/2017	Revised the cloud storage solution requirements to align with current capabilities and procedures. The focus of the requirements is now on cloud file sharing solutions. Added new requirements for passwords and vendor/contractor contractual agreements.
09/14/2019	Scheduled policy review.

5.0 Inquiries

Direct inquiries about this policy to:

State IT Policy Manager
Enterprise IT Architecture & Policy
Office of Information Technology
Ohio Department of Administrative Services
30 East Broad Street, 39th Floor
Columbus, Ohio 43215

1-614-466-6930 | DAS.State.ITPolicy.Manager@das.ohio.gov

State of Ohio Administrative Policies may be found online at
www.das.ohio.gov/forStateAgencies/Policies.aspx

Direct inquiries regarding sensitive data and cloud file sharing solutions to:

Office of Information Security & Privacy
Office of Information Technology
Ohio Department of Administrative Services

30 East Broad Street, 19th Floor
Columbus, Ohio 43215

1-614-644-9391 | state.isp@das.ohio.gov

Appendix A - Definitions

a. Availability. Ensuring timely and reliable access to and use of information.[1]

b. Blog. Web-based content consisting primarily of periodic articles or essays listed with the latest entry and visitor comments at the top. Blog topics can range from personal diaries to political issues, media programs and industry analysis. Blogs are also known as "Weblogs" or "Web logs."

c. Chat Room. An online forum where people can broadcast messages to people connected to the same forum in real time. Sometimes, these forums support audio and video communications, allowing people to converse and to see each other.

d. Cloud File Sharing Solutions. Cloud services that allow users to store and synchronize documents, photos, videos and other files in the cloud—and share them with other people. These services also allow users to share and synchronize data among multiple devices for a single owner. These services are accessible through desktops, notebooks, smartphones and media tablets, and provide a simple mechanism for synchronizing data across multiple devices.[2]

e. Confidentiality. Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [3]

f. Data. Coded representation of quantities, objects and actions. The word, "data," is often used interchangeably with the word, "information," in common usage and in this policy.

g. eDiscovery. "Discovery" refers to the process of complying with legal obligations to produce relevant documents and information to opposing counsel in the course of civil litigation or to prosecutors or government investigators in criminal or regulatory proceedings. "eDiscovery" refers to the production of files or other data held in an electronic form, such as e-mail.[4]

[1] "NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations," U.S. Department of Commerce National Institute of Standards and Technology, April, 2013 <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>.
[2] "Cloud File Sharing" *Gartner IT Glossary*. Web. 19 October 2016. http://www.gartner.com/it-glossary/cloud-file-sharing
[3] "NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations," U.S. Department of Commerce National Institute of Standards and Technology, April, 2013 <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>.
[4] Jamie Popkin, "E-Discovery for IT Professionals: An Exceptional Process that Requires Unique Core Competencies," *Gartner Research Note*, 17 February 2011 (Stamford, CT: Gartner, Inc., 2011).

h. Information Technology (IT) Resources. Any information technology resource, such as computer hardware and software, IT services, telecommunications equipment and services, digital devices such as digital copiers and facsimile machines, supplies and the Internet, made available to employees, contractors, temporary personnel and other agents of the state in the course of conducting state government business in support of agency mission and goals.

i. Instant Messaging. A software tool that allows real-time electronic messaging or chatting. Instant messaging services use "presence awareness," indicating whether people on one's list of contacts are currently online and available to chat.

j. Integrity. Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.[5]

k. Internet. A worldwide system of computer networks — a network of networks — in which computer users can get information and access services from other computers. The Internet is generally considered to be public, untrusted and outside the boundary of the state of Ohio enterprise network.

l. Listserv. An electronic mailing list software application that was originally developed in the 1980s and is also known as "discussion lists." A listserv subscriber uses the listserv to send messages to all the other subscribers, who may answer in similar fashion.

m. Malicious Code. Software or firmware intended to perform an unauthorized process that will have an adverse impact on the confidentiality, ***integrity***, or ***availability*** of an information system. Some examples include a virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.[6]

n. Online Forum. A Web application where people post messages on specific topics. Forums are also known as Web forums, message boards, discussion boards and discussion groups.

o. Peer-to-Peer (P2P) File Sharing. Directly sharing content like audio, video, data, software or anything in digital format between any two computers connected to the network without the need for a central server.

p. Personally Identifiable Information (PII). "Personally identifiable information" is information that can be used directly or in combination with other information to identify a particular individual. It includes:

- a name, identifying number, symbol, or other identifier assigned to a person,
- any information that describes anything about a person,

[5] "NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations," U.S. Department of Commerce National Institute of Standards and Technology, April, 2013 <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>.
[6] *Ibid.*

- any information that indicates actions done by or to a person,
- any information that indicates that a person possesses certain personal characteristics

q. Privileged User Accounts. Passwords associated with user accounts, which are assigned to individuals (commonly referend to as named accounts), that have elevated access to make changes to system parameters.

r. Save Password Option. An option on some systems that, when enabled, allows the user the choice of whether to have the user password memorized by the system so that it will not need to be re-entered upon subsequent access.

s. Sensitive Data. Sensitive data is any type of computerized data that presents a high or moderate degree of risk if released or disclosed without authorization. There is a high degree of risk when unauthorized release or disclosure is contrary to a legally mandated confidentiality requirement. There may be a moderate risk and potentially a high risk in cases of information for which an agency has discretion under the law to release data, particularly when the release must be made only according to agency policy or procedure. The computerized data may be certain types of personally identifiable information that is also sensitive such as medical information, social security numbers, and financial account numbers. It includes Federal Tax Information under IRS Special Publication 1075, Protected Health Information under the Health Insurance Portability and Accountability Act, and Criminal Justice Information under Federal Bureau of Investigation's Criminal Justice Information Services (CJIS) Security Policy. The computerized data may also be other types of information not associated with a particular individual such as security and infrastructure records, trade secrets and business bank account information.

t. Social Networks. Websites promoting a "circle of friends" or "virtual communities" where participants are connected based on various social commonalities such as familial bonds, hobbies or dating interests.

u. Telephone Service. Unless otherwise stated, telephone service includes both wired telephones and wireless telephones.

v. Wiki. A Web application that allows one user to add content and any other user to edit the content. The popular software used to implement this type of Web collaboration is known as "Wiki." A well-known implementation is Wikipedia, an online encyclopedia.

w. Wireless. Use of various electromagnetic spectrum frequencies, such as radio and infrared, to communicate services, such as data and voice, without relying on a hardwired connection, such as twisted pair, coaxial or fiber optic cable.