

Appropriate Use of IT Resources – Revision Summary

This revision adds requirements for cloud storage (page 4 #6), information related to public records (page 4 #9) and definitions (#3, 5, 13, 15)

Appropriate Use of IT Resources

SOURCE: ORC 2909, ORC 2913, ORC 2921, Ohio IT Policy; ITP-E.8 Ohio IT Policy; ITP-H.2 Ohio IT Policy; IT-04 Ohio EPA Policy; Password-PIN Security Ohio EPA Policy; Malicious Code Security

CONTACT: INFORMATION TECHNOLOGY SERVICES

Purpose

This policy establishes controls on the use of state-provided information technology (IT) resources to ensure appropriate use.

Background

The Ohio EPA furnishes a variety of *IT resources* to employees, contractors and temporary personnel to conduct the business of the agency. With such a proliferation of devices, services and software, greater care is required to prevent misappropriation of publicly-owned IT resources.

Just as important, the people of Ohio expect their *public servants* to devote their time to conduct the state's business. Public servants must be mindful of the public trust that they discharge, of the necessity for conducting themselves according to the highest ethical principles, and of avoiding any action that may be viewed as a violation of the public trust. As custodians of resources entrusted to them by the public, public servants must be mindful of how these resources are used.

Appropriate Use of IT Resources Policy

The Ohio EPA provides computers, services, software, supplies and other IT resources to employees, contractors and temporary personnel for supporting the work and conducting the affairs of the agency. As the user of IT Resources, the employee will be held accountable for any misuse. Information contained on IT Resources is subject to review by division/office managers. The scope of this policy includes State and Ohio EPA computer systems and the employees, contractors, temporary personnel and other agents of the Ohio EPA who use or administer such systems. Personal use, if permitted by Ohio EPA, shall be strictly limited and can be restricted or revoked at the agency's discretion at any time.

1. No Expectation of Privacy. This policy serves as notice to Ohio EPA employees, contractors and temporary personnel that they shall have no reasonable expectation of privacy in conjunction with their use of Agency-provided IT resources. Contents of 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.

- a. Impeding Access. Impeding the agency's ability to access, inspect and monitor IT resources is strictly prohibited. Ohio EPA employees, contractors and temporary personnel shall not encrypt or conceal the contents of any file or electronic communication on any Agency computer without proper authorization. Agency employees, contractors and temporary personnel shall not set or manipulate a password on any state computer, program, file or electronic communication without proper authorization.
2. Unacceptable Personal Use. Personal use of Agency provided IT resources shall be kept to a minimum and, whenever possible, done during lunch hours or authorized breaks. Any personal use of Agency provided IT resources that disrupts or interferes with Ohio EPA business, incurs an undue cost to the agency, interferes with the productivity of the employee, could potentially embarrass or harm the Ohio EPA, or has the appearance of impropriety is strictly prohibited which includes, but is not limited to, the following:
- a. Violation of Law. Violating or supporting and encouraging the violation of local, state or federal law.
 - b. Illegal Copying. Downloading, duplicating, disseminating, printing or otherwise using copyrighted materials, such as software, texts, music and graphics, in violation of copyright laws.
 - c. Operating a Business. Operating a business, directly or indirectly, for personal gain.
 - d. Accessing Personals Services. Accessing or participating in any type of personals ads or services, such as or similar to dating services, matchmaking services, companion finding services, pen pal services, escort services, or personals ads.
 - e. Accessing Sexually Explicit Material. Downloading, displaying, transmitting, duplicating, storing or printing sexually explicit material.
 - f. Sexually Oriented Messages or Images. Sending, soliciting, viewing or downloading sexually oriented messages or images.
 - g. Harassment. Downloading, displaying, transmitting, duplicating, storing or printing material that is offensive, obscene, threatening or harassing.
 - h. Offensive or Harassing Statements. Making offensive or harassing statements, including disparagement of others based on their race, national origin, sex, sexual orientation, gender identity, age, disability, veteran's status, religious or political beliefs.
 - i. Gambling or Wagering. Organizing, wagering on, participating in or observing any type of gambling event or activity, including the state of Ohio lottery.

- j. 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.
 - k. Incendiary Statements. Making incendiary statements which may incite violence or describe or promote the use of weapons or devices associated with terrorist activities.
 - l. Signature. Use of another's signature line.
 - m. Electronic Transmission of Data. Emailing or electronically transmitting state data or information for anything other than state business without proper authorization.
 - n. Solicitation. Except for agency-approved efforts, soliciting for money or support on behalf of charities, religious entities or political causes.
 - o. Destruction. Intentional or negligent destruction of IT resources.
 - p. Video/Audio Streaming. Excessive streaming of videos, music, audio files for personal use is prohibited.
3. Saving all files to the home directory or network shared drive is required. All files related to Agency work must be saved either to the home directory, a SharePoint site, or a network shared drive so that:
- a. Files are available for public records requests or legal discovery
 - b. Files can be backed up and restored properly
4. All Agency laptops must connect to network
All Agency laptops must connect to the network at least once a month to receive software patches and security updates. Owners of divisional shared laptops are responsible for connecting those laptops to the network.
5. 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, e-bay, Craig's list, and social networks**, unless organized or approved by the Ohio EPA is strictly prohibited. If an individual is approved to participate in any of these forms of communication as part of state business, cyber security awareness training will be provided advising avoidance of inadvertent disclosure of sensitive information and practices that could harm the security of agency computer systems and networks.

6. Use of Cloud Storage. Only state approved cloud storage solutions, Microsoft OneDrive for Business and SharePoint Online, shall be used to store, share and manage information. When using state cloud storage solutions, the following restrictions apply:
 - a. Data Storage: Only data related to state business shall be stored in state cloud storage solutions. Personal data shall not be stored in state cloud storage solutions.
 - b. Sensitive Data storage: Sensitive data shall not be stored in Microsoft OneDrive for Business. Sensitive data storage is permitted in SharePoint Online if rights management and data encryption is implemented by the agency. Data encryption shall be in alignment with the requirements outlined in Ohio IT Bulletin ITB-2007.02, "Data Encryption and Securing Sensitive Data."
 - 1) Any other cloud storage 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 store sensitive data.
7. 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.
8. Unauthorized Installation or Use of Hardware. Installing, attaching, or physically or wirelessly connecting any kind of hardware device to any Agency-provided IT resource, including computers and network services, without prior authorization is strictly prohibited. Connecting or attempting to connect a **wireless** device to the Ohio EPA's internal wireless service without proper agency approval is strictly prohibited.
9. Public Records. Public servants 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**.
10. Misrepresentation. Concealing or misrepresenting one's name or affiliation to mask unauthorized, fraudulent, irresponsible or offensive behavior in electronic communications is strictly prohibited.
11. Restrictions on the Use of Agency E-mail Addresses. Agency employees, contractors and temporary personnel shall avoid the appearance of impropriety and avoid the appearance of leveraging the stature of the Ohio EPA in the use of their assigned state e-mail address. State e-mail addresses, such as

firstname.lastname@epa.ohio.gov shall not be used for personal communication in public forums such as, or similar to, listservs, discussion boards, discussion threads, comment forums, or blogs.

12. Violations of Systems Security Measures. Any use of agency-provided IT resources that interferes with or compromises the security or operations of any computer system, or compromises public trust, is strictly prohibited.
 - a. Confidentiality Procedures. Using IT resources to violate or attempt to circumvent confidentiality procedures is strictly prohibited.
 - b. Accessing or Disseminating Confidential Information. Accessing or disseminating confidential information or information about another person without authorization is strictly prohibited.
 - c. Accessing Systems without Authorization. Accessing networks, files or systems or an account of another person without proper authorization is strictly prohibited. Ohio EPA employees, contractors and temporary personnel are individually responsible for safeguarding their passwords in accordance with Ohio EPA Policy, "Password-PIN Security."
 - d. Distributing Malicious Code. Distributing malicious code or circumventing malicious code security is strictly prohibited. Ohio EPA Policy, "Malicious Code Security," outlines requirements for protecting IT resources against threats from malicious code.
13. Awareness and Training. The Ohio EPA shall provide awareness and training on personal use of agency IT resources. All agency employees, contractors and temporary personnel shall be provided a copy of this policy.

Compliance

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination. In addition, public servants 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.

Definitions

1. 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.”
2. 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.
3. Cloud Storage. A solution that allows computer data to be stored remotely, providing users the ability to upload and access data over the internet from a variety of devices (e.g., computer, tablet, smartphone or other networked device).
4. Confidentiality. Confidentiality is the assurance that information is disclosed only to those systems or persons who are intended to receive the information. Areas in which confidentiality may be important include nonpublic customer information, patient records, information about a pending criminal case, or infrastructure specifications. Information systems that must ensure confidentiality will likely deploy techniques such as passwords, and could include encryption.
5. 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.
6. Instant Messaging. Instant Messaging is 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. Examples of instant messaging services are AOL Instant Messenger, Yahoo! Messenger and MSN Messenger.
7. 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.
8. 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 public servants in the course of conducting state government business in support of agency mission and goals.

9. Listserv. Listserv is 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.
10. Malicious Code. Malicious Code is a collective term for program code or data that is intentionally included in or inserted into an information system for unauthorized purposes without the knowledge of the user. Examples include viruses, logic bombs, Trojan horses and worms.
11. Online Forum. Online Forum is a Web application where people post messages on specific topics. Forums are also known as Web forums, message boards, discussion boards and discussion groups. They were predated by newsgroups and bulletin boards in the 1980s and 1990s.
12. 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. Examples of P2P networks are Kazaa, OpenNap, Grokster, Gnutella, eDonkey and Freenet.
13. 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,
 - Any information that indicates actions done by or to a person,
 - Any information that indicates that a person possesses certain personal characteristics
14. Public Servant. Any employee of the state, whether in a temporary or permanent capacity, and any other person performing a government function, including, but not limited to, a consultant, contractor, advisor or a member of a temporary commission.
15. Sensitive Data. Sensitive data is any type of computerized data that presents a high or medium 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 medium 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. 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.

16. Social Networks. Web sites 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. Examples include eHarmony, Facebook, Friendster, LinkedIn, Match.com, MySpace, Plaxo and Yahoo! Groups.
17. Telephone Service. Unless otherwise stated, telephone service includes both wired telephones and wireless telephones.
18. Voice Over IP (VOIP). A VoIP phone uses voice over IP (VoIP) technologies allowing telephone calls to be made over an IP network such as the Internet instead of the ordinary PSTN system.
19. 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.
20. 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.

NOTE: This policy is one of many Ohio EPA Security Policies. Ohio EPA Security Policies should be considered collectively rather than as separate or unrelated.

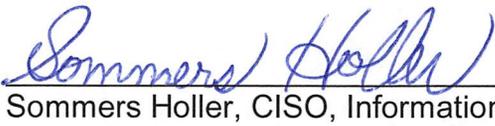
Revision History

Version	Date	Modified By	Description
1.0	08/2012	Skip Holler	Base Version
1.1	07/08/2013	Skip Holler	Added information related to VOIP
1.2	07/02/2014	Skip Holler	Added g drive, collaboration site, network shared drive use requirements and updated email domain from state.oh.us to epa.ohio.gov
1.3	07/24/2014	Skip Holler	Added section 4 talking about connecting laptops to the network. Deleted the original section 1 talking about phones and created a new policy titled: Wired and Wireless Telephone Policy.
1.4	05/11/2015	Skip Holler	Added sections 6 – Use of Cloud Storage and 9 – Public Records
1.4	07/06/2016	Skip Holler	Added 2(p) – Video/Audio Streaming

Approval date and signature of authorizing official:


Rick Magni, CIO, Information Technology Services

Date: 7-6-16


Sommers Holler, CISO, Information Technology Services

Date: 7-06-2016