



## Department of Commerce

Division of Financial Institutions

John R. Kasich, Governor

Jacqueline T. Williams, Director

OFFICE OF  
INSPECTOR GENERAL

2018 DEC 20 AM 10:14

December 12, 2018

Inspector General Randall J. Meyer  
Office of the Inspector General  
30 E. Broad St., Suite 2940  
Columbus, OH 43215

Re: Agency Response to Investigation 2018-CA00032

Dear Inspector General Meyer:

The Ohio Department of Commerce, Division of Real Estate and Professional Licensing, has reviewed your office's report of investigation and the recommendations contained therein. The Department respectfully submits the following responses to your recommendations:

1. Review the actions of Unnamed subject and determine if administrative action is warranted.

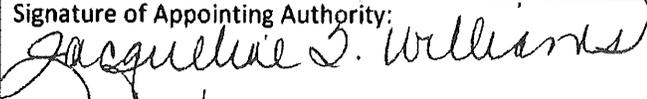
Response: The Department of Commerce completed an administrative review of the conduct of the employee referred to as Unnamed subject in Investigation 2018-CA00032 and terminated the employee on November 16, 2018.

2. Review the Comprehensive Computer Use policy, particularly the Email use section.

Response: The Department of Commerce issued the enclosed new Computer and IT Resource Use policy effective September 17, 2018. All Department employees were provided the new policy and required to acknowledge receipt.

Sincerely,

  
Jacqueline T. Williams  
Director

<p style="text-align: center;">State of Ohio</p>  <p style="text-align: center;">Department of Commerce</p>	<b>Subject/Policy:</b> Computer and IT Resource Use	Page 1 of 8 Policy #: 501.0
	<b>Rule/Code Reference:</b> HR-42	<b>Purpose:</b> This 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.
	<b>Effective Date:</b>  September 17, 2018	
	<b>Signature of Appointing Authority:</b>  <b>Date:</b> 9/10/18	

*This policy applies to all contractors, temporary personnel, and other agents of the state working at Commerce locations and all employees of the Ohio Department of Commerce, and will not supersede the language agreed to in the collective bargaining agreement.*

I. Definitions

- a. **Availability:** Ensuring timely and reliable access to and use of information.<sup>1</sup>
- 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.<sup>2</sup>

<sup>1</sup> “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>>.

<sup>2</sup> “Cloud File Sharing” *Gartner IT Glossary*. Web. 19 October 2016. <http://www.gartner.com/it-glossary/cloud-filesharing>

- e. **Confidentiality:** Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.<sup>3</sup>
- 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.<sup>4</sup>
- 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:** Communication between computer users that takes place in real time over the network. It is analogous to a telephone conversation but is text based rather than voice based.
- j. **Integrity:** Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.<sup>5</sup>
- 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.<sup>6</sup>
- 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.

---

<sup>3</sup> “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>>.

<sup>4</sup> 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).

<sup>5</sup> “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>>.

<sup>6</sup> *Ibid.*

- 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):** Information that can be used directly or in combination with other information to identify a particular individual. It includes
  - i. a name, identifying number, symbol, or other identifier assigned to a person,
  - ii. any information that describes anything about a person,
  - iii. any information that indicates actions done by or to a person,
  - iv. 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 referred 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.

## II. Policy

- a. The State of Ohio and Department of Commerce provides computers, services, software, supplies, and other IT resources to employees, contractors, temporary personnel and other agents of the state to support the work of Ohio government. Personal use, where permitted under this policy, shall be strictly limited and can be restricted or revoked at the discretion of the Department of Commerce at any time. Electronic resources such as the web, electronic mail, web mail, social media (if authorized), and instant messaging (IM) are provided to enhance the productivity of employees and improve customer responsiveness.
- b. 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.
- c. 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.
- d. 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:
  - i. Violation of Law: Violating or supporting and encouraging the violation of local, state or federal law.
  - ii. Illegal Copying: Downloading, duplicating, disseminating, printing or otherwise using copyrighted materials, such as software, texts, music, and graphics, in violation of copyright laws.
  - iii. Operating a Business: Operating a business, directly or indirectly, for personal gain.
  - iv. 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.
  - v. Accessing Sexually Explicit Material: Downloading, displaying, transmitting, duplicating, storing, or printing sexually explicit material.
  - vi. Harassment: Downloading, displaying, transmitting, duplicating, storing or printing material that is offensive, obscene, threatening, or harassing.
  - vii. Gambling or Wagering: Organizing, wagering on, participating in, or observing any type of gambling event or activity.
  - viii. 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.
  - ix. Solicitation: Except for efforts approved by the Director of the Department of Commerce, soliciting for money or support on behalf of charities, religious entities, or political causes.

- e. 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 Department of Commerce. If an individual is approved to participate in any of these forms of communication as part of state business, that person shall approved by the Chief Information Officer before participating.
- f. Only state approved cloud file sharing solutions 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:
  - i. Only data related to state business shall be stored in state approved cloud file sharing solutions.
  - ii. Sensitive data shall only be stored in Microsoft OneDrive for Business or SharePoint Online if approved by the Chief Information Officer. If approved, employees shall comply with the requirements outlined in Ohio Administrative Policy IT-14, "Data Encryption and Securing Sensitive Data."
    - 1. Sensitive state data shall not be downloaded from cloud file sharing solutions onto personal devices unless explicitly authorized by the user's agency.
- g. Installing or using software including, but not limited to, instant messaging clients and peer-to-peer file sharing software, or personally owned software, without approval of the Chief Information Officer is strictly prohibited. Installation and use of unlicensed software is strictly prohibited.
- h. 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 of the Chief Information Officer is strictly prohibited. Connecting or attempting to connect a wireless device to the state's wireless service without proper approval is strictly prohibited.
- i. 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.

- i. 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.
  - ii. 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.
- j. Concealing or misrepresenting one's name or affiliation to mask unauthorized, illegal, fraudulent, irresponsible, or offensive behavior in electronic communications is strictly prohibited.
- k. 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 shall not be used for personal communication in public forums such as, or similar to, listservs, discussion boards, discussion threads, comment forums, or blogs.
- l. 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.
  - i. Using IT resources to violate or attempt to circumvent confidentiality procedures is strictly prohibited.
  - ii. Accessing or disseminating sensitive data or personally identifiable information without authorization is strictly prohibited.
  - iii. Accessing networks, files or systems, emails, databases, or an account of another person without proper authorization is strictly prohibited even if one has elevated privileges. Employees, contractors, temporary personnel and other agents of the state are individually responsible for safeguarding their passwords.
  - iv. 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.
  - v. Employees, contractors, temporary personnel, and other agents of the state shall not leverage save password options.
  - vi. Distributing malicious code or circumventing malicious code security is strictly prohibited.

- m. Individuals shall protect computing devices, removable storage components and removable computer media from unauthorized access. Computing devices, computer media and removable components, such as disk drives and network cards, shall be stored in a secure environment when not in use. Devices should not be left unattended without employing adequate safeguards that would hinder unauthorized access. Safeguards shall also be taken to avoid unauthorized viewing of sensitive or confidential data, especially with portable computing devices used in public or common areas. Portable computing devices shall not be checked as baggage when traveling and they, along with associated removable computing components and computer media, must remain under visual control while traveling. If visual control cannot be maintained, then necessary safeguards should be employed to protect the physical device, storage components, removable media, and associated data. No computer hardware or software shall be removed from the premises of the Department, except with the approval from an authorized manager. Authorized managers are responsible for tracking location of equipment removed from the premises. Computers and software of the Department used off the premises shall be subject to the same limitations as set out in this Computer and IT Resource Use Policy as computers and software of the Department used on the premises of the Department.
- n. If a computing device (including personally owned devices authorized for official state use) or computing media containing departmental data is lost or stolen, employees must immediately report it to their immediate supervisor. The supervisor must follow established procedures to notify management and/or law enforcement. But, in case of a stolen device, it is preferable for an employee to first notify law enforcement to report the incident, then his or her supervisor. Employees shall follow-up with a written report which shall specify the time the computing device or media was noticed as missing, any circumstances surrounding its loss, and a description of the missing item.

### III. Penalties

- a. 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:
  - i. ORC Section 2909.04 – knowingly using a computer system, network or the Internet to disrupt or impair a government operation.
  - ii. ORC Section 2909.05 – causing serious physical harm to property that is owned, leased, or controlled by a government entity.
  - iii. ORC Section 2913.04 – accessing without authorization any computer, computer system, or computer network without consent of the owner.

- iv. ORC Section 2921.41 – using a public office to commit theft which includes fraud and unauthorized use of government computer systems.

IV. Contractual Agreements

- a. 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.

V. Compliance

- a. The Department of Commerce shall undertake measures to ensure that employees, contractors, temporary personnel, and other agents of the state adhere to agency policy.

Revision History

9/2020	Scheduled Review	
9/17/2018	Policy Update	