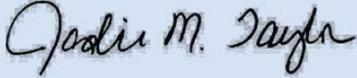


APPOINTING AUTHORITY APPROVAL:  	POLICY NUMBER: <b>IT002</b>  EFFECTIVE DATE: <b>01/10/12</b> REVIEWED: <b>04/03/13</b>
AUTHORITY: ADMINISTRATION, OHIO REVISED CODE SECTIONS 2909.04; 2909.05; 2913.04; 2921.41. STATE OF OHIO INFORMATION TECHNOLOGY POLICY ITP-E.8	APPROVAL DATE: <b>01/10/12</b> REVIEWED: <b>04/03/13</b>

**I. Purpose:**

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

**II. Policy:**

IC employees' access to the Internet shall be limited and can be further restricted or revoked at the agency's discretion at any time. Employees should only visit sites associated with official activities; in pursuit of information for official business; or those sites associated with other governmental agencies. However, the IC recognizes that it may be necessary for an employee to occasionally access the Internet while at work for personal use. The number and duration of such incidental personal uses shall be kept to a minimum. Incidental personal use is limited to an employee's lunch hour or authorized breaks whenever possible. Incidental personal use of the Internet must not result in direct costs to the agency or interfere with work performance. Employees shall be held accountable for their use of the Internet.

Employees shall have no reasonable 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 IC, under the direction of the Executive Director and the State of Ohio, 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.

**III. Applicability:**

This policy applies to all IC employees.

**IV. Definitions:**

- A. **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."

- B. 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.
- C. Confidentiality: 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.
- D. 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. Examples of instant messaging services include, but are not limited to, AOL Instant Messenger, Yahoo! Messenger and MSN Messenger.
- E. 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, not to be trusted and outside the boundary of the State of Ohio enterprise network.
- F. 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.
- G. Malicious Code: 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.
- H. 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.
- I. 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.
- J. 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, but are not limited to, eHarmony, Facebook, Friendster, LinkedIn, Match.com, MySpace, Twitter, Plaxo and Yahoo!Groups.
- K. 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.

**V. Procedures:**

Employees must take reasonable precautions when accessing the Internet to prevent breaches to the security of confidential information and the possibility of contamination to IC systems via viruses or spyware. Employees shall refrain from opening executable files downloaded from the Internet. In the event or suspicion that malicious code has been received, the employee shall report the activity to the IC IT Help Desk immediately.

**VI. Unacceptable Personal Use:**

Any use of IT resources, including incidental personal use, 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**. Use that is strictly prohibited includes, but is not limited to:

- 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. Harassment: Downloading, displaying, transmitting, duplicating, storing or printing material that is offensive, obscene, threatening, bullying or harassing.
- G. Gambling or Wagering: Organizing, wagering on, participating in or observing any type of gambling event or activity.
- H. Solicitation: Except for agency-approved efforts, soliciting for money or support on behalf of charities, religious entities or political causes.
- I. 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, blogs, wikis, peer-to-peer file sharing, and social networks, 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 complete IC approved 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.

- J. Unauthorized Installation or Use of Software: Installing or using unlicensed software or using software including, but not limited to, instant messaging clients and peer-to-peer file sharing software, unapproved web browsing software, or personally owned software, without proper IC approval.
- K. Misrepresentation: Concealing or misrepresenting one's name or affiliation to mask unauthorized, fraudulent, irresponsible or offensive behavior in electronic communications.

## **VII. Disciplinary Actions:**

Violation of this policy may result in disciplinary action under IC policy HR007 Disciplinary Guidelines up to and including removal. In addition, employees 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.