OFFICE OF BUDGET AND MANAGEMENT

COMPREHENSIVE INFORMATION TECHNOLOGY USE POLICY

Effective Date: May 12, 2008

1.1 Purpose

The purpose of this Policy is to establish controls on the use of information technology (IT) resources to ensure they are appropriately used for the purposes for which they were acquired and to set forth the parameters under which OBM employees may use such resources. At all times, OBM employees 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.

1.2 Scope

This Policy applies to every OBM employee and official. The scope of this Policy includes state computer and telecommunications systems and the employees, contractors, temporary personnel, and other agents of OBM who use and administer such systems.

1.3. Reference

a. O.R.C. § 125.18
b. Ohio Admin. Code 123: 3-1-01
c. OIT Policy ITP-B-6 (Internet Security) and OIT Policy ITP-E-8 (Use of E-mail and Other IT Resources)
d. O.R.C. §§ 2909.04 and 2909.05
e. O.R.C. § 2913.04
f. O.R.C. § 2921.41
g. OBM's Security of Sensitive Data Policy

1.4 Definitions

a. "Blog": Web-based content consisting primarily of periodic articles or essays listed with the latest entry and visitor comments at the top. Blogs 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 chat in audio and watch each other.

c. “Instant Messaging (IM)”: 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.

d. “IT Resources”: Any information technology resource, such as computer hardware and software, IT services, smart phones and personal digital assistants (PDAs), 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.

e. “Listserv”: An electronic mailing list software application that was originally developed in the 1980s and 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.

f. “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. They were predated by newsgroups and bulletin boards in the 1980s and 1990s.

g. “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.

h. “Social Networks”: Websites promoting a “circle of friends” or “virtual communities” where participants are connected based on various social familiarities such as familial bonds, hobbies or dating interests.

i. “Wiki”: A web application or software that allows one user to add content and any other user to edit the content.

1.5 Provisions

1.5.1 Unacceptable Use

IT resources are to be used primarily for state business purposes. 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. Inappropriate, offensive, and/or personal use that is strictly prohibited includes, but is not limited to, the following:

a. Excessive use or abuse of the Internet;
b. Violating or supporting and encouraging the violation of local, state or federal law;
c. Downloading, duplicating, disseminating, printing or otherwise using copyrighted materials, such as software, texts, music, and graphics, in violation of copyright laws;
d. Operating a business, directly or indirectly, for personal gain, or selling goods or services (i.e., sporting event tickets, school / club fundraising items);
e. Participation in any form of an on-line auction (e.g., eBay);
f. 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;
g. Downloading, displaying, transmitting, duplicating, storing, or printing sexually explicit material;
h. Downloading, displaying, transmitting, duplicating, storing or printing material that is offensive, obscene, threatening, or harassing;
i. Organizing, wagering on, participating in or observing any type of gambling event or activity;
j. Downloading, accessing, or playing games (i.e., solitaire, FreeCell, hearts), whether on an employee's hard drive or on the internet, on state equipment;
k. Sending unsolicited emails or facsimiles in bulk or forwarding electronic chain letters in bulk to recipients inside or outside the state environment;
l. Except for OBM-sponsored efforts, soliciting for money or support on behalf of charities, religious entities or political causes; and/or
m. 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*, *listservs*, *blogs*, *wikis*, *peer-to-peer file-sharing*, and *social networks*, unless organized or approved by the OBM Director or Chief Information Officer.

In addition, employees have the expressed obligation to assist in the protection of OBM's computer systems from malicious code "viruses." Employees should be cognizant of files with an ".exe" name extension and should exercise caution in downloading such files. In the event or suspicion that malicious code or virus has been received, the activity shall be reported to the Chief Information Officer or his/her designee.

1.5.2 Unauthorized Installation or Use of Software or Hardware

OBM's IT section provides each end-user with pre-approved software and hardware on state-approved IT resources. The installation and use of any

additional hardware or software requires authorization from the Chief Information Officer or his or her designee.

1.5.3 No Expectation of Privacy

OBM employees 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 email and instant messaging and the content thereof, are not confidential, except in certain limited cases recognized by state or federal law. OBM has the authority and right to review individual employee files, including email. In addition, OBM reserves the right to monitor and report findings to appropriate supervisors and authorities, including those who are the subject of a court order, subpoena, or other process of law.

1.5.4 Impeding Access

Impeding the state's ability to access, inspect and monitor IT resources is strictly prohibited. OBM employees shall not encrypt or conceal the contents of any file or electronic communications, unless required to do so for a legitimate business reason. OBM employees shall not, with a malicious intent to conceal information, set or manipulate a password on any state computer, program, file, or electronic communication. Concealing or misrepresenting one's name or affiliation to mask unauthorized, fraudulent, irresponsible or offensive behavior in electronic communications is strictly prohibited.

1.5.5 Restrictions on the Use of State Email Addresses

OBM employees shall avoid the appearance of impropriety and avoid the appearance of leveraging the stature of the state in the use of their assigned state email address. State email addresses, such as "firstname.lastname@ obm.state.oh.us," shall not be used for personal communications in public forums such as or similar to listservs, discussion boards, discussion threads, comment forums, or blogs.

1.5.6 Violations of Security Measures

Violations of security measures are strictly prohibited and include, but are not limited to, the following:

a. Any use of state-provided IT resources that interferes with or compromises the security or operations of any computer system, or compromises public trust;
b. Using IT resources to violate or attempt to circumvent confidentiality procedures;

c. Accessing or disseminating confidential information or information about another person without authorization;
d. Accessing networks, files or systems or an account of another person without proper authorization. OBM employees are individually responsible for safeguarding their passwords; and/or
e. Intentionally distributing malicious code or circumventing malicious code security.

1.5.7 Posting to the Intranet

OBM employees may post news and announcements directly to the Intranet. Examples of items appropriate for posting include agency publication announcements, benefits-related information and deadlines, OBM/state sanctioned events, project due dates, birth announcements, baby showers, farewell parties, and new employee information. All information posted to the Intranet shall comply with the requirements of this Policy.

1.5.8 Personally and Contractor Owned Computing Devices

All contractor-owned computing devices must receive prior written authorization from OBM's Chief Information Officer before deploying any device to and/or connecting with OBM's network. No OBM employee or official shall use a personal computing device, laptop computer, smart phone, or personal digital assistant (PDA) that is connected to an OBM computer or network, unless an exception has been granted by the Chief Information Officer. In such cases where an exception has been granted, the device shall comply with all state policies in regard to computer systems, including being subject to audit and review. OBM shall have no responsibility with respect to the maintenance or operation of a non-state owned computing device or the data stored thereon, even if the device or data is used in support of official state business or while acting as an agent of the state. OBM hereby expressly disclaims any agency liability for the safeguarding of personally owned computer devices or data, including protecting personal data from corruption.

1.5.9 Personnel With Computer System Administrative Rights

Employees or contractors designated with administrative access rights shall not abuse administrative rights or privileges associated with computer systems. Abuse of administrative rights or privileges includes, but is not limited to, the following activity:

a. Using system administrative rights to access or read e-mail associated with any user's e-mail account other than his or her own, without that user's permission or the prior written consent from the Chief Information Officer and the Human Resources;

b. Copying or transferring databases and files, including e-mail databases, e-mail accounts, or e-mail files, in preparation for unauthorized access to data and communications by anyone;
c. Providing administrative rights or privileges to another person for the purpose of obtaining unauthorized access to data files and communications, including e-mail;
d. Using administrative rights or privileges to change or disable any security, access control list, active directories, logging, or tracking function within the computer system in order to hide unauthorized access to files and communications, including e-mail.

1.5.10 Intentional System Damage and Degradation

OBM employees shall not deliberately attempt to damage or degrade computer and computer system performance or capability. Those OBM employees with special knowledge of purported "weaknesses" in computer systems, special passwords, or other information shall not use such knowledge to damage a system or file or to change or remove information in a system or file without prior authorization, including making such personal knowledge available to others for such purposes.

1.6 Penalties

Violation of this policy may result in disciplinary action, up to and including removal and/or termination of an applicable independent contractor or consultant agreement. In addition, employees, contractors, temporary personnel, and other agents of OBM who use and administer state computer and telecommunications systems may be subject to a civil action or criminal prosecution as a result of inappropriate use or misuse of IT resources.

1.7 Contact

The Chief Information Officer is available for questions or consultation regarding the provisions of this Policy.

1.8 Revision History

Date	**Description of Change**
3/16/1999	Initial Policy Issued
2/18/2003	Revisions to Policy Issued
5/12/2008	Revisions to Policy Issued