



POLICY
Ohio Department of Taxation

Policy Description:
Use of Internet, Email, and
Other IT Resources Policy

Policy No: ODT – IT – 001

Authorities:

Ohio IT Policy ITP – E.8

ODT – HR - 011

ODT – HR – 015

IRS Publication 1075

Divisions With Primary Responsibility:

Information Services & Internal Audit Divisions

Pages: 9 Pages

Effective Date: Oct. 1, 2010

Supersedes: June 30, 1999
May 1, 2006
July 15, 2008

1.0 PURPOSE

The purpose of this policy is to inform all Ohio Department of Taxation (ODT) employees and consultants (hereafter referred to as personnel) of their responsibilities and roles with regard to the usage of electronic mail (email), the Internet, and other “IT Resources” accessed through state-owned equipment or on personal equipment while acting in an official capacity or on behalf of ODT interests.

2.0 DEFINITIONS

2.1 Email is defined as written or typed messages, such as memos or letters, sent and/or received by communication links from person to person. Email often consists of the primary text of the message and any attachments, such as word processing files, spreadsheet files, documents, and graphics.

2.2 The Internet is defined as the publicly available worldwide system of interconnected computer networks that transmit data by packet switching using a standardized Internet Protocol (IP) and many other protocols. It is made up of thousands of smaller commercial, academic, and government networks. It carries various information and services, such as email, online chat and the interlinked web pages and other documents of the World Wide Web. The Internet provides for file transfers, downloading of information, remote log in, news, and many other services, as well as a variety of reference resources.

2.3 IT Resources are defined as all desktop computers, laptop computers, peripherals, and network equipment owned, leased, and/or supplied by the State of Ohio, as well as all computer services provided by ODT, including Internet access, email, and other similar services. All state-

owned computer software, licenses, and supplies are also included as IT Resources.

2.4 Sensitive Information is defined as any information a state agency maintains that can not be disclosed under penalty of law. For ODT this includes, but is not limited to:

- specific taxpayer information, whether related to businesses or individuals
- any Federal Tax Information (including SSNs and FEINs)
- any IT infrastructure or security related documentation that contains specific configuration settings, IP addresses, or other information that may be used to gain an advantage in compromising the integrity of our information systems, or physical security controls

3.0 AUTHORIZED ACTIVITIES

3.1 The Internet and email are business communication tools. Users are obliged to use these tools in a responsible, effective and lawful manner. Although by their nature email and/or “IT Resources” seem to be less formal than other written communication, the same laws apply.

3.2 While Internet, email, and online systems are primarily for business purposes, occasional and incidental personal use shall be permitted if it does not interfere with the work of personnel or affect the Department’s ability to perform its mission. Additionally, all usage must meet the conditions outlined in this policy and other Department policies, directives, and/or procedures. *Personal use shall be primarily conducted during authorized break periods e.g. breaks and/or lunches. As the computer is state property, its usage may be limited and can be restricted or revoked at the Department’s discretion at any time. Additionally, personal use of any IT Resource containing taxpayer information is strictly prohibited. This includes but is not limited to ITAS, IMOD, STARS and outside systems such as Lexis-Nexis.*

3.2.1 Authorized downloads. File types that are generally considered acceptable for use in a business environment include:

- Documents such as PDF files, spreadsheets, and white papers
- Business-related multi-media files such as clip art, pod casts, and training videos

3.3 All ODT IT Resources, including email and Internet systems, are the property of the state of Ohio. Email and Internet access shall be used primarily for state business or to advance ODT’s best interests.

3.4 All personnel who have been assigned an ODT email address are required to use this email account for all ODT related email communications.

4.0 UNAUTHORIZED ACTIVITIES

- 4.1 IT Resources are not to be used in a way that may be disruptive, offensive to others, or harmful to morale. IT Resources, including the state email system, shall not be used to solicit others for commercial ventures, religious or political causes, outside organizations, social events or other non-job-related solicitations. IT Resources shall not be used for operating a business for personal gain, sending chain letters, forwarding “free prize offers”, or expressing viewpoints on behalf of charities, religious entities or political causes. This includes the dissemination of various personal memos through the state’s email system. *(An exception to Section 4.1 would include events sponsored by the Department such as the Combined Charities Campaign.)*
- 4.2 IT Resources are not to be used for display, transmission, or downloading of sexually explicit images (pornography), messages, cartoons, or any communication that contains ethnic slurs, racial epithets, or anything that may be construed as harassment or disparagement of others based on their race, national origin, sex, sexual orientation, age, disability, religion, or political beliefs.
- 4.3 Downloading, duplicating, disseminating, printing or otherwise using copyrighted materials, such as software, texts, music and graphics, in violation of copyright laws is strictly prohibited. All software must be properly licensed and approved by ISD before installation. For further information refer to ODT Software Policy.
- 4.3.1 Unauthorized downloads.** Licensed or unlicensed software that requires an installation process for use may not be downloaded. This includes trial software. Submit a Customer Service Request (CSR) to obtain authorization for this type of software installation. File types that are generally considered not acceptable for use in a business environment include:
- Games
 - Peer-to-peer downloads
 - Programs for online gambling
 - Music or ring tones for personal use
 - Video movies and/or trailers not business-related
- 4.4 Computer viruses are more and more prevalent in today's world. They can cause considerable damage to a computer or entire network. An infected computer may not be readily identified, even though damage may be occurring. The utmost care must be taken in adhering to strict anti-virus precautions. These include:

- 4.4.1 Use caution when exchanging electronic files among computers. Do not attempt to copy files that are identified as containing viruses or other malicious code.
 - 4.4.2 It has been estimated that industry-wide nearly 1/3 of virus infections are introduced through email attachments. In ODT's environment, this statistic is approximately 99%. Therefore, caution must be used when opening email attachments from both known and unknown sources.
 - 4.4.4 Screen savers and desktop wallpapers often contain viruses and are discouraged from being used except those loaded as original software.
 - 4.4.5 When using a Web browser, never open plain text documents with the browser since malicious hidden commands could easily be embedded in the document that might threaten the security of your workstation or network. Instead, simply save the plain text documents that you need to read and then view them using a plain text editor such as Notepad.
- 4.5 ODT and the current software provider have developed procedures for categorizing various sites and ODT will maintain a list of these categories. Various Internet websites have been blocked as not appropriate for viewing on state IT Resources. The blocking or unblocking of these sites may change depending upon various factors including legitimate business needs. If, for a business reason, access is necessary to a site that is normally restricted, submit a System Security Request to obtain authorization to the site. As access to these sites may be time sensitive, requests will be expedited to minimize any down time(s).
- 4.6 In some instances, a user may be cautioned before being able to access a site. By completing the action requested by the screen, the user is able to access all sites within that category for approximately 15 minutes. After that time, the caution message will again ask the user if they wish to continue accessing these sites.
- 4.7 Unless organized or approved by ODT, any use of IT Resources to operate, participate in, and/or contribute to an external non-business related 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. Wikipedia, a popular on-line encyclopedia, has been made available for viewing but must not be used for modifying or contributing information using IT Resources.
- 4.8 In an effort to avoid the appearance of impropriety, **personal** email messages may not contain an ODT signature block indicating an individual's position within ODT or business contact information, such as the office address and/or office phone number. State email addresses, such as firstname_lastname @tax.state.oh.us or @ohio.gov, shall not be used for communications in public forums such as or similar to listservs,

discussion boards, discussion threads, comment forums, editorials, or blogs.

- 4.9** It is everyone's responsibility to notify ODT management of improper or undesirable use of the email and Internet systems.
- 4.10** Internal email messages **MUST NOT** be automatically forwarded to or through other email systems outside of ODT. All email bound for an external email address must be scrutinized to determine whether sensitive information is included in the email message, attachments, or email string. All sensitive information must be redacted and/or removed, or the secure email system must be utilized.
- 4.11** The concealment or misrepresentation of one's name or affiliation to mask unauthorized, fraudulent, irresponsible, or offensive behavior in electronic communications is strictly prohibited.
- 4.12** Users shall not set or manipulate a password on any ODT computer without prior authorization. Note: Users are authorized to set passwords associated with their assigned user IDs. System administrators are authorized to set passwords associated with the systems they are assigned to administer/manage/maintain. Users can password protect business related files in order to prevent unauthorized view or updates, as appropriate.
- 4.13** ODT computers automatically lock after 15 minutes of inactivity. In addition, users are required to manually lock their computer when they step away from their work areas.
- 4.14** Users are required to log off of ODT's network at the end of their business day. Computers should be left signed on through the encryption screen overnight (laptops must be secured with a locking cable when left in this state). This requirement is intended to ensure scheduled maintenance activities can be completed while minimizing disruptions during your work day.

5.0 AUDITING AND CENSORING

- 5.1** The Internal Audit Division will monitor and investigate Internet, email or other IT Resources usage without prior notification. The Internal Audit Division and/or the Information Services Security Unit shall monitor and investigate suspected abuse of this policy.
- 5.2** Monitoring and investigating of Internet, email or any other IT Resources usage will be done on a regular basis without regard to position. Monitoring tools are in place that will identify policy compliance.

- 5.3 One should not leave Internet sites open for extended periods when multi tasking. Leaving sites open for extended periods of inactivity may improperly reflect as periods of usage.
- 5.4 Abuse or evidence that an employee is not adhering to the guidelines set in this policy may result in the loss of Internet privileges and/or may subject the employee to progressive discipline up to and including termination and/or legal action. Abuse or evidence that a consultant is not adhering to guidelines established by this policy may result in removal from and/or end of the contractual engagement.
- 5.5 The Department of Taxation reserves the right to block selected Internet sites as well as monitor email content for inappropriate verbiage and use. If necessary, the Department may intercept the delivery of inappropriate email messages.
- 5.6 While attempts are made to block unwanted email, ODT cannot be liable for failure to block messages bearing offensive or harassing content received over the Internet.
- 5.7 Usage of IT Resources is subject to limitations imposed by supervisors to prevent excessive or improper use.

6.0 CONFIDENTIALITY AND PRIVACY

- 6.1 Personnel are reminded to use judgment on the type of information sent through email. Personnel should be aware that messages may be forwarded to others by the recipient, printed in a location seen by others, or directed to the wrong recipient. If a communication is determined to be private, use of interoffice mail marking the item “confidential” is a more appropriate vehicle for transmission.
- 6.2 As described in IRS Publication 1075, federal law prohibits the transmission of Federal Tax Information (FTI) via any method which is not encrypted or not secured. When it is necessary to transmit FTI, always use the ODT secure mail system.
- 6.3 Use of the Internet and email systems is not confidential. Websites visited leave traceable “footprints”. Additionally, emails may be forwarded to others and changed without knowledge of the sender. Internet, email or “IT Resources” users expressly waive any right of privacy in anything they create, store, send or receive on ODT’s computer system(s).
- 6.4 Employees shall not provide access to or otherwise disclose confidential records and information using Internet, email or other IT Resources. Ohio law specifically prohibits the disclosure of confidential information to any person who is not an employee of ODT. (ORC 5703.21) Special caution must be exercised to offer information only to a trusted source such as the taxpayer or their representative following the proper completion of a

Taxpayer Bill of Rights form. For more information with regard to confidentiality and disclosure, please refer to Policy ODT-HR-005. For specific information with regard to releasing information through email contacts, please refer to the on-line Disclosure Training on TAXI.

- 6.5** ODT reserves the right to inspect any computer either owned by ODT; brought into any ODT facility; or remotely connected to any ODT internal network. There shall be no expectation of privacy as ODT may monitor all computer usage including emails received and/or sent as well as Internet access using IT Resources. The Department reserves the right to view any files and electronic communications on IT Resources, monitor and log any electronic activities, and report the findings to appropriate ODT personnel and outside authorities. Efforts to impede this ability through unauthorized encryption or concealment are strictly prohibited. **Note:** Using ODT supplied encryption methods (e.g., hard disk encryption, PDA/smart phone encryption, secure mail, USB device encryption, etc.) is considered to be an authorized activity.

7.0 PUBLIC RECORDS AND RETENTION

- 7.1** IT Resources use various methods of transmitting data or information. The method of transmission does not change the criteria when considering if such information is a public record. Therefore, the content, transactional information, and any attachments associated with the email or IT Resources are considered a record if such information meets the criteria of the Ohio's public record's law, Ohio Revised Code section 149.011 (G).
- 7.2** Retention rules are similar whether the document exists in paper form or as an electronic image. Refer to Budget's Policy ODT-BUD-005 with regard to destruction and/or retention of all documents regardless of its form.

8.0 SYSTEMS SECURITY MEASURES.

- 8.1** Any use of Department or state provided IT Resources that interferes with or compromises the security or operations of any computer system, or compromises public trust, is strictly prohibited.
- 8.1.1 Confidentiality Procedures.**
Using IT Resources to violate or attempt to circumvent confidentiality procedures is strictly prohibited.
- 8.1.2 Accessing or Disseminating Confidential Information.**
Accessing or disseminating confidential information or information about another person through IT Resources without authorization is strictly prohibited.
- 8.1.3 Accessing Systems without Authorization.**

Accessing networks, files or systems or an account of another person without proper authorization is strictly prohibited. Public servants are individually responsible for safeguarding their passwords in accordance with Ohio IT Policy ITPB.3, “Password and PIN Security.”

8.1.4 Distributing Malicious Code.

Distributing malicious code or circumventing malicious code security is strictly prohibited. Ohio IT Policy ITPB.4, “Malicious Code Security,” outlines requirements for protecting IT Resources against threats from malicious code.

8.2 Secure Mail

Sending email outside of ODT is equivalent to sending a post card. Someone may view or intercept the message during transmission. ODT offers secure messaging, which should be used whenever there is a need to email sensitive data or FTI to someone outside of ODT. For more information and procedures please refer to the Secure Mail End User Training Guide on TAXI.

8.3 Personal Email Management (PEM/End User Spam Management)

ODT offers a spam management tool to help you manage incoming email. To receive notifications of incoming email trapped by the system, complete the on-line Spam Management Training course in TrAX.

9.0 LEGISLATIVE REQUIREMENTS

9.1 State of Ohio Requirements

Violation of this policy may result in disciplinary action or contractual penalties, and may be cause for 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 1347.12 - requires ODT to notify individuals if their personal information is accessed by an unauthorized person.
- 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.

9.2 Federal Requirements

Additionally, there are penalties for violating federal laws with regard to improper accessing and/or disclosure of FTI.

- Internal Revenue Code (IRC) Section 6103 is a confidentiality statute and generally prohibits the disclosure of FTI.
- IRS Publication 1075 offers security guidelines with regard to FTI for Federal, State, and Local Agencies
- IRC Section 7213 discusses unauthorized disclosure of FTI and penalties associated with such disclosure. IRC Sec.7213 (b) states, “any violation of disclosure shall be punishable upon conviction by a fine in any amount not exceeding \$1000, or imprisonment of not more than 1 year, or both, together with the costs of prosecution.”

10.0 REVISION HISTORY

Effective Date	Description
06/30/1999	99-01 Initial Internet, Electronic Mail and Online Services Further defined Directive #15 and provided guidance for use and potential abuse
05/01/2006	<ol style="list-style-type: none"> 1. Combined policies 99-01,99-02, 99-03 2. Further defined authorized and unauthorized activities 3. Listed blocked categories 4. Detailed confidentiality and penalties for violations
07/15/2008	<ol style="list-style-type: none"> 1. Described personal usage times 2. Removed description of categories blocked 3. Added information about public records and retention
10/01/2010	<p>Language to clarify various points throughout the policy</p> <ol style="list-style-type: none"> 1. Sensitive information section added 2. FTI prohibitions 3. IRS requirements for disclosure and/or accessing FTI