



Ohio

Department of  
Taxation

POLICY

John Kasich, Governor  
Joseph Testa, Tax Commissioner

30 E. Broad St., 22nd Floor  
Columbus, Ohio 43215

(614) 466-2166  
Fax (614) 466-6401

Policy: Use of Internet, Email, and Other IT Resources	Number: ODT-300	Effective: January 22, 2013
Issued By: Joseph Testa (Original signature on file with Internal Audit)	Published By: Information Services & Internal Audit Divisions	Four Year Review Date: January 22, 2017

### 1. Authority

The Tax Commissioner hereby issues Ohio Department of Taxation (herein referred to as the "Department") Policy ODT-300 in accordance with Ohio Revised Code (O.R.C.) § 5703.05. O.R.C. § 5703.05 grants the Tax Commissioner powers, functions, and duties including the authority to manage and direct all operations of the Ohio Department of Taxation.

### 2. Purpose

The purpose of this policy is to establish for all Department employees, contractors, or other agents (hereafter referred to as "personnel") responsibilities and roles regarding the use of the Internet, electronic mail (email) accounts, other IT resources, and the proper retention and timely destruction of email.

### 3. Applicability

This policy applies to all personnel who use or administer Internet, email or other IT resource systems of the Department.

### 4. Definitions

- 4.1. **Email** – 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.
- 4.2. **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 public, untrustworthy, and outside the boundaries of the state's enterprise network.
- 4.3. **IT resources** – Any information technology resource, such as computer hardware and software, IT services, network equipment and services, digital devices such as digital copiers and facsimile machines, supplies and the Internet, made available to personnel.
- 4.4. **Malicious Code/Malware** – 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 logic bombs, Trojan horses, viruses, and worms.
- 4.5. **Sensitive information** – Any Department information that is:

- Confidential Personal Information (CPI)
- Federal Tax Information (FTI)
- Payment Card Industry (PCI) Data
- Taxpayer Information

## 5. Policy

The Department provides networks, email systems, and IT resources to support the official duties of the Tax Commissioner and his/her employees. Use of these resources in a manner that violates this policy is strictly prohibited. License to use any of these resources may be restricted or revoked at the discretion of the Tax Commissioner or his/her designee.

### 5.1. Authorized uses

The Department's networks, email, and IT resources are to be used exclusively for official state purposes except as authorized. The following subsections are a list of examples of authorized uses of Departmental networks, email, and IT resources.

- 5.1.1. **Collective bargaining purposes.** When an applicable collective bargaining agreement permits union stewards or officers to use email or facsimile equipment or other expressly enumerated IT resource for contract enforcement, interpretation, or grievance processing matters. Such uses are limited and controlled by the terms of the applicable collective bargaining agreement.
- 5.1.2. **Limited personal use of the Department's Internet connection.** The Department permits limited personal use of the Internet during authorized breaks or lunches. The use is controlled by monitoring software prohibiting the accessing of unauthorized websites and prohibitions set forth in this policy.
- 5.1.3. **Use of Department's email.** Personnel (notably contractors and other temporary personnel) who have been assigned a Department email address are required to use this address for all Department related email communications.

### 5.2. Prohibited uses of the Department's networks, email, and IT resources

Any personal use that disrupts or interferes with governmental operations is prohibited (e.g., use that may be injurious to the state or that may have the appearance of impropriety).

The following subsections are a list of illustrative examples of prohibited uses of Departmental networks, email, and IT resources.

- 5.2.1. **Copyright violations.** Copying, downloading, duplicating, disseminating, printing or otherwise using intellectual property (e.g., software, texts, music, books, graphics) in violation of copyright laws.
- 5.2.2. **Federal Tax Information (FTI) misuse.** Accessing, downloading, displaying, transmitting, disseminating, duplicating, storing or printing FTI in any manner that is not expressly authorized by this policy or by I.R.C. § § 6103 and 7213.
- 5.2.3. **Gambling.** Any use in furtherance of organizing, wagering on, participating in or observing any type of gambling event or activity.
- 5.2.4. **Illegal uses.** Any use in any manner that violates local, state, or federal law. Applicable laws include but are not limited to I.R.C. § § 6103, 7213, 7213A, or 7431; 18 U.S.C. §

1905; O.R.C. § § 1347.12, 2909.04, 2909.05, 2913.04 or 5703.21; Ohio Administrative Code § 5703-31; Departmental policy on CPI.

- 5.2.5. **Impeding access.** Impeding the state's ability to access, inspect and monitor IT resources is strictly prohibited. Personnel must not encrypt or conceal the contents of any file or electronic communication on state computers without proper authorization. Personnel must not set or manipulate a password on any state computer, program, file or electronic communication without proper authorization.
- 5.2.6. **Inappropriate, sexually explicit or offensive content.** Accessing personals services (e.g., accessing or participating in any type of personals ads or services, dating services, matchmaking services, companion finding services, pen pal services, escort services, or personal ads); accessing, downloading, displaying, transmitting, disseminating, duplicating, storing or printing materials that are inappropriate, sexually explicit, lewd, obscene, threatening, discriminatory, or harassing.
- 5.2.7. **Distributing malicious code.** Distributing malicious code, such as malware or viruses, or circumventing security is strictly prohibited.
- 5.2.8. **Mass emailing.** Any use that transmits, disseminates, or duplicates unsolicited non-business related emails in bulk or facsimile transmissions in bulk or forwarding electronic chain letters in bulk to recipients inside or outside of the state networking environment.
- 5.2.9. **Misrepresentation.** Concealing or misrepresenting one's name or affiliation to mask unauthorized, fraudulent, irresponsible or offensive behavior in electronic communications is strictly prohibited.
- 5.2.10. **Misuse of third party databases.** Using a third party database including but not limited to LexisNexis, Westlaw, Hoovers, LEADS, and Accurint for any purpose outside the scope of employment or the Department's contract with such third party providers.
- 5.2.11. **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, and social networks, is strictly prohibited unless organized or approved by the Department. If an individual is approved to participate in any of these forms of communication as part of state business, that person must fulfill Department-defined security education and awareness requirements for proper use before participating. The content of the education and awareness requirements must include methods to avoid inadvertent disclosure of sensitive information and practices to avoid.
- 5.2.12. **Personal gain.** Any use to operate a business for personal gain or in furtherance of outside employment or contracts.
- 5.2.13. **Solicitation.** Any activity conducted for the purpose of advertising, promoting, or selling any product or service, or encouraging membership in any group, association or organization except when approved by the Tax Commissioner or his/her designee.
- 5.2.14. **Unauthorized installation or use of hardware.** Attempting to install, attach, or connect any kind of device to any state-provided IT resource, including computers and network services, without prior authorization is strictly prohibited.
- 5.2.15. **Violating system security controls.** The following actions are strictly prohibited: any use of state-provided IT resources that interferes with or compromises the security or operations of any computer system, or compromises public trust; using IT resources to violate or attempt to circumvent confidentiality procedures; accessing or disseminating

confidential information or information about another person without authorization; accessing networks, files or systems or an account of another person without proper authorization.

- 5.3. **No expectation of privacy.** Personnel have no expectation of privacy while using Departmental email or IT resources (e.g., telecommunications devices, computers, laptops, computer systems, state email and email accounts, jump drives, telecommunications devices, Internet usage), regardless of security devices (e.g., locks, passwords) provided by the state to protect or secure the property, or while using any private email or IT resources as part of the workplace environment or to assist in the performance of official duties. The Department has access abilities notwithstanding devices that protect or secure state property, and the Department routinely inspects and monitors state property through control activities (e.g., state email and Internet usage monitoring).
- 5.4. **Searches and seizures.** The Department reserves the right at any time to search and seize state property and to search personal property as part of the workplace environment or when it is used to assist with official duties.

#### 5.5. Email

- 5.5.1. Department email addresses, such as name@tax.state.oh.us or @ohio.gov, must not be used for communications in public forums such as or similar to listservs, discussion boards, discussion threads, comment forums, editorials, or blogs without prior authorization from the Tax Commissioner or designee.
- 5.5.2. Email messages must not be automatically forwarded to or through other email systems outside of the Department. 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.

#### 5.6. Prevention of fraud, abuse, waste, and theft involving Departmental networks, email, and IT resources

- 5.6.1. The Tax Commissioner has authorized the Internal Auditor or his/her designee to monitor and investigate usage and suspected abuse of this policy's provisions.
- 5.6.2. The Department reserves the right to monitor email content for inappropriate verbiage and use. The Department may intercept the delivery of inappropriate email messages.
- 5.6.3. While attempts are made to block unwanted email, the Department cannot be liable for failure to block messages bearing offensive or harassing content received over the Internet.
- 5.6.4. PCI data is NOT permitted to be sent via the email system. CPI is permitted to be sent using the secure mail system. FTI is permitted to be sent via the email system only in accordance with section 5.6.6 of this policy.
- 5.6.5. Personnel must not provide access to or otherwise disclose information using the email system in a prohibited manner. Ohio law specifically prohibits the disclosure of taxpayer information to any person who is not an employee of the Department (O.R.C. § 5703.21). Further, federal law specifically prohibits the unauthorized disclosure of FTI by personnel (I.R.C. § § 6103 and 7213). 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 (TBOR-1) form. For more information with regard to confidentiality and disclosure, please refer to Department policy on Taxpayer

Confidentiality. For specific information with regard to releasing information through email contacts, please refer to the online Disclosure Training on TAXI.

#### 5.6.6. **Sending FTI via email**

5.6.6.1. Other than in the manner outlined in sections 5.6.6.2 of this policy, all use of email for sending FTI is prohibited.

5.6.6.2. Generally, all email containing FTI sent via the email system must only be sent to recipients within the Department. FTI may be emailed to recipients within the Department in accordance with the following procedure: **Procedure on Emailing FTI to Internal Recipients**. Emailing FTI to external recipients is only permitted in limited circumstances in accordance with the following procedure: **Procedure on Emailing FTI to External Recipients**.

#### 5.6.7. **Email retention**

The content, transactional information, and any attachments associated with email and electronic records may be considered public records under O.R.C. § 149.011 (G). All email records must be retained and destroyed in accordance with the Department email retention guidelines outlined in the following procedure: **Procedure on the Retention of Emails**.

#### 5.7. **Collaborative Computing Tools**

Employees are prohibited from sharing FTI via the use of collaborative computing tools including but not limited to: GoToMeeting, Microsoft Live Meeting, WebEx, etc. This restriction specifically extends to the use of desktop sharing.

### 6. **Administrative consequences for violations**

In addition to potential civil or criminal sanctions for violating laws pertaining to misuse of Departmental networks, email, or other IT resources, a violation of this policy may result in disciplinary or other action.

- 6.1. Employees may be subject to progressive discipline up to and including termination and/or legal action.
- 6.2. The contractual arrangement with outside consultants, contractors, and/or vendors may be modified or terminated.