



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: General Data Security | Number: ODT-301 | Effective: September 1, 2013 |
| Issued By: Joseph Testa (Original signature on file with Internal Audit) | Published By: Information Services Division | Four Year Review Date: September 1, 2017 |

1. Authority

The Tax Commissioner issues Ohio Department of Taxation (herein referred to as the "Department") Policy ODT-301 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 the Department's operations.

2. Purpose

The purpose of this policy is to establish awareness of Department security policies and convey the importance of compliance.

3. Applicability

This policy applies to all Department employees and contractors.

4. Definitions

- 4.1. **Confidential Personal Information (CPI).** Personal information that is not a public record for purposes of O.R.C. § 149.43.
- 4.2. **Federal Tax Information (FTI).** Federal tax returns or return information received from the Internal Revenue Service (IRS).
- 4.3. **Payment Card Industry (PCI) Information.** Credit card or debit card information.
- 4.4. **Taxpayer Information.** Information that includes state tax returns or return information, regardless of the source of the information
- 4.5. **Sensitive Information.** Information that is:
 - Confidential Personal Information (CPI)
 - Federal Tax Information (FTI)
 - Payment Card Industry Information (PCI) Data
 - Taxpayer Information

5. Policy

All Department employees and contractors are responsible for protecting taxpayer information from unauthorized access, modification, duplication, destruction, or disclosure—whether accidental or intentional.

Taxpayer information may consist of CPI, FTI, PCI, and/or taxpayer information that is provided to the Department directly by a taxpayer, business or other government entity.

All employees and contractors are responsible for ensuring they adhere to security policies. They are also responsible for reporting any security violations to their supervisor, Internal Audit, or the ISD Security Unit.

Periodic and random reviews may be conducted to ensure ongoing compliance with information protection policies.

5.1. Restrictions on FTI and PCI Data

- 5.1.1. FTI can only be accessed, stored, or processed on state owned devices. FTI shall not be sent via end-user messaging technologies, (e.g., GoToMeeting, GoToMyPC, WebEx, internet chat sessions, etc.).
- 5.1.2. PCI information shall not be retained or stored on Department systems or non-state owned computing devices. Unprotected credit card information shall not be sent via end-user messaging technologies, (e.g., email, internet chat sessions, etc.).
- 5.1.3. Any other sensitive information must not be accessed or stored on any non-state owned computing device. All state-owned equipment used to access sensitive information remotely will be equipped with encryption and/or password protection. Any exceptions must be pre-approved by Department Executive Management.

5.2. Duty to Report

If Department confidential or sensitive information is lost, stolen, or compromised, employees and contractors must immediately report this loss to their immediate supervisor. The immediate supervisor must notify their division administrator who in turn, will notify the IT Security Manager and a decision will be made whether all affected parties must be notified in compliance with O.R.C. §1347.12.

6. Administrative Consequences for Violations

Employees and contractors may be held civilly or criminally liable for violating laws related to misuse or mishandling of CPI or FTI. Employees or contractors may also be subject to disciplinary action, up to and including termination or contract termination, for failure to follow this and other policies related to Departmental networks, email or other IT resources.