



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

Table with 3 columns: Policy details, Number, Effective date, Issued By, Published By, and Four Year Review Date.

1. Authority

The Tax Commissioner issues Ohio Department of Taxation (herein referred to as the "Department") Policy ODT-302 in accordance with Ohio Revised Code (O.R.C.) § 5703.05.

2. Purpose

The purpose of this policy is to preserve the integrity of all assigned IT assets by establishing roles and responsibilities.

3. Applicability

This policy applies to all Departmental employees and contractors.

4. Definitions

- 4.1. Caretaker - An individual who oversees shared IT assets...
4.2. CPI - Personal information that is not a public record...
4.3. Custodian - An individual who is issued a Department IT asset.
4.4. Delegated Custodian - A supervisor who assumes the role of the IT custodian...
4.5. Federal Tax Information - Federal tax returns or return information...
4.6. IT Asset - All desktop computers, laptop computers, servers...
4.7. Loaned Asset Tracking Sheet - Standard form used by caretakers...
4.8. Long Term Absence - An absence greater than 30 calendar days.

- 4.9. **Patch** – Any update, update rollup, service pack, feature pack, critical update, security update, or hotfix that is used to improve or to fix a software product.
- 4.10. **Sensitive Information** – Any information a state agency maintains that cannot be disclosed under penalty of law. For the Department 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 Department information systems or physical security controls
- 4.11. **Shared Desktop** – Workstations that are readily available in various work locations for temporary use by employees away from their primary work area.
- 4.12. **Standard Workstation** – A desktop computer and/or laptop computer, along with associated hardware such as monitor, keyboard, mouse and speakers. A standard workstation does not include a desktop printer.

5. Policy

The Department provides IT assets to support the official duties of the Tax Commissioner and Department employees. It is necessary to maintain accurate records to ensure that IT assets are properly accounted for and tracked.

5.1. Policies of the Ohio Department of Administrative Services (DAS) with applicability to Asset Management

5.1.1. DAS Policies on Asset Management

Employees must comply with DAS policies on asset management. Employees may obtain a copy of these policies from human resources or DAS's website by opening the following hyperlink: [DAS > Policies](#)

5.1.2. Statewide Information Technology (IT) Standards

Employees must comply with State of Ohio IT policies on asset management. Employees may obtain a copy of these policies from human resources or DAS's website by opening the following hyperlink: [DAS > Information Technology > State of Ohio IT Policies](#).

5.2. IT Asset Ownership Responsibilities

This section provides a description of the three key IT asset ownership responsibilities.

- 5.2.1. A custodian is responsible for properly securing, maintaining, and accounting for their assigned IT assets, including but not limited to:
- complying with ISD instructions for applying updates and patches to their assigned workstation(s)
 - delegating ownership during a long-term absence
 - logging off the Department's network at the end of the business day
 - following instructions provided in software and patch deployment notifications
- 5.2.2. A delegated custodian is responsible for assuming the IT custodian's responsibilities as detailed above for employees that are scheduled for a long term absence and establishing an encryption user ID and password on the delegated asset. The delegated custodian should contact the Service Desk if assistance is needed.

- 5.2.3. A caretaker is responsible for:
- assuming the responsibilities of an custodian as detailed above
 - ensuring shared assets are available for temporary use
 - maintaining the loaned IT asset tracking sheet

5.3. IT Asset Request, Returns and Relocations

This section outlines the procedures for initiating IT asset related service requests for transfers, moves, adds, separations, and changes.

- 5.3.1. **IT Asset Requests** – Employees and contractors requesting an IT asset must submit a service request to ISD.
- 5.3.2. **IT Asset Relocations** – Employees and contractors requesting an IT asset relocation request must submit a service request to ISD. The relocation of IT assets may only be performed by ISD employees. Satellite office relocations will be coordinated through an ISD liaison.
- 5.3.3. **IT Asset Returns** – If ISD, the custodian, or their supervisor determines that an IT asset is no longer used or needed, a service request can be submitted to return the asset to ISD or the end user can contact the Service Desk.
- 5.3.4. **Separation of Service** – Upon separation of service, a custodian's IT assets must be returned to ISD. ISD will generate the request to pick up IT assets once notified by Human Resources that a separation from service has occurred.
- 5.3.5. **Ownership Transfer** – All IT asset ownership transfers must be initiated through an ISD service request.
- 5.3.6. **Staff Transfers** – All employee transfers will require the employee to receive a new workstation. The employee's previous supervisor must submit a service request to return their former employee's IT assets. The employee's new supervisor must submit a service request for the employee's new IT assets.

5.4. Securing Laptops

All laptops must be secured using the precautions outlined below.

5.4.1. Encryption

All Department laptops are configured with full hard disk encryption and are required to be fully encrypted.

Laptops must be powered off before being transported. Locking the computer or placing it in a hibernate and/or standby status is not sufficient as this process does not allow the encryption software to activate.

Telecommuters must power off their laptops at the end of their business day unless otherwise instructed due to maintenance activities (e.g., software and patch deployments, technical troubleshooting, etc.).

5.4.2. Passwords

Written passwords must not be kept with the laptop or the key fob (SecurID token). All written passwords must be stored in a secure location (e.g., purse, wallet, etc.).

5.4.3. **Locking Computer Security Cables**

A computer security cable is issued with each Department laptop.

All unattended laptops must be properly secured. Unattended laptops must be 1) locked in a cabinet, or 2) secured to a fixed object such as a cabinet or desk using a computer security cable. This provision includes, but is not limited to 1) a department facility; 2) a telecommuter's home; 3) a taxpayer site; or 4) a public location.

5.5. **Traveling with a Laptop**

5.5.1. **Automobile Travel**

During automobile travel, the laptop must be placed in a secure location that is not visible from the car windows (e.g., trunk of car).

Laptops must not be left unattended in a vehicle overnight unless securely installed in a Department Criminal Investigations vehicle.

5.5.2. **Air Travel**

During air travel, the laptop may not be checked baggage or left with airline/airport personnel. It must be kept as close to the traveler as possible, and remain in sight of traveler whenever possible. If it becomes necessary to place the laptop in an overhead bin during travel, the traveler is responsible for regaining possession of the laptop as quickly as practical at the end of the flight.

5.5.3. **Off-site Laptop Use**

While working on a laptop off-site, employees and contractors must take proper precautions to ensure the safety of the laptop and Department data. These precautions include: 1) be aware of people lurking about in an attempt to view the information displayed on the screen; 2) lock the computer screen when not in use; 3) secure the laptop to a fixed object when left unattended; and 4) power off the laptop before packing it in order to transport it elsewhere.

5.6. **Duty to Report**

If an IT asset is lost, stolen, or compromised employees and contractors must immediately report the loss to their supervisor and complete the Lost or Stolen Devices Form located on Tax-i. The IT Security Manager will coordinate a response with Human Resources, Internal Audit, Information Services Division, Legal, Fiscal Services, and Department Deputies. This provision includes, but is not limited to:

- CDs/DVDs
- Copiers/fax machines
- Floppy disks
- Hard drives (internal or external)
- PDAs/Smart phones
- SecurID tokens (two factor authentication)
- Tapes or tape cartridges
- USB flash drives

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.