



  
**POLICY**  
*Ohio Department of Taxation*

**Policy Description:**  
Off-Site Vendors

---

**Policy No:** ODT – IT - 006

---

**Pages:** 4 Pages

---

**Effective Date:** 7/15/2008

**Division With Primary Responsibility:**  
Information Services Division

**Revised Date:**

---

## **1. Policy Purpose**

The purpose of this policy is to establish guidelines for all off-site vendors.

## **2. Policy Scope**

This policy applies to all vendors, including contractors and sub-contractors, working under contract with the Ohio Department of Taxation (ODT), who do not have access to ODT computer systems.

## **3. Policy Description**

### **3.1 Policies**

Vendors are required to review and follow all ODT policies, and acknowledge receipt and acceptance of the policies. Policy sign-off sheets will be retained on file in the Information Services Division, and may be required to be updated periodically.

### **3.2 Mandatory Training**

All vendors are required to complete ODT Disclosure Training and may be required to be updated periodically. Training sign-off sheets will be retained on file in the Information Services Division.

### **3.3 Auditing**

ODT computer systems are audited and audit logs are reviewed on a regular basis. Any attempt to alter computer system configurations without proper authorization is strictly prohibited.

### **3.4 Email**

All incoming messages are automatically scanned for viruses and malicious code.

### **3.5 Federal Tax Information (FTI)**

FTI is any data that is provided to ODT by the IRS. ODT is required to report any loss of FTI to federal authorities. Therefore, any loss of FTI must be reported to ISD Security Management immediately upon discovery. ISD Security will investigate and ensure that the proper authorities are notified.

### **3.6 Incident Reporting**

All security incidents are required to be reported as soon as the incident is discovered. During normal business hours (Monday thru Friday, 7 a.m. – 5 p.m.) security incidents should be reported to the Customer Response Center (614-752-1880). In the event a security incident is discovered after hours, the incident must be reported to the ISD Security Manager, ISD Administrator, or Chief Information Officer. Contact information for these individuals is included on the after-hours contact list which is published regularly by the Customer Response Center. All ISD management personnel should have the after hours contact list on hand/available.

### **3.7 Information Sharing**

Internal IP addresses, system names, network topology, and Internal user ids and account properties are confidential information and are to be treated as such. This information is not to be included in any document to be shared with anyone outside of ODT without an express “need to know”. All such requests must be submitted in writing and approved by ISD Security Management prior to disclosure.

No ODT information that is considered to be sensitive or confidential is permitted to be transmitted externally without encryption. ODT has both secure email and a secure FTP server (see below) for transferring sensitive data to external sources.

### **3.8 Personally Identifiable Information (PII)**

ODT is required by law to report any loss of PII to state authorities and the victims associated with the loss. Any loss of PII must be reported to ISD Security Management immediately upon discovery.

### **3.9 Personally Owned Devices**

Only state-owned devices are permitted to connect to ODT’s internal network. No vendor or personally owned, PCs, laptops, PDAs, etc. will be allowed to connect.

No ODT information is to be downloaded and/or stored on personally owned electronic devices, without the proper authorization. Authorization will only be granted in extreme cases and will require that the device containing the information be encrypted.

Vendors working with their own equipment outside ODT’s network (e.g., laptops, flash drives, etc.) are required to receive authorization from ISD Senior Management prior to use. Use of these devices will require (at a minimum) encryption software to be in place.

In the event that ODT authorizes external devices for use on an ODT project, all ODT data must be removed from the device at the request of ODT management, or at the end of the project. Also, personnel moving off of the project prior to the completion of the project will be required to state “in writing” that all ODT data has been removed from their computer devices.

**3.10 Secure Email**

ODT offers a secure mail system which is required for use in transferring sensitive information that is less than 15 megabytes. Contact the Customer Response Center at 614-752-1880 for more information.

**3.11 Secure FTP**

ODT offers a secure FTP server which is required for use in transferring sensitive information that is greater than 15 megabytes. Contact the Customer Response Center at 614-752-1880 for more information.

**3.12 Test Data and Test IDs**

Test data is not permitted to be removed from ODT with prior authorization from ISD Senior Management. Care must be taken to ensure that all data is transferred and stored in a secure manner. ODT has both secure email and a secure FTP server (see above) for transferring sensitive data to external sources.

Test IDs are to reside strictly on systems designed as “development” or “test” systems. Test IDs are not be permitted on “Production” system except in extreme cases where there is no other way to verify the functionality of a system. In these rare instances, care must be taken to prevent test IDs from corrupting production data.

Service accounts will be established to support services and/or scheduled jobs. Individual User IDs are not to be used for these activities. It is ODT’s policy to limit access levels of service accounts to the lowest level of access possible. Service accounts with high levels of administrative authority are strongly discouraged.

**4. Definitions**

<b>Terms</b>	<b>Definitions</b>
<p>Personally Identifying Information (PII)<sup>1</sup></p>	<p>includes an individuals name (only when stored in combination or linked to one of the items below):</p> <ul style="list-style-type: none"> <li>• Social Security Number</li> <li>• Taxpayer identification number</li> <li>• Driver’s license number or state identification card number</li> <li>• Medical information</li> <li>• Information that can be used to access financial resources (such as bank account number, credit or debit card number, EFT numbers, etc.); or</li> <li>• Other personal information required by law to be maintained in a secure manner</li> </ul>
<p>Security Incident<sup>2</sup></p>	<p>A reported adverse event or group of adverse events that has proven to be a verified IT security breach. An incident may also be an identified violation or imminent threat of violation of IT security policies, or a threat to the security of system assets. Some examples of possible IT security incidents are:</p> <ul style="list-style-type: none"> <li>• Loss of confidentiality of information</li> <li>• Compromise of integrity of information</li> <li>• Loss of system availability</li> <li>• Denial of service</li> <li>• Misuse of service, systems or information</li> </ul> <p>Damage to systems from malicious code attacks such as viruses, Trojan horses or logic bombs</p>

**5. Revision History**

<b>Effective Date</b>	<b>Name</b>	<b>Description</b>

<sup>1</sup>Electronic Personal Information Security Breach Notification Protocol for Agency Directors, issued by DAS Directors Office

<sup>2</sup>Statewide IT Policy Investment and Governance Division, State of Ohio IT Policy, Security Incident Response, ITP-B.7, dated 6/14/2006