



# POLICY

Ohio Department of Taxation

**Policy Description:**  
REMOTE ACCESS  
SECURITY POLICY

---

**Policy No:** ODT – IT - 003

---

**Authorities:**

Ohio IT Policy ITP – B.5

ODT – HR - 015

ODT – IT - 001

ODT – IT - 002

**Division With Primary Responsibility:**

Information Services Division & Internal Audit

**Pages:** 4 Pages

---

**Effective Date:** October 1, 2007

**Revised Date:**

---

## 1. Policy Purpose

The purpose of this policy is to implement controls that will assist in protecting The Ohio Department of Taxation's (ODT's) electronic information from being inadvertently compromised by authorized personnel using remote access into ODT's network.

These requirements are designed to minimize the potential exposure to ODT from damages which may result from remote access capabilities. Damages include, but are not limited to: the loss or compromise of sensitive or confidential taxpayer data, intellectual property, damage to public image, damage to critical ODT internal systems, etc.

## 2. Policy Scope

This policy applies to all ODT employees, contractors, consultants, temporaries, and other workers, including all personnel affiliated with third parties (hereinafter all collectively referred to as "employees") using remote access to connect to ODT's network using either a state owned or non-state owned computer. This includes reading or sending emails, viewing intranet and internet web resources, and accessing any data on ODT systems.

Remote access implementations that are covered by this policy include, but are not restricted to: dial-in, broadband, cable, and/or wireless connections.

## 3. Policy Description

Only approved employees may use the benefits of remote access. If an employee is authorized to use remote access from a non-state owned computer, they are responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and, except for access necessary when traveling, paying associated fees to the ISP.

Remote access use is to be controlled using ODT's authentication process. Any exceptions must be jointly authorized and approved by Internal Audit and ISD. It is the responsibility of employees with remote access privileges to ensure that access to ODT is not used by unauthorized individuals to gain access to ODT information system resources. Employees who are granted remote access privileges must remain constantly aware that remote access connections between their location and ODT are logical extensions of ODT's network and that they provide a potential path to the organization's most sensitive information. The authorized employee must take every reasonable measure to protect ODT's assets and data.

General access to the Internet by immediate household members or others through ODT's network on non-state computers is not permitted. Each remote access employee is responsible to ensure their remote access account is not used to violate any ODT policies, perform illegal activities, or to facilitate any outside business interests.

Additionally,

- A. Remote access gateways will be set up and managed by ODT's Information Services Division or their designee.
- B. Only approved methods of remote access may be used to connect to ODT's network. Approval may be granted by submitting a [system security request form](#).
- C. ODT shall revoke access privileges immediately upon notification of the separation or termination of any individual with remote access privileges.
- D. ODT will review remote access usage logs on a regular basis. Employees who have not had remote system activity for a period of sixty days may have the remote access ability suspended.
- E. Employees agree to apply safeguards to protect ODT information from unauthorized access, viewing, disclosure, alteration, loss, compromise, damage, or destruction. Appropriate safeguards include the use of discretion of when and where to access remotely, prevention of inadvertent or intentional viewing by unauthorized employees and others.

#### **4. Personally or Publicly Owned Devices:**

- A. As required by ODT, all computers connected to ODT internal networks via remote access must use approved anti-virus software, have personal firewall protection, and have up to date security patches installed.
- B. By using remote access technology with non-state equipment, it is understood that non-state equipment is a de facto extension of ODT's network and, as such, it is subject to many of the same rules and regulations that apply to state owned equipment. While connected to state IT resources, the employee is obligated to follow the same policies as when using state equipment. This includes but is not limited to Internet usage.

- C. Personal Digital Assistants (PDAs) or smart phones which are configured to access ODT email and/or other ODT information must be equipped with encryption software (which will be supplied by ODT) and password protected, as feasible. Employees **MUST NOT** automatically forward work email messages to or through email systems outside of ODT.
- D. Flash drives which are not owned or supplied by ODT, but contain ODT confidential or sensitive information must be password protected and encrypted. Flash drives owned or supplied by ODT will be formatted to work exclusively with ODT computers, or they will be encrypted and password protected. Any exceptions will be documented and signed waivers will be kept on file in the ISD Security Office.
- E. Problems with remote access should be reported to the Customer Response Center (614) 752-1880. Employees using non-state computers assume all liability for problems associated to the remote access and damages as a result of these problems to their non-state computers.
- F. While connected to ODT systems, usage may be monitored by ODT or by law enforcement personnel if called upon to assist ODT in investigating possible wrongdoing.
- G. When conducting work on a non-state owned computer, user must be aware that information may still need to be retained according to record retention schedules and is subject to public records requests.

## 5. Virtual Private Network (VPN)

When connecting to ODT's network remotely, in most cases, the connection is made over a virtual private network (VPN). A VPN is a secure connection established between the remote computer and ODT's network, which runs over the Internet. It is ODT's policy to allow only one network connection at a time while connected to ODT's network. This policy is designed to prevent a remote computer from accessing multiple private networks at the same time, which is known as split tunneling.

## 6. Confidentiality of Sensitive Data

- A. Federal and/or State regulations and procedures have not been changed or compromised as a result of this policy with regard to confidentiality and the handling of sensitive documents. Additionally, IRS Publication 1075 states in part, "*Only agency-owned computers and software will be used to process, access, and store federal tax information.*" Therefore, only state owned equipment may house, store, and/or process federal tax information.
- B. Sensitive information such as social security numbers, drivers' license numbers, state identification numbers, or financial account numbers **should not** be accessed or stored on any personal computing device which is not state owned. 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 the ODT Executive Management.

- C. If ODT confidential or sensitive information is lost or compromised, (includes stolen) the employee must immediately report this loss of data to their immediate supervisor. The immediate supervisor must notify their division administrator who in turn, will notify the CIO and a decision will be made whether all affected parties must be notified in compliance with R.C. 1347.12.

## **7. Expenses and/or Liability**

ODT assumes no responsibility for any expenses incurred by employees in connecting to remote access services. Further, no part of this policy shall be construed as an endorsement or permission to work from alternative work sites as a substitute for an individual's post of duty.

## **8. Enforcement**

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

## **9. Revision History**

<b>Effective Date</b>	<b>Name</b>	<b>Description</b>
7/15/07	Remote Access ODT-IT-003	Initial Policy adopted and distributed to all employees.