



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: Remote Access Security	Number: ODT-304	Effective: July 1, 2016
Issued By: Joseph Testa (Original signature on file with Internal Audit)	Published By: Information Services Division	Three Year Review Date: July 1, 2019

1. Authority

The Tax Commissioner issues Ohio Department of Taxation (herein referred to as the "Department") Policy ODT-304 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 provide guidance for using remote access to connect to the Department's network.

3. Applicability

This policy applies to all Department employees and contractors.

4. Policy

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

Remote access use is to be controlled using the Department's authentication process. Any exceptions must be jointly authorized and approved by Internal Audit and ISD. It is the responsibility of the employee or contractor with remote access privileges to ensure that no unauthorized individual gains access to Department information system resources. Any employee or contractor granted remote access privileges must remain aware that remote access connections between their location and the Department are extensions of the Department's network. Therefore, remote access provides a potential path to the organization's most sensitive information. The authorized employee or contractor must take every reasonable measure to protect ODT's assets and data.

Access to the Internet by users other than employees and contractors who have received approval, including immediate household members or others through the Department's network on non-state computers is not permitted. Remote access employees or contractors are responsible for ensuring their remote access account is not used to violate any Department policies, perform illegal activities, or participate in any outside business interests.

4.1. Additional Safeguards and Responsibilities

- 4.1.1. Remote access gateways will be set up and managed by ISD or its designee.
- 4.1.2. Only approved methods of remote access may be used to connect to the Department's network. Approval may be granted by submitting a service request form.
- 4.1.3. The Department shall revoke access privileges immediately upon notification of the separation or termination of any individual with remote access privileges.
- 4.1.4. The IT Security Manager will review remote access usage logs on a regular basis. Any employee or contractor who has not had remote system activity for a period of sixty days may have the remote access ability suspended.
- 4.1.5. Employees and contractors agree to apply safeguards to protect Department information from unauthorized access, viewing, disclosure, alteration, loss, compromise, damage, or destruction. Employees and contractors must use discretion regarding when and where to access remotely to prevent unauthorized disclosure or viewing or disclosure by others.

4.2. Personally or Publicly Owned Devices

- 4.2.1. All computers connected to Department internal networks via remote access must have approved anti-virus software, personal firewall protection, and up to date security patches installed and operational.
- 4.2.2. Any access to Department IT resources, such as the Department network or Department e-mail, is an extension of that resource. Therefore, any device connected to any Department IT resource is subject to the same rules and policies as state-owned equipment. Similarly, employees and contractors connected to Department IT resources through non-state owned equipment are also subject to the same rules and policies as when using state-owned equipment.
- 4.2.3. Smartphones configured to access Department email and/or other Department information must be equipped with encryption software and password protected. The Department may provide this software. Employees and contractors may not automatically forward work email messages to or through email systems outside of the Department.
- 4.2.4. All external memory devices, such as flash drives and hard drives, used in the Department's environment must be encrypted and password protected, regardless of ownership. All Department workstations are equipped with software to enforce this policy. Any exceptions must be approved and documented by the ISD Security Unit.
- 4.2.5. While connected to Department systems usage may be monitored.
- 4.2.6. When conducting work on a non-state owned computer, employees and contractors must be aware that information may still need to be retained according to record retention schedules and is subject to public records requests.

4.3. Virtual Private Network (VPN)

When remotely connected to the Department's network the connection is generally made over a virtual private network (VPN). A VPN is a secure connection established between the remote computer and the Department's network, which runs over the Internet. Only one network connection at a time is permitted per user login while connected to the Department's network.

Two-factor authentication is required when accessing the Department's network over a remote connection.

4.4. Expenses and/or Liability

The Department assumes no responsibility for any expenses incurred by any employee or contractor utilizing remote access services. 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.

5. Administrative Consequences for Violations

Employees and contractors may be held civilly or criminally liable for violating laws related to unauthorized disclosure of sensitive information. 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.