



Ohio

Department of Taxation

John Kasich, Governor
Joseph Testa, Tax Commissioner

30 E. Broad St., 22nd Floor
Columbus, Ohio 43215

(614) 466-2166
Fax (614) 466-6401

POLICY

Policy: Off-Site Contractors	Number: ODT-IT-002	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-IT-002 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 guidelines for all off-site contractors.

3. Applicability

This policy applies to all contractors working off-site who do not have access to Department IT Resources.

4. Definitions

- 4.1. **Contractor** – An individual or business paid a fee or other compensation for particular services.
- 4.2. **Contractor Division Liaison (CDL)** – The individual in the division where the Contractor is providing service responsible for coordinating onboarding and offboarding of the Contractor.
- 4.3. **Contractor Facilitator (CF)** – The individual in the division where the Contractor is providing service that is responsible for ensuring the Contractor is providing the services as indicated in the contract, as well as the person who is approving the hours worked by the Contractor.
- 4.4. **IT Resource** – Any information technology resource, such as computer hardware and software, IT services, network equipment and services, digital devices such as digital copiers and facsimile machines, supplies and the Internet, made available to personnel.
- 4.5. **Security Incident** – Any real or suspected adverse event or group of adverse events in relation to the security of any IT Resource, or an act violating an explicit or implied security policy. Some examples of possible incidents include loss of sensitive information, disruption or denial of service, misuse of service, systems or information, changes to system hardware, firmware or software characteristics without proper authority, loss of system availability, malicious code attacks, etc.
- 4.6. **Sensitive Information** - Sensitive information is any type of computerized data that presents a reasonably high degree of risk if released or disclosed without authorization. Sensitive information includes personally identifiable information (e.g., taxpayer identification number, social security number, medical information, bank account numbers, state identification number, etc.). Sensitive

information also includes federal tax information, which is any data provided to the Department by the Internal Revenue Service.

5. Policy

- 5.1. **Policies** – Contractors are required to review and follow all Department policies applicable to Contractors, and acknowledge receipt of such policies, within five business days after onboarding with the Department. Policy signoff sheets will be retained on file with the CDL. Such policy review may be required to be updated periodically.
- 5.2. **Background Checks** – Contractors may be required to submit to various levels of background checks depending on their level of access to Department data, such as FBI fingerprinting, citizenship/residency, local law enforcement checks, and tax filing compliance.
- 5.3. **Mandatory Training** – Contractors are required to complete any Department training applicable to Contractors as soon as practicable after onboarding with the Department. Training may be required to be updated periodically. Information related to completion of training (e.g., signoffs, completion certificates, etc.) shall be maintained by the CDL.
- 5.4. **Auditing** – Department IT Resources are audited and audit logs are reviewed on a regular basis. Any attempt to alter computer system configurations without proper authorization is strictly prohibited.
- 5.5. **Email** – All incoming messages to the Department are automatically scanned for viruses and malicious code. Department email sent to an off-site Contractor may not be automatically re-routed to a personal or other outside email account.

Sensitive Information should not be included in the body of an email; rather it should be attached as a password protected document (zipped if possible).

Attachments sent via email should be less than 25 megabytes.

Please contact the Customer Response Center at 614-752-1880 if there are any questions.

- 5.6. **Secure FTP** – Secure FTP should be used for transferring information that is greater than 25 megabytes. Please contact the Customer Response Center at 614-752-1880 with any questions.
- 5.7. **Sensitive Information** – The Department reports losses of sensitive information as required by law. Any potential loss shall be reported to the Contractor's CF and/or the Department's Chief Information Security Officer (CISO) immediately upon discovery.
- 5.8. **Security Incident Reporting** - All potential Security Incidents are required to be reported to the Contractor's CF and/or CISO as soon as discovered.
- 5.9. **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 may not be included in any document to be shared with anyone outside of the Department without an express "need to know." All such requests must be submitted in writing and approved by the CISO prior to disclosure. No Department information that is considered to be Sensitive Information or confidential may be transmitted externally without encryption.
- 5.10. **Test Data and Test IDs** – Test data may not be removed from the Department without prior authorization from the CISO. Care must be taken to ensure that all data is transferred and stored in a secure manner. Test IDs are to reside strictly on systems designed as "development" or "test" systems. Test IDs are not permitted on "production" systems except in extreme cases where there is no other method to verify the functionality of a system, and such permission must be obtained from the CISO. Service accounts will be established to support services and/or scheduled jobs. Individual User IDs may not be used for these activities. It is the Department's policy to limit access levels of services accounts to the lowest level of access necessary.
- 5.11. **Personally Owned Devices** - Only state-owned IT Resources are permitted to connect to the Department's internal network. No Contractor or personally owned IT Resource may be connected.

No Department information may be downloaded and/or stored on personally owned electronic devices without explicit permission from the CISO. Authorization will only be granted in extreme cases and will require that the device containing the information be protected by valid and current encryption software.

Contractors working with their own equipment outside of the Department's network (e.g., laptops, flash drives) are required to receive authorization from the CISO prior to use. Use of these devices will require valid and current encryption software to be in place. All Department data must be removed from the device at the request of Department management, or at the end of the project. Contractors moving off a project prior to completion are also required to remove all Department data.

6. Administrative Consequences

In addition to potential civil or criminal sanctions for violating laws pertaining to misuse of Department IT Resources, a violation of this policy may result in termination or modification of the contractual arrangement with the Contractor.