



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: Security Incident Response	Number: ODT-306	Effective: August 5, 2013
Issued By: Joseph Testa (Original signature on file with Internal Audit)	Published By: Information Services Division	Four Year Review Date: August 5, 2017

1. Authority

The Tax Commissioner issues Ohio Department of Taxation (herein referred to as the "Department") Policy ODT-306 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 an incident response team (IRT) for the Department.

3. Applicability

This policy applies to all Department employees and contractors.

4. Definitions

4.1. **Adverse Event** – Any observable occurrence in a system or network with a negative consequence. Adverse events sometimes provide an indication that an incident is occurring; however, not all adverse events are security incidents (SIs). Examples of adverse events include:

- System crashes
- Network packet floods
- Unauthorized use of system privileges
- Defacement of a web page
- Execution of malicious code that destroys data

4.2. **Federal Tax Information** - Federal tax returns or return information received from the Internal Revenue Service (IRS).

4.3. **Security Incident** – A reported adverse event or group of adverse events that has been verified as an 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 SIs are:

- Loss of confidentiality of information
- Compromise of integrity of information
- Loss of system availability
- Denial of service
- Misuse of service, systems, or information

- Damage to systems from malicious code attacks such as viruses, Trojan horses or logic bombs

5. Policy

5.1. Incident Response Team Composition

The Department has established an IRT consisting of individuals from the following divisions:

- Budget
- Chief Counsel
- Communications
- Criminal Investigations
- Human Resources
- Information Services
- Internal Audit

Because of the nature and variety of SIs, any Department employee may be called on by management to participate in the efforts of the IRT.

5.2. Supporting Documentation

The Department's Incident Response (IR) Reference Guide outlines specific details related to the following information:

- List of team members
- Roles and responsibilities
- Level of authority for resources and staff
- Event detection
- Evaluation and response
- SI reporting
- Communication methods
- Escalation procedures

The Department developed an IR Plan for use by the IRT to evaluate and determine whether an adverse event has become an SI. The IR Plan includes the following information:

- Adverse Event Evaluation
- Adverse Event Classification
- Incident Containment
- Elimination
- Notification of a Personal Information Security Breach
- Recovery

5.3. Security Incident Reporting

The Department is required by the Department of Administrative Services, Office of Information Technology (OIT) to immediately report all significant SIs to the OIT Office of Information Security and Privacy.

The Department is required by federal law to immediately notify the Treasury Inspector General for Tax Administration of any SI that may affect Federal Tax Information.

Reporting shall not be delayed in order to obtain additional information. The Department must continue to report information as it is collected.

In addition to federal and state notifications, the Department may be responsible for notifying partner networks if there is a possibility the SI poses a risk to the partner network and/or its data.

5.4. Risk Assessments

Significant SIs require the Department to perform new risk assessments of any compromised systems.

5.5. Incident Response Testing

The Department will conduct annual IR testing exercises which simulate SIs. These tests shall measure the effectiveness of the IR capability and identify potential weaknesses. Tests may include involvement from service providers, e.g., OIT, off-site storage vendor, etc.

All system test results will be maintained on file in the ISD Security Unit.

6. 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.