



POLICY

Ohio Department of Taxation

Policy Description:
SECURITY INCIDENT
RESPONSE POLICY

Policy No: ODT – IT - 008

Authorities:

IRS Publication 1075 – Tax Information Security Guidelines
for Federal, State and Local Agencies and Entities

Ohio IT Policy ITP – B.7 – Incident Response

ODT-HR-004 – Progressive Discipline

Division With Primary Responsibility:

Information Services Division & Internal Audit

Pages: 4 Pages

Effective Date: April 6, 2009

Revised Date:

1. Policy Purpose

The purpose of this policy is to establish an Incident Response Team for the Ohio Department of Taxation (ODT).

The team's purposes are 1) to minimize the potential exposure to ODT from damages which may result from a security incident, 2) quickly and efficiently contain the incident, 3) preserve evidence when necessary, 4) restore functionality of computer systems and data, 5) analyze incidents to prevent future disruptions, and 6) provide notification to the proper authorities described herein.

2. Policy Scope

This policy applies to all ODT employees, contractors, consultants, temporaries and other workers affiliated with third parties (herein after all collectively referred to as ODT representatives) who use and administer ODT systems. Because of the nature and variety of security incidents, anyone in the organization may be called on by management to participate in the efforts of the Incident Response Team.

3. Policy Description

3.1 Incident Response Team Composition

ODT has established an Incident Response team consisting of individuals from various divisions throughout the Department. These divisions include, but are not limited to:

- Chief Counsel
- Communications
- Enforcement
- Information Services
- Internal Audit
- Human Resources

3.2 Supporting Documentation

Refer to ODT's Incident Response Reference Guide for specific details outlining the following information:

- List of team members
- Roles and responsibilities
- Level of authority for resources and staff
- Event detection
- Evaluation and response

- Security incident reporting
- Communication methods
- Escalation procedures

ODT developed an Incident Response Plan for use by the Incident Response Team to evaluate and determine whether an adverse event has become an incident. The IR Plan includes the following information:

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

ODT Problem Management Procedures can be found on TAXI. ISD management personnel should have a hardcopy of this documentation available.

An Incident Response Lessons Learned Procedure has been established to reduce the possibility of similar incidents exposing our environment to threats and/or losses.

3.3 Security Incident Reporting

ODT is required by the Ohio Office of Information Technology (OIT) to report all significant security incidents to the OIT Service Delivery Division (SDD) Enterprise Operations Security office.

Federal Law requires ODT to notify the Treasury Inspector General for Tax Information (TIGTA) of any incident that may affect Federal Tax Information (FTI).

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

3.4 Risk Assessments

Significant security incidents require ODT to perform new risk assessments of any compromised systems.

3.5 Legal Review

All Incident Response Policies, Procedures and support reference materials are subject to legal review to address the following items:

- Evidence chain of custody is protected
- Actions are legally defensible and enforceable
- Compliance with overall agency and state policies
- ODT due diligence is demonstrated
- ODT conforms with national, state or local laws or regulations
- Confidentiality for all investigative data and evidence is maintained
- ODT staff or other agents of the state are protected from legal liability
- ODT is safeguarded from legal liability during a system compromise if an intruder was allowed access while evidence was gathered or agency assets were used to launch an attack on another organization

3.6 Incident Response Testing

As part of Incident Response, ODT will perform the following tests annually:

- Critical System Backups – This testing ensures ODT’s ability to restore data and systems after an adverse event or security incident has occurred.
- Critical Systems and Application Software – will be verified and maintained by ISD. ODT will store copies of software off site (with a 3rd party vendor). ISD will update this software when significant changes to the systems occur.
- Redundant Configurations – ISD will test these configurations and, if applicable, will perform fail over tests.
- Incident Response Team testing – ISD will test these capabilities.

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

3.7 Security Awareness

ODT’s Security Awareness Training includes incident response topics.

4. Discipline

Failure to comply with this policy may result in the imposition of discipline in accordance with ODT work rules including, but not limited to, Neglect of Duty, Insubordination, and/or Ohio Revised Code Section 124.34.

5. Definitions

Terms	Definitions
Adverse Event ¹	Any observable occurrence in a system or network with a negative consequence. Examples of adverse events include system crashes, network packet floods, unauthorized use of system privileges, defacement of a web page, and execution of malicious code that destroys data. Adverse event sometimes provide an indication that an incident is occurring. However, not all adverse events are security incidents.
Incident ¹	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: <ul style="list-style-type: none"> • 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

¹ Statewide IT Policy Investment and Governance Division, State of Ohio IT Policy, Security Incident Response, ITP-B.7, dated 6/14/2006

9. Revision History

Effective Date	Name	Description