

OIT Enterprise Procedure

Procedure: OEP-SEC.4001 Statewide Incident Response Reporting

Issued by: Office of Information Security and Privacy

Effective:
10/10/2017

Approved by: Russell Forsythe
State Chief Information Security Officer
Office of Information Security and
Privacy

Published through:
Enterprise IT
Architecture and Policy

Overview

This procedure defines the steps to be followed by State of Ohio agencies reporting information, computer system, privacy or network security incidents. This procedure pertains to the types of incidents described within the **Definitions** below. It does not apply to general system outages.

Procedure

State Agencies

1.0 Agency Security Point of Contact

1.1 Agencies shall establish a security point of contact (SPoC) and register this contact information with the Ohio Department of Administrative Services (DAS) Office of Information Technology (OIT) Office of Information Security and Privacy (OISP). SPoC contact information shall include:

- Name
- Title
- Organization
- Telephone number
- Mobile phone number (if applicable)
- After hours contact number
- E-mail address
- Mailing address

1.2 SPoC information shall be sent through the following channel to OISP:

- E-mail: enterprise.sirt@das.ohio.gov

2.0 Reporting an Incident

2.1 Upon becoming aware of a security or privacy incident, agencies shall report the incident by calling the Customer Service Center (CSC) at **1-877-644-6860** or **1-614-644-6860**.

2.2 When the CSC call center personnel answer the phone, they will ask the caller for their name and organization along with a description of the problem. At this time the caller should specifically indicate that they are reporting a security incident by stating the following:

- **“I Have a Security Incident to Report.”**

2.3 The caller should be prepared to provide as much of the following information as possible as it pertains to the incident. Agencies should report the incident even if the information is incomplete.

- Date and time detected, date and time occurred, and duration of the event
- Current status of the incident
- Brief description of the incident
- Was there any sensitive data or personally identifiable information involved?
- What services are impacted?
- What applications are impacted?
- Specifics about the affected systems such as software and network
- Have there been any previous occurrences of this incident?
- What personnel was involved?
- Who else has been notified (e.g. supervisor, law enforcement, etc.)?
- What is the possible source or cause of the incident?
- If the incident has occurred before, when? Are there previous reports available?
- Any additional information

2.4 A security incident ticket number will be assigned and shall be retained by the caller. The security incident ticket number shall be provided and referred to for subsequent communications regarding the incident.

3.0 Incident Updates and Containment

3.1 The agency SPoC shall also report updates and ultimately the subsequent containment of the incident to the CSC at **1-877-644-6860** or **1-614-644-6860**. When the CSC call center personnel answer the phone, they will ask the caller for their name and organization.

3.2 The agency SPoC will be required to provide the CSC with the security incident ticket number assigned when the incident was opened.

3.3 At this time, the agency SPoC should specifically indicate that they are reporting a follow-up to a security incident by stating either of the following:

- **“I am calling to update security incident ticket NNNNN,” OR**
- **“I am calling to report security incident ticket NNNNN as now contained.”**

3.4 Following confirmation of the authorized caller, the CSC will update/close the ticket accordingly.

3.5 Agencies shall forward the results of their lessons learned analysis to the Enterprise Information Security and Privacy Incident Response Team (SIRT).

- Email: enterprise.sirt@das.ohio.gov

4.0 Enterprise SIRT Coordinator

4.1 The Enterprise SIRT Coordinator is responsible for coordinating appropriate efforts to resolve the incident.

- When notified of an incident, the Enterprise SIRT Coordinator will assess the situation and determine if, and when, the Enterprise SIRT should be assembled.
- Incident notifications [not to include the identity of impacted agency or agency specifics] shall be disseminated to agency SPoCs along with any information pertaining to the resolution of the incident.

4.2 The Enterprise SIRT Coordinator is responsible for coordinating appropriate efforts to resolve the event and for communicating the event to the agency SPoC.

4.3 OISP shall maintain a central list of agency SPoCs contact information and, as needed, disseminate alerts to State of Ohio agencies. Alert notifications will not include the name of impacted agency or agency specifics.

- Agency SPoCs will be notified via e-mail that an incident is in progress.
- In the event that e-mail is unavailable, agency SPoCs will be notified via telephone that an incident is in progress.

Definitions

Agency Security Point of Contact - The contacts from each agency supported by Office of Information Security and Privacy (OISP) for security-related incidents. These contacts are responsible for reporting incidents to OISP and for appropriately communicating incident related information within their agencies.

Denial of Service (DoS) - The prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided.)¹

Enterprise Security Incident Response Team (SIRT) – The Enterprise SIRT works in concert with the service owners and other senior DAS OIT staff to define and implement incident response policies, standards, procedures, and guidelines. This program monitors the current information systems security conditions on an ongoing basis and identifies needed changes to maintain the desired state for best practices in the area of incident response. Included in the desired state is monitoring by the Enterprise SIRT to assure compliance with security policies.

Incident - A security incident threatens the confidentiality, integrity or availability of state information resources. Some examples of incidents include:

- Loss or theft of a computing device or media (e.g., laptop, smartphone, storage device, authentication token)
- Denial of Service (DoS)
- Improper system usage or access
- Information spillage
- Malicious code (e.g., virus, worm, Trojan horse)
- Phishing messages
- Social engineering

Information Spillage - Refers to instances where sensitive information is inadvertently placed on information systems that are not authorized to process such information. Such information spills often occur when information that is initially thought to be of lower sensitivity is transmitted to an information system and then is subsequently determined to be of higher sensitivity.²

Malicious Code - Software or firmware intended to perform an unauthorized process that will have an adverse impact on the confidentiality, integrity, or availability of an information system. Some examples include a virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.³

Personally Identifiable Information - “Personally identifiable information” is information that can be used directly or in combination with other information to identify a particular individual. It includes:

- a name, identifying number, symbol, or other identifier assigned to a person,
- any information that describes anything about a person,
- any information that indicates actions done by or to a person,
- any information that indicates that a person possesses certain personal characteristics.

Sensitive Data - Sensitive data is any type of computerized data that presents a high or moderate degree of risk if released or disclosed without authorization. There is a high degree of

¹ “National Information Assurance (IA) Glossary,” Committee on National Security Systems, 26 April, 2010, <http://www.ncsc.gov/nittf/docs/CNSSI-4009_National_Information_Assurance.pdf >.

² “NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations,” U.S. Department of Commerce National Institute of Standards and Technology, April, 2013 <<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>>.

³ *Ibid.*

risk when unauthorized release or disclosure is contrary to a legally mandated confidentiality requirement. There may be a moderate risk and potentially a high risk in cases of information for which an agency has discretion under the law to release data, particularly when the release must be made only according to agency policy or procedure. The computerized data may be certain types of personally identifiable information that is also sensitive such as medical information, social security numbers, and financial account numbers. It includes Federal Tax Information under IRS Special Publication 1075, Protected Health Information under the Health Insurance Portability and Accountability Act, and Criminal Justice Information under Federal Bureau of Investigation's Criminal Justice Information Services (CJIS) Security Policy. The computerized data may also be other types of information not associated with a particular individual such as security and infrastructure records, trade secrets and business bank account information.

Token - Something that the Claimant possesses and controls (typically a key or password) that is used to authenticate the Claimant's identity.⁴

Revision History

Date	Description of Change
8/10/2006	Original procedure.
3/28/2011	Group names and addresses updated.
5/23/2017	Updated the contact information, role and office references in the procedure to align with the current organizational structure.
10/10/2017	Additional updates to further align with current security procedures and terminology.
10/10/2018	Scheduled review.

⁴ Burr, E. William, Donna F. Dodson, Elaine M. Newton, Ray A. Perlner, W. Timothy Polk, Sarbari Gupta, Emad A. Nabbus, "NIST Special Publication 800-63-2, Electronic Authentication Guideline," .S. Department of Commerce National Institute of Standards and Technology, August 2013
<<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf>>.

Inquiries

Direct inquiries about this procedure to:

Office of Information Security and Privacy
Office of Information Technology
Ohio Department of Administrative Services
30 E. Broad Street, 19th Floor
Columbus, Ohio 43215

Telephone: 614-644-9391
E-mail: state.isp@das.ohio.gov

References

Ohio Administrative Policy IT-01, Authority of the State Chief Information Officer to Establish Ohio IT Policy: This policy communicates the IT policy-making authority of the state chief information officer (state CIO), who is also the assistant director for the Ohio Department of Administrative Services (DAS). Under the direction of the director of DAS, the state CIO shall establish policies and standards for the acquisition and use of common information technology by state agencies, including, but not limited to, hardware, software, technology services, and security, and the extension of the service life of information technology systems, with which state agencies shall comply.⁵

Ohio IT Standard ITS-SEC-02, Security Controls Framework: This state IT standard specifies the minimum requirements for information security in all agencies and identifies the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 as the framework for information security controls implementation for the state.

This procedure replaces all previously issued procedures regarding statewide security incident reporting.

⁵ As outlined in Ohio Revised Code Section 125.18.