


Incident Response Policy

POLICY NUMBER: 2100-07	EFFECTIVE DATE: 10/10/2017	APPOINTING AUTHORITY APPROVAL: 
REPLACES POLICY DATED: 12/5/2012	AUTHORITY: Ohio Revised Code Section 125.18	

1.0 PURPOSE

The purpose of this policy is to define the requirements for an enterprise and an Ohio Department of Administrative Services (DAS) *information security and privacy incident response* capability.

A glossary of terms found in this policy is located in Section 8.0 Definitions. The first occurrence of a defined term is in *bold italics*. In addition, references to National Institute of Standards and Technology Special Publication 800-53, “Security and Privacy Controls for Federal Information Systems and Organizations,” family identifiers and control numbers are provided in parentheses next to requirement headers, where applicable.

2.0 SCOPE

This policy defines the requirements necessary to provide a coordinated information security *incident* response for all of DAS. The requirements of this policy apply to all DAS programs and include all *DAS-managed system assets*. The policy also applies to all DAS business unit managers as well as system and *service owners*.

3.0 BACKGROUND

Information technology (IT) is an integral part of how DAS conducts business and maintains information in support of its stated mission. Therefore, DAS must be prepared to respond when information security and privacy incidents occur. Poorly handled incidents can result in compromised evidence, loss of time, conflicting information, negative publicity, and loss of data *confidentiality, integrity, and availability*. Responses to an IT security incident can range from simply recovering compromised systems to the collection of evidence for the purpose of criminal prosecution. Therefore, preparation and planning and ensuring that the right resources are available are critical to DAS' ability to adequately detect, respond to and recover from an incident.

4.0 REFERENCES

- 4.1 **National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Security and Privacy Controls for Federal Information Systems and Organizations:** NIST SP 800-53 provides guidelines for selecting and specifying security controls for federal government information systems.

- 4.2 **Ohio Administrative Policy IT-13, Data Classification:** Ohio Administrative Policy IT-13 provides a data classification methodology to state agencies for the purpose of understanding and managing data and information systems with regard to their level of confidentiality and criticality.
- 4.3 **Ohio Administrative Policy IT-14, Data Encryption and Securing Sensitive Data:** Ohio Administrative Policy IT-14 provides guidance to agencies as they take steps to protect sensitive data and information.
- 4.4 **Office of Information Technology (OIT) Enterprise IT Procedure OEP-SEC.4001, Statewide Incident Response Reporting:** Defines the steps to be followed by State of Ohio agencies reporting information, computer system, privacy or network security incidents.
- 4.5 **DAS Policy 200-14, Teleworking:** DAS Policy 200-14 outlines the requirements for DAS teleworking.
- 4.6 **Ohio Revised Code 1347.15, Access rules for confidential personal information:** This section of Ohio Revised Code (ORC) outlines what needs to be included in the rules that each state agency adopts under Chapter 119 of the Revised Code, regulating access to the confidential personal information the agency keeps, whether electronically or on paper.
- 4.7 **State of Ohio IT Guideline, Information Technology Business Continuity Planning:** This IT guideline provides state agencies guidance in the development and implementation of a comprehensive IT business continuity plan that, in the event of a business disruption, will help enable the continuation of critical processes and the delivery of essential services at an acceptable level.

5.0 POLICY

All *information security and privacy incidents* shall be immediately reported to the Customer Service Center (CSC) in accordance with OIT Enterprise IT Procedure OEP-SEC.4001, “Statewide Incident Response Reporting”:

- **CSC Phone:** 614-644-6860 or 877-644-6860
- **CSC Email:** csc@ohio.gov

The DAS Office of Information Security & Privacy (OISP) shall maintain an enterprise information security and privacy incident response team (SIRT) and shall provide oversight for all information security and privacy incidents. The OISP shall define procedures for an information security and privacy incident response capability, which includes requirements for incident preparation, detection and analysis, containment, eradication and recovery, lessons learned analysis, records management, training and testing.

5.1 **Definition of Security and Privacy Incidents:** A security incident threatens the confidentiality, integrity or availability of state information resources. Privacy incidents are considered to be a subset of security incidents for the purposes of this policy. Incidents may fall into one or more of following categories:

5.1.1 **Loss or Theft:** The loss or theft of a computing device or media used by the agency, such as a laptop, smartphone, storage device, or authentication *token*. This may also include the loss/theft of hard copy documents containing *sensitive data* or *personally identifiable information (PII)*.

5.1.2 **Denial of Service (DoS):** An attack that successfully prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. Examples of these types of attacks include:

- Attacks, including physical attacks, which adversely affect or degrade access to critical services.
- Persistent or significant DoS attacks (e.g., attempted DoS attacks aimed specifically at DNS servers or routers).
- Use of state devices to initiate or facilitate *Distributed Denial of Service (DDoS)* attacks.
- Attempts, either failed or successful, to cause failures in critical infrastructure services or loss of critical *supervisory control and data acquisition systems (SCADA)*.

5.1.3 **Improper Usage or Access:** Acceptable computing use or access laws, rules, or policies are violated. This includes suspected criminal use of systems or services, including: identify theft and the disclosure, improper access, destruction, or alteration of any state managed systems or data. Improper usage or access includes potential violations of ORC Chapter 1347.

5.1.4 **Information Spillage:** Information spillage refers to instances where sensitive information is inadvertently exposed to unauthorized disclosure. 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. Examples include:

- Sensitive information placed on information systems that are not authorized to process such information;
- Information thought to be public is posted on a state website, but is later determined to contain non-public data;

- Non-public information added to a system, which is not accredited to house non-public information; and
- Misdirected or improperly sent email or postal mail with sensitive information.

5.1.5 **Malicious Code**: Successful installation of malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application.

For the purposes of this policy, malicious logic that is successfully quarantined by antivirus software or that falls within normal or expected behaviors is not considered an incident.

5.1.6 **Phishing Messages**: Email containing malicious code designed to trick users into providing sensitive information (e.g. user names, passwords, information that could be contained in a secret question like “What’s your pet’s name?”; or “What’s your mother’s maiden name?”, etc.).

5.1.7 **Scans/Probes/Attempted Access**: Any activity that seeks to access or identify a state computer, open ports, protocols, service, or any combination for later exploit.

5.1.8 **Social Engineering**: A bad actor working to trick a user into providing sensitive information (e.g., user names, passwords, or any sensitive data, or physical access that the user can provide).

5.1.9 **Unauthorized Access**: To gain or attempt to gain logical or physical access, without permission, to a network, system, application, data, sensitive hard copy records, or other resource. This also includes changes to system, *firmware*, hardware or software configuration characteristics without the state's knowledge, instruction or consent.

5.2 **Incident Training Requirements (IR-2)**: The OISP will provide basic incident response training for security points of contact (SPoCs), data privacy points of contact (DPPoCs), and enterprise incident response team members.

The OISP will provide training to security personnel responsible for enterprise SIRT activities, at least annually, or when required by information system changes. Simulated events shall be incorporated into the training to facilitate effective response by personnel in crisis situations. Automated mechanisms shall be employed to provide a more thorough and realistic incident response training environment.

- 5.3 **Incident Testing Requirements (IR-3)**: The OISP, in conjunction with SPoCs and the enterprise SIRT, shall conduct annual incident response testing exercises, which simulate incidents. These tests shall measure the effectiveness of the incident response capability and identify potential weaknesses. Tests shall be designed to stress the incident response capability and should leverage the use of automated tools as much as practical. Tests shall be coordinated with other organization plans (e.g., business continuity, disaster recovery, etc).
- 5.4 **Incident Handling (IR-4)**: The OISP shall define procedures for an incident response capability, which includes security incident preparation, reporting, detection & analysis, containment, and eradication & recovery. These incident handling activities are combined with contingency planning activities, as needed. Lessons learned from ongoing incident handling activities are incorporated into incident response procedures, training and testing.
- 5.5 **Incident Communication and Coordination Mechanisms**: The incident response capability established by the OISP shall include separate and different communication and coordination mechanisms in case of the failure of one mechanism.
- 5.5.1 **Contact Information**: Contact information shall be captured for team members, law enforcement agencies, business partners and others within and outside of the organization (primary and backup contacts), including on-call and escalation information.
- 5.5.2 **Incident Reporting Mechanisms**: Incident reporting mechanisms shall be clearly defined (e.g., phone numbers, e-mail addresses, online forms, etc.).
- 5.5.3 **Incident Tracking System**: An incident tracking system shall be utilized to record pertinent information about information security incidents.
- 5.5.4 **Communication and Coordination Resource Needs**: The OISP shall determine the hardware, software and facilities needed to support the communication and coordination of incident response activities (e.g., smartphones, encryption software, war rooms, secure storage facilities, etc.).
- 5.6 **Incident Preparation**: Preparation is a key element of incident response. Refer to the State of Ohio IT Guideline, “Information Technology Business Continuity Planning,” for additional information. System owners shall maintain documentation, such as:
- Inventory of System Interconnections
 - Data Sharing Agreement Inventory

- Hardware Inventory, including asset specifics and owner (assigned to) information for mobile, endpoint, server, and virtual devices
- Software Inventory
- System Inventory, including system and business owner and contact information; operating, database, and application software; and physical and network location
- Network Topology, including subnet information for endpoint, server, wireless and voice networks
- Vendor Managed System Inventory, including system, vendor and business owner and contact information; operating, database, and application software; physical and network location; and contact information for the vendor security team
- All enterprise assets should report to a common source for Network Time Protocol (NTP)

5.7 **Incident Response Risks**: The OISP shall evaluate what risks may be associated with a given IT security incident and develop procedures to ensure critical tools, data and equipment are available to facilitate containment and recovery. The procedures shall address:

5.7.1 **Incident Response Contact List**: The CSC shall continue to maintain an incident response contact list, which contains names, desk phone numbers, mobile phone numbers, email addresses, organization names, titles, and incident response roles and responsibilities for all key incident response resources. These resources include, but are not limited to, enterprise SIRT members, key DAS management personnel, public information officers, legal counsel, law enforcement officials, and agency incident response contacts.

5.7.2 **Incident Analysis Resources**: The OISP shall identify the resources that will be used as part of the incident response process. This includes the hardware and software that will be used for incident analysis (e.g., digital forensic workstations; laptops; spare workstations, servers and networking equipment or the virtualized equivalents; packet sniffers; removable media; etc.) as well as port lists; documentation for operating systems, applications, intrusion detection, and antivirus; network diagrams; lists of critical assets; current baselines; cryptographic hashes of critical files; etc. Automated mechanisms shall be used to support the incident handling process.

5.8 **Incident Reporting**: Incident reporting procedures are documented in Ohio Enterprise IT Procedure OEP-SEC.4001, “Statewide Incident Response Reporting.”

5.9 **Detection and Analysis**: The enterprise SIRT shall provide guidance on how to detect and analyze incidents that use common attack vectors.

- 5.10 **Incident Containment**: The enterprise SIRT shall quickly determine containment strategies in an effort to minimize damage.
- 5.11 **Evidence Preservation**: The enterprise SIRT shall take appropriate steps to preserve sufficient evidence to ensure accurate incident records, facilitate the investigation and determine the extent of the damage.
- 5.12 **Eradication & Recovery**: The enterprise SIRT procedures shall clearly convey when and how systems shall be restored to normal operation, confirm the systems are functioning normally, and, if applicable, remediate vulnerabilities to prevent similar incidents. All affected hosts shall be remediated.
- 5.13 **Lessons Learned**: After a major incident, the DAS system or service owner shall hold a lessons learned meeting with all involved parties as soon as possible. A member of the enterprise SIRT shall participate in these meetings as well as members of the impacted DAS business units.
- 5.14 **Enterprise SIRT Responsibilities (IR-7)**: Enterprise SIRT responsibilities shall include, conducting training on incident response processes and procedures; leading incident response exercises; and engaging in proper incident handling, monitoring, and reporting as it pertains to incidents. The enterprise SIRT shall coordinate with and provide support to agency SPoCs and agency information security and privacy incident response teams to ensure incidents are properly identified, contained, and remediated and to assist in recovery efforts.
- 5.14.1 The enterprise SIRT shall consist of the following core members or their designees:
- State Chief Information Officer (CIO)
 - State Chief Information Security Officer (CISO)
 - State Chief Privacy Officer
 - DAS Chief Legal Counsel
 - DAS Communications Manager
 - Customer Service Center (CSC) Manager
 - DAS Lead Incident Coordinator
 - DAS OISP Incident Handlers
 - DAS OIT IT Operations Managers (e.g., Security Engineering, Desktop Services, Unified Network Services, Enterprise Shared Solutions, Enterprise Open Systems, Enterprise Computing Services, Application Management, Multi-Agency radio Communications System)

- For specific incidents, additional members shall be added as identified by the incident coordinator (building security, vendor representatives, etc.)

5.15 **DAS Information Security and Privacy Incident Response Team:** A DAS information security and privacy incident response team shall include members from the enterprise SIRT and the following representatives or their designees:

- OISP assigned Information Security Officer or SPoC
- Impacted Business Unit Managers
- DPPoC
- Human Resources Manager
- Information Technology Managers
- Physical Security and Facilities Manager (as needed)
- Procurement Manager (as needed)

5.15.1 The SPoC shall serve as the primary coordinator with the OISP.

5.16 **Incident Response Plan (IR-8):** The enterprise SIRT shall develop, maintain, and distribute (as appropriate) an enterprise incident response plan. As a minimum, the plan shall contain the following elements:

- Organization and structure of the enterprise information security and privacy incident response capability
- Enterprise and agency incident response roles & responsibilities
- Protocols for communication during incident response
- Guidance for incident evaluation (e.g., collection, analysis, classification, forensic/evidentiary considerations)
- Best practices for incident containment, eradication, recovery & reporting
- Lessons learned procedures
- Incident reporting metrics

5.17 **Incident Response Records Management:** The OISP shall monitor and maintain records of reported information security incidents. Guidance on maintaining incident response records is contained in section 6.0 Procedures.

5.18 **Personal Information Security Breach Notifications:** The OISP shall work with enterprise and agency information security and privacy incident response teams to ensure that incident notifications, including those under ORC 1347.12 and 1347.15 and any applicable federal regulations, are sent to the appropriate parties.

- 5.18.1 **Outside Entities:** If the incident resulted in a breach of a system containing data from an outside entity like the Centers for Medicare and Medicaid Services (CMS), the Internal Revenue Service (IRS), or the Social Security Administration (SSA), notifications must be made immediately, or within the timeframe of the applicable outside entity, but not more than 24-hours, to the external agency. Timely notification to affected individuals may also be required.

6.0 PROCEDURES

- 6.1 **Maintaining Incident Response Security Records:** The enterprise SIRT shall safeguard and restrict access to incident data because it often contains sensitive information. Incident response security records shall contain the following:
- 6.1.1 The current status of the incident, (e.g., new, in progress, forwarded for investigation, resolved, etc.)
 - 6.1.2 A summary of the incident
 - 6.1.3 Indicators related to the incident
 - 6.1.4 Other incidents related to this incident
 - 6.1.5 Actions taken by all incident handlers on this incident
 - 6.1.6 Chain of custody, if applicable
 - 6.1.7 Impact assessments related to the incident
 - 6.1.8 Contact information for other involved parties (e.g., system owners, system administrators)
 - 6.1.9 A list of evidence gathered during the incident investigation
 - 6.1.10 Comments from incident handlers
 - 6.1.11 Next steps (e.g., rebuild the host, upgrade an application)

7.0 COMPLIANCE

As of the effective date of this policy, DAS OISP, Enterprise SIRT, system and service owners, and business managers may not be completely aligned to the requirements outlined in the policy. A general implementation framework for the requirements of this policy includes:

- 7.1 DAS OISP, Enterprise SIRT, system and service owners, and business managers shall have six months from the effective date of the policy to implement the requirements outlined within this policy.

8.0 DEFINITIONS

Availability - Ensuring timely and reliable access to and use of information.¹

¹ "NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems

Confidentiality - Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.²

DAS-managed System Asset - Information, hardware, software and services required to support state business, and identified during the risk assessment process as assets that need to be protected. Primary responsibility for managing these system assets may be assigned to DAS OIT personnel or other outside entities.

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.)³

Distributed Denial of Service (DDoS) - A Denial of Service technique that uses numerous hosts to perform the attack.⁴

Firmware - Computer programs and data stored in hardware, typically in read-only memory (ROM) or programmable read-only memory (PROM), such that the programs and data cannot be dynamically written or modified during execution of the programs.⁵

Incident - A security incident threatens the confidentiality, integrity or availability of state information resources.

Incident Handling - The mitigation of violations of security policies and recommended practices.⁶

Information Security and Privacy Incident Response - A security incident threatens the confidentiality, integrity or availability of state information resources. Privacy incidents are considered to be a subset of security incidents for the purposes of this policy.

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.⁷

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>>.

² *Ibid.*

³ “CNSS Instruction No. 4009, National Information Assurance (IA) Glossary,” Committee on National Security Systems, 26 April 2010 <http://www.ncsc.gov/publications/policy/docs/CNSSI_4009.pdf>.

⁴ *Ibid.*

⁵ *Ibid.*

⁶ Cichonski, Paul, Tom Millar, Tim Grance, Karen Scarfone, “National Institute of Standards and Technology Special Publication 800-61 Rev. 2 Computer Security Incident Handling Guide,” U.S. Department of Commerce National Institute of Standards and Technology, August, 2012 <<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>>.

⁷ “NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, Initial Public Draft,” U.S. Department of Commerce National Institute of Standards and Technology, February, 2012, <<http://csrc.nist.gov/publications/drafts/800-53-rev4/sp800-53-rev4-ipd.pdf>>.

Integrity - Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.⁸

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.⁹

Personally Identifiable Information (PII) - “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 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.

Service Owner - A service owner is responsible for the delivery (design, performance, integration), continual improvement and management of assigned IT services.

Supervisory Control and Data Acquisition Systems (SCADA) - Networks or systems generally used for industrial controls or to manage infrastructure such as pipelines and power systems.¹⁰

⁸ “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>>.

⁹ *Ibid.*

¹⁰ “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>.

Token - Something that the Claimant possesses and controls (typically a key or password) that is used to authenticate the Claimant's identity.¹¹

9.0 INQUIRIES

Direct inquiries about this policy to:

Office of Information Security & Privacy
Office of Information Technology
Ohio Department of Administrative Services
30 East Broad Street, 19th Floor

1.614.644.9391 | state.isp@das.ohio.gov

DAS Policies may be found online at
<http://das.ohio.gov/Divisions/AdministrativeSupport/EmployeeServices/DASPolicies.aspx>

Additional information regarding the Office of Information Security & Privacy may be found online at InfoSec.Ohio.Gov.

10.0 REVISION HISTORY

Date	Description
12/01/2009	New policy for DAS, replaces OIT policy dated 11/02/07.
12/05/2012	Policy reissued under Director Robert Blair.
10/10/2017	Policy updated to reflect current incident response practices and the content was moved into the current policy template.
10/10/2020	Scheduled policy review.

11.0 ATTACHMENTS

None.

¹¹ 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>>.