

# INFORMATION SECURITY AND PRIVACY POLICY SECURITY INCIDENT RESPONSE

---

IT POLICY NUMBER: 2100-07

EFFECTIVE DATE: 12/05/2012

APPROVED BY:

A handwritten signature in black ink, appearing to read "Robert Blair".

Robert Blair, Director  
Department of Administrative Services

## 1.0 PURPOSE

The purpose of this policy is to ensure that the Ohio Department of Administrative Services (DAS) implements and maintains an adequate security response capability for reported or identified security events and incidents.

## 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 owned or operated computer and telecommunications systems and the managers of DAS business units and IT systems who use or administer such systems. This policy does not apply to DAS customers.

## 3.0 BACKGROUND

Information technology (IT) is an integral part of how DAS conducts business and maintains information in support of its stated mission. As the use of technology increases, the threats associated with IT security incidents continue to grow. As a result, DAS must be prepared to respond when incidents occur. Lack of preparation can have significant consequences as organizations attempting to respond to an incident with limited or no advance planning may actually cause more damage. 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 for an incident and ensuring that the right resources are available are critical to DAS' ability to adequately detect, respond to and recover from an IT security incident.

## 4.0 REFERENCES

- 4.1. **Ohio IT Bulletin; ITB-2007.02; Data Encryption and Securing Sensitive Data:** This IT Bulletin provides guidance to agencies on protecting sensitive data.
- 4.2. **DAS/OIT Enterprise Procedure; OEP SEC.4001; Statewide Incident Response Reporting:** This statewide procedure defines the steps to be followed by State of Ohio agencies reporting information, computer system, or network security incidents.
- 4.3. **DAS Procedure; Incident Response:** This DAS procedure defines the steps to follow for DAS' response to any type of critical incident, including security incidents, that affects DAS' applications, systems, networks, infrastructure or capability to deliver services.
- 4.4. A glossary of terms found in this policy is included in Section **8.0 – Definitions**.

## 5.0 POLICY

DAS is issuing this policy to ensure compliance with related state policies and to protect DAS' IT resources. More detailed security standards and procedures supporting the implementation of this policy will be maintained separately.

The cornerstone of DAS' security incident response capability is the DAS Incident Response Procedure. Management shall ensure that the DAS Incident Response Procedure is followed whenever a security incident or other critical incident is reported or identified.

DAS shall implement additional incident response capabilities as they become feasible. As a minimum, such capabilities shall include the provisions of this DAS policy.

Should DAS experience a security event, which is a system anomaly; attempted breach; possible illegal activity; or possible serious wrongdoing related to a system, application, network, computer, or device capable of storing data, it shall have a structured means of evaluating that event to determine if it indeed rises to the level of an actual security incident, which is a verified breach or violation of an IT asset.

### 5.1 Preparation

DAS shall define procedures for how it will detect, evaluate and respond to security events, and report, prepare for, manage and recover from IT security incidents. Such procedures shall incorporate a DAS response plan based on the scope, impact and potential damage of an incident. DAS preparation procedures shall include:

- 5.1.1 Incident Response Team. DAS has defined and continues to develop an incident response team (IRT) that is lead by the DAS/OIT Incident Coordinator. The team includes Program Incident Coordinators and Technical Incident Coordinators and is responsible for responding to,

managing, supporting and participating in incident response activities. The IRT acts at the time of an information security incident to minimize and contain damage, gather evidence and resume normal processing. The team may also provide assistance to other agencies in the mitigation of incidents and vulnerabilities. Roles, responsibilities and levels of authority are defined for IRT members in the DAS Incident Response Procedure and DAS Incident Response Contact List.

- 5.1.2 IR Documentation. DAS has created an incident management guide documenting IRT roles, responsibilities and level of authority for resources and staff participating in DAS' incident response plan. The guide addresses security event detection, evaluation and response; and security incident reporting, communication methods, and escalation procedures. In the future it shall also address all aspects of an IR plan as defined in Section 5.2 of this policy.
- 5.1.3 Recovery Preparation. DAS shall evaluate what risks to DAS 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:
  - 5.1.3.1 System Back-ups. DAS Programs shall create and maintain trusted system, data and application back-ups. Back-ups shall be tested on a regular basis to maintain a high confidence of a successful recovery. Back-ups shall be created on a regular basis and securely maintained. For sensitive data, DAS Programs shall address the requirements found in Ohio IT Bulletin; ITB-2007.02; Data Encryption and Securing Sensitive Data.
  - 5.1.3.2 System and Application Software Versions. DAS Programs shall maintain verified copies of all critical system and application installation software. The Programs shall ensure the system and application software versions and security related patches are current and securely maintained.
  - 5.1.3.3 Configuration Redundancy. Redundant configurations can facilitate the recovery of IT systems or assets while preserving evidence of a compromised IT asset. All systems deemed mission critical shall have redundant configurations.
  - 5.1.3.4 System and Application Test Results. DAS shall maintain a file or log of trusted system or application test results such as cryptographic checksums or authoritative lists of services to increase the level of confidence of a restored system asset.

These procedures may be the same or be complementary to the procedures developed to address business continuity issues.

- 5.1.4 IR Contact List. DAS has developed and continues to refine and maintain an incident response contact list. The contact list shall include the names, telephone numbers, pager numbers, mobile telephone numbers, email addresses, organization names, titles, and incident response roles and responsibilities for all key incident response resources, including but not limited to IRT members, key DAS management personnel, public information officers, legal counsel, law enforcement officials, and Agency Incident Response Contacts.
- 5.1.5 Readiness Testing. DAS shall establish procedures for testing and evaluating incident response capabilities on a periodic basis. As a minimum, DAS shall conduct an incident response evaluation and readiness test on an annual basis.

## 5.2 Incident Response Plan

DAS has defined and continues to develop and maintain an IR plan to evaluate IT security events to determine if an event has become an incident and to detail DAS' IRT actions in response to an identified security incident. The plan is documented in DAS' Incident Response Procedure and DAS' Incident Response Contact List. The DAS IR plan shall include the following elements:

- 5.2.1 Event Evaluation. DAS shall determine how to evaluate IT security events. The evaluation process shall assess if an IT security incident has occurred and to what extent data or other state assets have been compromised. Events shall be investigated with the assumption that the event will be found to be an IT-specific security incident until proven otherwise. Security events such as fire, flood, civil disorder, natural disaster, bomb threat or other such environmental anomalies that are determined not to have risen to the level of a security incident shall nevertheless be handled in accordance with DAS' business continuity process as appropriate. DAS IT security event evaluation procedures shall include at a minimum:
  - 5.2.1.1 Security Events Log. An IT security event log shall be securely maintained. At a minimum, the log shall include who reported the event, when the event was reported, a description of the event, whether the event included illegal activity, serious wrongdoing, and/or missing or otherwise compromised sensitive data, how the event was identified, what actions were taken, and who performed each action.
  - 5.2.1.2 Event Data Collection and Analysis. As part of event evaluation, DAS shall collect and securely maintain information concerning

reported events to assess whether a security event is a general system anomaly or potential security incident. Data collection and analysis shall focus on identifying who, what, when, where and how of a reported security event. Collected information shall be properly documented and safeguarded. Evidence such as system and network log files, user files, system administrator logs and notes, back-up tapes and intrusion detection system (IDS) logs, alarms or alerts shall be securely maintained and the chain of custody preserved by:

- Ensuring the evidence has not been altered;
- Ensuring the evidence is accounted for at all times;
- Verifying the passage of evidence from one party to another is fully documented; and
- Verifying the passage of evidence from one location to another is fully documented.

5.2.1.3 Event Classification. DAS IR resources shall review the results of an event evaluation and determine if there is sufficient evidence to determine if an actual IT security incident has occurred. If sensitive data is compromised by accident or without an identified, specific attacker or vulnerability, the adverse event may still require treatment as a security incident to ensure proper handling, investigation, and notification. DAS IR plans shall be executed for security events that are determined to be security incidents. DAS shall determine an appropriate level of response regarding the impact, scope and potential damage of any incident. Such DAS procedures shall include at a minimum:

5.2.1.3.1 Security Incident Evidence File. An evidence file shall be created to log and maintain an inventory of all actions taken, action timestamps and correspondence associated with a security incident. The security incident evidence files shall be securely maintained and safeguarded throughout the incident response actions. Incident evidence shall be maintained and safeguarded to preserve the evidence chain of custody.

5.2.1.3.2 IR Communication. Individuals, agencies and organizations identified in DAS' IRT Contact List shall be notified in accordance with DAS' Incident Response Procedure. For incidents involving illegal activity, and/or serious wrongdoing (where appropriate), and/or missing or otherwise compromised sensitive data, the DAS/OIT Incident Coordinator shall verify that the DAS Chief Legal Counsel and the Ohio State

Highway Patrol are notified. For incidents involving missing or otherwise compromised sensitive data, the DAS/OIT Incident Coordinator shall verify that the Ohio State Chief Information Security Officer and State Chief Privacy Officer are notified. DAS shall contact Agency Incident Response Coordinators should an incident likely affect other agencies. Communication shall be on a need to know basis and shall be considered confidential information during a security incident investigation.

5.2.1.3.3 Forensic Back-ups. DAS shall develop criteria that will determine whether IRT resources shall create forensic back-ups of compromised systems. Any such back-ups shall be obtained using techniques consistent with retaining forensic evidence such as sector or binary techniques. Any such back-ups shall be maintained in a secure location and preserved following chain of custody requirements identified in Section 5.2.1.2 of this policy.

5.2.2 Incident Containment. DAS shall deploy containment strategies to identify and eliminate an incident's impact to compromised systems, limit the extent of the incident, prevent further damage and regain normal operations of affected systems. DAS containment measures should take into consideration the assessment of an incident including its scope, impact, and damage, results of the incident evaluation, DAS business continuity plans and DAS procedures regarding response methods. Containment measures shall also be evaluated against the potential loss or corruption of security incident evidence in the event the DAS elects to pursue the intruder for possible legal actions or remedy. Containment methods may include, but are not limited to:

- Ensuring redundant systems and data have not been compromised;
- Monitoring system and network activity;
- Disabling access to compromised shared file systems;
- Disabling specific system services;
- Changing passwords or disabling accounts;
- Temporarily shutting down the compromised or at risk systems; and
- Disconnecting compromised or at risk systems from the network.

5.2.3 Elimination. DAS shall develop and employ procedures to eliminate unauthorized access and remove unauthorized modifications prior to returning compromised systems to service. DAS shall ensure systems are protected against like or similar types of incidents in the future. Elimination methods may include, but are not limited to:

- Changing passwords on compromised systems. Highly recommended if evidence indicates the system password files were compromised.
- Disabling compromised accounts;
- Reinstalling compromised systems from trusted back-ups;
- Identifying and removing an intruder's access methods such as backdoors;
- Installing system patches for known weaknesses or vulnerabilities;
- Reinstalling system user files from trusted versions;
- Reinstalling system settings from trusted sources;
- Reinstalling system start-up routines from trusted versions; and
- Adjusting or deploying firewall or IDS technologies to detect access and intrusion methods.

5.2.4 Notification of a Personal Information Security Breach. DAS shall determine if the incident resulted in a breach of a system containing personal information as defined by Ohio Revised Code 1347.12 and then notify affected individuals as required by Ohio Revised Code 1347.12. All incidents involving missing or otherwise compromised sensitive and/or personal information shall be reported to the Ohio State Chief Information Security Officer and State Chief Privacy Officer.

5.2.5 Recovery. DAS shall evaluate and determine when to return compromised systems back to normal operations. Access to compromised system assets shall be limited to authorized personnel until the security incident has been contained and root cause of the incident eliminated. If DAS returns the system to operations before full analysis and elimination procedures are completed, DAS shall assess the risk to ongoing operations while increasing system monitoring and heightening security awareness. Analysis and elimination procedures shall be completed as soon as possible, recognizing DAS systems are vulnerable to another occurrence of the same type of intrusion. Recovery procedures shall address:

5.2.5.1 Recovery Requirements. DAS shall define the requirements to be met and their priority before returning an affected or compromised system to normal operations.

5.2.5.2 Validate Restored Systems. DAS shall validate the restored systems through system or application regression tests, user verification, penetration tests, vulnerability testing and test result comparisons.

5.2.5.3 Increased Security Awareness. DAS shall heighten awareness and monitor for a recurrence of the IT security incident.

5.2.6 Lessons Learned. DAS shall capture and disseminate incident lessons learned to reduce the possibility for similar incidents and thereby enhance the overall IT security posture. DAS shall establish a lessons learned capability by:

5.2.6.1 Post Mortem Analysis. In accordance with DAS' Incident Response Procedure, DAS shall perform a post mortem analysis and review meeting within five days of completing the incident investigation. Extended delays may reduce the effectiveness of relating critical information. Questions to be addressed may include, but are not limited to:

- Did detection and response systems work as intended? If not, what methods would have prevented the incident?
- Are there additional procedures that would have improved the ability to detect the incident?
- What improvements to existing procedures and tools would have aided in the response process?
- What improvements would have enhanced the ability to contain the incident?
- What correction procedures would have improved the effectiveness of the recovery process?
- What updates to DAS policies and procedures would have allowed the response and recovery processes to operate more smoothly?
- How could user and system administrator preparedness be improved?
- How could communication throughout the detection and response processes be improved?
- Was the incident identified during the DAS' risk assessment process as a potential threat?
- What was the impact in terms of financial loss, loss of public trust, legal liability or harm to public health and welfare?

Results of these points shall be documented and incorporated into a report for senior DAS management.

5.2.6.2 Lessons Learned Implementation. DAS shall apply as applicable new and improved methods from lessons learned in their post mortem analysis process.

5.2.6.3 Risk Assessment. DAS shall perform a new risk assessment if the impact of a security incident was significant.

5.2.6.4 Incident Reporting. Pursuant to DAS/OIT Enterprise Procedure OEP SEC.4001, "Statewide Incident Response Reporting," DAS/OIT

serves as Ohio's centralized reporting authority for IT security incidents and shall implement internal procedures to fulfill that role.

### 5.3 Legal Review

DAS shall conduct a legal review of incident response procedures. The review shall determine if IR procedures:

- Protect evidence chain of custody;
- Comply with overall DAS and state policies;
- Conform to federal, state or local laws; and
- Maintain the confidentiality of all investigative data and evidence.

### 5.4 Education & Awareness

DAS shall ensure that incident response concepts are addressed in education and awareness programs. The programs shall address:

- How to identify and report suspected intrusion;
- Use of response tools and environments in accordance with defined incident response roles and responsibilities;
- Communication methods;
- Existing and new intrusion threats; and
- Preserving the chain of custody for incident evidence.

## 6.0 PROCEDURES

Standards and procedures shall be developed at various levels within the DAS organization in order to effectively and efficiently implement this policy. The primary procedure governing DAS' security incident response is the DAS Incident Response Procedure.

## 7.0 COMPLIANCE

It is the responsibility of management to implement and ensure compliance with the laws, rules, policies, procedures, standards, and license agreements applicable to the use of IT resources within their functional areas.

## 8.0 DEFINITIONS

**Agency Incident Response Contacts** – These contacts are responsible for reporting incidents to the Office of Information Security and Privacy and for appropriately communicating incident related information within their agencies.

**Chain of Custody** - Defined actions taken to ensure that collected evidence has not been compromised, can be accounted for at all times and securely documents the passage of evidence from one party or location to another. Chain of custody procedures are essential for helping to preserve evidence for legal proceedings.

**Cryptographic Checksums** - A secret or coded value used to ensure data blocks are stored or transmitted without error. The value is created by calculating the binary values in a block of data using an algorithm, which is encoded and stored with the results with the data. Transmitted or retrieved data will be confirmed by recalculating the checksum

**DAS** – Department of Administrative Services.

**DAS Contractors** – For the purposes of this policy, DAS contractors are defined as contracted staff and vendor technicians.

**DAS Employees** – For the purposes of this policy, DAS employees are defined as all employees and representatives of DAS, whether they are permanent staff or temporary staff.

**DAS-owned** – Purchased with DAS funds or otherwise acquired by DAS; property of DAS.

**DAS-provided** or **DAS-supplied** – Made available to users by DAS.

**Elimination** - Defined step or process within an incident response plan with the goal of eradicating the root cause of a security incident.

**Event** - Any observable occurrence in a system or network. Examples of events include the system boot sequence, a system crash and packet flooding within a network. Events sometimes provide an indication that an incident is occurring.

**Forensic Back-ups** - Back-ups using techniques to generate an identical sector-by-sector back-up of a storage medium.

**Incident** - A reported security event or group of events that has proven to be a verified IT security breach, or a violation of IT security policies, or a threat to the security of system assets that results in at least one of the following categories:

- Loss of confidentiality of information
- Loss or theft of device capable of storing data
- 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

**Incident Response** - A structured and organized response to any IT security event or incident that threatens an agency's system assets including systems, networks and telecommunication systems.

**Incident Response Contact List** - A list of resources identified as part of an agency's incident response team. The contact list includes the names, contact numbers, organization, roles and responsibilities of all team members.

**Incident Response Team** - A group of professionals within an organization trained and chartered to respond to identified IT security incidents. The incident response team has both an investigative and problem solving component and should include management personnel with the authority to act, technical resources with the knowledge and expertise to rapidly diagnose and resolve problems, and communication personnel to keep appropriate individuals and organizations properly informed and develop public image strategies as necessary.

**IT Resources** – Any information technology resources, such as computer hardware and software, IT services, telecommunications equipment and services, networks, digital devices such as digital copiers and facsimile machines, supplies, and the Internet.

**Management** – Management refers to supervisory staff responsible for the completion of activities to fulfill DAS' mission. If Position A is shown as subordinate to Position B on the Table of Organization, then Position B is supervisory in nature for the purposes of this policy.

**OIT** – Office of Information Technology.

**Privately-owned** - Purchased with personal or corporate (vendor or contractor) funds; not provided by the state.

**Recovery** - A defined step or process within an incident response plan with the goal of returning the affected or compromised systems to normal operations.

**Risk Assessment** – A process for identifying, analyzing and responding to information technology security risks. Risk assessment attempts to maximize the results of positive events and minimize the results of negative events.

**Sensitive Data** – Any electronic information that a state agency maintains and must not disclose under penalty of law, or "personal information" that consists of any individual's name, including the last name along with the individual's first name or first initial, in combination with and linked to any one or more of the following data elements: social security number; driver's license number or state identification card number; or financial account number or credit or debit card number. Sensitive data also includes any other electronic information that the agency determines to be high-risk should the information be accessed by unauthorized parties.

**State-owned** - Purchased with state funds or otherwise acquired by the state; property of the state of Ohio.

**System Assets** – System assets include information, hardware, software, and services required to support the business of DAS and identified during the risk assessment process as assets that require protection.

**Users** - For the purposes of this policy, users are defined as employees, contractors, temporary personnel and other agents of the state who administer or use privately-owned (if authorized) or state-owned IT Resources on behalf of the state.

## 9.0 RELATED RESOURCES

OIT/Risk Management Services Incident Management Guide

## 10.0 INQUIRIES

For information regarding this policy, please contact:

Office of Information Security & Privacy  
Office of Information Technology  
Ohio Department of Administrative Services  
30 East Broad Street, Suite 4083  
Columbus, Ohio 43215  
Telephone: 614.644.9391  
Email: [state.isp@oit.ohio.gov](mailto:state.isp@oit.ohio.gov)  
Web: [infosec.ohio.gov](http://infosec.ohio.gov)

Department of Administrative Services policies can be found online at:

<http://das.ohio.gov/Divisions/DirectorsOffice/EmployeesServices/DASPolicies/tabid/463/Default.aspx>

## 11.0 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.

## 12.0 ATTACHMENTS

None.