



---

# Information Security Incident Response Plan

---

November 3, 2008

**Bret West, Administrator, Operations Division (DAS Chief Information Officer)  
(503) 378-2349, ext. 287**

**Debbie Fery, Manager, Technology Support Center (DAS Chief Information Security Officer)  
(503) 373-0938**

## TABLE OF CONTENTS

Introduction.....	3
Authority.....	4
Terms and Definitions.....	4
Roles and Responsibilities.....	5
Program.....	6
Education and Awareness.....	10
Communications.....	10
Compliance.....	11
Implementation.....	12
Approval.....	14
Incident Report Form.....	Appendix A

## Introduction

---

ORS 182.122 requires agencies to develop the capacity to respond to incidents that involve the security of information. Agencies must implement forensic techniques and remedies, and consider lessons learned. The statute also requires reporting incidents and plans to the Enterprise Security Office. The Oregon Consumer Identity Theft Protection Act (ORS 646A.600) requires agencies to take specific actions in cases where compromise of personally identifiable information has occurred. This plan addresses these requirements.

The Department of Administrative Services (DAS) has developed this Information Security Incident Response Plan to implement its incident-response processes and procedures effectively, and to ensure that DAS employees understand them. The intent of this document is to:

- describe the process of responding to an incident,
- educate employees, and
- build awareness of security requirements.

An incident response plan brings together and organizes the resources for dealing with any event that harms or threatens the security of information assets. Such an event may be a malicious code attack, an unauthorized access to information or systems, the unauthorized use of services, a denial of service attack, or a hoax. The goal is to facilitate quick and efficient response to incidents, and to limit their impact while protecting the state's information assets. The plan defines roles and responsibilities, documents the steps necessary for effectively and efficiently managing an information security incident, and defines channels of communication. The plan also prescribes the education needed to achieve these objectives.

## Authority

---

Statewide information security policies:

Policy Number	Policy Title	Effective Date
107-004-050	Information Asset Classification	1/31/2008
107-004-051	Controlling Portable and Removable Storage Devices	7/30/2007
107-004-052	Information Security	7/30/2007
107-004-053	Employee Security	7/30/2007
107-004-100	Transporting Information Assets	1/31/2008
107-004-110	Acceptable Use of State Information Assets	10/16/2007
107-004-xxx	Information Security Incident Response	draft

DAS information security policies:

Policy Number	Policy Title	Effective Date
107-01-010	Acceptable Use of DAS Information Assets	8/14/08
107-01-070	Approval For Purchase of LAN/Desktop Products or Services	10/22/01
107-01-080	Information Technology Security	6/22/00
107-01-130	Archive and Records Management	11/20/05
107-01-140	Passwords	04/04/07
107-01-180	Information Asset Classification and Transportation	5/28/08
107-01-190	Information Security Incident Response	November 2008

## Terms and Definitions

---

**Asset:** Anything that has value to the agency.

**Control:** The means of managing risk, including policies, procedures, guidelines, practices or organizational structures. They may be administrative, technical, management, or legal in nature.

**Incident:** A single event or a series of unwanted or unexpected events that involve information security (see definition of "information security event"), causing harm or threatening information assets and requiring non-routine preventative or corrective action.

**Incident Response Plan:** A written document that specifies the approach to addressing and managing incidents.

**Incident Response Policy:** A written document that defines organizational structure for incident response, defines roles and responsibilities, and lists the requirements for responding to and reporting incidents.

**Incident Response Procedures:** Written document(s) that specify the series of steps taken in response to incidents.

**Incident Response Program:** The combination of incident response policy, plan, and procedures.

**Information:** Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, including electronic, paper and verbal communication.

**Information Security:** Preservation of confidentiality, integrity and availability of information; security procedures should also ensure that information is authentic and reliable, and that it comes from an accountable source.

**Information Security Event:** An abnormal, observable, and measurable occurrence involving an information asset.

**Risk:** The possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood.

**Threat:** A potential cause of an unwanted incident, which may result in harm to a system or the agency.

## **Roles and Responsibilities**

---

**Agency Director:** This person is responsible for information security in the agency, which means reducing exposure to risks and ensuring that the agency's activities do not introduce undue risk to the enterprise. The director must also ensure compliance with state enterprise security policies, standards, and security initiatives. The director also ensures compliance with state and federal regulations.

**Client Agencies:** State agencies that use the DAS Technology Support Center (TSC) for LAN/Desktop services.

**DAS Chief Information Officer (DAS CIO):** This person establishes and implements the overall DAS information security plan. The CIO is also responsible for convening the DASIRT when an incident occurs.

**DAS Chief Information Security Officer (DAS CISO):** This person implements security efforts within DAS. The CISO is responsible for communicating with the State Incident Response Team (SIRT) within 24 hours of an incident, and for coordinating the agency's actions with SIRT in response to an incident that involves information security.

**DAS Incident Response Team (DASIRT):** The DASIRT responds to any information security incident that affects DAS. The team then develops an appropriate action plan. DASIRT is responsible for gathering agency information about the incident, aggregating that information, tracking it and reporting it. DASIRT safeguards the incident information entrusted to it. DASIRT is not a standing organization. The DAS CIO forms a new DASIRT whenever an incident occurs. At a minimum, a DASIRT will consist of:

- DAS Chief Information Security Officer
- DAS Chief Information Officer
- Division administrator (or designee) owning compromised data
- DAS Public Information Officer
- If needed, the CIO will add other staff resources to the DASIRT; additional membership may include staff from Employee Services, Technology Support Center (TSC), Enterprise Application Services, Department of Justice, and the State Data Center.

**Incident Commander:** When an incident occurs, this person leads the DASIRT response. The DAS CIO will decide who serves as Incident Commander when he or she convenes the DASIRT.

**Information Owner:** This person creates initial information classification, approves decisions on controls and access privileges, performs periodic reclassification, and ensures regular reviews for value and updates to manage changes to risk.

**User:** This person is responsible for complying with policies, procedures and practices.

## Program

---

Managing information security within DAS is a complex matter. Two divisions are responsible for statewide security:

- The Enterprise Information Strategy and Policy Division (EISPD) establishes statewide security policy and helps agencies implement statewide policies.
- The State Data Center (SDC) implements security policies and practices for all agencies that use the SDC infrastructure.

Internally, the DAS Operations Division (DAS Ops) is responsible for implementing statewide policies, establishing DAS policies, and ensuring that information assets are secure. The Operations Division Administrator serves as DAS' Chief Information Officer (CIO); the Technology Support Center Manager serves as DAS' Chief Information Security Officer (CISO). These two positions work with staff from across the agency on information security issues.

The DAS Information Technology Management Council provides the strategic direction for DAS information technology and security. Council membership includes at least one representative from every DAS division; several DAS division administrators are members of the council, as is the DAS Chief Audit Executive. The council meets monthly.

Typically, IT policy development uses the following process:

1. DAS CIO identifies the need for a security policy
2. The council considers an initial draft of the policy. Discussion occurs. A subcommittee refines the draft
3. Subcommittees work on revisions and develop a final recommendation
4. The committee discusses evolving policy and develops a final product
5. The DAS CIO presents committee recommendation to DAS Executive Team
6. The DAS Director signs final policy
7. The Director's Office communicates final policies to staff and posts them on the DAS Web site. In some cases, supervisors must obtain employees' signatures to verify they have read the policies and understand them.

As in most organizations, the CIO and CISO do not own most DAS data. The DAS policy on information asset classification and transportation places responsibility for assessing risk and for taking appropriate actions to mitigate risk with data owners throughout the agency.

The CIO uses several vehicles for communicating new policies and other security-related information to DAS employees. Messages on information security appear in the monthly DAS internal newsletter. Security is an agenda item at monthly all-DAS supervisors meetings. E-mails to all staff go out periodically when issues surface, and when the Enterprise Security Office (ESO) sends out "brandable" newsletters. Also, a link to all operating policies appears on the DAS home page.

The Incident Response Program includes this plan and the relevant policies and procedures. DAS employees should read the following documents to gain a complete understanding of the program:

1. DAS Information Security Incident Response, Policy Number 107-01-190, located on the DAS Web site at [http://oregon.gov/DAS/OP/internal\\_policies.shtml](http://oregon.gov/DAS/OP/internal_policies.shtml).
2. DAS Procedure: The Incident Report appears as Appendix A to this plan.

**The Enterprise Security Office must receive notice within 24 hours of detecting an incident.**

When an incident involving security of information occurs, responders will quickly communicate with the appropriate people in order to allow timely corrective action. This plan shows how DAS will handle response to an incident, incident communication, incident response plan testing, training for response resources and awareness training.

The DAS CIO will conduct an annual review of the Information Security Incident Response policy, plan and procedures. A review will also take place if significant changes occur in the mean time. The goal of the reviews is to ensure adequacy and effectiveness of the incident response program. The DAS CIO is responsible for development, review, evaluation, and testing of all elements of the plan. Reviews will cover the following:

- Assessing opportunities for improvement
- Integrating lessons learned from prior incidents and testing
- Changes in DAS' environment
- New threats and risks
- Business circumstances
- Legal and policy implications
- Technical environment

To test the incident response plan and verify DASIRT's ability to execute, the DAS CIO will plan and conduct an annual exercise. Specifically, this exercise will include the following:

- Use the plan to test the team response.
- Identify needed updates to the plan.
- Verify contact numbers.
- Verify the use of sound forensics procedures (i.e., examine acquired evidence).

Client agencies of the DAS TSC are the owners of their own data. Client agencies may use this plan as a model for their own incident response plans. The directors of client agencies will decide the membership of an incident response team.

Identification

Identification of an incident is the process of analyzing an event and determining whether it is "normal." If the process reveals that the event is a potentially harmful incident, the DAS CISO will take appropriate action. The DAS CISO routinely examines events to determine their impact and their potential for harm. The DAS CISO is responsible for identification of an incident.

The term "incident" refers to an adverse event that affects one or more of DAS' information assets. The term also applies to the threat of such an event. Examples include the following:

- Unauthorized use
- Denial of service

- Malicious code
- Network system failures (widespread)
- Application system failures (widespread)
- Unauthorized disclosure or loss of information
- Information security breach
- Other

Incidents may result from any of the following:

- Intentional and unintentional acts
- Actions of state employees
- Actions of vendors or constituents
- Actions of third parties
- External or internal acts
- Credit card fraud
- Potential violations of statewide or DAS internal policies
- Natural disasters and power failures
- Acts related to violence, warfare or terrorism
- Serious wrongdoing
- Loss of building key card
- Other

### Incident Classification

Once the DAS CISO determines an event to be an incident, several methods exist for classifying the incident. The DAS CISO considers the following factors when evaluating incidents:

- Criticality of systems that are (or could be) made unavailable
- Value of the information compromised (if any)
- Number of people or functions impacted
- Business considerations
- Public relations
- Enterprise impact
- Multi-agency scope

The DASIRT is responsible for classifying an incident.

### Triage

The objective of the triage process is to gather information, assess the nature of an incident and begin making decisions about how to respond to it. Preventing the situation from becoming more severe is critical. The following factors receive consideration during triage:

- What type of incident has occurred?
- Who is involved?
- What is the scope?
- What is the urgency?
- What is the impact thus far?
- What is the projected impact?
- What can be done to contain the incident?
- Are there other vulnerable or affected systems?

- What are the effects of the incident?
- What actions have been taken?
- Recommendations for proceeding.
- Analysis to identify the root cause of the incident.

The DASIRT is responsible for incident triage.

### Evidence Preservation

Carefully balancing the need to restore operations against the need to preserve evidence is a critical part of incident response. Gathering evidence and preserving it are essential for proper identification of an incident, and for business recovery. Follow-up activities, such as personnel actions or criminal prosecution, also rely on gathering and preserving evidence.

The DAS CISO is responsible for leading efforts to preserve evidence. Technology Support Center staff will provide the needed technical expertise. Should additional expertise prove necessary, the DAS CISO will contact ESO for help.

### Forensics

If an incident involves computers, the DAS CISO will direct TSC to analyze computing devices to identify the cause, or to analyze and preserve evidence.

The DASIRT will practice the following general forensic guidelines:

- Keep good records of observations and actions taken.
- Make forensically-sound images of systems and retain them in a secure place.
- Establish chain of custody for evidence.
- Provide basic forensic training to incident response staff, especially in preservation of evidence.

### Threat/Vulnerability Eradication

After an incident, efforts will focus on identifying, removing and repairing the vulnerability that led to the incident, and thoroughly cleaning the system. To do this, responders must quickly identify vulnerability to ensure the incident does not recur. The goal is to prepare for the resumption of normal operations with confidence that the initial problem has been fixed. Data owners are responsible for working with the DAS CISO to develop and implement a remediation plan for every incident.

### Confirm Elimination of the Threat or Vulnerability

After removal or elimination of the cause of an incident, and after restoration of data or related information, the next priority is to confirm the mitigation of all threats and vulnerability, and to verify that new threats have not emerged. The DAS CISO and data owner will be jointly responsible for confirming elimination of all threats and vulnerability.

### Resumption of Operations

Resuming operations is a business decision, but the preceding steps are critical to ensure that resuming operations is safe. Division administrators must consult with data owners to decide when resumption will occur. Division administrators have responsibility for notifying the DAS CISO that the incident is closed.

## Post-incident Activities

Following every incident, the DAS CIO will lead an after-action analysis. The analysis may consist of one or more meetings or reports. The purpose of the analysis is to give participants an opportunity to share and document details about the incident, and to make use of lessons learned. The meetings should occur within one week of closing the incident. The DAS CIO will schedule these meetings and will determine who should attend, based on the details of each incident. Invitees may include the DASIRT, SIRT, Employee Services representative(s), the DAS PIO, DAS Director or Deputy, staff from other agencies, or any other person involved in addressing the incident.

## Education and Awareness

---

DAS' education and awareness programs must address incident response roles and responsibilities. The programs should cover the following:

- Users' awareness: DAS' all-supervisors meetings include discussion of information security issues. DAS' internal newsletter also serves as a forum for discussing such issues. DAS leadership will roll out new policies, including security policies, to staff through e-mail. Supervisors must ensure that each staff member reads and understands DAS information policies. Using a tri-fold brochure and prominent Web presence, the DAS CIO will roll out this plan to all staff. Supervisors will distribute paper copies to staff who do not have access to computers.
- Education: Training is essential for standing members of the DASIRT, for data owners, and for division administrators. Specific training plans will be developed for standing members and for those employees likely to be involved in an incident.

## Communications

---

Because of the sensitive and confidential nature of information and communication surrounding an incident, all communication must take place through secure channels. Communicate details of any incident only face-to-face or by phone. Do not communicate details by e-mail, voice mail messages or interagency shuttle mail. If you must exchange reports and data electronically, use encryption. Label all relevant material ***“Confidential: Exempt from Public Records Law.”***

The DASIRT will take responsibility for establishing internal and external communications plans for security incidents. Because the details and implications of each incident will vary, the DASIRT will develop specific plans for each incident.

The DAS Public Information Officer is responsible for coordinating internal and external communications. Among the factors to be considered when developing a communications plan are the following:

- Requirements of the Oregon Consumer Identity Theft Protection Act (**note: actions taken in response to violations or potential violations of this Act must be coordinated in advance with the Enterprise Security Office**)
- Requirements of regulations such as Payment Card Industry – Data Security Standards (PCI), Health Insurance Portability and Accountability Act (HIPPA), Internal Revenue Service regulations, etc.
- Additional risks incurred by releasing specific incident information

- Asset classification level of the information involved in an incident
- Agency credibility
- Determining who needs to know various levels of detail
- Managing the message in a positive manner.

The DAS PIO will be responsible for media relations during incidents. The DAS PIO, as a DASIRT team member, will decide who talks to the media and will lead efforts to develop the primary message and media response for each incident. No employee may discuss an incident with anyone until receiving specific approval from the DAS PIO, DAS CIO, DAS Director, or DAS Deputy Director. This restriction does not apply to discussions among DAS staff and the ESO or State Data Center as part of the investigation.

Only the following people should receive reports of the details of any incident:

- Those people who need the information to conduct the investigation
- Those who need the information to take corrective action
- Those who need the information to prepare a communications plan.

The purpose of limiting the flow of information is to contain risks to compromised systems, the agency, or customers and vendors.

Depending on the circumstances of an incident, the following contacts may be relevant:

Contact	Phone Number
DAS Employee Services Manager	(503) 378-4006
DAS Director's Office	(503) 378-3104
State Chief Information Security Officer	(503) 378-4896
Oregon State Police Criminal Lieutenant	(503) 378-3720
Department of Justice	(503) 947-4540
DAS Risk Management	(503) 373-7475
Other affected agencies	Varies
If security breach affects more than 1,000 consumers, contact all major consumer-reporting agencies that compile and maintain reports on consumers on a nationwide basis; inform them of the timing, distribution and content of the notification given to the consumers.	
Contact the credit monitoring bureaus in advance if directing potential victims to call them:	
• Equifax	1-800-525-6285
• Experian	1-888-397-3742
• TransUnion	1-800-680-7289

## Compliance

---

DAS is responsible for implementing and ensuring compliance with all applicable laws, rules, policies, and regulations.

- ORS 182.122 – Information Systems Security in Executive Department

- ORS 646A.600 – Oregon Consumer Identity Theft Protection Act. DAS maintains personal information of consumers and will notify customers if personal information has been subject to a security breach in accordance with the Act. The notification will occur soon as possible, in one of the following manners:
  - Written notification
  - Electronic, if this is the customary means of communication between you and your customer
  - Telephone notice provided that you can directly contact your customer.

Delay notification if a law enforcement agency determines that it will impede a criminal investigation.

If a federal, state or local law enforcement agency determines there is no reasonable likelihood of harm to consumers, or if the personal information was encrypted or made unreadable, notification is not required.

#### *Substitute notice*

Substitute notice is permissible if the cost of notifying customers would exceed \$250,000, or if the number of people to be contacted is greater than 350,000. Substitute notice is also permissible if you lack the means to contact consumers. Substitute notice consists of the following:

- Conspicuous posting of the notice or a link to the notice on your Web site
- Notification to major statewide Oregon television and newspaper media

#### *Notifying credit-reporting agencies*

If the security breach affects more than 1,000 consumers, DAS will report to all nationwide credit-reporting agencies, without reasonable delay, the timing, distribution, and the content of the notice given to the affected consumers.

- OAR 125-800-005 through 125-800-0020 – State Information Security.
- Payment Card Industry-Data Security Standards (PCI). PCI requires organizations to develop an incident response plan and be prepared to respond immediately to a data breach by following the plan, which must address business recovery and continuity, data backup processes, and communication strategies. This plan is intended to fulfill those requirements.
- Health Insurance Portability and Accountability Act (HIPAA). HIPAA requires entities to implement policies and procedures to address security incidents, requires the creation of a security incident response team, or another reasonable and appropriate response and reporting mechanism. This plan is intended to fulfill those requirements.

In addition to the laws and regulations reported above, DAS must also follow all applicable statewide information security policies. The tables on page 4 of this document provide the statewide and internal policies that must be followed.

## **Implementation**

---

The DASIRT is committed to formulating and implementing appropriate response strategies. This plan addresses that commitment by giving direction and support for the DAS Information Security Incident Response policy.

DASIRT will:


- Respond to DAS information security incidents.

- Develop and maintain trained technical staff with the capability to forensically gather and analyze evidence while observing necessary evidence-preservation practices.
- Test the incident response plan and verify DASIRT's ability to execute.
- Maintain a comprehensive list of key contacts that is regularly updated with status information.

The DAS CIO and DAS CISO will be responsible for reviewing, testing and implementing this plan. Review of the plan will occur annually, and testing of the plan will take place at least once every two years.

Approval

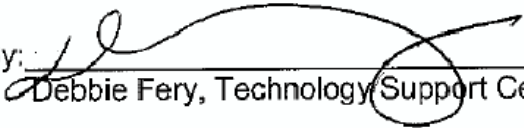
---

By:   
Scott Harra, DAS Administrator

11/4/08  
Date

By:   
Bret West, Operations Division Administrator (DAS CIO)

11/6/08  
Date

By:   
Debbie Fery, Technology Support Center Manager (DAS CISO)

11-6-08  
Date

## INCIDENT REPORT – Appendix A

<b>Initial Call</b> <i>(General information – no details of incident)</i>	
<b>Reported:</b> Date:	Time:
<b>Reported by</b>	
Name:	Title:
Agency/Department:	Location:
Phone:	Secondary Phone:
<b>Other Contacts</b>	
Name/Title:	Phone:
Name/Title:	Phone:
<b>Assistance from DAS CISO needed with the incident? Timeframe?</b>	
<b>Agency Priority:</b>	
<b>DASIRT</b> <i>(internal use only)</i>	
<b>Date and Time of Call Back to Initiator:</b>	
<b>Date and Time Incident Occurred:</b>	
<b>Type:</b> <input type="checkbox"/> Electronic <input type="checkbox"/> Paper <input type="checkbox"/> Verbal	
<b>PII Disclosed:</b> <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Unknown (Personally Identifiable Information) John Doe <u>or</u> J Doe <b><i>Plus</i></b> SS# <u>or</u> Driver's License/State ID <u>or</u> Passport # <u>or</u> financial account #/cc#/dc# with pw/pin/security code	
<b>Category:</b>	
<input type="checkbox"/> Malware	<input type="checkbox"/> Hack <input type="checkbox"/> DoS
<input type="checkbox"/> Web Defacement	<input type="checkbox"/> Unauthorized Access
<input type="checkbox"/> Information Disclosed	<input type="checkbox"/> Lost <input type="checkbox"/> Stolen
<b>Multi-agency:</b> <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Unknown	
<b>Compliance Regulations (HIPAA, PCI, IRS):</b>	
<b>Incident Description:</b>	
<b>System(s) Affected:</b>	
<input type="checkbox"/> N/A	
<b>Impact:</b>	

<b>What is the current status of the incident?</b>
<b>Who has been notified of the incident (director, Security Office, CIO)?</b>
<b>Additional contacts:</b>
<b>Assistance or recommendations:</b> <input type="checkbox"/> N/A
<b>What files/logs need to be preserved for investigation?</b> <input type="checkbox"/> N/A
<b>Actions taken so far and by whom:</b>
<b>DASIRT Team members:</b>
<b>Next Steps:</b>
<b>Additional Notes:</b>
<b>SDC Security Contacted:</b> <input type="checkbox"/> Yes <input type="checkbox"/> No <b>Details:</b>
<b>Incident Handler:</b>
<b>Case Closed:</b> <input type="checkbox"/> Yes <input type="checkbox"/> No <b>Details:</b>

**Lessons Learned:**