Department of Administrative Services
Security Incident Response Plan
5/23/08

The purpose of this plan is to protect the confidentiality, integrity and availability of DAS data and clearly outline roles and responsibilities in the event of a security incident.

A security incident is a single or a series of unwanted or unexpected information security events that result in harm, or pose a significant threat of harm to information assets or data, and require non-routine preventative or corrective action.

An information security event is an observable, measurable occurrence in an information asset or data that is a deviation from normal operations.

Examples of security incidents include:

- an unauthorized acquisition of electronic or hard copy data that materially compromises the security, confidentiality, or integrity of level 3 or level 4 data owned by the Department of Administrative Services;
- a loss of physical assets such as keycards or ID badges that could lead to unauthorized access to restricted areas or mobile computing devices which may contain sensitive information;
- defacing a DAS Web site;
- password alterations not initiated by the user;
- infection of a workstation from a virus, worm, spyware or other malicious software;
- Internet browser pop-ups that cannot be closed.

A security incident can have significant consequences for our customers, state employees, and the agency. In the event of a security incident, staff members must immediately take the following steps (in this order):

1. Report the incident to your supervisor or division administrator.

2. Do not continue working on a compromised computer. In the case of a physical security incident, do not continue working in the area as this may destroy useful information. Do not turn off a compromised computer.

3. The supervisor or division administrator should immediately call the DAS Security Officer, (503) 373-0938, or the DAS Operations Division Administrator, (503) 378-2349, ext. 287. The DAS Security Officer will gather enough information to lock access, notify others who can lock access, contact vendors who can turn off access, etc. The goal is to determine the specific details of the breach , the form of breach, the level of data involved, the potential to gain other access to other systems, and other necessary information.

4. If personally identifiable information is compromised during an incident, the DAS CIO will begin the process mandated under ORS 646A.600-628.

5. DAS Security Officer contacts the DAS CIO and Enterprise Security Office (ESO). ESO must be contacted within 24 hours of confirmation of a security incident.

6. The DAS CIO shall notify the DAS Director and/or Deputy Director.

7. The DAS Security Officer will coordinate investigations with the ESO Incident Response Team.

8. The DAS Director/Deputy Director will work with the DAS Public Information Officer to determine, depending upon the extent and the classification level of the breach, whether public notification is warranted.

9. Determine whether any internal regular users of the data set must know about the incident; if so, notify "need to know" users that data has been compromised or exposed.

10. DAS Security Officer completes the attached Incident Report within 8 business hours and submits to the ESO. After the investigation, ESO and or the DAS Security Officer will work with the business unit and or owners of the data, or systems involved, or review business processes to reduce the risk of this breach occurring again.

Technical staff involved in an investigation of a security breach must adhere to the following guidelines:

- If the breach involved electronic systems, **do not** access or alter compromised systems (e.g., do not log on or change passwords; do not log in as ROOT).
- Do not turn off the compromised machine. Instead, isolate compromised systems from the network (e.g., unplug the cable).
- Preserve logs and electronic evidence.
- Log all actions taken after the breach is detected.
- If using a wireless network, change SSID on the AP and other machines that may be using this connection (with the exception of any systems believed to be compromised).
- Be on high alert and monitor all systems that may be connected to the security breach.
- If the breach involves physical data on paper, on a laptop, mobile device, or physical media, the owner or person in most recently in possession of the data should note the data involved and the circumstances of the breach (e.g., time, place, and any other pertinent information).

SECURITY INCIDENT REPORT

Department of Administrative Services

Reported by:	Phone Number:
Date:	Time:

Division:

Classification level of data involved in incident:

Number of individuals affected:

Specific data elements and form involved:

Did the breach involve credit card transaction(s)?

Did the breach involve personally identifiable information (such as social security numbers)?

Describe what happened:

What is has been done to limit risk (within 2 hours of report of breach)?

What was done after the data breach was discovered?

How did the person reporting the event come to find out about the breach?

Post-Incident Review and Outcomes