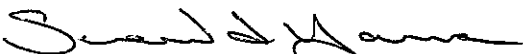


| | |
|---|---------------------------------|
| SUBJECT: Information Security Incident Response | NUMBER: 107-01-190 |
| DIVISION: Operations Division | EFFECTIVE DATE: 11/18/08 |
| APPROVED:  | |

| | |
|--------------------------------------|---|
| <p><u>POLICY/PURPOSE:</u></p> | <p>Policy: The Department of Administrative Services (DAS) has established an incident response program to respond to electronic, paper or verbal information security incidents. All divisions and all employees must follow the DAS Incident Response Plan (IRP) whenever an information security incident is suspected or actually occurs.</p> <p>Purpose: The purpose of this policy is to create effective responses to information security incidents that affect the availability, integrity, or confidentiality of the Department of Administrative Services' (DAS) information assets. The policy defines the structure for incident response, roles and responsibilities, and the requirements for reporting incidents.</p> <p>Staff must immediately report incidents that involve information security, along with assessments of vulnerability and risk, to the DAS Chief Information Security Officer (CISO). Timely reporting enables prompt corrective action and allows for thorough information gathering and reporting.</p> <p><u>Reporting Information Security Incidents</u> The DAS CISO must report security incidents to the DAS Chief Information Officer (CIO), DAS Director, and the SIRT within 24 hours of occurrence. The CISO will communicate with the SIRT to coordinate, investigate, and respond to an information security incident when needed.</p> <p><u>Information Security Incident Response Plan</u> DAS has developed an Incident Response Plan (IRP) to respond to agency incidents. The plan appears on the DAS website at http://oregon.gov/DAS/OP/docs/policy/internal/DAS Incident Response Plan.pdf. The plan includes roles and responsibilities, processes, and procedures for handling information security incidents.</p> |
| <p><u>AUTHORITY:</u></p> | <p>Enterprise Information Strategy and Policy Division Statewide Policy 107-004-120, Information Security Incident Response; ORS 182.122; OAR 125-800-005, 125-800-0010 and 125-800-0020.</p> |
| <p><u>APPLICABILITY:</u></p> | <p>This policy applies to all DAS divisions and all DAS employees. This policy does not apply when staff members are involved in investigations of non-DAS incidents. Investigations of non-DAS incidents follow the incident response plan(s) of the other agency(s) involved.</p> |
| <p><u>DEFINITIONS:</u></p> | <p>Asset: Anything that has value to the organization.</p> <p>Availability: The reliability and accessibility of information assets and resources to authorized individuals in a timely manner.</p> |

DEFINITIONS

CONT:

Confidentiality: A security principle that works to ensure that information is not disclosed to unauthorized subjects.

Incident: A single or a series of unwanted or unexpected information security events (see definition of "information security event") that result in harm, or pose a significant threat of harm to information assets, an agency, or third party and requires non-routine preventative or corrective action.

Incident Response Plan: Written document that states the approach to addressing and managing incidents.

Incident Response Policy: 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) of the series of steps taken when responding to incidents.

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

Information: Any knowledge 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. In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.

Information Security Event: An observable, measurable occurrence in respect to an information asset that is a deviation from normal operations.

Information Security Incident: See definition of "Incident."

Integrity: A security principle that makes sure that information and systems are not modified maliciously or accidentally.

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.

GUIDELINES:

- I. Reportable incidents must meet all four of the criterion below:
 - Involves information security (see definitions)
 - Is unwanted, unexpected, or accidental
 - Shows harm, intent to harm, or significant threat of harm
 - Response requires non-routine action

DAS Internal Policy

Information Security Incident Response

107-01-190

| | |
|--------------------|---|
| | <p>Reporting is mandatory for any incident that meets all these criteria. Reporting by DAS staff is recommended for any incident meeting at least one but fewer than all four criteria. The DAS Information Security Incident Response Plan provides detailed reporting requirements.</p> <p>Examples of non-reportable incidents include the following:</p> <ul style="list-style-type: none"> • Criminal violations with no information security component, such as theft of a car (no information security involved) • Increased Web site activity, due to popularity, that leads to site unavailability (not unwanted or unexpected) • Briefcase containing publicly disclosable information is lost (no harm, no intent to harm, or no significant threat of harm) • Computer virus detected on a workstation that is successfully contained by anti-virus software (no non-routine action required) • SPOTS card fraud/losses (routine process already established with U.S. Bank) <p>Examples of reportable incidents include the following:</p> <ul style="list-style-type: none"> • Any incident relevant to the Oregon Consumer Identity Theft Protection Act • Lost or stolen documents containing sensitive information • Conversation containing sensitive information overheard by unauthorized person who discloses the information to the public • A virus or worm has become widespread • Web site defaced • Unauthorized access to information • Any kind of sabotage that effects information • Denial of service attacks • Loss of building key card |
| <p>II.</p> | <p>If an employee is unsure whether an information security event is an incident, err on the side of caution and report the event to your supervisor and the DAS CISO per established procedures.</p> |
| <p>III.</p> | <p>Employees may report security incidents anonymously by calling the Enterprise Security Office 24-hour Hotline at (503) 378-5930. Employees who report anonymously must be aware that they will not receive any feedback on the status of any investigation. Employees reporting anonymously should also be aware that they might become involved as the investigation progresses.</p> |