This policy creates effective information security incidents response and handling capabilities for state agencies. Effective incident response and handling protects the availability, integrity, or confidentiality of state information assets. The policy sets out a structure for incident response and reporting. The policy identifies roles and responsibilities.

OAR 125-800-0020 directs Department of Administrative Services (DAS) to create a State Incident Response Team (SIRT). Under this policy agencies must quickly communicate information security incidents to designated agency staff and SIRT. Quick reporting enables timely corrective action.

Each agency will establish capabilities to respond to information security incidents involving information in any form whether electronic, data, paper, or verbal. Agencies may establish this capability by using internal or a combination of internal and external resources.

Agency capabilities at a minimum must include:
- An incident response plan
- Processes and procedures to implement the incident response plan
- A point of contact to interface with the State Incident Response Team (SIRT)

Agency incident response plan must identify:
- Incident response roles and responsibilities
- Resources and procedures for incident:
  - Preparation and planning
  - Monitoring
  - Identification
  - Evaluation
  - Reporting
  - Response
  - Investigation
  - Recovery and remediation
  - Follow-up and lessons learned
  - Internal and external incident communications
- Awareness training for information security incident responsibilities, identification and reporting
- Training for designated response resources
- Process for testing and updating plan periodically

Statewide Incident Response Team:
Primary members of SIRT are Enterprise Security Office (ESO) staff, State Data Center (SDC) staff, and other agencies as needed or required by law. ESO will be the point of contact for SIRT.
The SIRT will be identified as the Oregon State Incident Response Team to ensure clear communication when working with other agencies or jurisdictions.

**Reporting Information Security Incidents**
Each agency must report information security incidents no later than 24 hours after discovery. Agency point of contact will work with ESO to establish method of reporting. The SIRT will communicate with the agency point of contact to coordinate, investigate, and respond to an information security incident when needed.

**Roles and Responsibilities**

**DAS:**
ESO: The Department of Administrative Services (DAS) has the authority and ESO has the responsibility for exercising DAS’ authority for the Statewide Incident Response Program (SIRP). The SIRP will establish enterprise standards and guidelines for statewide and agency-level information security incident response. The ESO staff serves as primary members of the SIRT. The ESO is the point of contact for SIRT and coordinates the SIRT. In addition, the ESO will establish and maintain a forensics program capable of assisting agencies.

SDC: The Department of Administrative Services has the authority and The State Data Center (SDC) has the responsibility for exercising DAS’ authority for monitoring the state network and assets under SDC control. This includes the identification and communication of security threats. The SDC is responsible for promptly alerting the agency and reporting to ESO any identified security threats to state resources. The SDC has authority to manage incidents and take action to address incidents involving the state network and assets under the control of SDC in accordance with enterprise policies and as outlined in the SDC service catalog.

**SIRT:** The SIRT will respond to information security incidents that potentially impact multiple agencies or which pose a significant risk to the state. The SIRT is responsible for coordinating inter-agency security incident response resources and communications during or about an information security incident that impacts multiple agencies. The SIRT will collect, classify and catalog all reported information security incidents. When an information security incident occurs that does not require SIRT involvement, the SIRT may assist agencies in responding to an information security incident upon request. The SIRT will maintain confidentiality in accordance with involved agencies policies, rules and legal requirements on all information security incidents reported to it. ESO will chair or appoint the chair.

**Agency:**
Establish an information security incident response capability. Upon identification of a potential incident, the agency will immediately initiate its incident response plan. Agency must designate a point of contact to communicate information security incidents to the SIRT. The agency will support the SIRT in its response including, but not limited to, providing the necessary resources, providing all requested information, and taking actions as directed by SIRT.
Employee:
Escalate potential information security incidents according to agency response plan, policies and procedures.

Compliance:
State agencies may, based on their individual business needs or legal requirements, exceed the requirements outlined in this policy but must, at a minimum, achieve the defined requirements in this document.

State agencies have until May 1, 2009 to comply with this policy unless other statutes or laws require earlier compliance

AUTHORITY: The Oregon Revised Statutes 182.122 and 182.124, OAR 125-800-005, 125-800-0010 and 125-800-0020 establish the authority for this State of Oregon Enterprise Information Security Policy.

APPLICABILITY: This policy applies to all Executive Branch agencies as defined in ORS 174.112, except as provided in ORS 182.122 and 182.124 and OAR 125-800-0020 (3)(a) and (b) and (4) as they apply to the State Board of Higher Education and the Oregon University System, the Oregon State Lottery, Secretary of State, State Treasurer, and the Attorney General.

DEFINITIONS: Asset: Anything that has value to the organization.

Availability: The reliability and accessibility of information assets and resources to authorized individuals in a timely manner.

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.

Information: Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, including electronic, paper and verbal communication.
Statewide Policy
Information Security Incident Response 107-004-120

DEFINITIONS

CONT: 

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 involving 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 likelihood of a threat agent taking advantage of a vulnerability and the resulting business impact. A risk is the loss potential, or probability, that a threat will exploit a vulnerability.

GUIDELINES:

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

II. Examples of non-reportable incidents include but are not limited to the following:
   - 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)

III. Examples of reportable incidents include but are not limited to the following:
   - Any incident relevant to the Oregon 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 wide spread
   - Web site defaced
   - Unauthorized access to information
   - Any kind of sabotage that effects information
   - Denial of service attacks

IV. The Enterprise Security Office recognizes that agencies may need additional education and awareness training regarding information security incidents and is committed to assisting agencies.

V. If unsure whether a situation is an incident, agencies should err on the side of caution and report.