

OREGON MILITARY DEPARTMENT	NUMBER: AGC-248.017
FINANCIAL ADMINISTRATION DIVISION	EFFECTIVE DATE: 8 Apr 2010
SUBJECT: Information Security Incident Response	

1. **APPLICABILITY:** These policies/procedures apply to all Oregon Military Department (OMD) employees and authorized representatives.
2. **AUTHORITY/REFERENCE:** Statewide Policy 107-004-120, Information Security Incident Response; ORS 182.122; OAR 125-800-005, 125-800-0010 and 125-800-0020.
3. **ATTACHMENTS:** None
4. **DEFINITIONS:**

Asset: Anything that has value to the organization.

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

Confidentiality: A security principle that prevents disclosure of information to unauthorized personnel.

Incident: 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, an agency, or third party and require non-routine preventative or corrective action.

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

Incident Response Policy: Written document that defines organizational structure for incident response, defines roles and responsibilities and detailed requirements for incident response and reporting.

Incident Response Procedures: Written document(s) of the series of steps taken when responding to incidents.

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

Information: Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics.

Information Security: Preservation of confidentiality, integrity and availability of information, including authenticity, accountability, non-repudiation and reliability.

Integrity: A security principle that prevents information and information systems from intentional or accidental modification.

Risk: The likelihood of detection then taking advantage of a security vulnerability and the resulting business impact. A risk measurement is the loss potential or probability that a threat will exploit the vulnerability.

5. **PURPOSE:** The purpose of this policy is to create a coordinated and effective response to information security incidents that affect the availability, integrity, or confidentiality of the Oregon Military Department's information assets. The policy defines the structure for incident response, roles and responsibilities, and the requirements for reporting incidents.

Staff must immediately report incidents that involve information security, along with assessments of vulnerability and risk, to the OMD Information Security Officer (ISO) in the Financial Administration Division (AGC) located at the Joint Force Headquarters Building in Salem, Oregon. Timely reporting enables prompt corrective action and allows for thorough information gathering and reporting.

6. **APPLICABILITY:** Incidents involving Operations Security (OPSEC) incidents of the Oregon National Guard must and will follow processes and procedures established by the Oregon National Guard.
7. **POLICY/PROCEDURES:** The Oregon Military Department has established an incident response program to respond to electronic, paper or verbal information security incidents. All divisions, programs, and all employees must follow the OMD Incident Response Plan whenever an information security incident is suspected or occurrence is certain.

a. **Reportable Incidents**

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.

Reporting is mandatory for any incident that meets all these criteria. Reporting by OMD staff is recommended for any incident meeting at least one but fewer than all four criteria. The OMD Information Security Incident Response Plan provides detailed reporting requirements.

Examples of non-reportable incidents include 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 information which can be disclosed to the public 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 or Corporate Travel Card fraud/losses (routine process already established with U.S. Bank).

Examples of reportable incidents include the following:

- Any incident relevant to the Oregon Consumer Identity Theft Protection Act. For more information see: http://dfcs.oregon.gov/id_theft.html
- 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 devices (laptop, blackberry, cell phone, computer discs, etc., containing sensitive information).

b. Decision to Report

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 OMD ISO per established procedures.

c. Anonymous Reporting

Employees may report security incidents anonymously by calling the Enterprise Security Office (DAS-ESO) 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 be aware they may become involved as the investigation progresses.

//s//

KARL D. JORGENSEN
Director of Financial Administration
Oregon Military Department