

OREGON MILITARY DEPARTMENT	NUMBER: AGC-248.010
FINANCIAL ADMINISTRATION DIVISION	EFFECTIVE DATE: 8 Apr 2010
SUBJECT: Information, Network and User Security	

1. **APPLICABILITY:** These policies/procedures apply to all Oregon Military Department (OMD) employees and authorized representatives.
2. **AUTHORITY/REFERENCE:** 2005 Oregon Laws Chapter 739, Oregon Administrative Rules (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 works to ensure that information is not disclosed to unauthorized subjects.

Controls: Means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature.

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 makes sure that information and systems are not modified maliciously or accidentally.

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

Security Policy: Documentation that describes senior management's directives toward the role that security plays within the organization. It provides a framework within an organization's established needed levels of information security to achieve the desired confidentiality, availability and integrity goals. A policy is a statement of information values, protection responsibilities, and the organization's commitment in managing risks.

Sensitivity: A measure of the importance assigned to information by its owner, for the purpose of denoting its need for protection.

5. **PURPOSE:** To emphasize Oregon Military Department's commitment to information security and provide direction and support for information security in accordance with business requirements and relevant laws and regulations. This policy also serves to protect information assets and reduce the risk of human error and misuse of information assets.

6. **POLICY/PROCEDURES:**

a. **Roles and Responsibilities**

OMD Deputy Director: Responsible for information security in the agency by reducing risk-exposure and ensuring the agency's activities do not introduce undue risk to state government as a whole. Ensures the Oregon Military Department complies with statewide security policies, standards, and initiatives, and state and federal regulations.

OMD Chief Information Officer (CIO): Promulgates, establishes and implements this policy. The CIO is also responsible for administering and managing the Incident Response when an incident occurs. The OMD CIO also serves as the Director of Financial Administration.

OMD Information Security Officer (ISO): Implements information security efforts within OMD. The OMD ISO serves as the point of contact for the Incident Response and coordinates OMD's information security. The OMD ISO also serves as the OMD Systems Administrator.

OMD Records Officer: Coordinates OMD's records management program. The OMD Records Officer also serves as the Financial Administration Division's Operations and Procurement Coordinator.

Division and Program Records Coordinators: Appointed by each division director and major program managers to work with OMD's Records Officer and the staff within his/her division or program to identify records (including electronic records) and ensure compliance with retention schedules and other state regulations.

Information Owner: A person or group of people who must establish the necessary controls to generate, collect, process, disseminate and dispose of specified information.

User: A person with authority to access state information or systems including the state network; responsible to comply with policies, procedures and practices.

b. Security Components

Risk Management: Effective risk management is critical for OMD to successfully implement and maintain secure environments. OMD works with the Safety and Risk Unit of DAS to establish effective safety and risk management systems. These systems are designed to:

- Identify risks
- Analyze risks
- Mitigate risk exposures (through loss control activities)

Each division, work unit or program using state information assets will perform periodic risk assessments to identify, assess, and prioritize risks against certain risk-criteria. The results will help the division, work unit or program determine the appropriate priorities, actions and controls to manage risks. No set of controls will achieve complete security. The cost of added information security controls must correspond to the sensitivity or value of the information protected. Divisions, work units and programs may consult with the OMD ISO regarding risk assessments and the assessment-process outlined below:

1. Identify the risks.
 - a. Identify the divisions', work unit's or program's information assets and the associated information owners.
 - b. Identify threats to those assets.
 - c. Identify vulnerabilities that the identified threats might exploit.
 - d. Identify the impacts of a loss of confidentiality, integrity or availability of the assets.
2. Analyze and evaluate the risks.
 - a. Assess the business impacts that might result from security failures; consider the consequences of a loss of confidentiality, integrity or availability of the assets.
 - b. Assess the realistic likelihood that security failures might occur in light of prevailing threats and vulnerabilities, the impacts associated with the assets, and the controls currently in place.
 - c. Estimate the level of risk.
 - d. Determine whether the division, work unit or program considers the risk acceptable.
3. Select a risk management strategy.
 - a. Apply appropriate controls to mitigate the risks.
 - b. Accept the risks.
 - c. Avoid the risks.
 - d. Transfer the associated business risk to other parties.
4. Document the objectives and controls in place to mitigate or treat the risks.

Each division director, work unit manger or program manager (or designee) will review the divisions', work unit's or program's risk assessment. Divisions, work units or

programs will forward their risk assessments to the OMD ISO for consolidation and review of the OMD CIO.

Security Policy: Information security policies provide direction to OMD employees, managers, and authorized representatives, consistent with the department's business requirements, governing laws and regulations. The policies establish the department's approach to managing information security and align with relevant statewide policies. The department's information security policies can be accessed via the Internet on the Financial Administration Division's home page.

The OMD ISO will review the department's information security policies bi-annually – or more frequently if significant changes occur – to ensure their continued suitability, adequacy and effectiveness. The OMD ISO and CIO report to the Oregon Military Department Executive Management Team and receive their guidance and direction in policy-development. The Executive Management Team may suggest new policies or revise existing policy-language. The OMD ISO works with the department's decentralized information systems specialists (working within specific programs) in continually assessing opportunities to improve OMD's information security policies and the department's administering of security in response to new threats or risks, business circumstances, legal or policy implications, and the technical environment.

Organization of Information Security: OMD's Financial Administration Division maintains the responsibility to implement the requirements of statewide policies and to establish internal policies to ensure the security of the department's information assets.

The Director of Financial Administration serves as OMD's Chief Information Officer. The Oregon Military Department's Information Security Officer reports to the OMD CIO. These two positions work with staff from across the agency on information security issues.

Asset Management: The objective of asset management is to achieve and maintain appropriate protection of OMD's assets. This applies to all records regardless of physical form, which may include the following examples (not an exhaustive list): Paper, microfilm, microfiche, audio and video recordings, electronic mail, photographs, optical or digital disks, CD-ROM and other recording media, and databases. Information Assets must be safeguarded at all times whether through open discussion, phone conversations, e-mail, social media, and the mailing, shuttle or other transporting of documents.

OMD ensures an appropriate level of protection for its information assets. Department of Defense Security Classifications and Security Clearances in use within our state military environment pre-date statewide policy on Asset Classification and will remain in use. Information generated, maintained and used within the state government environment of OMD is considered "For Official Use Only" under Department of Defense Security Classification and can only be released outside of the organization under delegated authorization of The Adjutant General. Information requiring higher security classifications can only be shared with individuals with "a need to know" and having

security clearances appropriate to the level of security classification assigned to the information. Asset management is subject to the limitations and conditions of the Oregon Public Records Law, which defines information that is open or exempt from public disclosure.

Human Resources Security: All OMD employees and authorized representatives (volunteers, contractors, and third-party users) who use the department's information and information assets will receive instructions about their responsibilities. OMD will determine and apply suitable roles for users to reduce the risk of theft, fraud or misuse.

OMD will address security responsibilities prior to employment, via position descriptions and associated terms and conditions of employment. Where appropriate, candidates for employment, volunteer work, contractors, and third-party users will receive adequate screening, especially for roles that require access to sensitive information. Additionally, management will apply security principles and processes throughout an employee's employment. Employees and authorized representatives will receive appropriate information security awareness training annually. Employees must also be familiar with relevant policies and procedures for their job function. When an employee or authorized representative terminates their job/association within OMD, management will oversee the return of all equipment and removal of all access rights.

Physical and Environmental Security: The objective of physical and environmental security is to prevent unauthorized access, damage, theft, compromise, and interference to OMD information and facilities. In locations that house critical or sensitive infrastructure, information or assets, the department utilizes appropriate physical and electronic security barriers and entry controls. These controls ensure that only authorized personnel gain access. The department uses armed security and key cards with photo IDs where appropriate.

Communications and Operations Management: OMD will establish appropriate policies and procedures to manage and operate all information-processing facilities. Where appropriate, the department will segregate duties to reduce the risk of negligent or deliberate misuse of systems or information. The department will take precautions to prevent and detect the introduction of malicious code and unauthorized mobile code. These actions will protect the integrity of software and information.

To prevent interruptions to business activities, and unauthorized disclosure, modification, removal or destruction of information assets, OMD will control and physically protect all media. The department will protect information from unauthorized disclosure or misuse by establishing and communicating procedures to handle and store information. Exchanging sensitive information or software with other agencies and organizations must involve a documented exchange-agreement that references the information classification level and any specific procedures.

During transport beyond OMD's physical locations the department will protect media that contains information against unauthorized access, misuse or corruption. To detect

unauthorized access to agency information and information systems, OMD will use monitoring techniques.

Access Control: Business and security requirements will guide the control of access to information, information systems, information-processing facilities and business processes. To prevent unauthorized access, OMD implements formal procedures to control access rights to information and systems, and restricts access to operating systems to only authorized users.

Users will receive instruction about their responsibility to maintain effective access controls, particularly the use of passwords. Management will ensure all authorized users understand their responsibility to appropriately protect unattended equipment. Users must protect mobile computing devices and telework areas in proportion to identified risks.

Management of Information Security Incidents: OMD will maintain and follow its separate policy on Information Security Incident Response.

//s//

KARL D. JORGENSEN
Director of Financial Administration
Oregon Military Department