

<b>OREGON MILITARY DEPARTMENT</b>	<b>NUMBER: AGC-248.006</b>
<b>FINANCIAL ADMINISTRATION DIVISION</b>	<b>EFFECTIVE DATE: 8 Apr 2010</b>
<b>SUBJECT: Acceptable Use of State Information Assets</b>	

1. **APPLICABILITY:** These policies/procedures apply to all Oregon Military Department (OMD) employees and authorized representatives.
2. **AUTHORITY/REFERENCE:** Statewide (DAS) Policy 107-004-110, and ORS 184.305, ORS 184.340, ORS 291.037 and ORS 291.038.
3. **ATTACHMENTS:** Acknowledgement Form: **Acceptable Use of State Information Assets**
4. **PURPOSE:** The purpose of this policy is to inform authorized users, of state information assets maintained within OMD, of the appropriate and acceptable use of information, computer systems and devices, telecommunications devices, and other office technology.
5. **POLICY/PROCEDURES:**

**a. State Business**

Information, computer systems and devices, telecommunications and other office technology resources are provided to employees and authorized representatives primarily to conduct the business of OMD and of the state. Information Assets may be used, **within the restrictions and limitations stipulated in this policy**, for personal business – see the Personal Use section of this policy.

Supervisors are responsible for determining whether a valid business reason exists for providing cell phones, pagers, and PDAs (*Blackberries*) to employees. Supervisors are also responsible for ensuring users of cell phones, pagers, and PDAs understand the restrictions and limitations on personal use of these devices. Information designated as “restricted”, “critical”, “For Official Use Only” or any other security designation may be compromised by the use, loss or theft of any portable device. Users are restricted from using any OMD provided portable device while driving, unless hands-free technology is incorporated and as allowed by law.

**Active Control of Portable and Removable Storage Devices:** Portable and removable storage devices may include, but are not limited to palmtops, laptops, mobile phones, flash drives, floppy diskettes, CDs, or DVDs. These devices may be transporting an Information Asset that must be safeguarded at all times. Users are required to know what

information is stored on devices in their care. Users must employ active control over their devices to ensure protection against theft of equipment, unauthorized disclosure of information, misuse of equipment, or unauthorized access to information assets. Managers and supervisors must authorize the use of these devices (and any information asset stored on them) outside of the physical boundaries of OMD. Theft or unauthorized disclosure of information assets must be immediately reported to the Information Security Officer working in the Financial Administration Division (AGC).

**b. Systems and Information are State Property**

OMD owned technology assets and the information on them are the sole property of the State of Oregon subject to its sole control unless an overriding agreement or contract exists to the contrary. No part of state agency systems or information is, or shall become, the private property of any system user. The state owns all legal rights to control, transfer, or use all or any part or product of its systems. All users shall safeguard all information and comply with this policy and any other applicable state policies and rules that apply.

**c. Access and Control**

OMD reserves, and intends to exercise, all rights relating to all information assets. When necessary, agency administration will direct the use of automated tools to trace, review, audit, access, intercept, block, restrict, screen, delete, recover, restore, publish or disclose any information, in accordance with disclosure of information policies. OMD will grant users access only to systems and information required to do their work, and may withdraw permission for any or all use of its assets at any time without cause or explanation. The objectives of this policy will be communicated to all employees upon hire and annually thereafter.

**Information Security:** All agency information assets must be protected to ensure confidentiality, integrity, and availability of information from the time of creation, through useful life and through proper disposal. The loss, misuse, or unauthorized access to or the modification of this information could adversely affect the interest or the conduct of programs, or the privacy to which individuals are entitled. All employees and authorized representatives of the Oregon Military Department will actively and at all times ensure control and custody of the agency's information assets. This includes, but is not limited to the transporting of sensitive or critical documents, whether hard copy or electronic. These types of information assets must be in ones' physical control or an appropriate record of transfer/custody must be recorded along with security instructions.

**d. Public Records and Control by Oregon Military Department**

All information stored within OMD-owned technology assets are the property of the State of Oregon. Users will comply with all applicable public records retention laws, rules, and policies.

**e. Professional Conduct**

OMD-owned technology assets must not be used in a manner that is false, unlawful, offensive, or disruptive. Users shall not use technology assets to intentionally view, download, store, transmit, retrieve or communicate any material or communication that:

- Is harassing or threatening;
- Is obscene, pornographic or sexually explicit;
- Is defamatory;
- Is discriminatory in reference to race, age, gender, sexual orientation, religious or political beliefs, national origin, health, or disability;
- Is untrue or fraudulent;
- Is illegal or promotes illegal activities;
- Is intended for personal profit;
- Condone hate, bigotry, discrimination, or prejudice;
- Facilitates Internet gaming or gambling; or,
- Contains offensive humor.

**f. Legal Compliance**

Users shall be in compliance with copyrights, licenses, contracts, intellectual property rights, and laws associated with data, software programs, and other materials made available through state systems.

**g. Security**

Users shall respect the confidentiality of other users' information and shall not attempt to:

- Access third party systems without prior authorization by the system owner;
- Obtain other users' login names or passwords;
- Attempt to defeat or breach computer or network security measures;
- Intercept, access, or monitor electronic files or communications of other users or third parties without approval from the author(s) or responsible business owner(s);
- Peruse the files or information of another user without specific business need to do so or prior approval from the author(s) or responsible business owner(s).

**h. Data Integrity**

Users shall not knowingly destroy, misrepresent, or otherwise change the data stored in state information systems in such a way as to reduce the accuracy or reliability of the data.

**i. Operational Efficiency**

Users shall not operate or use information assets in a manner likely to impair the availability, reliability, or performance of state business processes and systems, or unduly contribute to system or network congestion.

**j. Accounts and Account Passwords**

Users will follow all relevant policies and procedures to ensure access to information assets are properly authorized. The first time that an individual logs on to a OMD computer, they are required to choose a password. The password they choose must be at least 8 characters long. Users need to choose a password that they will remember because there is no record of the password they choose. For security purposes, passwords should not be written down. Passwords expire 90 days from the day they were chosen or last changed. Users may change their password more often than every 90 days, but once a password has been used, it may never be used again. If a password has been compromised, the user should report the incident to the IS staff immediately and then change their password. Users are responsible for anything done using there user ID and password.

**k. Software Installation, Downloads, Security**

Users shall not download or install non-approved software (examples include photos, data not related to work, or executable files) from the Internet or other external sources (including portable computing and storage devices) without prior consent from his or her supervisor and the approval of the Systems Administrator/Information Security Officer working in the Financial Administration Division. Information Systems Support staff working in Oregon Emergency Management and Oregon Youth Challenge will bring forward requests from supervisors within their program areas to the Systems Administrator/Information Security Officer working in the Financial Administration Division for approval. The Director of Financial Administration/Chief Information Officer may override consents, approvals, or denials.

**l. Remote Login**

Users shall not log into OMD networks from remote locations unless they are using approved and provided remote access systems or software. Remote access from non-state devices to access e-mail via a Web page is allowed.

**m. Use of e-mail**

Personal use of e-mail is allowed on a limited, reasonable basis. OMD may monitor e-mails on a random basis or for cause. E-mail messages and attachments shall not include offensive content and must comply with Human Resource Services Division (DAS) Statewide Policy 50.010.01, Discrimination and Harassment Free Workplace.

Users shall not send e-mail or other electronic communications that attempt to hide the identity of the user or represent the user as someone else. Users shall not use scramblers, re-mailer services, drop-boxes, or identity-stripping methods without the approval of the State Chief Information Security Officer. Such requests shall be pre-approved by the user's supervisor and the OMD's Director of Financial Administration/Chief Information

Officer prior to being submitted to the State of Oregon's State Chief Information Security Officer.

E-mail may be used for limited union business per applicable collective bargaining agreements.

E-mails are public records; all applicable archiving and public records laws, rules, and policies shall be followed.

Confidential information transmitted externally shall be appropriately protected.

Users may only use e-mail software approved by the Oregon Military Department's Systems Administrator/Information Security Officer and installed by Information Systems Support staff.

**n. Hardware Installation**

Users shall not attach any hardware device to a state provided computer that the user does not employ in the users' assigned work. Privately owned devices (including, but not limited to Personal Digital Assistants, thumb drives, digital cameras, laptop computers, MP3 players, etc.) shall not be connected to state networks, computers (including remote-use computers) or other equipment without the approval of the user's supervisor and the OMD's Systems Administrator/Information Security Officer. All hardware connected to state systems shall be appropriately configured, protected, and monitored so it will not compromise state information assets.

**o. Personal Use**

Using the Internet increases the risk of exposing state information assets to security breaches. Limited personal use of the Internet is allowed during the lunch or break periods.

For the purposes of this policy, business use includes but is not limited to accessing information related to employment with the state, including all rights per applicable collective bargaining agreements. Approved business use sites include but are not limited to ILearn, Public Employees Benefits Board, Public Employees Retirement Systems, Employee Assistance Program, the Oregon Jobs Page, and the Oregon Savings Growth Plan.

At the discretion of Information Systems Support staff and OMD's Systems Administrator/Information Security Officer in consultation with the Director of Financial Administration/Chief Information Officer, will block sites deemed to pose a security risk or are otherwise considered unacceptable. Limited personal use includes access only to sites on the Internet that have not been blocked. Limited personal use does not include playing computer games (whether via the Internet, personal copies, or those included

with approved software programs). Examples of how state information systems may not be used include, but are not limited to:

- Hosting or operating personal Web pages;
- Non-business related postings to Internet groups, chat rooms, Web pages or list serves;
- Any activity requiring the use of a credit card or other payment by the user for non-business related procurements;
- Creating, sending, or forwarding chain e-mails; or,
- Accessing Web sites or other services containing content forbidden under the **Professional Conduct** section of this policy.

State systems are capable of logging key strokes; therefore, users are strongly discouraged from conducting personal business requiring personally identifiable information. Examples include electronic banking and online shopping.

The use of Instant Messaging (IM) or other communications/messaging alternatives (wikis, blogs, etc.) are allowed for business purposes. However, use must be approved by Information Systems Support staff and the OMD's Systems Administrator/Information Security Officer in consultation with the Director of Financial Administration/Chief Information Officer.

OMD may monitor the use of information systems at random or for cause. Some Web sites will be blocked using software and commercially available lists of objectionable sites. Personal use of cell phones or PDAs is prohibited except in an emergency situation. Guidelines for phone usage while in travel status are governed by the Oregon Accounting Manual Policy 40.10.00 PO and by collective bargaining agreements. Any personal use of cell phones or PDAs is also subject to taxation of the user.

**p. Personal Use of Audio CDs, DVDs, MP3s, etc.**

Employees may play audio CDs and DVDs using state equipment provided it does not interfere with their own or others' work, and approved by the employee's supervisor. Users are not allowed to transfer music from the CD/DVD to the workstation or notebook hard drive. Audio CDs that require the user to install software on the workstation or notebook computer may not be played. OMD workstations or notebook computers may not be used to make CDs or to burn audio or video disks for personal use. OMD workstations or notebook computers may not be used to transfer music to portable players or MP3 devices such as iPods. Peer-to-Peer (P2P) file sharing may result in copyright violations or may open communication channels through firewalls, and is prohibited on state networks.

**q. Personal Use of Encryption**

To ensure that the state has continuous access to information on computer systems, users shall not use personal hardware or software to encrypt e-mail, voicemail, or any other data stored in or communicated by state computer systems and networks, except in

accordance with written prior permission of the Director of Financial Administration/Chief Information Officer.

**r. Personal Solicitation**

Users shall not use state information systems for personal solicitation. For example, systems shall not be used to lobby, solicit, recruit, sell, or persuade for or against commercial ventures, products, religious, political causes or outside organizations.

**s. Violation**

Violation of the terms of this policy can result in limitation, suspension, or revocation of information and telecommunications technology use privileges and can lead to other disciplinary action up to and including dismissal from state service. Knowingly violating portions of this policy may be construed as “Computer Crime” under Oregon Revised Statute (ORS) 164.377.

*//s//*

KARL D. JORGENSEN  
Director of Financial Administration  
Oregon Military Department