


<b>SUBJECT:</b> Acceptable Use of DAS Information Assets	<b>NUMBER:</b>	107-01-010
<b>DIVISION:</b> Operations Division	<b>EFFECTIVE DATE:</b>	8/14/08
<b>APPROVED:</b> 		

<b><u>POLICY/PURPOSE:</u></b>	<p><b>Policy:</b> Information, computer systems and devices, telecommunications devices and other office technology assets are made available to users to optimize the business processes of the Department of Administrative Services. Any use of these assets shall comply with this policy.</p> <p><b>Purpose:</b> The purpose of this policy is to inform authorized users of Department of Administrative Services (DAS) technology assets of the appropriate and acceptable use of information, computer systems and devices, telecommunications devices, and other office technology.</p>
<b><u>AUTHORITY:</u></b>	Enterprise Security Office Policy #107-004-110, Acceptable Use of State Information Assets; DAS Office of the Director Policy #107-001-0015, Internal Controls for the Management of Cellular-based Communications Devices.
<b><u>APPLICABILITY:</u></b>	All DAS Employees and other users as defined below.
<b><u>ATTACHMENTS:</u></b>	Attachment A
<b><u>DEFINITIONS:</u></b>	<p><b>DAS-owned Technology Assets</b> means information systems, computer systems and devices, telecommunications systems, copiers, fax machines, and other office technology resources.</p> <p><b>Data and Information</b> means representation of facts, including, but not limited to, digital records, files, and electronic communications.</p> <p><b>Personal Use</b> means the use of DAS-owned technology assets for purposes other than conducting the business of DAS and the state.</p> <p><b>Telecommunications Technology</b> means the hardware, software, and services for transmitting voice, data, video, and images over a distance. This includes cell phones and personal digital assistants (PDAs).</p> <p><b>User</b> means all DAS employees, volunteers, agents, vendors and contractors, including those users affiliated with third parties who access state information assets, and all others authorized to use state information and telecommunications technology for the purpose of accomplishing the state's business objectives and processes.</p>
<b><u>GUIDELINES:</u></b>	
<b>I.</b>	<p><b>State Business</b> Information, computer systems and devices, telecommunications and other office technology resources are provided to DAS employees primarily to conduct the business of the agency and of the state. In a limited number of cases, these assets may be used for personal business according to the guidelines discussed in the <b>Personal Use</b> section (XV) below. Supervisors are responsible for determining whether a valid business reason exists for providing</p>

**SUBJECT:** Acceptable Use of DAS Information Assets

**NUMBER:**

107-01-010

**DIVISION:** Operations Division

**EFFECTIVE DATE:**

8/14/08

cell phones or PDAs to employees. Supervisors are also responsible for ensuring that users of cell phones and PDAs understand the restriction on personal use of these devices and understands that information designated as "restricted" or "critical" may be compromised by the use, loss or theft of any portable device. Users of cell phones or PDAs and their supervisors must read, understand and follow the elements of statewide policy 107-001-0015 referenced above. Users are discouraged from using any portable device while driving.

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

DAS-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 comply with this policy and any other applicable state policies and rules that apply.

**III. Access and Control**

DAS reserves, and intends to exercise, all rights relating to all information assets. When necessary, agency administration will direct the use of automated discovery 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. DAS will grant users access only to systems and information required to do their work. DAS may monitor the use of these systems at random or for cause, and will revoke user access in a timely manner. DAS may withdraw permission for any or all use of its systems at any time without cause or explanation. The objectives of this policy will be communicated to all employees upon hire and annually thereafter.

Issuance of cell phones and PDAs must be coordinated through the DAS Cellular Communication Plan Coordinator. The coordinator is responsible for the duties outlined in Section 3 of statewide policy 107-001-0015. For DAS, the coordinator shall be the Technology Support Center Purchasing Specialist, with that position's supervisor as the backup.

**IV. Public Records and Control by DAS**

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

**V. Professional Conduct**

DAS-owned technology assets shall 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;
- condones hate, bigotry, discrimination, or prejudice;
- facilitates Internet gaming or gambling; or,
- contains offensive humor.

**SUBJECT:** Acceptable Use of DAS Information Assets

**NUMBER:**

107-01-010

**DIVISION:** Operations Division

**EFFECTIVE DATE:**

8/14/08

<b>VI.</b>	<b><u>Legal Compliance</u></b> 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.
<b>VII.</b>	<b><u>Security</u></b> Users shall respect the confidentiality of other users' information and shall not attempt to: <ul style="list-style-type: none"><li>• access third party systems without prior authorization by the system owner;</li><li>• obtain other users' login names or passwords;</li><li>• attempt to defeat or breach computer or network security measures;</li><li>• 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);</li><li>• 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).</li></ul>
<b>VIII.</b>	<b><u>Data Integrity</u></b> 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.
<b>IX.</b>	<b><u>Operational Efficiency</u></b> 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.
<b>X.</b>	<b><u>Accounts and Account Passwords</u></b> Users will follow all relevant policies and procedures to ensure that access to information assets is properly authorized. Users will comply with all provisions of DAS Policy 107-01-140 regarding the proper use of passwords.
<b>XI.</b>	<b><u>Software Installation, Downloads, Security</u></b> 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 Technology Support Center.
<b>XII.</b>	<b><u>Remote Login</u></b> Users shall not log into DAS networks from remote locations unless they are using approved and provided remote access systems or software.
<b>XIII.</b>	<b><u>Use of e-mail</u></b> Personal use of e-mail is allowed on a limited, reasonable basis. DAS 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 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

**SUBJECT:** Acceptable Use of DAS Information Assets

**NUMBER:**

107-01-010

**DIVISION:** Operations Division

**EFFECTIVE DATE:**

8/14/08

Security Officer. Such requests shall be pre-approved by the user's supervisor and the DAS Chief Information Officer prior to being submitted to the State Chief Information Security Officer.

E-mail may be used for limited union business per SEIU collective bargaining agreement.

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

Confidential information transmitted externally must be appropriately protected.

Users may only use e-mail software approved and installed by the Technology Support Center.

**XIV. Hardware Installation**

User's shall not attach any hardware device to a state provided computer that the user does not employ in the user's 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 users supervisor and the Technology Support Center. All hardware connected to state systems shall be appropriately configured, protected, and monitored so it will not compromise state information assets.

**XV. 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 Public Employees Benefits Board, Public Employee's Retirement System, Employee Assistance Program, the Oregon Jobs Page, and the Oregon Savings Growth Plan.

TSC, at the discretion of the DAS Security Officer and Employee Services Manager and with advice from the DAS IT Management Council, 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.

**SUBJECT:** Acceptable Use of DAS Information Assets

**NUMBER:**

107-01-010

**DIVISION:** Operations Division

**EFFECTIVE DATE:**

8/14/08

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 the DAS Security Officer, documented, adequately secured, and must comply with public records and archiving laws and regulations.

DAS 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 Oregon Accounting Manual Policy 40.10.00 PO and by Article 36, Section 1 of the 2007-09 Special Agencies Collective Bargaining Agreement. Any personal use of cell phones or PDAs is also subject to taxation of the user.

**XVI. 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 other's work. 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. DAS workstations and notebook computers may not be used to make CDs or to burn audio or video disks for personal use. DAS workstations or notebooks may not be used to transfer music to portable players or MP3 devices such as Apple iPods. Peer-to-Peer (P2P) file sharing may result in copyright violations or may open communication channels through firewalls, and is prohibited on the state network.

**XVII. 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 DAS Chief Security Officer.

**XVIII. 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, or political causes or outside organizations

**XIX. 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 ORS 164.377 (see Attachment A)

**XX. Exceptions**

Exceptions to this policy shall be made in accordance with Exceptions to Policy 107-001-0020.

**SUBJECT:** Acceptable Use of DAS Information Assets

**NUMBER:**

107-01-010

**DIVISION:** Operations Division

**EFFECTIVE DATE:**

8/14/08

### Attachment A

**164.377 Computer crime.** (1) As used in this section:

(a) To “access” means to instruct, communicate with, store data in, retrieve data from or otherwise make use of any resources of a computer, computer system or computer network.

(b) “Computer” means, but is not limited to, an electronic, magnetic, optical electrochemical or other high-speed data processing device that performs logical, arithmetic or memory functions by the manipulations of electronic, magnetic or optical signals or impulses, and includes the components of a computer and all input, output, processing, storage, software or communication facilities that are connected or related to such a device in a system or network.

(c) “Computer network” means, but is not limited to, the interconnection of communication lines, including microwave or other means of electronic communication, with a computer through remote terminals or a complex consisting of two or more interconnected computers.

(d) “Computer program” means, but is not limited to, a series of instructions or statements, in a form acceptable to a computer, which permits the functioning of a computer system in a manner designed to provide appropriate products from or usage of such computer system.

(e) “Computer software” means, but is not limited to, computer programs, procedures and associated documentation concerned with the operation of a computer system.

(f) “Computer system” means, but is not limited to, a set of related, connected or unconnected, computer equipment, devices and software. “Computer system” also includes any computer, device or software owned or operated by the Oregon State Lottery or rented, owned or operated by another person or entity under contract to or at the direction of the Oregon State Lottery.

(g) “Data” means a representation of information, knowledge, facts, concepts, computer software, computer programs or instructions. “Data” may be in any form, in storage media, or as stored in the memory of the computer, or in transit, or presented on a display device. “Data” includes, but is not limited to, computer or human readable forms of numbers, text, stored voice, graphics and images.

(h) “Property” includes, but is not limited to, financial instruments, information, including electronically produced data, and computer software and programs in either computer or human readable form, intellectual property and any other tangible or intangible item of value.

(i) “Proprietary information” includes any scientific, technical or commercial information including any design, process, procedure, list of customers, list of suppliers, customers’ records or business code or improvement thereof that is known only to limited individuals within an organization and is used in a business that the organization conducts. The information must have actual or potential commercial value and give the user of the information an opportunity to obtain a business advantage over competitors who do not know or use the information.

(j) “Services” include, but are not limited to, computer time, data processing and storage functions.

(2) Any person commits computer crime who knowingly accesses, attempts to access or uses, or attempts to use, any computer, computer system, computer network or any part thereof for the purpose of:

(a) Devising or executing any scheme or artifice to defraud;

(b) Obtaining money, property or services by means of false or fraudulent pretenses, representations or promises; or

(c) Committing theft, including, but not limited to, theft of proprietary information.

(3) Any person who knowingly and without authorization alters, damages or destroys any computer, computer system, computer network, or any computer software, program, documentation or data contained in such computer, computer system or computer network, commits computer crime.

(4) Any person who knowingly and without authorization uses, accesses or attempts to access any

**SUBJECT:** Acceptable Use of DAS Information Assets

**NUMBER:**

107-01-010

**DIVISION:** Operations Division

**EFFECTIVE DATE:**

8/14/08

computer, computer system, computer network, or any computer software, program, documentation or data contained in such computer, computer system or computer network, commits computer crime.

(5)(a) A violation of the provisions of subsection (2) or (3) of this section shall be a Class C felony. Except as provided in paragraph (b) of this subsection, a violation of the provisions of subsection (4) of this section shall be a Class A misdemeanor.

(b) Any violation of this section relating to a computer, computer network, computer program, computer software, computer system or data owned or operated by the Oregon State Lottery or rented, owned or operated by another person or entity under contract to or at the direction of the Oregon State Lottery Commission shall be a Class C felony. [1985 c.537 §8; 1989 c.737 §1; 1991 c.962 §17; 2001 c.870 §18]