

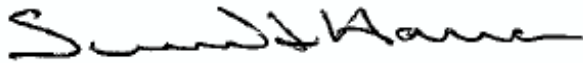
**SUBJECT:** Acceptable Use of State Information Assets

**NUMBER:** 107- 004-110

**DIVISION:** Enterprise Information Strategy and Policy

**EFFECTIVE DATE:** 01-01-2010

**APPROVED:**



**POLICY/  
PURPOSE:**

The purpose of this policy is to inform authorized users of state agency information assets of the appropriate and acceptable use of information, computer systems and devices.

**AUTHORITY:**

ORS 184.305, ORS 184.340, ORS 291.015, ORS 291.016, ORS 291.018, ORS 291.026, ORS 291.034, ORS 291.037, and ORS 291-038, ORS 811.507 and HB 2377 [2009 Session]

**APPLICABILITY:**

All individuals who have been granted access to state agency information-related technology or systems, including but not limited to, "User" as defined in the Definitions section below. This section 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. Other agencies may follow this policy at their option.

**DEFINITIONS:**

**Control**

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

**Encryption**

Use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without the use of a confidential process or key.

**Information Asset**

Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics that has value to the organization.

**Information System**

Computers, hardware, software, storage media, networks, operational procedures and processes used in the collection, processing, storage, sharing or distribution of information within, or with an access beyond ordinary public access to, the state's shared computing and network infrastructure.

**Mobile Communication Device (MCD)**

A text messaging device or a wireless, two-way communication device designed to receive and transmit voice or text communication including mobile Global Positional System (GPS).

**User**

All state employees, volunteers, their agents, vendors and contractors, including those users affiliated with third parties who access state information assets, and all other authorized to use state information technology for the purpose of accomplishing the state's business objectives and processes.

## Statewide Manual

**POLICY NAME: Acceptable Use of State Information Assets**

**POLICY NUMBER: 107-004-110**

**ATTACHMENTS:** Attachment A - ORS 164.377, Computer Crime  
Attachment B - Acceptable Use Agreement

### **GUIDELINES:**

#### **I. State Business:**

Information, computer systems and devices are made available to users to optimize the business process of the State of Oregon. Any use of information, computer systems and devices shall comply with this policy. Agencies will put in place policies, procedures and practices that enable compliance, deter misuse, and detect policy violations. Notwithstanding specific prohibitions in this policy, public officials carrying out agency missions or functions permitted by law are not prohibited by any part of this policy from performing their official duties or responsibilities. State agencies shall approve and document any exceptions to this policy. Agencies may adopt more restrictive policies based on business requirements. Users of state information assets are responsible for complying with the provisions of this policy and agency-promulgated supporting policies, procedures and practices.

#### Key Terms

See the "DEFINITIONS" section for explanation of key terms used in this policy.

#### Systems and Information are State Property

State information, computer systems and devices are provided for business purposes only and information on those systems 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 may become the private property of any system user. The state owns all legal rights to control, transfer, or use all of any part or product of its systems. All uses shall comply with this policy and any other applicable state policies and rules that apply. State agencies are responsible for controlling and monitoring their systems and protecting their information assets. All information stored within applications, systems and networks are the property of the State of Oregon. Users shall comply with public records retention laws and rules.

#### Access and Control

The State of Oregon reserves, and intends to exercise, all rights relating to all information assets. State agencies are responsible for granting and monitoring users' access only to systems and information required to do their work, and for revoking user access in a timely manner. A state agency may withdraw permission for any or all use of its systems at any time without cause or explanation.

#### **II. Lawful, Ethical and Inoffensive Use**

##### Professional Conduct

Use of state information assets shall not be false, unlawful, offensive, or disruptive. State networks and systems shall not be used to intentionally view, download, store, transmit, retrieve any information, communication or material which: is harassing or threatening; is obscene, pornographic or sexually explicit; is defamatory; makes discriminatory 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 to foster hate, bigotry, discrimination or prejudice; facilitates Internet gaming or gambling; or contains offensive humor.

##### Legal Compliance

Use of state information systems shall be in compliance with copyrights, license, contracts, intellectual property rights and laws associated with data, software programs, and other materials made available through those systems.

**Security**

Any use of state information systems shall respect the confidentiality of other users' information and shall not attempt to: (i) access third party systems without prior authorization by the system owners; (ii) obtain other users' login names or passwords; (iii) attempt to defeat or breach computer or network security measures; (iv) intercept, access, or monitor electronic files or communications of other users or third parties without approval from the author or responsible business owners; (v) peruse the files or information of another user without specific business need to do so and prior approval from the author or responsible business owner.

**Data Integrity**

Users shall not knowingly destroy, misrepresent, or otherwise change the data stored in state information systems.

**Operational Efficiency**

Operation or use of information assets shall be conducted in a manner that will not impair the availability, reliability or performance of state business processes and systems, or unduly contribute to system or network congestion.

**Accounts and Account Passwords**

III. All users shall be properly authorized and authenticated to use state information assets.

**Software Installation, Downloads, Security**

**Downloads**

Non-approved software, including screen savers, shall not be downloaded or installed from the Internet or other external sources (including portable computing and storage devices) without prior consent from the state agency. Any software that would result in copyright violations shall not be downloaded onto state systems.

**Remote Login**

Access to state agency networks from remote locations is not allowed except through the use of agency-approved and agency-provided remote access systems or software. Agencies may allow remote access from non-state devices to access e-mail via a Web page.

**Use of E-mail**

E-mail is to be used only for state related business; however, agency directors may allow employees limited, incidental personal use. Sending e-mail or other electronic communications that attempts to hide the identity of the user or represent the user as someone else is prohibited. No use of scramblers, re-mailer services, drop-boxes or identity-stripping methods is permitted. E-mail may be used for union business per the contract. E-mails are public record and state agencies and all users are responsible for ensuring compliance with archiving and public records laws. Confidential information transmitted externally shall be appropriately protected.

**Hardware Installation**

Hardware devices shall not be attached to a state provided computer that the user does not employ in the user's assigned work. Privately owned devices shall not be connected to state networks, computers (including remotely used computers) or other equipment without approval of the agency prior to connection. All hardware attached to state systems shall be appropriately configured, protected and monitored so it will not compromise state information assets.

IV.

**Personal Use**

**Personal Use of Internet, Networks and Services**

Using the Internet increases the risk of exposing state information assets to security breaches. The state can only accept this risk for business use; however agency directors may allow employees limited, incidental personal use as long as there is no or insignificant cost to the state and such use does not violate these guidelines. State agencies have sole discretion to determine if an employee's use is personal or business. Business use includes accessing information related to employment with the state, including all rights per the union contract. Approved sites for this purpose are PEBB, PERS, EAP, the Oregon JOBS page, Oregon Savings Growth Plan, and union contractual information. Use in cases of emergency or to check weather conditions may be deemed acceptable based on agency policy. Use shall not include playing computer games, whether Internet, personal, or those included with approved software applications. State systems may not be used for: hosting or operating personal Web pages; non business-related postings to Internet groups, chat rooms, Web pages, or list serves; or creating, sending, or forwarding chain e-mails. State agencies may allow the use of Instant Messaging (IM) and other communications/messaging alternatives for business purposes. Agencies may allow the use of streaming video/audio for business purposes. However, these uses shall be approved, documented, adequately secured, and comply with public records and archiving laws.

**Personal Use of Audio CDs, DVDs**

State agencies may allow users to play audio CDs or DVDs using state equipment (per state agency policy) provided it does not interfere with their or other's work. Users are not allowed to transfer music from the CD to the workstation or notebook hard drive or MCD. Audio CDs that require the user to install software on the workstation or notebook computer or MCD may not be played. State agency workstations and notebook computers may not be used to make "compilation" CDs or to "burn" audio or video disks for personal use. State workstation and notebook computers are not be used to transfer music to portable music players. Peer-to-Peer (P2P) file sharing is prohibited on the state network. State agencies shall approve and document any exceptions.

**Personal Use of Encryption**

Personal hardware or software may not be used to encrypt any state or agency owned information so as to deny or restrict access to a public official who has a valid, job-related interest or purpose in the information, except in accordance with express prior permission and direction from the agency director.

**Personal Solicitation**

State Information systems shall not be used 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.

**Public Use of State Systems**

Agency-provided e-mail systems and Internet access for the public shall be appropriately secured in order to properly protect state information assets.

**Monitoring, Control and Compliance**

State agencies are responsible for monitoring use of information systems and assets. Agencies will, at a minimum, monitor on a random basis and for cause. Monitoring systems or processes will be used to create usage reports and resulting reports will be reviewed by agency management for compliance.

**Violation**

|   |                            |
|---|----------------------------|
| <u>Statewide Manual</u>                                 |                            |
| POLICY NAME: Acceptable Use of State Information Assets | POLICY NUMBER: 107-004-110 |

**POLICY NUMBER: 107-004-110**

**PROCEDURES:**

## Action

- Each agency director is responsible for:

- a. Ensuring that their agency has sufficient safeguards in place to ensure that expenditures for state information assets are restricted to those necessary for the conduct of official business. This includes ensuring that there are sufficient internal controls.

- The division administrator is responsible to enforce this policy and:

- c. Maintaining accurate record of violations of this policy.

- The Manager of the Authorized User is responsible for:

- d. At least annually, review and validate Plan Charges and Authorized Users to ensure that expenditures meet the requirements under this policy.

- The Authorized User is responsible for:

**Statewide Manual**

**POLICY NAME: Acceptable Use of State Information Assets**

**POLICY NUMBER: 107-004-110**

- a. Taking reasonable steps to ensure the physical security of state information assets. Report missing, lost or stolen state information assets to their Manager immediately.
- b. Using the state information assets in a manner consistent with the Acceptable Use Agreement.
- c. Taking reasonable steps to prevent the release of confidential or sensitive information either during the voice/data transmission or from the loss/theft of a MCD.
- d. Understanding that sanctions, including dismissal, may result from the unauthorized use of state information assets.
- e. Understanding that using a MCD while driving a vehicle on state business requires the use of a hands-free accessory unless specifically exempt. Any traffic violations or payment of fines imposed for violation of any applicable laws are the User's personal responsibility.