

<b>Oregon Public Employees Retirement System</b>	<b>Posted date</b> March 12, 2010	<b>Number</b> 1.10.01.01.008.POL
<b>Signature</b> <i>Paul N. Cleary</i>	<b>Approval date</b> March 10, 2010	<b>Page</b> 1 of 6
<b>Policy:</b>	Acceptable Use of Information Systems	
<b>Objective:</b>	Directs authorized individuals and third parties on the appropriate and acceptable use of the agency's information, computer systems, and devices.	
<b>References:</b>		

### Policy

This policy applies to all employees and individuals working for third parties that have an authorized business relationship with the agency and who have been granted access to agency information independent of its form. This policy is modeled after and complies with the DAS [Acceptable Use of State Information Assets](#) policy.

As a condition of continued employment or contract with PERS, employees and authorized third parties will conduct their assigned duties with ethical conduct consistent with this policy. The agency may withdraw permission for any or all personal or business use of its systems at any time without cause or explanation.

In the performance of duties at PERS, employees are individually entrusted with a great responsibility to administer the Public Employees Retirement System with the highest degree of integrity in their daily actions and decisions. PERS employees are professionals who take their responsibilities to PERS members, employers, and other stakeholders seriously. PERS employees are responsible stewards of the information they use and for the privacy and security of the agency's customers, members, and stakeholders.

In the performance of assigned duties, individuals and third parties shall take all reasonable precautions to protect sensitive information stored within agency systems and maintain lawful, ethical, and respectful behavior that includes, but is not limited to, the following core principles:

- actions shall comply with all federal, state, and local laws; and statutes and regulations;
- actions shall not include those that can be reasonably construed as being deceitful, offensive, fraudulent, or dishonest, obscene, harassing, threatening, or defamatory, nor as violent in any form, including physical, verbal, or written;
- actions shall not include those that are pornographic or sexually explicit;
- actions shall not include those that are discriminatory with regard to race, age, gender, sexual orientation, religious or political beliefs, national origin, health, or disability;
- actions shall not include those that waste or misuse agency and state resources;
- actions shall not include those that use, delete, or alter agency data and information without proper authorization and justification;

---

Origination date: December 13, 2000  
Last revision date: February 23, 2010  
Last review date: February 23, 2010

- 
- actions shall not include using state assets for personal gain or profit; and
  - actions shall not include any activity, investment, or interest that might reflect unfavorably on the reputation of the agency and its employees.

### **Terms of Use**

Use of PERS' system and e-mail shall comply with all applicable state, federal, and local laws, and all statewide policies and agency policies, including [Personal Use of State Resources](#) policy 1.01.00.00.031.

All information stored within agency systems are the property of the state of Oregon. All systems and information contained therein are the sole property of the state of Oregon and subject to its control unless an overriding agreement or contract exists to the contrary. No part of agency systems or information is, or shall become, the private property of any system user. Any and all use of information, unless exempted by law, is subject to public disclosure.

The agency reserves, and intends to exercise, all rights relating to information used in its systems. When necessary, the agency will access and review any information in accordance with applicable policies. The agency deploys various monitoring tools and techniques to ensure compliance with appropriate laws, regulations, and policies.

Oregon Revised Statute (ORS) 192.502(12) exempts employee, member, and retiree address; Social Security number; telephone number; other non-financial membership information; and employee financial information from public disclosure. Individuals with access to this information must use the appropriate measures to protect the members' privacy in accordance with the [Data Classification](#) policy (1.10.01.01.003) and [Information Handling Standards](#) located on the Information Security Intranet site.

Individuals are responsible for the security of their account passwords. Passwords shall not be shared with others under any circumstances without appropriate management direction. Passwords must be changed at least every 90 days. Individuals must surrender agency property, encryption keys, passwords, or other security mechanisms at termination of employment or contract.

Remote access must be for PERS business purposes and approved by management. Individuals shall not log into PERS systems from remote locations unless they are using PERS-approved and provided remote access systems, except that access to e-mail via the Web is allowed with management approval.

### **Allowed Use**

PERS provides users with information and system resources to conduct business for the state of Oregon. Any use of information and/or systems must comply with this policy. Business use includes accessing information related to an employee's assigned duties and employment with the state, including all rights per the collective bargaining agreement. Other approved sites related to

---

Origination date: December 13, 2000

Last revision date: February 23, 2010

Last review date: February 23, 2010

---

employment with the state are PEBB, PERS, EAP, IAP, DAS, BOLI, the Oregon Jobs page, Oregon Savings Growth Plan, and the agency's Intranet.

Certain use of state provided equipment in cases of emergency or to check weather conditions may be deemed acceptable based on management approval.

Based on their assigned duties or an authorized contract, individuals and third parties that have access to information contained within the agency's systems or premises are given access to that information on a need-to-know basis. Management may allow individuals access to view their own account information for business purposes only.

Users are allowed to play audio CDs or DVDs using state equipment provided it does not interfere with their work or others' work and such use does not violate the other provisions of this policy.

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, employees are allowed limited, incidental personal use during their lunch break only as long as there is no or insignificant cost to the state (see [Personal Use of State Resources](#) policy, 1.01.00.00.031). Personal use allowed during lunch breaks includes online banking, shopping, and social networking sites, which do not violate the other provisions of this policy. Take extra precautions when on the Internet to protect the agency's systems and information from malware and data theft. Banking and shopping transactions are discouraged and are taken at your own risk. Management has sole discretion to determine whether a use is limited or incidental. Management has the right to block access to sites at any time without notice if they deem blocking access is necessary for the protection of PERS information and systems.

E-mail is to be used for state business. Employees are allowed limited, incidental personal use during their lunch breaks only as long as there is no or insignificant cost to the state (see [Personal Use of State Resources policy](#), 1.01.00.00.031) and such use does not violate the other provisions of this policy. E-mail may be used for union business per the collective bargaining agreement. E-mails are public record and all individuals are responsible for ensuring compliance with archiving and public records laws. Information transmitted externally shall be appropriately protected as outlined in the [Data Classification](#) policy 1.10.01.01.003.

### **Use Not Allowed**

Individuals shall not download or install unapproved programs from the Internet or other external sources (including portable computing and storage devices) without prior management approval. This includes, but is not limited to, photos, screen savers, music programs, video clips, software applications, utilities, and other executable code that are not business related. An employee or third party may request an exception using the form located on the Intranet. All exceptions must be documented and approved by management. The Helpdesk shall maintain a list on the Intranet of pre-approved software that individuals can download or install without using the exception process.

Individuals shall not attach any hardware device to an agency provided computer except for preapproved peripheral devices such as PDAs, digital cameras, flash drives, etc. To install any

---

Origination date: December 13, 2000

Last revision date: February 23, 2010

Last review date: February 23, 2010

hardware device to an agency provided computer, individuals must contact the Helpdesk. Privately owned devices (i.e., PDAs, digital cameras, flash drives, etc.) shall not be connected to PERS networks, computers (including remotely used laptops), or other equipment without approval of the Helpdesk prior to connection. All hardware attached to state systems shall be appropriately configured, protected, and monitored so it will not compromise state information assets. The Helpdesk will assist individuals in connecting pre-approved, privately-owned devices, but should not be expected to provide ongoing support of those devices.

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

Non-exempt employees shall not access PERS systems, including e-mail, when they are not scheduled to work.

Using Instant Messaging applications for personal use is prohibited. Using Peer-to-Peer (P2P) networking applications is prohibited at all times.

### **Public Use of Systems**

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

### **Compliance**

Violation of terms of this policy can result in limitation, suspension, or revocation of systems use privileges, and can lead to disciplinary action up to and including dismissal from state service or cancelation of contract. Knowingly violating portions of this policy may be construed as a computer crime under [ORS 164.377](#). Civil penalties may be imposed by the courts or the Oregon Government Standards and Practices Commission under ORS 244.350.

A valid collective bargaining agreement or contract shall supersede any conflicting terms in this policy.

### **Employee acknowledgment:**

I have read and understand the Acceptable Use of Information Systems policy. I further understand this document shall be retained in my personnel file, where I may refer to it at any time. I understand that failure to comply with this policy may lead to disciplinary action up to and including dismissal.

---

Employee print name

---

Employee signature

---

Date

---

Origination date: December 13, 2000

Last revision date: February 23, 2010

Last review date: February 23, 2010

**Roles and Responsibilities**

<b>Role</b>	<b>Responsibility</b>
User	Contact direct supervisor to request permission to download or install software.
	Contact direct supervisor to request approval and make arrangements for remote access.
	Contact direct supervisor to request approval for hardware connection to PERS' systems.
	Contact direct supervisor to request an exception.
	Contact direct supervisor to request approval for encryption services.
	Contact direct supervisor, information security officer, or Human Resources section to report any violations of this policy.
Direct Supervisor/Manager	Approve or deny request for software. If approved, send request to Helpdesk.
	Approve or deny request for remote access. If approved, send request to Helpdesk.
	Approve or deny request for encryption services. If approved, send request to Helpdesk.
	Approve or deny request for hardware. If approved, send request to Helpdesk.
	Approve or deny request for exception. Document all approved exceptions to this policy.
	Contact your direct supervisor, the information security officer, or Human Resources section to report any violations of this policy.
	Contact Helpdesk for approval and assistance whenever the need arises to remove the user's identity from e-mail.
	Contact Human Resources and the information security officer for guidance on any reported violation of this policy.
Human Resources	Notify direct supervisor and information security officer of allegations of non-compliance.
	Investigate allegations of non-compliance of this policy.

Origination date: December 13, 2000

Last revision date: February 23, 2010

Last review date: February 23, 2010

---

<b>Role</b>	<b>Responsibility</b>
	Recommend appropriate action to supervisor, administrator, and executive director.
Information Security Officer	Review and update policy as needed.
	Provide data and/or analysis as needed.

---

Origination date: December 13, 2000

Last revision date: February 23, 2010

Last review date: February 23, 2010

SL2