




**OREGON DEPARTMENT OF FISH AND
WILDLIFE POLICY**
Information Services Division

Title:	Acceptable Use of State Information Assets	ISD_610_01
Supersedes:	February 1, 2008 ISD_610_01 Use of Electronic Systems	
Applicability:	All state employees, volunteers, their agents, vendors and contractors, including those affiliated with third parties who access state information assets, and all others authorized to use state information technology for the purpose of accomplishing the state's business objective and processes.	
Reference:	ODFW HR_410_02 Code of Conduct DAS Statewide Policy 107-004-110 Acceptable Use of State Information Assets	
Effective Date:	October 15, 2010	Approved: 

I. PURPOSE

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

II. DEFINITIONS

- A. **Chat Room** – Where participants join a virtual group discussion using their PCs and the Internet. The discussion may or may not have a moderator and comments are communicated in writing.
- B. **Blogging** – A journal with one or many contributors of text, images, media objects, and data commonly displayed in reverse chronological order that can be viewed with a web browser.
- C. **Computer system** – Hardware and software generally used for data processing. Examples include, but are not limited to desktop PCs, laptops, handheld devices, servers, data storage devices, network devices (routers, switches, hubs, etc.), operating systems, applications, programs, and utilities.
- D. **Confidentiality** – A security principle that works to ensure information is accessible only to those authorized and for specific purpose intended of conducting agency business.

- E. **Controls** – Means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature.
- F. **Desktop Image (also known as Wallpaper)** – The background image of a computer display screen, on which windows, icons, and other graphical items appear. The Desktop Image differs from a Screen Saver in that a simple and static picture is displayed without the use of a computer program.
- G. **Downloading** – Is the transfer of a file from one computer system to another. In context of this policy the term ‘downloading’ generally refers to the act of an individual user and not the normal process of a computer operating system or approved applications.
- H. **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.
- I. **Information Asset** – Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics that has value to the organization.
- J. **Information Systems** – Computers, hardware, software, storage media, networks, operational procedures and processes used in the collection, processing, storage, sharing or distribution of information within, or with any access beyond ordinary public access to, the state's shared computing and network infrastructure.
- K. **Information Technology** – A general term used to define all hardware, software, data, and services as a valued asset to the agency.
- L. **Integrity** – A security principle that works to ensure a consistent and predicable framework of information and systems where assets are not modified maliciously or accidentally.
- M. **Network** – An interconnected group of computers and other technology for the sharing of information between two or more systems.
- N. **Peripheral Device** – Any device that connects, shares, or transfers data to a computer system. This includes, but is not limited to, PDAs (Personal Digital Assistants), USB (Universal Serial Buss) devices, external disk drives, digital cameras, printers, video/audio players, or controllers.
- O. **Personal Use** – Activity not considered essential or relevant to the daily business of the agency and is limited or incidental with no or insignificant cost to the state.
- P. **Public Facing** – In direct view by the general public within a state office or while in the presence of the public.

- Q. **Risk** – The likelihood of a threat to a known vulnerability and the resulting business impact measured by loss potential, or probability.
- R. **Screen Saver** – A picture or moving graphical image that is activated after a certain length of inactivity. A screen saver was originally intended to protect the image quality of a computer monitor but is now often a measure to secure unauthorized access to a computer. The Screen Saver differs from a Desktop Image in that a computer program is required to generate images, often moving, instead of simple display of a static picture.
- S. **Transaction Based** – An agreement, communication, or commitment often involving the exchange of items of value, goods, services or money.
- T. **User** – All state employees, volunteers, their agents, vendors and contractors, including those users affiliated with third parties who access state information assets, and all others authorized to use state information technology for the purpose of accomplishing the state's business objectives and processes.
- U. **Web Browser** – An application that enables a user to display and interact with text, images, videos, music and other information from the Internet.
- V. **Web Enabled** – A device with the capability of launching a web browser or communicating to the Internet. This includes devices such as, but is not limited to, desktop PCs, portable computers, printers, tablets, PDA's, web cameras, remote devices, and cellular telephones.
- W. **Wallpaper** – see 'Desktop Image'

III. POLICY

A. State Business

It is the policy of the Oregon Department of Fish and Wildlife to provide access to information, computer systems and devices for the purpose of conducting business in support of the agency's mission, goals and objectives. The purpose of any data, computer system or device is for the exclusive use of state business except as defined by agency policy. It is the duty of all users to protect all state information assets entrusted to their use from accidental or purposeful disclosure, modification or loss. Users of state information assets are responsible for complying with the provisions of this policy, supporting policies, procedures and practices.

B. 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 or any part or product of its

systems. All uses shall comply with this policy and any other applicable state policies and rules that apply. The agency is 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.

C. Access and Control

Users of state information assets are responsible for complying with the provisions of this policy and supporting policies, procedures and practices. The State of Oregon reserves, and intends to exercise, all rights relating to all information assets. The agency is 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. The agency may withdraw permission for any or all use of its systems at any time without cause or explanation.

D. Professional Conduct

Use of state information assets shall not be false, unlawful, offensive, or disruptive. Agency networks and systems shall not be used to intentionally, download, store, transmit, retrieve, or display 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.

E. Legal Compliance

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

Users shall comply with public records retention laws and rules.

F. Security

To properly safeguard state information assets including data, employees are expected to be knowledgeable of basic security principles including the use of passwords and risk avoidance.

Any use of state information systems shall respect the confidentiality of other users' information and shall not attempt to:

- a) Access third party systems without prior authorization by the system owners;
- b) Obtain other users' login names or passwords (including subordinates, coworkers, or others);
- c) Attempt to defeat or breach computer or network security measures;
- d) Intercept, access, or monitor electronic files or communications of other users or third parties without approval from the author or responsible business owners;
- e) 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.

Portable Electronics, including laptops, PDA's, USB drives, cell phones and other portable devices, may contain a substantial amount of agency data. Employees are to manage the physical and electronic security of such devices in accordance with the sensitivity of the data contained on the device. This may include startup passwords, security cables, and proper storage locations.

Any potential security breach or indiscriminate loss of agency information assets (hardware, software, or data) must be reported immediately to the Information Systems Division.

G. Data Integrity

Users shall protect data stored in state information systems from negligent or malicious acts that may destroy, misrepresent, or otherwise change the data.

Users shall store and retain data files only on agency provided network servers or other systems approved by the Information Systems Division for permanent storage of data. Data folders on laptops must be automatically synchronized to permanent storage on file servers. Only temporary data files or copies of original data files may be stored on local (C:) hard drives.

H. 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.

Standard configuration and deployment of information assets will be utilized wherever possible maximize agency resources and reduce operational costs. (See sections on Hardware, Software)

I. Accounts and Account Passwords

All users shall be properly authorized and authenticated to use state information assets. Every user of the agency computer network shall be issued a unique authentication ID and password to ensure the overall security and integrity of agency data and services. At no time shall employees share passwords with supervisors, co-workers, vendors, family members, or others.

Users are fully responsible for all activity that occurs on their accounts and are expected to secure their access to state information assets from inadvertent use. Generally this is accomplished by logging out or otherwise locking access that prevents unauthorized use.

J. Downloads

Users may download simple data files, images, video, or audio (Word, Excel, MPG, JPEG, WAV, text, or raw data) in the course of conducting agency business. Any image, video, or audio file that would result in copyright or license violations shall not be downloaded onto state systems.

The Information Systems Division provides resources for product standards, licensing, and exceptions to meet agency needs. Users may not download or install software programs, applications, utilities, weather bugs, toolbars, web browsers, or screen-savers to agency information assets unless pre-approved by the Information Systems Division. Many products are licensed or restricted by copyright while others may create compatibility or maintenance problems. This includes freeware, shareware, and trial versions. Users may download, view, or display any desktop image (wallpaper) on agency computers provided the image is not restricted by copyright or license and is consistent with all other agency policy.

All computer system updates are provided by the Information System Division through automated updates or other approved processes. Automated updates within licensed software (example Real Player, Adobe) should be disabled unless otherwise instructed by the Information Systems Division technical support.

K. Remote Login

Access to state agency networks from remote locations or devices is not allowed except through the use of agency-approved and agency-provided remote access systems or software. The agency may provide remote access from privately owned devices to specific business applications such as email. However, such access must have prior approval by supervising management and otherwise comply fully with this policy.

Establishing connectivity to private networks or devices using Virtual Private Network (VPN) or other forms of remote access is not allowed for security reasons unless properly established and secured by the Information System Division.

L. Use of E-Mail

E-mail is to be used only for state related business or as allowed by policy. 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.

M. Hardware Installation

Hardware devices shall not be attached (wired or wireless) to a state provided computer or device 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 prior approval of the Information Systems Division except as permitted by policy. All hardware attached to state systems shall be appropriately configured, protected, and monitored so it will not compromise state information assets.

N. Software Application Installation

Software applications (including freeware, shareware, privately owned, or trial versions) shall not be loaded to a state provided computer or device that has not received prior approval of the Information Systems Division. Privately owned software shall not be loaded to state networks, computers (including remotely used computers) or other equipment. All software applications loaded to state systems shall be appropriately configured, protected, and monitored so it will not compromise state information assets.

O. 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 or as allowed by policy (see section on Personal Use). 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 immediate safety may be allowed by policy (see section on Personal Use).

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.

Instant Messaging (IM), other communications/messaging alternatives, streaming video and streaming audio are for business purposes only. However, these uses shall be agency approved, documented, adequately secured, and comply with public records and archiving laws.

P. Use of Encryption

The agency may provide hardware or software encryption for the purposes of storing, transmitting, or otherwise protecting agency information assets. Users may use such products only for the intended business purpose and as procedures indicate. Users will not attempt to circumvent or defeat any encryption device or system.

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.

Q. 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.

R. Personal Use

Any personal use is intended to provide a work friendly environment and must never compromise the integrity, policy, or etiquette of this agency. Such personal use should be considered limited or incidental where there is no or insignificant cost to the state. However, this privilege comes with specific responsibilities and boundaries that must be respected.

The agency director has authorized limited personal use of state information assets as outlined in this section. Any personal use must fully comply with this policy. Public facing systems are exclusively for official business and not intended for personal use. The agency has the sole discretion to determine if an employee's use is personal or business.

In general, any personal use of agency information assets is:

- a) For viewing purposes only and not transacting personal business or purchases;
- b) Permitted during breaks or lunch periods but not before or after scheduled work times;
- c) Does not negatively reflect on the agency or otherwise hamper productivity;
- d) Incidental and respectful of coworkers;
- e) A public record and open to discovery and audit;
- f) Permitted on systems that are not in direct view by the public;
- g) Allowed only as defined by policy.

1. **Personal Use of CDs, DVDs**

Users may play music or display pictures from personally owned CDs or DVDs using state equipment (per state agency policy) provided it does not interfere with their or other's work. Users may also set the desktop image (wallpaper) using pictures contained on a personally owned CD or DVD provided it meets all criteria as described in policy. Users are not otherwise allowed to transfer or store personally owned music, pictures, or any other files 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. State agency workstations and notebook computers may not be used to make "compilation" CDs/DVDs or to "burn" audio or video disks for personal use. State workstation and notebook computers may not be used to transfer music, pictures, or other files to portable players. Peer-to-Peer (P2P) file sharing is prohibited on the state network. State agencies shall approve and document any exceptions.

2. **Personal Use of Internet Web Browser**

Users may access information on the Internet for the purposes of viewing information only. Transaction based activities are not permitted any time and include, but are not limited to, banking activities, purchasing products, and stock market trading.

3. **Personal Use of Internet Email**

Users may access personal web email using a web enabled device if such activity does not require any software downloads or special setup. Personal email accounts may not be synchronized or auto-forwarded to state information assets or to the agency email systems (Outlook or connectors). Users may use their personal email accounts to download desktop images (wallpaper) as allowed by policy.

4. **Personal Use of Agency Email**

Users may access the agency's email system to send or receive limited and incidental personal messages without file attachments. Attachments may include, but are not limited to, photos, music, files, or other documents. Personal email accounts may not be auto-forwarded to state systems. Users may also employ other functions of the agency email such as the calendar, tasks, notes, or contacts for limited and incidental purposes.

5. **Personal Use of Instant Messenger (IM)**

Personal use of Instant Messenger (IM) or other web based messaging systems is not permitted.

6. **Personal Use of Chat Rooms and/or Blogging**

Contributing to a Chat Room or Blogging is not permitted. Users may view or research topics only.

7. Personal Use Downloading Files

Downloading of any other files, software, music, or images to/from state information assets for personal use is not permitted unless otherwise stated in policy

8. Personal Use of Printers, CD-RW, DVD-RW and Other Peripherals

The use of peripheral devices for personal use is not permitted. Consumable items typically used in conjunction with peripheral devices are for business purposes only including, but not limited to paper, ink, media, memory cards or USB keys.

9. Exempt Equipment and Devices

Agency management has the sole discretion to determine if any state information asset is exempt from personal use due to possible risk, physical location, or sensitivity of equipment.

10. Technical Support

Technical support is not provided for any personal use or for home computers used for remote access to agency systems (as otherwise permitted by policy).

11. Liability / Responsibility

Any personal use of agency information assets or services is done so at the exclusive risk by the employee, including but not limited to the potential of identity theft and credit fraud. Employees' personal information may be collected and retained by system settings (such as cookies, audit devices, asset management, or data retention systems). Any personal use of agency systems may be subject to disclosure per public record law. Employees may not alter, or attempt to alter such devices designed to protect agency data or systems. Technical support for personal use is not provided by the agency.

S. Public Use of State Systems

Agency-provided e-mail systems and Internet access for the general public, if any, shall be appropriately secured in order to properly protect state information assets. Such access must be pre-approved and established within the context of policy.

T. Monitoring and Control

The agency is responsible for monitoring use of information systems and assets. The agency 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. The agency may, without prior notice, collect and examine any electronic communication, stored data, or system logs for the purposes of managing information systems and assets and compliance with policy.

If sensitive information is intentionally or unintentionally viewed or accessed, the employee should immediately notify his or her supervisor. In addition, the supervisor must report the incident to the Information Systems Division.

U. Public Record Law

Users are responsible for retaining and storing data file and folders per State Agency General Records Retention Schedules electronically or physically. Information can be found at http://arcweb.sos.state.or.us/rules/OARS_100/OAR_166/166_300.html

V. Violation

Violation of terms of this policy can result in limitation, suspension or revocation of access to state information assets and can lead to other disciplinary action up to and including dismissal from state service.

Inappropriate use of state information assets by an employee must be documented and promptly reported to the Human Resources Division Administrator.

Knowingly violating portions of this policy may also constitute "computer crime" under ORS 164.377 (see Attachment A). It is the duty of all users to report any activity that could compromise the security of state assets or be considered computer crime immediately to management and the Information Systems Division.

W. Exceptions

Exceptions to policy will be documented and approved by the agency director or deputy director and/or the Information Systems Division Administrator prior to incorporation with any agency information system. Documentation must include the date the exception is requested, a description of the situation, and the expected date of resolution.

Notwithstanding specific prohibitions in this policy, ODFW employees 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.

X. Procedures

All new and returning employees shall be given a copy of the policy and the policies referred herein, an opportunity to read and ask questions, and shall sign the Information Systems Certification Form (Attachment B).

Upon implementation of the February 1, 2008 policy, any current employee may voluntarily sign the Information Systems Certification Form and send it to the Human Resources Division for placement in the employee's personnel file.

All copies of signed Information Systems Certification Forms should be sent to the Human Resources Division for placement in the employee's personnel file.

Attachment A

ORS 164.337 – 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 devices 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 issued 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 or 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 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]

OREGON DEPARTMENT OF FISH AND WILDLIFE

INFORMATION SYSTEMS CERTIFICATION FORM

By my initials, I certify that I have read each of the policies referenced below, and have been given an opportunity to ask and to receive answers to any questions I might have concerning the provisions of these policies. I understand the provisions of these policies as they apply to my employment with the Oregon Department of Fish and Wildlife.

Initials

ISD_610_01

Acceptable Use of State Information Assets

ISD_630_01

Security of Information Systems

This form shall be retained in my official personnel file.

Employee Name (type or print clearly)

State Employment Number

Employee Signature

Date

Employee's signature confirms only that the supervisor has discussed and given a copy of the material to the employee. The employee's signature does not indicate agreement or disagreement with the contents of this material.

Manager/Supervisor Signature

Date