OREGON DEPARTMENT OF FISH AND WILDLIFE POLICY
Information Services Division

Title:	**Acceptable Use of State Information Assets**	**ISD_610_01**
Supersedes:	ISD_610_01 Acceptable Use of State Information Assets dated October 15, 2010	
Applicability:	All state employees (their agents), volunteers, 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:	HR_410_02 Code of Conduct ISD_620_01 Information Asset Classification ISD_620_02 Transporting Information Assets	
Effective Date:	**December 1, 2014**	**Approved:**

I. PURPOSE

This policy establishes the appropriate and acceptable use of state information assets (e.g. computers, peripherals, portable computing devices, software, data, network, and others) for all users.

II. DEFINITIONS

A. **Agency:** General term that refers to the Oregon Department of Fish and Wildlife and employees.

B. **Blog (Blogging):** A web site containing the writer's or group of writers' own experiences, observations, opinions, etc., and often having images and links to other web sites. While actively contributing, participation is considering blogging.

C. **Chat Room:** Where participants join a virtual discussion using computers or other electronic devices. Typically using the Internet but may be other mobile connectivity. The discussion may or may not have a moderator and comments are communicated in writing, voice, images, videos, and other forms of multimedia.

D. **Cloud Services (Also known as Cloud Computing):** A model for delivering information technology services or applications (free or fee based) in which resources are

retrieved from the Internet through web-based tools, rather than from a user's PC or from agency network servers. Data and software applications are stored or hosted from remote data servers. Cloud computing allows access to information as long as an electronic device has access to the Internet.

Examples of Cloud Services include iPOS, data backup storage, Google Docs, stock market analytical tools, internet email, on-line collaboration, Software as a Service (SAS), hosted networking and servers.

E. **Computing Device:** Any electronic hardware and its associated software used for some form of data processing. May be stationary or portable. Examples include, but are not limited to desktop computers, laptops, tablets, handheld devices, servers, data storage devices, network devices (routers, switches, hubs, etc.), operating systems, applications, programs, and utilities.

F. **Confidentiality:** A security principle that works to ensure information is accessible only to those authorized for a specific intended purpose.

G. **Downloading:** Is the transfer of a file or group of files (data, audio, video or other) from one computing device 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 key.

I. **Information Asset**: Any, data, application, computer, peripheral, portable device or other technology used to store, transport, modify, display, or report information that has value to the organization regardless of its physical form or characteristics.

J. **Information Systems:** Computers, hardware, software, peripheral, portable computing devices, storage media, networks, operational procedures and processes used in the collection, processing, storage, sharing or distribution of information assets.

K. **Information Technology:** A general term used to define individual or subset of components belonging to an Information System.

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 computing devices and other technology for the sharing of information between two or more information systems.

N. **Peripheral Device:** Any device that connects, shares, or transfers data to an information system. This includes, but is not limited to, mouse, keyboard, printers, scanners, smart phones, USB (Universal Serial Buss) devices, external disk drives, digital or video cameras, and microphones.

O. **Personal Use:** Activity not considered essential or relevant to the daily business of the agency.

P. **Portable Computing Device**: Any mobile electronic device typically having a screen, input device and powered by battery. Often has the ability to interface with other portable computing devices, the Internet, or computer systems.

Q. **Public Facing:** In direct view by the general public within a state office or while in the presence of the public. May also be a service intended for use by the general public.

R. **Risk:** The likelihood of a threat to a known vulnerability and the resulting business impact measured by loss potential, business impact or probability.

S. **Screen Lock (previously Screen Saver):** A feature that activates after a certain length of inactivity or by other methods to secure the computing device from access. May or may not present a static graphical image for privacy. Requires the user to re-enter a passphrase, fingerprint, swipe a pattern or other method of authorization to re-enter.

T. **Screen Saver:** An outdated term describing a method of protecting older computer monitors (Cathode Ray Tube) from damage and also a method to secure computing devices from unauthorized access. See 'Screen Lock'.

U. **Software as a Service (SaaS):** Software provided over the Internet that may be leased, purchased, or free. Use is governed by contract or terms of agreement but cannot be fully downloaded or owned. Often is a single product offering that fills a specific business need.

V. **Transaction Based:** An agreement, communication, or commitment often involving the exchange of items of value, goods, services or money.

W. **User:** All state employees (and their agents), volunteers, 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.

X. **Web Browser:** An application that enables a user to display and interact with text, images, videos, music and other information from the Internet.

Y. **Web Enabled:** A device with the capability of launching a web browser or otherwise communicating to the Internet. This includes devices such as, but is not limited to, desktop PCs, portable computing devices, web cameras, and smart phones.

Z. **Wallpaper:** The background image of a display screen, on which other windows, icons, and other graphical items appear. May be in the form of a static image or 'live' wallpaper where the image changes, flows, or moves.

III. POLICY

A. State Business

It is the policy of the Oregon Department of Fish and Wildlife to provide access to information systems and computing devices for the purpose of conducting business in support of the agency's mission, goals and objectives. The purpose of any data, computing device or system 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

All information assets created, stored, modified or transported within agency applications, systems, computing devices or networks are the sole property of the State of workplace. 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 inspect, monitor, control, transfer, or limit use of state information assets at any time regardless of the device that collects, stores, or displays such information unless an overriding written agreement exists to the contrary.

C. Safety

It is critically important to use technology safely and not create a hazard to yourself or others especially while using portable computing devices. Distractions while walking, driving or other work conditions may create a dangerous situation leading to injury or death. Certain actions may also create legal liability if you are aware of a risk to others and contribute to the behavior (such as texting to someone driving that is also texting). Users must not use, or contribute to the unsafe use of any portable computing devices while walking, driving, or otherwise in an unstable working environment.

D. 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.

E. Professional Conduct

Use of state information assets shall not be used for false, unlawful, offensive, or disruptive actions. 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.

F. **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, rules, and agency's policy and procedures governing the safe keeping and proper destruction of information assets.

Knowingly violating portions of this policy may also constitute "computer crime" under ORS 164.377 and subject to misdemeanor and felony charges.

G. **Security**

To properly safeguard state information assets including data of all types, employees are expected to be knowledgeable of basic security principles including the use of authentication (login ID and password or other forms of secure identification), risk avoidance (taking elevated actions based on situation or value), data classifications levels (importance or sensitivity of information), and properly storing/transporting information assets (securing and protecting). It is the duty of all users to report any potential security breach or indiscriminate loss of agency information immediately and without delay to the Information Systems Division.

Any use of state information systems 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, breach, or bypass computer or network security measures;**

d) **Use or attach personal or unauthorized devices, applications, or systems to agency computing or telecommunication devices except as explicitly allowed by policy;**

e) **Intercept, access, or monitor electronic files or communications of other users or third parties without approval from the author or responsible business owners;**

f) **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.**

Employees are to manage the physical and electronic security of such devices in accordance with the sensitivity of the data contained on the device and the likelihood of disclosure. This may include startup passwords, security cables, and safely transporting and storing portable devices.

Also see policy ISD_630_02 'Portable Data Storage' and ISD_620_02 'Transporting Information Assets'.

H. Incident Reporting

Any potential security breach or loss of agency information assets (hardware, software, or data) must be reported immediately to your direct supervisor. In cases of significant risk (e.g. electronic or physical break-in, lost or stolen computing devices that are unsecured), a data compromise (e.g. known exposure to unauthorized individuals), or anything impacting the security of Level 3 'Sensitive' or Level 4 'Restricted' information (e.g. SSN, banking numbers, or customer credit card information) must report to the Information Systems Division within 1 hour of discovery to minimize the potential harm to the agency. Executive Leadership Members have access to emergency contact information during off hours.

I. Data Integrity

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

Users shall store and retain data files only on agency provided network file storage or other systems approved by the Information Systems Division for permanent storage of data. Data folders on laptops, tablets, and other portable computing devices must be automatically or manually synchronized to permanent network storage

Storing data to any local storage (e.g. C: drive, flash memory, USB, SD or memory cards) is only for temporary data files or copies of original data files. Data stored on local devices is not recoverable in the event of accidental deletion or equipment failure.

J. Operational Efficiency

Computing devices, applications, and information assets shall be used in such 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 used wherever possible to maximize agency resources and reduce operational costs. Whenever possible, rights and privileges will be assigned to the user by their role in the agency, not the individual themselves.

K. Accounts and Account Passwords

Every user of the agency computer network shall, at a minimum, 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.

All permanent and temporary users have a base account created automatically that includes an individualized home directory to store files. Additional access privileges are granted or

revoked by request of the users' direct supervisor or any supervisor within the direct chain of command.

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 or intentional use by anyone except the account owner. Generally this is accomplished by logging out or otherwise locking access that prevents any unauthorized use when the account or device is not in use.

Supervisors may request that two or more users (with separate login ID) share common data resources (such as project files, folders, and databases).

L. **Downloads**

In the course of conducting agency business users may download or stream data files including those containing text, database, images, audio, or video to any computing device or system.

Users may download, view, or display wallpaper on agency computing devices provided the image is consistent with all other agency policy. Dynamic or 'live' wallpaper is allowed only if it does not consume computing resources of the agency network or other computing devices.

At no time for business or personal use shall a user download any file, folder, application, image, video, or audio file that would result in copyright or license violation.

Updates to software, operating systems, apps, and other products are provided by automated updates or other approved processes by the Information System Division. Users shall not attempt to modify settings that disrupts or otherwise changes this process.

Users may not download or install software programs, applications, utilities, weather bugs, toolbars, web browsers, or screen locks (screen savers) to agency information assets unless pre-approved by the Information Systems Division. This includes freeware, shareware, and trial versions. Many products are licensed or restricted by copyright while others may create compatibility or maintenance problems. When requested to 'accept terms and conditions' to continue, users must contact the Information Systems Division for further direction.

The Information Systems Division provides resources for product evaluations and exceptions to standard deployments upon request to meet agency needs.

M. **Cloud Services**

The use of cloud services (free or fee based) that store, access, or share agency data for temporary or permanent use must be pre-approved by the Information Systems Division prior to use. In virtually all cases, the use of cloud services enters the agency into a legal agreement, possibly financially, and may pose a security, audit, public discovery, licensing, and other risks to the agency or state systems. Examples include, but not limited to, cloud based file backup or transfer services, software as a service (SaaS), remote application hosting, and others.

Note: The general use of web browsers for to research or view information is not a cloud service and may be used without limitation unless otherwise limited by policy or license agreement.

Also see section on 'Downloads' for further information.

N. Software as a Service (SaaS)

Software as a Service is managed by policy in the same way as software installed directly on agency computers or other devices from a CD/DVD or other media. At no time shall agency data be stored or transferred to SaaS services (free or fee based) prior to review of Terms of Conditions agreements and authorization by Information Systems Division and Contract Services.

Also see sections on 'Software Licensing' and 'Software Installation'

O. Remote Login

Access to state agency networks, computers, or devices from remote locations is not allowed except through the use of approved remote access systems, software, or devices. This includes but not limited to remote desktop access, Virtual Private Network (VPN), peer to peer networking, or other forms of remote access.

Remote access from locations other than the users work station or at times outside the users work schedule must have prior approval by their supervising manager and otherwise comply with agency policy.

For use of public facing business applications such as email (Mallard), iPOS control center, FTP (File Transfer Protocol) and other services, see policy ISD_610_02 'Bring Your Own Device' (BYOD).

P. Use of E-Mail

E-mail is to be used only for agency 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-mails are public record and all users are responsible for ensuring compliance with archiving and public records laws. Confidential or Personally Identifiable Information (PII) may be restricted or not permitted depending on the data classification. Users must assume email is unsecure and could be intercepted, copied, or resent to unwanted recipients.

Q. Hardware and Software Installation

All hardware and software shall be operated within the users assigned work responsibilities and shall be appropriately configured, licensed, protected, and monitored so as not to create unnecessary business risk to any state information asset.

The Information Systems Division may establish hardware, software, data, and other technology standards for systems or devices for any agency use. This includes IT assets that are attached (physically or wirelessly) to the agency's computer network or stand-alone systems and devices of similar computing functions.

Privately owned hardware or software shall not be connected or installed at any time to state networks, computers (including remotely used computers) or other computing devices except as permitted by policy.

An exception process will document any deviations to established standards as necessary to meet business needs.

R. Software Licensing

All software in use by the agency will be properly licensed. Software licensing requirements are set by each manufacturer or developer so legal use requirements vary greatly. Any software that requests the user to 'accept' terms and conditions as part of the installation process must be properly licensed for agency use.

Software applications (including freeware, shareware, privately owned, or trial versions) shall not be loaded to a state provided computer or device except as allowed by policy or ISD procedures.

Violations of software licensing can result in substantial fines and penalties for the individual and/or agency.

Also see section 'Hardware and Software Installation'.

S. Use of Encryption

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

Hardware or software may not be used to encrypt any information asset 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 prior permission and direction from the agency director.

T. 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.

U. **Business Use of Internet, Networks and Services**

The state provides access to the Internet, networks, and other services for the purposes of conducting state business and limited personal use as defined in policy (See section on Personal Use). Business use includes access to information related to employment with the state, provisions outlined in the SEIU Collective Bargaining Agreements. Examples include but are not limited to state benefits and services such as, PEBB, PERS, EAP, e-Paystub, Oregon JOBS, and Oregon Savings Growth Plan. Unless otherwise allowed, such use is expected to be limited or incidental. As an exception, uses that involve an emergency or immediate safety issues are allowed. (Also see section on Personal Use).

Agency computing devices and systems may not be used to play games regardless of the source of the game. State systems may not be used for hosting or operating personal web pages, chat rooms, or list serves; or for creating, sending, or forwarding chain e-mails, spam messages, or other information disruptive to business operations.

Streaming video and streaming audio are for business purposes only to minimize agency costs and impact to other agency business.

V. **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.

Personal use are applicable to all state owned information assets or those assets assigned to users as part of their job duties. This includes, but is not limited to, all computer hardware, software, peripherals, network resources and portable computing devices.

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. The agency leadership 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 conducting purchases;**

b) **Permitted during breaks or lunch periods but not before or after scheduled work times;**

c) **Not a negative reflection 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 USB, CD, DVD, Blue Ray and Other Removable Media**

Users may play music or display pictures from personally owned media using state equipment (per state agency policy) provided it does not interfere with their or other's work. Users may also set the wallpaper using pictures contained on a personally owned media disk 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 media to the workstation or any state information asset. Media that requires the user to install additional software may not be played. State owned computing devices may not be used to make "compilation" media disks or to "burn" audio or video disks for personal use. State workstations, laptops, and other computing devices may not be used to transfer personal music, pictures, or other files to portable computing devices. Watching movies or videos for personal use is not permitted. Peer-to-Peer (P2P) file sharing is prohibited on the state network. Any exceptions must be pre-approved by the Information Systems Division.

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, bidding and stock market trading.

See policy ISD_610_02 'Bring Your Own Device' (BYOD) for use of the agency's public Internet with personally owned devices.

3. **Personal Use of Public Internet *(Wi-Fi or wired)***

The agency operates both a secure internal network for employees and an unsecure 'public' network primarily intended for visitors and guests. Agency owned computing devices are configured to use the secure internal network and must not be connected to the unsecure public network.

Any personal use while using a state owned computer or computing device is detailed in section 'Personal Use of Internet Web Browser' above.

See policy ISD_610_02 'Bring Your Own Device' (BYOD) for use of the agency's public Internet with personally owned devices.

4. **Personal Use of Internet Email**

Users may access their own personal web email 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 (Exchange, Outlook or Mallard connectors) unless otherwise defined in policy.

5. **Personal Use of Agency Email**

Users may access the agency's email system to send or receive limited and incidental personal messages. However, personal messages must not include file attachments, such as, but 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 personal purposes.

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

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

7. **Personal Use of Chat Rooms and Blogs**

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

8. **Personal Use of Social Media sites**

Users may view or research topics only. Contributing to Social Media sites for personal uses is not permitted.

9. **Personal Use of Gaming or Gambling sites**

Personal use of gaming or gambling sites is not permitted.

10. **Personal use of Bidding or Auction sites**

Users may view or research topics only. Active bidding is not permitted.

11. **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.

12. **Personal Use of Printers and Other Peripherals**

The use of printers and other peripheral devices for personal use is not permitted unless specified elsewhere in policy. 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.

Agency printers may only be used in conjunction with activities related to employment with the state. See section 'Use of Internet, Networks and Services' for applicability.

13. **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, sensitivity of equipment, or does not represent a positive public image.

14. **Technical Support**

The agency has no obligation to provide technical support for any personal devices regardless if they are authorized and allowed by policy and being used for work related purposes.

15. **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 (e.g. cookies, audit devices, system logs, 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.

W. Public Use of State Systems

Oregon Department of Fish and Wildlife (ODFW) computing systems and networks are generally for the exclusive use of agency employees and are not intended for use by any member of the general public, visitor or family member. However, certain computer systems and services are designated by the agency to be public facing (e.g. ODFW web site). For the protection of all agency information assets, any system designated as public facing must meet or exceed the minimum established security standards set by the Department of Administrative Services (DAS) and the Information Systems Division. Each system is subject to security audits to test and validate that it conforms to applicable security standards.

Public Wi-Fi Internet access may be available for use by the general public at various ODFW offices. Each office location will manage the distribution of the access codes and operational expectations in the manner that best serves the office and its customers. Wi-Fi devices and security protocols are managed by the Information Systems Division to protect state information assets and may not be altered for any purposes.

X. Monitoring and Control

All employees are responsible for monitoring the proper use of information systems and all assets directly within their care.

The agency will, at a minimum, monitor the use of information systems on a random basis and for cause. Monitoring systems or processes will be used to create usage reports that will be reviewed by agency management and/or the Human Resources Division for policy 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.

Y. Public Record Retention

Within their designated authority, users are responsible for retaining and purging data file and folders (electronically or physically) per State Agency General Records Retention Schedules.

Statewide information can be found at:
http://sos.oregon.gov/archives/Pages/records_retention_schedule.aspx

Agency specific information can be found at:
http://arcweb.sos.state.or.us/doc/recmgmt/sched/special/state/sched/20100010odfwrrs.pdf

Z. **Violation**

Violation of terms of this policy can result in limitation, suspension or revocation of access to state information assets without notice 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.

AA. **Exceptions**

Exceptions to Information Systems policy may be granted if approved by the agency Director, Deputy Director, the Information Systems Division Administrator or their delegates. Exceptions must be documented and include the date the exception is requested, a description of the situation, scope or person(s) involved, and the expected date of resolution (if any).

Notwithstanding specific prohibitions in this policy, agency 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.

BB. **Procedures**

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

Information Systems Division policies are periodically updated and revised. Users are expected to be knowledgeable of changes and remain accountable to the latest provisions.

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]

Attachment B

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_610_02	Bring Your Own Device
_____	ISD_620_01	Information Asset Classification
_____	ISD_620_02	Transporting Information Assets
_____	ISD_630_01	Security of Information Systems
_____	ISD_630_02	Portable Data Storage

_____ _____

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. A copy of this form shall be retained in official personnel file.

_____ _____

Manager/Supervisor Signature Date