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 March 1, 2020	
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 objectives.	
Reference:	HR_410_02 Code of Conduct HR_450_06 'Telecommuting and Teleworking' ISD_620_01 Information Asset Classification ISD_620_02 Transporting Information Assets ISD_620_03 Mobile Computing Devices 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 ISD_640_01 Cloud Computing	
Effective Date:	**Aug 1, 2020**	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 other technology) for all users.

II. DEFINITIONS

A. **Agency:** General term that refers to the Oregon Department of Fish and Wildlife (ODFW) 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**): Agency data created, processed, or stored (uploaded) on resources that are not provided directly by the agency or State of Oregon. 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.

Examples of Cloud Services include, but are not limited to, Electronic Licensing System (ELS), Google Docs, Sales Force, WuFoo, Xhibit, Watercraft Inspection & Decontamination (WID), In-Reach, OnXMaps internet e-mail, on-line collaboration, and any data storage external to ODFW systems.

E. **Computing Device:** Any electronic hardware and its associated software used for processing information or data. 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. **Confidential:** Information that is entrusted, private, or restricted and is accessible only to those authorized for a specific intended purpose.

G. **Downloading:** Is the transfer of a file or group of files (business documents, audio, video, applications, code, or other forms of electronic media) 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 process or 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 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 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 or other self-contained power source. 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 computer 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. **Social Media:** Websites and applications that enable users to create and share content or to participate in social networking. Includes forms of electronic communication through which users create online communities to share information, ideas, personal messages, and other content.

T. **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.

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

V. **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.

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

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. All data, computing devices, or systems are for the exclusive use of state business except as otherwise exempted by agency policy. It is the duty of all users to protect 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 Oregon. No part of state agency systems or information is, or may become, the private property of any person. 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.

C. **Safety**

It is the expectation that all employees will maintain a safe working environment while using technology resources that does not create a hazard to yourself or others especially while using portable computing devices. Distractions while walking, driving, field work, and other conditions may create a dangerous situation leading to injury or death. Certain actions may also create liability if you are aware of a risk to others and contribute to the behavior.

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 perform their work and for timely revoking user access when no longer required. The agency may withdraw permission for use of its devices or systems at any time without cause.

E. **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; obscene, pornographic or sexually explicit; defamatory; discriminatory to race, age, gender, sexual orientation, religious or political beliefs, national origin, health, or disability; untrue or fraudulent; illegal or promotes illegal activities; 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 maintain compliance with copyrights, licenses, contracts, intellectual property rights, and laws associated with data, software 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 and 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. See section 'Incident Reporting' for additional expectations.

Any use of state information systems shall not attempt to:

- Access third party systems without prior authorization by the system owners.
- Obtain other users' login names or passwords (including subordinates, coworkers, or others).
- Attempt to defeat, breach, or bypass computer or network security measures.
- Use or attach personal or unauthorized devices, applications, or systems to agency computing or telecommunication devices except as explicitly allowed by policy.
- Intercept, access, or monitor electronic files or communications of other users or third parties without approval from the author or responsible business owners.
- Access or attempt to access files or information without specific and authorized business purpose.
- Access, copy, divulge, or distribute any information asset labeled or otherwise identifiable as L3 'Restricted' or L4 'Critical' except as expressly authorized in the employee position description to perform approved job functions. Or as documented by the Information Release Authority as described in policy ISD_620_01 'Information Asset Classification'.

Employees are to manage the physical and electronic security of devices entrusted to their care in accordance with the sensitivity of the data contained on the device and the likelihood of disclosure. This includes, but not limited to, secure passcodes, 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 security breach (real or potential) or loss of agency information assets (hardware, software, or data) must be reported immediately and without delay to your direct supervisor and to the Information Systems Division. 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 'Restricted' or Level 4 'Critical' 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. Off hours or emergency contact can be made through the Executive Leadership Team (ELT) as necessary.

I. Data Integrity

Users shall protect data entrusted to their care 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.

Storing data to any external storage devices (e.g. CD, DVD, flash memory, USB, SD, or memory cards) is only for temporary use or copies of original data files.

Local data folders on laptops (C: drive), tablets, and other portable computing devices must be for temporary use only. Files must be automatically or manually synchronized to permanent network storage.

Note: Data stored on local devices and external devices is not recoverable in the event of accidental deletion, equipment failure or disaster.

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.

Lifecycle management will establish operational expectations for the replacement of information assets (both hardware and software) based on parameters designed to maintain system efficiencies, reduce operational costs and minimize security risks. Also, see policy ISD_610_04 'Information Technology Lifecycle'.

K. **Accounts and Account Passcodes**

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 disclose or share passwords with supervisors, co-workers, vendors, or family members.

Computing devices may be assigned to users that operate as a stand-alone device. Although functionality of the device may have a dedicated purpose or limited functionality, it is an extension to agency resources and requires regular security patches and updates of the passcode, pattern, pin, and current biometric identification as required on connected devices.

Although some devices or systems may not enforce passcode requirements, using a weak passcode is not permitted at any time such as repetitive digits, last four numbers of phone number, any row, column, corners of a keypad, or insufficient numbers/characters.

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. This is accomplished by logging out or otherwise locking access that prevents any unauthorized use when the account or device is unattended.

All user accounts are created with basic access rights to information systems. Additional access privileges are granted or revoked based on position duties or by request of the user's direct supervisor or any supervisor within the direct chain of command. For example, supervisors may request that two or more users (with separate login ID) share common data resources (such as project files, folders, and databases).

Minimum password/passcode requirements are established by state and agency standards and applicable to all information asset devices, applications, and systems. Wherever possible,

the minimum standards will be electronically enforced, but shall be otherwise self-imposed at a minimum to match the current specifications for password length, complexity, and renewal.

Shared access accounts for devices or applications are not permitted without prior authorization by the Information Systems Division. Exceptions must not create a security or audit risk to the agency operations.

Service accounts intended for direct interaction between computing devices or systems are allowed if there is no user interaction required and the authentication for such accounts significantly exceeds the normal password requirements in terms of length and complexity.

Accounts with high access privileges or determined to be high risk are required to use multifactor authentication (MFA) methods to sign in.

Cloud accounts must conform to agency standards by using only a state issued e-mail address or another assigned user ID. Passwords must match the current specifications for password length, complexity, and renewal.

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 images on agency computing devices provided the image is consistent with all other agency policy. 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 could disrupt or defeat this process.

Users may not download or install software programs, applications, or utilities, 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, security, or maintenance problems.

Users must not click 'I Agree/Accept' to accept terms and conditions unless prior reviewed by the agency procurement officer (ASD) or those with written delegated authority as doing so will commit the agency into any binding agreement. A listing of products already reviewed can be found on the ISD Inside pages.

Requests for product evaluations and exceptions to standard deployments can be submitted electronically to the Information Systems Division for consideration.

M. **Cloud and Hosted Services**

The use of all cloud and hosted services (free or fee based) must be pre-approved by the Information Systems Division prior to use in accordance with agency (ISD_640_01) and state policy (107-04-150). Approval may require additional authorization by the State Chief Information Officer. Requests for cloud or hosted services must document security risks, protection of data (including L1 'Public'), sustainability, legal responsibilities, public discovery, licensing, audit, and other risks to the agency or state operations.

Note: The general use of web browsers to view or research information is not considered 'cloud computing' and therefore not limited by this requirement.

Also see section on 'Downloads' for additional information.

N. **Software as a Service (SaaS)**

Software as a Service is managed by policy in the same way as other Cloud Services. 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.

Also see sections on 'Cloud Services', 'Software Licensing', and 'Software Installation'

O. **Remote Login**

Remote access to agency networks, devices, computer resources, administrative consoles, and applications requires the use of agency owned devices through the use of approved remote access systems, software, or devices with encryption. This includes but not limited to Remote Desktop Access (RDC), Virtual Private Network (VPN), peer to peer networking, and other forms of remote access.

Remote access from agency devices or networks to non-ODFW networks, computers, or devices (including other state agencies) is not allowed unless configured by the Information Systems Division.

Remote access from personal devices (e.g. home computer/personal smartphone) is not permitted except for those computer services available to the public or designed to interface with public networks (e.g. Outlook Web Access, FTP). Also see policy ISD_610_02 'Bring Your Own Device' (BYOD).

Remote access is for business use only and requires prior approval by the supervising manager and any use must otherwise comply with agency policy. See policy HR_450_06 'Telecommuting and Teleworking' regarding alternate worksite requirements.

P. **Use of E-Mail / Instant Messaging**

E-mail and Instant Messaging is for agency related business only or as allowed by policy and SEIU Collective Bargaining Agreements. Sending e-mail, Instant Messaging, 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 and Instance Messages are public record and all users are responsible for ensuring compliance with archiving and public records laws. Personally Identifiable Information (PII) is not permitted unless encrypted using an approved method. Data classification may prohibit certain confidential information from e-mail or Instant Messaging. Email uses a 'store and forward' process utilizing multiple post offices. Once e-mail leaves the security of the ODFW network, users must assume messages can be intercepted, copied or resent to unanticipated 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 ISD_610_02 'Bring Your Own Device'.

R. **Software Licensing**

All software applications in use by the agency will be properly licensed and conforming to terms and conditions for use. This is equally applicable to freeware, shareware and trial versions as it is to fee-based products and cloud applications. Software licensing requirements are established by each manufacturer or developer so legal use requirements vary greatly. All software (local or cloud) requires pre-approval by ISD for agency use.

Users must not click 'I Agree/Accept' to accept terms and conditions unless prior reviewed by the agency procurement officer (ASD) or those with written delegated authority as doing so will commit the agency into any binding agreement. A listing of products already reviewed can be found on the ISD Inside pages.

Privately owned software applications cannot be transferred or used on state systems for any purpose.

Violations of software licensing can result in substantial fines and penalties for the individual and/or agency far exceeding the cost of the license itself.

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 following operational procedures. Users will not attempt to circumvent or defeat any encryption device or system.

Hardware or software encryption may not be used on 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. Business use includes access to information related to employment with the state and provisions outlined in the SEIU Collective Bargaining Agreements. Examples include but are not limited to state benefits and services such as, PEBB, PERS, EAP, WorkDay, e-Paystub, Oregon JOBS, and

Oregon Savings Growth Plan. Unless otherwise allowed such use is expected to be limited or incidental. As an exception, emergency or immediate safety issues are allowed. Also see section on 'Personal Use'.

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.

The agency Director has authorized limited personal use of state information assets as outlined in this section. This includes, but is not limited to, all computer hardware, software, peripherals, network resources, portable computing devices, and those assets assigned to users as part of their job duties. 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:

- Permitted during breaks or lunch periods but not before or after scheduled work times.
- For viewing purposes only and not transacting personal business or conducting purchases.
- Not a negative reflection on the agency or otherwise hamper productivity.
- Incidental and respectful of coworkers.
- A public record and open to discovery and audit.
- Permitted on systems that are not in direct view by the public.
- Allowed only as defined by policy.

1. Personal Use of USB Memory / Memory Stick

Use of any personally owned memory device must be incidental and only when an agency owned device is not practical or readily available. Personally owned memory devices may be connected to agency computers only for the purposes of transferring data files and only when the memory device is connected directly to the computer's USB port, USB card reader, or otherwise connects as a USB portable storage device.

Use of any personally owned memory device is limited to information with classification Level 1 'Published'.

Note: Agency owned USB memory devices should be used ONLY for conducting agency business and never for personal use.

2. Personal use of CD, DVD, Blue Ray and Other Removable Media

Users may play music or display pictures from personally owned media provided the personally owned music, pictures or any other files are not transferred or stored on any state-owned information asset. Such use must not interfere with their work or the work of other employees. 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. Watching movies or videos for personal use is not permitted. State workstations, laptops, and other computing devices may not be used to transfer personal music, pictures or other files to other computing devices. Users may set a background image using pictures contained on a personally owned media disk provided it meets all criteria as described in policy.

3. **Personal Use of the Internet**

Users may access personal information on the Internet for the purposes of viewing information only. Personal 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 the employees personally owned devices.

4. **Personal Use of Internet E-mail**

Users may access their own personal web e-mail if such activity does not require any software downloads or special setup. Personal e-mail accounts may not be synchronized or auto-forwarded to state information assets or to the agency e-mail systems (Exchange, Outlook or Mallard connectors) unless otherwise defined in policy.

5. **Personal Use of Agency E-mail**

Users may access the agency's e-mail system to send or receive limited and incidental personal messages that comply with agency's expectations and policies. Users may also employ other functions of the agency e-mail such as the calendar, tasks, notes, or contacts for limited and incidental personal purposes. Personal messages must not include file attachments unless otherwise allowed by policy, if any. This includes, but is not limited to attachments containing photos, music, video, files, or other documents. Personal e-mail accounts may not be auto-forwarded to state systems.

Personal Use of Instant Messenger (IM)

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

Personal Use of Chat Rooms and Blogs

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

Personal Use of Social Media Sites

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

Personal Use of Gaming or Gambling Sites

Personal use of gaming or gambling sites is not permitted.

6. **Personal use of Bidding or Auction Sites**

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

7. **Personal Streaming**

Personal viewing, streaming, or downloading of movies, music, or other video and audio is not permitted.

8. **Personal Hosting**

State systems may not be used for hosting or operating personal web pages, social media content, chat rooms, or list serves; for creating, sending or forwarding personal messages; conducting personal business; or other purposes not related to agency business operations.

9. **Personal Use Downloading Files**

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

10. **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 agency 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.

11. **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.

12. **Technical Support**

The agency has no obligation to provide technical support for any personal use of agency resources or devices regardless if such use is otherwise allowed by policy

13. **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**

Computing devices, systems, and networks are not generally 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 for public use (e.g. ODFW web site, KIOSK terminals, ELS, FTP, commercial applications, public Wi-Fi). 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 Cyber Security Services office (CSS) and the Information Systems Division. Each system is subject to security audits to validate 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. Any employee using the public Wi-Fi must comply with policy provisions.

X. **Monitoring and Control**

The agency will, at a minimum, monitor the use of information systems for performance and security purposes, and as necessary for audit compliance and 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 files 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:

https://sos.oregon.gov/archives/Pages/state_admin_schedules.aspx

Z. **Policy Violation**

Violation of terms of information technology policies 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 as determined by Human Resources. In certain cases, information is protected by law and misuse could result in civil and criminal prosecution.

Inappropriate use of state information assets by an employee must be documented and promptly reported to the Information Systems Division or Human Resource Division for further review and action as necessary.

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 senior 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.

IV. PROCEDURES

All new and returning employees will be provided access to this policy and related ISD policies referred herein, provided an opportunity to read and ask questions.

Information Systems Division policies, standards and practices are periodically updated or revised. Users are expected to be knowledgeable of changes and remain accountable to the latest provisions as posted.

Submit a signed copy of the Information Systems Acknowledgment Form to the Human Resources Division for placement in the employee's personnel file acknowledgment is completed electronically through Workday.

Acknowledgment of form 'Expectations Working with Sensitive Information' is also required for employees with access to information with asset classifications of L3 'Restricted' or L4 'Critical'. A copy of all documents can be found on the ISD Inside page.

ORS 164.377 – Computer Crime

(1) As used in this section:

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

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

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

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

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

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

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

(h) "Intimate image" means a photograph, film, video, recording, digital picture or other visual reproduction of a person whose intimate parts are visible or who is engaged in sexual conduct.

(i) "Intimate parts" means uncovered human genitals, pubic areas or female nipples.

(j) "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.

(k) "Proprietary information" includes any scientific, technical or commercial information including any design, process, procedure, list of customers, list of suppliers, customers' records or business code or improvement thereof that is known only to limited individuals within an organization and is used in a business that the organization conducts. The

information must have actual or potential commercial value and give the user of the information an opportunity to obtain a business advantage over competitors who do not know or use the information.

(l) "Services" includes, but is not limited to, computer time, data processing and storage functions.

(m) "Sexual conduct" means sexual intercourse or oral or anal sexual intercourse, as those terms are defined in ORS 163.305 (Definitions), or masturbation.

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

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

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

(c) Committing theft, including, but not limited to, theft of proprietary information or theft of an intimate image.

(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) (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; 2015 c.350 §1; 2017 c.318 §13]