OREGON DEPARTMENT OF FISH AND WILDLIFE POLICY
Information Services Division

Title:	Security of Information Systems	ISD_630_01
Supersedes:	ISD_630_01 Security of Information Systems 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:	State policy 107-004-052 Cyber and Information Security State policy 107-004-150 Cloud and Hosted Systems	
Effective Date:	Jan 1, 2024	**Approved**: 

I. PURPOSE

This policy establishes security expectations of users to ensure the confidentiality, integrity, and availability of all data and computing resources within their care.

II. DEFINITIONS

A. **Availability:** Authorized users have access to information and associated assets when required.

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

C. **Copyright Laws:** Laws to control all use of an original work, such as a photograph, picture, book, movie, music, or software for a particular use or time.

D. **Critical Equipment Areas:** Areas with physical or content-sensitive electronic systems or data that serve an essential role in the computing environment.

E. **Disaster Recovery Plan:** A plan to recover destroyed electronic information.

F. **Electronic Records:** Records stored on a medium, such as magnetic tape/disk, optical disk, solid state memory, that requires computer equipment for retrieval and processing.

G. **IDF (Intermediate Distribution Facilities):** The IDF is the distribution point for fiber optic, twisted pair, coaxial and other proprietary cables to the devices, workstations, and equipment located in a given area.

H. **Information Technology (IT) Assets:** Any data, application, computer, peripheral, portable computing 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.

I. **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.

J. **Least Rights Model:** Providing sufficient access rights to perform the job, but no more.

K. **Network:** An interconnected group of computing devices and other technology for the sharing of information between two or more information systems.

L. **Network Sniffers:** Any tool or application used to decode or capture computer data. This would include, but is not limited to, keystroke recorders, password crackers, and packet analyzers.

M. **Passphrase (also password, passcode):** A passphrase is a sentence like string of text or words used for authentication that is longer than a traditional password, easy to remember and difficult to crack.

N. **Resource Owners:** Individuals responsible for information technology assets such as data, hardware, and software.

O. **Security:** The practice of preserving integrity, availability, and confidentiality of information through the use of access controls, encryption, and other forms of technologies along with training, audits, and policy.

P. **System Security Controls:** Means of managing risk, including policies, procedures, guidelines, practices, or organizational structures, which can be of administrative, technical, management, or legal in nature.

Q. **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.

R. **User ID:** The user identification used to authenticate to a computing device or network.

III. POLICY

It is the responsibility of every user to protect the confidentiality, integrity, and availability of data and technology assets entrusted to their use. Users must comply with state and agency plans, policies, procedures, and standards for the protecting of state information assets. Information resources shall be utilized only for their intended business purpose as defined by state or agency policies, laws, and regulations. Users are to be aware of potential security risks associated with their job functions and receive the necessary training to mitigate risk. All users are expected to timely complete statewide mandatory security awareness training.

A. Organizational Security

Managers are ultimately responsible for staff adhering to security practices, completing security awareness training, and providing the necessary resources to mitigate business risks. Managers are also responsible for establishing and promoting a security-aware culture.

Users are accountable for their actions and must understand the relationship of policy to their work functions and the information entrusted to their care. It is the duty of all users to

protect information assets from loss or disclosure. They are to report any potential security breach or indiscriminate loss of agency information immediately and without delay to the Information Systems Division (ISD).

The Information Security Officer (ISO) is responsible for auditing, investigating, documenting, and remediating security threats and violations. The ISO has the authority to identify and maintain evidence, quarantine infected systems, take actions to curtail a cyber threat, and minimize or stop a security breach from occurring.

B. **Access Controls**

Unique login IDs are assigned to all users. The combination of user ID and passphrase define the minimum authentication identity for users (login ID) on a system or application.

Users are responsible for all actions performed under their assigned user login ID.

Users will secure their computing devices and network accounts using private, unique, and complex passphrases.

Devices are to be logged out or locked from access by others when not in use.

Access to information systems and computing resources are based on business need using a least rights access model (only the necessary access privileges to perform authorized duties) and roles-based access model (privileges are assigned by the function performed by the user).

Without explicit authorization by supervisor, no attempt will be made to access sensitive/confidential information designated as L3 'Restricted' from locations other than official duty stations, at agency offices, or as approved in a work at home agreement.

C. **Multifactor Authentication**

Multi-Factor Authentication (MFA) is an additional authentication to the user's logon and passphrase requiring another method or device. It is used to access any application or systems designated as a high risk of unauthorized access, requires use of elevated privileges (such as admin or super user access), or otherwise considered a high risk or known target of cyber-attacks.

D. **Virtual Private Network**

The use of an encrypted Virtual Private Network (VPN) is required by users when working remotely from home or otherwise traveling on agency business to secure data communications. At no time shall the user attempt to disable or defeat VPN services. ISD may also enable additional or alternate security services to meet certain business or security requirements.

E. **Encryption**

ISD establishes the use of encryption technology to protect data and communications by coding computing systems, applications, and data to prevent unauthorized access. Encryption is generally enabled at a system level and requires no additional user interaction. However, when encryption is available as a user enabled option, it must be utilized as outlined in policy and procedures to protect sensitive agency information assets.

F. **Biometrics**

The use of biometrics (facial, fingerprint, voice, and other) may be used with combination with alpha, numeric, and special characters as a secure logon authentication method. ISD may require the use of biometrics authentication based on security requirements, business use and device type.

G. **Access Security**

User account ID and passwords are assigned to all users for their unique access to network resources and applications. At no time shall users share their account passwords or other authentication methods with another user.

Minimum password/passcode standards are applicable to all information asset devices, applications, and systems. Wherever possible, these minimum standards will be electronically and automatically enforced. For all other cases, and to the maximum extent possible, the password/passcode must meet the same standards for password length, complexity, and expiration.

Shared access accounts to devices or applications for the purposes of multiuser access are not permitted without prior authorization by ISD. Such specialized accounts must be compliant with all licensing and terms of conditions.

Service accounts designed for direct interaction or sharing of information between two computing devices without the need for user interaction are not permitted without prior authorization by ISD. Such specialized accounts must otherwise meet security protocols.

Users may not store passwords with any software, utility, or cloud services except for the agency approved secure password manager that is protected by encryption and multi factor authentication.

It is permissible to document or write down passwords and passphrases for later reference providing it is not stored on, or with the device that would allow access by others if lost or stolen.

Keys, access cards, and MFA tokens must not be loaned to other users or left unattended.

H. **Application Security (software)**

Prior to the use of any software application a review must be completed by ISD to address potential security threats, compatibility issues, lifecycle updates, and other potential operational risks. This is applicable to all fee based, free, shareware, and demonstration products.

I. **Cloud Application or Hosted Services**

Prior to the use of any cloud application or hosted service a cloud risk assessment must be submitted and approved by ISD per state policy 107-004-150 Cloud and Hosted Systems Policy. This is to evaluate the potential security threats, business continuity, data integrity, and other business risk factors. Additional review and authorization may be required by Enterprise Information Services (EIS) based on risk factors, costs, and other criteria. This is applicable to all fee based, free, shareware, and demonstration products.

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

require monthly audits of active users unless they are electronically linked to the agency's network to automatically deprovision a user when employment ends.

J. **Information Asset Classification**

All information technology assets will be classified as per state and agency requirements.

Data owners determine, within documented guidelines, which access controls are to be used based on the value of the asset and associated risks for the resource(s) under their supervision.

See policy ISD_620_01 'Information Asset Classification' for additional information.

K. **Data (Information) Security**

Users shall not access or attempt to access files or folders beyond their scope of authority.

Users shall not attempt to capture passwords, run network sniffers, or attempt to bypass security features, disrupt Information Technology (IT)services, or misuse system resources.

Data security shall be enforced based on the asset classification level of the information itself. This includes data while in use, at rest (stored), or transported. If the data contains information classification of different levels (comingled) then the highest classification shall be used.

See policy ISD_ 620_01 'Information Asset Classification' and ISD_620_02 'Transporting Information Assets' for additional information.

L. **Data Sharing Agreement**

A written data sharing agreement is required when sharing information of classification L2 'Limited' or higher with an external organization except as otherwise required by statute, federal law, interagency agreement, or contractual agreement of confidentiality (e.g., when otherwise subject to limitations of the Freedom of Information Act (FOIA) or the Oregon Public Records Law, or both). See policy ISD_620_01 Information Asset Classification for additional information.

M. **Clean Desk Practice**

Users are required to secure all sensitive/confidential information in their possession when away from their workspace and at the conclusion of the workday. This includes both electronic and physical hardcopy information.

Computer workstations, laptops, and portable devices must be logged out and secured whenever unattended for any length of time.

Printed materials with sensitive/confidential information must be immediately removed from printers or fax machines and properly secured when the user is not present.

Mass storage devices such as CD, DVD, USB drives, or external hard drives must be stored and secured when not in use.

Use only the designated and locked confidential disposal bins for the secure destruction of sensitive hardcopy materials. Contact ISD for secure disposal of electronic devices.

N. **Physical and Environmental Security**

Agency owned computing devices must be connected (physical or wireless) only to agency provided networks while in use at Oregon Department of Fish and Wildlife (ODFW) offices. Users that work remotely or at home must utilize VPN to securely connect devices to agency or state provided networks.

Guests, contractors, partners, volunteers, and employees are permitted to use their own computing devices but only when connected with the designated **public** network jacks or designated **public** Wi-Fi connections. Any use must also comply with all agency policies.

Meeting rooms or other public areas that have accessible network jacks designated for agency use must be clearly labeled indicating the connections are for ODFW use only.

Networking areas such as Intermediate Distribution Frames (IDFs), data centers, and telecommunications rooms are to be equipped with access controls (proximity cards, passwords, master keys, etc.) that limits access only to authorized personnel. In situations where such equipment is located in a common space, a secure cabinet, or other mechanism must be used to achieve the proper security practices.

- Areas shall be clearly posted with a sign indicating a restricted area by authorized staff only.
- No food or drinks are allowed in these areas at any time.
- Vendor access must be verified as legitimate and anticipated.
- Non-authorized employees and visitors must be supervised at all times.

Users are not to reconfigure any network device or systems by relocating, reconfiguring wires (change ports), connect or disconnect devices, or otherwise modify unless under direct guidance by ISD personnel.

O. **Operational Security Management**

All computing devices will be actively monitored for security threats by central security applications to protect the integrity of the ODFW network and data.

Security patch management will be maintained on a regular schedule for all end point devices including, but not limited to, computers, mobile devices, servers, network appliances, switches, routers, and other system devices. Users are expected to make all devices available to receive security updates by regularly connecting to the network or otherwise approved methods.

Mobile devices, including but not limited to, smart phones and tablets, will be equipped with Mobile Device Management (MDM) controls as appropriate for the device.

P. **System Development and Maintenance**

The installation of new systems or applications will follow a documented process with appropriate approvals and controls. New systems and applications will be tested in a pre-release environment before implementation into production.

ISD will establish operational standards for software, hardware, licenses, systems, and network devices. Any unauthorized installation or use is prohibited.

Q. **Vulnerability Testing and Patch Management**

Computing devices will be regularly scanned for malware and updated remotely by ISD. Users are expected to make devices available for patching as directed. Externally facing applications will be scanned on regular intervals for possible code security vulnerabilities. ISD may disable devices or applications without notice should it be necessary to address any risk factors.

R. **Security Incident Reporting**

Users will notify the agency Information Security Officer (ISO) without delay of any unusual or suspicious activity on their computer or other computing devices, such as unauthorized user access or strange activity indicating possible malicious software activity/attacks.

The ISO will investigate security incidents and report to the agency director, deputy director, ISD administrator, or agency security council as appropriate.

See policy ISD_610_01 Acceptable Use of State Information Assets for addition information.

S. **Business Continuity**

An agency IT business continuity plan and IT business disaster recovery plan will be maintained to address all mission-critical systems and to ensure a structured response to loss of core services. In addition, incident response plans shall be maintained to respond to less critical events.

T. **Compliance**

Electronic records or logs will be maintained for the purpose of validating user compliance to policy, procedures, investigations, and general systems maintenance.

Users are expected to be compliant with product licensing, software terms and conditions, and copyright laws. Use of unlicensed software, copyright infringement, or non-compliance with terms and conditions subjects ODFW to risk of litigation and fines. Violations may result in disciplinary action up to and including dismissal, civil, and criminal prosecution.

Only the agency contracts administrator or those with written delegated authority have the authority to bind the agency into licensing agreements by clicking 'I Accept'. Software including freeware and shareware includes End User License Agreements (EULA), Terms of Conditions (TOC), and other contractual rights and privileges.

Knowingly violating portions of this policy may also constitute "computer crime" under ORS 164.377.

U. **Privacy Disclosure**

There is no stated right to privacy for any computing devices used on state assets and network systems either for agency business or personal use (as allowed by policy). Various security scans and system audits will be performed to test and validate system security controls for their effectiveness and to identify malicious or inappropriate use of technology assets based on industry best practices and those established in policy for state agencies. Specific information gathered or monitored is held in confidence on a need-to-know basis and is not shared except as required by established security practices, policy, or law.

The ISD administrator/deputy, agency director/deputy may authorize access to any user's network account or data files for business necessary administrative purposes. The Human Resources (HR) administrator/deputy may authorize access to any user's network account or data files for purposes of fulfilling the duties and responsibilities of the HR department. In addition, a manager within direct chain of command may also request access to any network account or data files of a subordinate employee.

IV. POLICY GROUP

This policy is part of a suite of Information Technology policies that collectively sets the expectations and use of computing devices and related technologies under the main policy ISD_610_01 'Acceptable Use of Information Systems'.