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 December 1, 2014	
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:	ISO 17799 ISO 27001	
Effective Date:	**March1, 2020**	**Approved:** Erica Klein

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

N. **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.

O. **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.

P. **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.

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

III. POLICY

It is the responsibility of every employee to protect the confidentiality, integrity, and availability of ODFW data and technology assets entrusted to their use.

A. Organizational Security

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

2. End users: End 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 report any potential security breach or indiscriminate loss of agency information immediately and without delay to the Information Systems Division.

3. Information Security Officer: This individual is responsible for auditing, investigating and reporting security violations. The Information Security Officer has the authority to identify and maintain evidence, clean infected systems, and prevent a security breach from spreading.

B. Access Control

Unique login ID's are assigned by the Information Systems Division to all users. The combination of user ID and passcode define the identity of users (login ID) on a system.

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

Users will secure their computing devices and network accounts, using private passwords or passphrases, and lock access to their devices when not in active use.

Access to information systems and computing resources are based on a specific, identified business need using a least rights access (only the necessary access privileges to perform authorized duties) and roles-based access models (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 from locations other than official duty stations at agency offices.

Multi-Factor Authentication (MFA) is required for access to all systems designated as high risk for unauthorized access, users authorized with elevated privileges (such as admin or super user access), and any account access that is considered a high risk or known target of cyber-attacks.

For the purposes of business continuity, the Information Systems Division administrator/deputy, agency director/deputy may authorize access to any network account or data files. The Human Resources administrator/deputy may authorize access for purposes of fulfilling the duties of the HR department. In addition, a manager within direct chain of command may also authorize access to any network account or data files of a subordinate.

C. **Personal Security**

Adherence to ODFW security policies and standards is mandatory for all users unless a documented exception has been approved and issued by ISD.

Users are not allowed to share accounts or passwords, run password checkers on system password files, run network sniffers, attempt to bypass security features, disrupt service, abuse system resources, misuse e-mail, access or attempt to access files or folders beyond their scope of authority, or allow the use of unlicensed software.

Password/passcode/passphrase strength is measured by the combination of alpha, numeric, and special characters (in some cases biometrics or patterns) with a minimum combination set by the Information Systems Division per device type.

It is permissible to document or write down passwords for later reference providing it is not stored on, or associated with the device, and so anyone other than intended owner could gain access accidentally or intentionally. Software for recording and issuing passwords electronically are allowed only with approval by the Information Systems Division.

D. **Application Security (software or cloud)**

Prior to the use of any software application or cloud services a review must be completed by the Information System Division 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. Unlicensed software is not permitted at any time.

E. **Data (Information) Security**

Data security shall be enforced based on the asset classification of the information itself or if comingled at the highest classification of the collective data. Handling, transporting, and storing of data assets are described in other policies and procedures.

F. **Data Sharing Agreement**

A written data sharing agreement is required for sharing information with an asset classification level 2 or above to external organizations and occurs on a regular or ongoing basis except as required by statute. At a minimum, the data sharing agreement must describe the expected level of protection from further distribution or use, notice of public information request, notice of accidental disclosure, expiration date, and expectations of destruction (if any).

G. **Information Asset Classification**

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

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

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

H. **Clean Desk Practice**

Employees are required to secure all sensitive/confidential information in their workspace at the conclusion of the work day and when they are expected to be away from their workspace for an extended period of time. This includes both electronic and physical hardcopy information.

Computer workstations/laptops must be locked (logged out) when unattended and at the end of the work day. Portable computing devices that may be easily stolen must be shut down and stored away.

Mass storage devices such as CD, DVD, USB drives, or external hard drives containing sensitive information must be secured when not in active use.

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

Use the designated locked confidential disposal bins for the secure destruction of sensitive materials.

File cabinets and drawers containing sensitive information must be kept closed and locked when unattended and not in use.

Passwords must be kept personally secure and not stored in the office or with a device.

Keys and physical access cards must not be left unattended.

> * For the purposes of this section, 'sensitive' is defined as all information with an asset classification of L3 'Restricted', L4 'Critical', and any L2 'Limited' where the data owner has established restricted access.

I. **Physical and Environmental Security**

ODFW owned computing devices must be connected (physical or wireless) only to networks/Internet designated for agency use, unless otherwise enabled with approved Virtual Private Network (VPN) security.

Guests, contractors, partners, volunteers, and employees are permitted to use their own computing devices with the **public** network/Internet connections designed for that purpose and such use complies with agency policies. All other network connections are for exclusive use with agency owned computing devices.

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.

Sensitive 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. Users are not permitted to attempt access or otherwise connect, disconnect, or alter equipment unless under direct guidance by ISD personnel.

1. Critical areas shall be clearly posted with a sign indicating a restricted area by authorized staff only.
2. No food or drinks are allowed in sensitive networking areas at any time.
3. Staff must accompany non-authorized employees and visitors when inside critical equipment areas.

J. **Operational Security Management**

Users will notify the Information Security Officer 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 Information Security Officer will investigate security incidents and report to the agency director, deputy director, ISD administrator, or agency security council as appropriate.

All computing devices (networked and non-networked) will be protected with anti-malware software, data encryption, and actively monitored 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 end user devices, servers, network appliances, switches, routers, and other system devices. Users are expected to network connect or otherwise make all devices available to receive security updates.

Mobile devices will be equipped with Mobile Device Management (MDM) controls as appropriate for the device.

K. **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.

Externally facing applications will be scanned on regular intervals for possible code security vulnerabilities.

The Information Systems Division will establish operational standards for software, hardware, licenses, systems, and network devices. Any unauthorized installation or use is prohibited regardless of source.

L. **Business Interruption**

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.

M. **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.

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

N. **Disclosure**

Various security scans will be performed to test and validate system security controls for their effectiveness and to identify malicious or inappropriate use of technology assets according to industry best practices and those set for state agencies as an enterprise. Specific information gathered or monitored is held in strict confidence on a need to know basis and is not shared except as required by established security practices, policy, or law. 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).

IV. POLICY GROUP

This policy is part of a suite of ODFW Information Technology policies that collectively sets the expectations and use of computing devices and related technology, and falls under the principle policy ISD_610_01 'Acceptable Use of Information Systems'.