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 April 1, 2005	
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:	ISO 17799 / ISO 27001	
Effective Date:	**December 1, 2014**	**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:** Information is accessible only to those authorized to have access.

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 or optical disk, that requires computer equipment for retrieval and processing.

G. **IDF (Intermediate Distribution Facilities):** The IDF room on each floor is the distribution point for fiber optic, twisted pair, coaxial, fiber and other proprietary cable to the devices, workstations and equipment rooms located on that floor.

H. **Information Technology Assets:** Data, code, or hardware such as, but not limited to, data files, databases, application software, operating systems, personal computers, peripherals, servers, and networking components.

I. **Integrity:** The accuracy and completeness of information and processing methods are safeguarded.

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

K. **Network:** A system of computing devices interconnected by telephone wires, or other means, in order to share information.

L. **Network Services:** Services such as e-mail, data storage, electronic connectivity, application delivery and the Internet.

M. **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.

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

O. **Security:** Information is secure only when its integrity can be maintained, its availability ensured, its confidentiality preserved and its access controlled**.**

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 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 and processes.

R. **User ID:** User identification used in logging onto 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**

<u>Management</u>:
All managers are ultimately responsible for staff adhering to security practices and providing the necessary resources to mitigate business threats. Managers are also responsible for establishing and promoting a security-aware culture.

End users:
End users are accountable for their actions and must understand the relationship of policy to their work functions and access to agency systems.

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. Any breach of security must be reported without delay and directly to the Information Security Officer or a manager in the Information Systems Division (ISD).

B. Access Control

All users are issued unique system login identification (login ID). Users are responsible for all actions performed under their personal 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). This process minimizes security access risks and maximizes business functions.

For the purposes of business continuity, the Information Systems Division Administrator, Human Resources Division Administrator, Director or Deputy Director may authorize access to any network account or data files. 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 exception is documented and approved 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, examine other users' personal files unless asked to do so by the file owner, copy unlicensed software, or allow the use of unlicensed software.

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

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

It is permissible to write down passwords for later reference providing it is not stored on, or associated with the device, so that anyone other than intended could gain access accidentally or intentionally.

Public domain software is not allowed (freeware, shareware, etc.) except when approved by the Information System Division. Unlicensed software is not permitted at any time.

D. Information Asset Classification

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

Controls over assets are developed and implemented based on the value of the asset and associated risks.

Resource owners determine, within documented guidelines, which access controls are most appropriate for the resource(s) under their supervision.

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

E. Physical and Environmental Security

ODFW owned computing devices are to be connected only to networks/Internet connections designated for agency use only. Portable devices that are enabled with agency approved security protocols may be used on public or home networks when away from the office.

Guests, contractors, partners, volunteers, and employees are permitted to use their own computing devices only on the public network/Internet connections designed for that purpose. All other network connections are for exclusive use with agency owned computing devices or as allowed in ISD policy. Meeting rooms or other public areas that have accessible network jacks designated for agency use must be clearly labeled or signs 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 from ISD or designated local office staff. 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.

a) Critical areas shall be clearly posted with a sign indicating a restricted area by authorized staff only.

b) No food or drinks are allowed in sensitive networking areas at any time.

c) Staff must accompany non-authorized employees and visitors when inside critical equipment areas.

F. Communications and Operations Management

Users will notify the Information Security Officer of any unusual or suspicious activity on their PC and other electronic devices, such as malicious software activity/attacks or unauthorized user access.

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-virus software and other security applications approved and installed by the Information Systems Division to protect the integrity of the ODFW network and data.

G. 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 before released or used in production.

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.

H. Business Interruption

An incident response plan will be maintained for all mission-critical systems to ensure a structured response to loss of core services.

I. Compliance

Electronic records or logs will be maintained for the purpose of validating user compliance to policy and current procedures and for the purpose of investigations and general systems maintenance. ODFW respects copyright laws and insists that its employees (their agents), volunteers, vendors and contract workers do likewise.

Downloading or copying unlicensed software is theft and will not be tolerated. Illegally copied software subjects ODFW to risk of litigation. The use of unlicensed or copied software is copyright infringement, and may result in disciplinary action up to and including dismissal and criminal prosecution.

> CAUTION: Software including freeware and shareware often has End User License Agreements (EULA), Terms of Conditions (TOC), and other contractual rights and privileges. Most employees do not have the authority to bind the agency to such agreements by clicking 'Accept'.

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 law or policy. 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).

II. PROCEDURES

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'.