OREGON DEPARTMENT OF FISH AND WILDLIFE POLICY
Information Services Division

Title:	**Information Asset Classification**	**ISD_620_01**
Supersedes:	None	
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:	Policy ISD_620_02 Transporting Information Assets Policy ISD_630_02 Portable Data Storage	
Effective Date:	**December 1, 2014**	**Approved:**

I. PURPOSE

This policy establishes a classification standard that defines the level of confidentiality for all information assets and to ensure the data is protected and managed at a level appropriate to the classification.

Not all information assets have the same value, importance, or sensitivity to the agency and therefore must be classified with different levels to indicate the level of protection necessary.

II. DEFINITIONS

A. **Information Asset:** 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.

B. **Classification:** A systematic arrangement into groups or categories according to a set of established criteria.

C. **Disclosure:** The act of intentionally or unintentionally revealing, exposing, or distributing information to others without the proper authority or authorization.

D. **Information Owner:** A person or group of people with authority and responsibility for establishing controls for collecting, processing, storing, dissemination, and disposal of information assets.

E. **Personally Identifiable Information (PII):** Information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.

As defined by ORS 646A.602(11), personal information means:

(a) Consumer's first name or first initial and last name in combination with any one or more of the following data elements when the data elements are not rendered unusable through encryption, redaction, or other methods, or when the data elements are encrypted and the encryption key has also been acquired:

(A) Social Security number;

(B) driver's license number or state identification card number issued by the Department of Transportation;

(C) passport number or other United States issued identification number; or

(D) financial account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to a consumer's financial account.

(b) Any of the data elements or any combination of the data elements described in paragraph (a) of this subsection when not combined with the consumer's first name or first initial and last name and when the data elements are not rendered unusable through encryption, redaction, or other methods if the information obtained would be sufficient to permit a person to commit identity theft against the consumer whose information was compromised.

F. **Sensitive Information:** Any information where the loss, misuse, modification, or unauthorized access could adversely affect the privacy to which individuals or entities are entitled.

G. **User:** All state employees (and their agent), 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.

III. POLICY

A. Classification Requirements

All information assets owned or in custodial care by ODFW will be classified and managed based on its confidentiality and sensitivity requirements. Proper levels of protection will be implemented to protect information assets according to its relative classification. Information asset classification is required by all agencies under the statewide Enterprise Information Strategy and Policy 107-004-050.

B. **Applicability**

This policy collectively applies to all information assets regardless of how the information is stored, accessed or displayed and includes, but not limited to, electronic files (of all types), paper documents, and film regardless of where the asset is stored or how long it is retained.

C. **Asset Classification Levels**

All information assets shall be classified per the classifications described below. ODFW must use this schema of classifications for consistency with other state entities and common understanding of classification levels.

Also see section 'Labeling Information Assets'

Level 1 'Published'

Information of low sensitivity that is not protected from disclosure, that if disclosed will not jeopardize the privacy of security of agency employees, clients, partners, or cause harm to natural resources under the care of the agency. This includes information regularly made available to the public via electronic, verbal, or hard copy media.

Examples: Press releases, brochures, pamphlets, public access Web pages, social media postings, and other materials created for public consumption. May also include general information about the agency itself and its operations, regulations, and resources expressed, or provided in, any form within the normal course of ODFW business operations.

The agency will consider the default classification to be Level 1 'Published' for all information assets unless otherwise marked, identified, or communicated.

Level 2 'Limited'

Sensitive information intended for ***general*** business use that may be exempt from public disclosure because, among other reasons, such disclosure may jeopardize the privacy or security of agency employees, clients, partners, individuals, or natural resource assets. All employees and users shall follow any disclosure policies and procedures before providing this information to external parties.

Security efforts at this level are more casual and focus on protecting the confidentiality, integrity, and availability of information assets from unnecessary exposure throughout normal business activities. Information accessed by unauthorized individuals could result in loss of credibility to the agency or individuals, and financial loss but generally would be considered minimal. Security threats at this level include unauthorized or untimely disclosure of information.

Examples: Unpublished biological findings, audit reports, location data of wildlife, stocking locations or projections, and certain activities responding to legal or legislative actions.

Level 3 'Restricted'

Sensitive information intended for ***limited*** business use that may be exempt from public disclosure because, among other reasons, such disclosure will jeopardize the privacy or security of agency employees, clients, partners or individuals or natural resource assets. Information in this category may be accessed and used by internal parties only when specifically authorized to do so in the performance of their job duties. External parties requesting this information for authorized agency business must be under contractual obligation (for example, confidentiality/non-disclosure agreement) of confidentiality with the agency prior to receiving it.

Security efforts at this level are rigorously focused on confidentiality, integrity, and availability. Information accessed by unauthorized individuals likely will result in financial loss, identity theft, or compromise business activities. Security threats at this level include unauthorized disclosure, alteration or destruction of data as well as violation of privacy practices, statutes or regulations.

Examples: Personally Identifiable Information (PII as defined by statute), Social Security Number (SSN), bank routing information, detailed network diagrams, privileged attorney-client information, and ongoing investigations that may be criminal.

Level 4, 'Critical'

Information that is deemed extremely sensitive and is intended for use by ***named individual(s) only***. This information is typically exempt from public disclosure because, among other reasons, such disclosure would potentially cause major damage or injury up to and including death to the named individual(s), agency employees, clients, partners, or cause major harm to the agency or natural resource assets.

Security efforts at this level are strictly focused on confidentiality and integrity. Information accessed by unauthorized individuals could likely result in financial loss, serious and possibly unrecoverable harm to persons or the agency. Security threats at this level include unauthorized disclosure, alteration or destruction of data as well as violation of privacy practices, statutes or regulations.

Examples: Disclosure about names, locations, or other facts of individuals involved in a protection or undercover program. Information related to active investigations or prosecution of domestic violence or hate crimes. Information that results in a specific, credible, and significant threat to people, buildings, programs, or operations.

D. Labeling Information Assets

Proper labeling enables all parties to correlate the information asset with the appropriate level of handling and sensitivity.

The agency will assume a default classification of Level 1 'Published' for all information assets unless otherwise marked, identified, or communicated. Level 1 'Published' assets will not generally be labeled. However, for certain purposes may be marked for clear identification of

uses such as public information requests, news releases, or general email communications if including such marking has value.

For all assets designated as level 2 'Limited', 3 'Restricted, and 4 'Critical' information labeling must occur on the asset itself or at a higher aggregate level instead of each specific document, file, or data asset. For example, it may be effective to label information assets by folder, screen level, form type, system, or report. Any labeling strategy that effectively alerts the user accessing the information about its classification level and effectively prevents accidental misuse or disclosure would comply with this policy.

For Information assets that cannot be logically or physically separated by a single asset classification, please refer to section 'Information Isolation'.

Including the classification level in taglines, subject lines, and file names or by any process that indicates the correct classification is encouraged. However, to avoid accidental misclassification and exposure of sensitive information, it is not recommended to set a default email tagline (e.g. 'Information in this email is Level 1 Published') for every message.

E. Information Ownership

By virtue of the position description, the agency will establish information owners for all information assets within the agency's lines of business. Owners may be individuals or groups of individuals with the authority and oversight for the asset. The information owner(s) will be responsible to:

- For all classification levels
  - Establish the initial classification for any asset
  - Update the classification of the information asset as needed
  - Follow state and agency document retention rules regarding the proper disposition of assets

- For asset classifications level 2 'Limited', 3 'Restricted, and 4 'Critical'
  - Label the asset to clearly indicate the classification level using best practices according to the level of sensitivity
  - Communicate and educate staff regarding appropriate handling and transporting procedures
  - Approve decisions regarding access privileges or other controls

F. Information Release Authority

The director, deputy director, and division administrators are designated as 'Release Authorities'. It is their responsibility to authorize the release of Level 3 'Restricted' or Level 4 'Critical' asset information externally from the agency. Such authorization may be given implicitly or by delegated authority documented within an employee's position description indicating the type, conditions, and intended purpose. It is the responsibility of the releasing authority (or delegate) to ensure the distribution complies with this and all other policies, have proper controls in place (as necessary and appropriate for the type of data, frequency of

release, and number of records), and reasonably not expected to diminish the public trust unnecessarily.

G. **Compliance**

All users are responsible for the care and protection of information assets to prevent inappropriate disclosure and minimize risk corresponding with the designated classification level. Users shall immediately contact management if any information asset is not properly labeled, used improperly (exceeding guidelines), or disclosed inappropriately. Inappropriate disclosure may result from assets that are lost or stolen but also left unsecured on a desk, computer screen, portable computing devices, or otherwise not properly secured.

H. **Asset Handling and Protection**

Each information asset classification will have a set of controls, designed to provide the appropriate level of protection for the information asset based on the value and risk potential to the agency. At a minimum;

Level 1 '**Published**'

There are no restrictions on the use, distribution, or accessibility. May be copied or transferred unrestricted to various media types (paper, scanned image, photograph, or electronic file/folder) or to various media devices (CD/DVD/Blue Ray, USB key, portable storage devices, smart phones, and portable computing devices including laptops) or distributed by various sources (postal mail, email, web, FTP, social media, cloud services). May be transported off-premises without restriction. However, original records must be stored appropriately and safely according to agency policy, procedure, or practice.

Level 2 '**Limited**'

Restrictions on the use, distribution, or accessibility are as defined by the user's position authority or designated by the asset owner. Unless stated otherwise, may be copied or transferred to various media types (paper, scanned image, photograph, or electronic file/folder) or to various media devices (CD/DVD/Blue Ray, USB key, portable storage devices, smart phones, and portable computing devices including laptops) or distributed by various sources (postal mail, email, web, FTP, social media, cloud services). Users should exercise best judgment in accordance with good security and confidentiality practices and the potential liability to the agency financially and politically.

Level 3 '**Restricted**'

Use, distribution, and accessibility are limited to only those with specific position authority. Criminal background checks are often required. Information assets of this level may not be shared with other employees or partners without specific and documented authorization. Assets of this level (digital or otherwise) may **not** be copied or transferred to other media types (e.g. paper, scanned image, photograph, or electronic file/folder) or to various media devices (e.g. CD/DVD/Blue Ray, USB key, portable storage devices, smart phones, and portable computing devices including laptops) or distributed using various sources (e.g. postal mail, email, web, FTP, social media, cloud services) except as

defined by the Information Release Authority or authorized business process. Electronic data must be secured at AES 256bit encryption or stronger unless such conditions cannot be met and exemption is approved by the ISD administrator. Physical records must be securely stored in locked cabinets or other suitable containers while not in use.

Level 4 '**Critical**'

Use, distribution, and accessibility are highly restricted on a need to know basis only. Criminal background checks are required. Information assets of this level may not be shared in any way except with employees or partners of the same authorization level, in the process of conducting business, and is fully protected from accidental disclosure during the process. Assets of this level (digital or otherwise) must **not** be copied or transferred to other media types (e.g. paper, scanned image, photograph; or electronic file/folder) or to various media devices (e.g. CD/DVD/Blue Ray, USB key, portable storage devices, smart phones, and portable computing devices including laptops) or distributed by various sources (e.g. postal mail, email, web, FTP, social media, cloud services) unless specifically designated to do so by the Information Release Authority . Electronic data must be secured as AES 256bit encryption or stronger. Physical security must be maintained at all times to the highest reasonable level including multiple layers of access controls. Information of this classification must be stowed anytime it is not in active use to prevent any accidental or unauthorized disclosure.

Also see policy ISD_620_02 'Transporting Information Assets'.

I. Information Isolation

Information belonging to multiple information asset classifications should be logically or physically separated otherwise the aggregate information must be protected by the higher of the classification levels.

Whenever and wherever possible, information assets classified as 'Level 4 Critical' should be stored separately in a secure area that significantly limits physical and electronic access on a must need to know basis.

J. Public Record Law

Information assets regardless of classification remain subject to the limitations and conditions of laws, rules, and regulations including, but not limited to, federal and state disclosure laws, Oregon Public Record Law, and Oregon Archives Rules.

K. Violations

Violations of this policy or associated policies, standards, guidelines, or procedures can result in limitation, suspension, or revocation of system privileges and can lead to other disciplinary action up to and including dismissal for employees or termination of contracts for contractors, vendors, or business partners. In certain cases, violations could also result in civil and criminal prosecution.

L. **Asset Destruction and Retention**

Assets should be destroyed in a manner consistent with agency and state retention rules, practices, schedules, and regulations using the means appropriate to the asset's classification to ensure sensitive information are not compromised. Assets of higher level of classifications will require more stringent and secure methods of disposal as defined by policy and procedures.

M. **Procedures**

This policy is part of a suite of 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'.

N. **Guidelines**

The organizational roles are illustrated in the following table:

Division Administrators	Assure the information assets created by their respective divisions are identified, have assigned information owners, and are appropriately classified. Determine if formal interagency agreements and vendor contracts have the appropriate language needed for the exchange of information.
Information Owner	Establish and review the appropriate classification level of information assets within their authority. Periodically review and reclassify assets as needed based on changing business priorities, laws, or regulations. Define and communicate the proper handling and security breech mitigation procedures.
Managers and Supervisors	Understand this policy and awareness of any classified data within their working unit(s). Educate staff on the proper guidelines, procedures, and practices established for asset classification. Promptly report any misuse of data, security breech, violations of procedures, compromise of sensitive information, or improperly identified assets.
All Users of Information Assets	Understand this policy, appropriate use of classified data, and your role protecting information assets. Promptly inform your immediate supervisor or other management of any suspected misuse of data, a security breech, violations of procedures, compromise of sensitive information, or improperly identified assets.