OREGON DEPARTMENT OF FISH AND WILDLIFE POLICY
Information Services Division

Title:	Transporting Information Assets	ISD_620_02
Supersedes:	ISD_620_20 Transporting Information Assets dated March1, 2020	
Applicability:	Data Classification level 2 'Limited', 3 'Restricted', 4 'Critical'. 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:	ODFW Policy ISD_620_01 Information Asset Classification DAS Statewide Policy 107-004-100 Transporting Information Assets	
Effective Date:	Jan 1, 2024	**Approved**: 

I. PURPOSE

This policy establishes the expectations to safeguard state information technology (IT) assets from unauthorized disclosure, unintentional access, modification, misuse, loss, or corruption during physical or electronic transport. Establishes minimum safeguards to protect information assets throughout the delivery/transport cycle.

II. DEFINITIONS

A. **Classification:** A systematic arrangement into groups or categories according to the set of established criteria. See policy ISD 620_01 Information Asset Classification.

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

C. **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.

D. **Guidelines:** A statement of policy or procedure that is applicable to a wide range of situations.

E. **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.

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

G. **Information Technology:** A general term used to define all hardware, software, data, and services as a valued asset to the agency.

H. **Risk:** The likelihood of a threat to a known vulnerability and the resulting business impact measured by loss potential, business impact, or probability.

I. **Sensitive Information:** Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the interest or the conduct of programs, or the privacy to which individuals are entitled.

J. **Transport:** The process of relocating information assets from one system to another by either physical or electronic means. Could be a relocation of the original asset or a copy.

K. **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. Responsibilities

Users are responsible to assure appropriate security controls are implemented and maintained for the protection of all information assets (physical or electronic) during preparation, transportation, and delivery. Controls are specific to the asset's classification level (e.g. L1 'Published', L2 'Limited', L3 'Restricted' or L4 'Critical') and intended to prevent unauthorized disclosure, unintentional access, modification, misuse, loss, or corruption.

Users are responsible for the proper packaging of all assets, clearly and correctly identifying the classification per policy ISD_620_01 'Information Asset Classification' and placing the package(s) in the appropriate secure location for shipping.

Information owners of Level 2 'Limited' assets are responsible to clearly identify, establish, and communicate the appropriate controls for transporting assets of this level. Because controls may vary greatly on assets of this classification due to unique and varied business factors, users should consult the information owner if controls for assets labeled Level 2 'Limited' are unstated or unclear.

Information owners of Level 3 'Restricted' and Level 4 'Critical' assets are responsible to clearly establish, document, and communicate additional controls, if any, that exceed expectations within policy.

B. **Exceptions**

Level 1 'Published' - This policy excludes Level 1 'Published' information assets from any specific controls unless otherwise electronically enforced or otherwise required. For this classification, use reasonable care when handling, storing, or transporting.

Level 2 'Limited' - This policy defers any specific handling requirements for Level 2 'Limited' information assets to the information asset owner(s). Agency information asset owners may establish specific procedures or handling instructions as necessary for assets within their area of responsibility.

C. **Packaging, Storing and Shipping Information Assets**

The number and type of precautions taken to adequately protect information assets during packaging, storing, or transporting must be in relation to the risk to the agency if the asset is lost, stolen, damaged, exposed, or otherwise compromised.

Users should consider email, instant messaging, chat, and social media as unsecure and likely to create an uncontrolled copy of any electronic message or file. Therefore, only appropriate for use only with Level 1 'Public' assets or as authorized by data owners of Level 2 'Limited' assets.

Users shall, to the maximum extent appropriate utilize the following best practices as applicable and appropriate to asset classification and risk.

Physical assets:

1. Packaging is sufficient to protect the asset from possible damage likely to arise in transit such as crushing, shock, moisture, extreme temperatures, or magnetic fields.
2. Address labels are attached securely and resistant to water and forms of smudging.
3. Include on the inside of the package information including the sender, recipient, package contents, classification, and any special handling procedures.
4. Employ the use of tamper-evident packaging which reveals any attempt to gain access.
5. Locked containers that prevent uncontrolled access.
6. Maintain a log of packages sent including at a minimum the date shipped, method of shipping, destination, contents, and employee ID.
7. Use reliable transport or carriers that have been approved and/or certified to transport assets based on the risk, volume, and sensitivity.
8. Incorporate security and liability language into contracts and/or agreements with vendors that transport sensitive agency information.
9. Splitting the consignment into more than one delivery dispatched on different dates or routes.
10. When transporting in state owned or privately-owned vehicles keep items out of sight and doors locked whenever parked. Do not leave items overnight in vehicles.
11. Store packages awaiting shipping or delivery in a secure location.

12. Secured in a lockbox for afterhours delivery.
13. Delivery by hand.

Electronic assets:

1. Electronically mark the asset level using sensitivity labels as applicable.
2. Use authentication passwords, codes, images, or devices.
3. Encryption of the files, folders, database, or entire device.
4. Use SFTP (Secure File Transfer Protocol) or HTTPS (Hyper Text Transfer Protocol Secure) to send electronic files.

D. Specific Limitations by Classification

ASSET CLASSIFICATION LEVEL				
	Level 1	**Level 2**	**Level 3**	**Level 4**
LIMITATION	**Published**	**Limited**	**Restricted**	**Critical**
Restrictions	Excluded	None, except as designated by the Information Owner.	The information asset must be prepared and secured for transport by an employee with authorization to Level 3 'Restricted' information prior to hand-off for actual transit. May not be sent via electronic means unless encrypted at reset and during transport.	The information asset must be prepared and secured for transport by an employee with authorization to Level 4 'Critical' information prior to hand-off for actual transit. Never sent through email, instant message, chat, or social media services.
Packaging	Excluded	Reasonable and normal to prevent damage, loss or unauthorized access.	Reasonable and normal to prevent damage, loss, and unauthorized access.	Extensive care using as many recommended precautions as reasonably possible.
Storage	Excluded	None, except as designated by the Information Owner.	Temporary only - must be delivered without delay and secured at all other times.	Locked, out of sight, or in guarded possession at all times.
Carrier/ Transport	Excluded	None, except as designated by the Information Owner.	Any carrier or method that does not introduce unnecessary risk during transport.	Limited to those certified or approved for transporting highly sensitive information. Includes USPS.
Transfer of Custody	Excluded	None, except as designated by the Information Owner.	Signature or electronic verification required.	Documented and recorded by logbook or other established and documented process.
Exceptions	Excluded	Must be approved by the information owner.	Must be approved by executive level management (ELT) and documented.	Must be approved by the director's office and documented in writing as part of the asset controls.

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'.