OREGON DEPARTMENT OF FISH AND WILDLIFE POLICY
Information Services Division

Title:	**Transporting Information Assets**	**ISD_620_02**
Supersedes:	None	
Applicability:	Data Classification level 2 'Limited', 3 'Sensitive, 4 'Restricted' 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: ODFW Policy ISD_620_01 Information Asset Classification DAS Statewide Policy 107-004-100 Transporting Information Assets		
Effective Date:	**December 1, 2014**	**Approved:**

I. PURPOSE

This policy establishes the expectations to ensure the security of state information assets from intentional or accidental disclosure, unauthorized 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_02 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:** Data in any form that has value to the agency. Includes but not limited to assets on media paper, film, tape, hard drives, USB keys and electronic files of all types. Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics that has value to the organization.

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

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

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

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

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, volunteers, their agents, 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 utilized in the protection of the information assets (physical or electronic) during preparation, transportation, receiving, and final delivery. Controls are specific to the asset's classification level (Published, Limited, Sensitive, or Secure) and intended to prevent unauthorized disclosure, misuse, loss, corruption or unintended modification until received by the designated recipient.

Users are responsible for the proper packaging of all assets, clearly and correctly identifying the classification (if other than Level 1 'Published') and placing the package(s) in the designated 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 are unclear.
Information owners of Level 3 'Sensitive' and Level 4 'Critical' assets are responsible to clearly establish, document, and communicate additional controls, if any, that are not already provided within policy.

B. **Exclusion**

Level 1 'Published' - This policy excludes Level 1 '**Published**' information assets from this policy or any specific controls. 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). Follow the procedures, processes, and/or limitations established for each asset item. If none are specified, use reasonable and appropriate care.

C. **Guidelines for packaging, storing and shipping information assets**

The following guidelines are for transporting information assets of all classifications. Agency information asset owners may establish specific procedures or handling instructions as necessary for assets within their area of responsibility.

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 shall, to the maximum extent appropriate, ensure that physical assets (including electronic assets that are physically transported), utilize the following best practices as applicable and appropriate:

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 other 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) Employees transporting assets in state owned or privately owned vehicles must be kept out-of sight, locked, and preferably in possession at all times.

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. Use authentication passwords, codes, images, or devices.
2. Encryption of the files, folders, database, or entire device.
3. Email, Instant Messaging, and Social Media should always be considered as unsecure and likely to create an uncontrolled copy of any electronic message or file.
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 'Sensitive' information prior to hand-off for actual transit May not be sent via email unless encrypted or secured	The information asset must be prepared and secured for transport by an employee with authorization to Level 4 "Restricted information prior to hand-off for actual transit Must not be sent through common email, instant message, or social media services
Packaging	Excluded	Reasonable & normal to prevent damage or loss, or unauthorized access	Reasonable & normal to prevent damage, loss, or 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 (such as personal vehicle)	Limited to those certified or approved for transporting highly sensitive information
Transfer of Custody	Excluded	None, except as designated by the Information Owner	Signature or electronic verification required	Documented and recorded
Exceptions	Excluded	If process is defined by Information Owner, exceptions must be approved by management level employee	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

E. Procedure

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'.