DAS DEPARTMENT OF ADMINISTRATIVE SERVICES

Statewide Policy

SUBJECT:	Transporting Information Assets	**NUMBER:**	107-004-100
DIVISION:	Enterprise Information Strategy and Policy	**EFFECTIVE DATE:**	01-31-08

APPROVED: Kri Kaub

POLICY/ PURPOSE:

Purpose: The purpose of this policy is to ensure the security of state information assets when in transit. Information assets can be vulnerable to unauthorized access, misuse or corruption during physical transport. Minimum safeguards must be implemented to protect sensitive information from accidental or intentional unauthorized access, modification, destruction, disclosure, misplacement or permanent loss throughout the delivery/transport cycle.

Policy: Each agency must use appropriate security controls for transportation of sensitive information assets (physical media – e.g. tape, disk, paper) during transit and beyond the physical boundaries of a facility from loss, destruction or unauthorized access. Each agency that sends, receives or transports confidential or sensitive information to or from another facility or agency/entity is responsible to assure that the information is protected appropriately during transit. The determination of the sensitivity level of an asset is governed by the statewide policy 107-004-050 Information Asset Classification in which it is the responsibility of the information owner to identify sensitive information and ensure appropriate protection.

AUTHORITY: This policy is established under the authority of 2005 Oregon Laws Chapter 739, OAR 125-800-005, 125-800-0010 and 125-800-0020.

APPLICABILITY: This policy applies to all Executive Branch agencies as defined in ORS 174.112, except as provided in ORS 182.122 and 182.124 and OAR 125-800-0020 (3)(a) and (b) and (4) as they apply to the State Board of Higher Education and the Oregon University System, the Oregon State Lottery, Secretary of State, State Treasurer, and the Attorney General.

ATTACHMENTS: None.

DEFINITIONS:

Information: Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics.

Information Owner: Person with authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

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.

GUIDELINES: Agencies should evaluate transport options based on the level of sensitivity of the

information being transported, the level of risk involved in the transport, and the possible impact of loss or damage to the asset to determine the appropriate means of transportation for different assets. The guidelines provided should be evaluated and applied to the transport of sensitive information where appropriate.

The Department of Administrative Services Enterprise Security Office can provide guidance and consultation to state agencies on best practices to be employed for providing secure transportation of sensitive information.

Considerations for protecting sensitive information assets being transported between sites include:

a. Carrier considerations
    1. Use reliable transport or carriers.
    2. Agency management should review carrier transport procedures, identify, and approve carriers appropriate for asset transport based on the risk, volume, and sensitivity of the asset being transported, e.g. the US Postal Service may be appropriate for delivery of documents such as checks but not be appropriate for transporting data backup media with large volumes of sensitive information.
    3. Develop procedures to check the identification of carriers where appropriate.
    4. Incorporate security and liability language into contracts with vendors transporting sensitive state information, including transit to destruction facilities.
    5. Sensitive information transported in vehicles by employees should be logged, inventoried, and kept locked and out-of-sight when the employee is not in the vehicle.
b. Packaging considerations
    1. Packaging should be sufficient to protect the contents from any physical damage likely to arise during transit and in accordance with any manufacturer specifications (e.g. for software), for example protecting against any environmental factors that may reduce the media's restoration effectiveness such as exposure to heat, moisture or electromagnetic fields.
    2. Employ the use of tamper-evident packaging (which reveals any attempt to gain access).
    3. Clearly delineate on a form inside the package the number, type, and destination of media.
    4. Use secure and clear address labeling.
c. Storage considerations
    1. Store packages with sensitive information in a secure location prior to pick up.
    2. Store packages with sensitive information in a secure location/compartment in the delivery vehicle.
    3. Sensitive packages should be stored in a secure location by receiving entity.

d. Transfer of custody considerations
   1. Where feasible and appropriate, the person releasing and the person receiving the package should sign a log to maintain a chain of custody at each point of transfer. In some cases, e.g. the retrieval of assets from a lock box, it may be appropriate that the receiving person should log the pick up of the asset.
   2. The log should include date and time picked up, number of packages, destination, etc.
   3. The delivery driver should validate the information on the log and sign it.
   4. Establish procedures for logging distribution of packages within an organization (e.g. State Data Center, Publishing and Distribution, etc.).

e. Controls, means of managing risk including policies, procedures, guidelines, practices, or organizational structures, which can be of administrative, technical, management or legal nature, should be adopted, where necessary, to protect sensitive information from unauthorized disclosure or modification, including:
   1. Use of locked containers.
   2. Where appropriate and feasible, employ data encryption.
   3. Delivery by hand.
   4. In exceptional cases, splitting of the consignment into more than one delivery and dispatch by different routes.
   5. Deposit in a secure lockbox for after-hours delivery with a shipping receipt.
   6. Procedures, as appropriate, for transfer and receipt of information including, as required, notification and acknowledgment of receipt.