

SUBJECT: Transporting Information Assets **NUMBER:** 107-004-100
DIVISION: Enterprise Information Strategy and Policy **EFFECTIVE DATE:** June 27, 2007

APPROVED:

Quincy A. Ball

**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 or temporary or permanent loss throughout the delivery/transport cycle.

Policy: Each agency must use proper security controls for transportation of confidential/sensitive information assets (physical media – e.g. tape, disk, paper) during transit and beyond the physical boundaries of the agency. Each agency that sends, receives or transports confidential or sensitive information to or from another agency is responsible to assure that the information is protected appropriately during transit from loss, destruction or unauthorized access.

Following are requirements that must be implemented to protect confidential/sensitive information assets being transported between sites:

- a. Classify information prior to transport so it can be appropriately handled. It is the responsibility of the information owner to identify sensitive information and ensure it is appropriately protected.
 1. Courier
 - i. Reliable transport or couriers must be used.
 - ii. A list of authorized couriers must be approved by management.
 - iii. Procedures to check the identification of couriers must be developed.
 - iv. Incorporate security and liability language into contracts with vendors transporting sensitive state information, including transit to destruction facilities.
 2. Packaging
 - i. Packaging must 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.
 - ii. Employ the use of tamper-evident packaging (which reveals any attempt to gain access).
 - iii. The number, type, and destination of media must be clearly delineated on a form inside the package.
 - iv. Use secure and clear address labeling.

Statewide Policy

POLICY NAME: Transporting Information Assets

POLICY NUMBER: 107-004-100

3. Storage
 - i. Store packages with sensitive information in a secure location prior to pick up.
 - ii. Store packages with sensitive information in a secure location/compartiment in the delivery vehicle.
 - iii. Sensitive packages must be stored in a secure location by receiving entity.
 4. Logging
 - i. At each point of transfer, a log must be signed by the person releasing and the person receiving the package to maintain a chain of custody.
 - ii. The log must include date and time picked up, number of packages, destination, etc.
 - iii. The delivery driver must validate the information on the log and sign it.
 - iv. Establish procedures for logging distribution of packages within an organization (e.g. State Data Center, Publishing and Distribution, etc.).
- b. Controls must 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.

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: **Asset:** Anything that has value to the organization.

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

Statewide Policy

POLICY NAME: Transporting Information Assets

POLICY NUMBER: 107-004-100

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

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.