DHS Policy
Oregon Department of Human Services

Administrative Services

Policy Title:	Transportation of Information Assets				
Policy Number:	DHS-090-010	Version:	1.0	Effective Date:	Upon Approval

Signature on file in the office of the Chief Administrative Officer — *05/12/08*

Approved By: *DHS Chief Administrative Officer* — Date Approved

Overview

Description: The Department of Administrative Services (DAS) policy, Transporting Information Assets (107-004-100), requires the Department of Human Services (DHS) to develop and implement policies and procedures to limit risks associated with transporting confidential information assets.

Purpose/Rationale: The purpose of this policy is to address the protection of DHS information assets when in transit. Information assets can be vulnerable to unauthorized access, misuse, or corruption during physical transport. Safeguards must be implemented to protect sensitive information from accidental or intentional unauthorized access, modification, destruction, disclosure or temporary or permanent loss during physical transport.

Applicability: All persons or entities transporting information including, full and part-time employees, volunteers, contractors, temporary workers, and those employed by others to perform work on behalf of DHS, and are exposed to DHS information assets or systems, are covered by this policy and must comply with associated policies, procedures and guidelines.

Failure to Comply: Failure to comply with this policy and associated policies, standards, guidelines, and procedures may result in disciplinary actions up to and including termination of state service for employees or termination of contracts for contractors, partners, consultants and other entities. Legal actions also may be taken for violations of applicable regulations and laws.

Policy

1. **General**
   All persons or entities transporting information must use proper security controls for transportation of confidential/sensitive information assets during transport. All persons or entities that send, receive or transport confidential or sensitive information to or from another person or entity is responsible to assure that the information entrusted to them is protected appropriately during transit from loss, destruction or unauthorized access.

2. **Controls**
   a. Controls must be adopted, where necessary, to protect sensitive information from unauthorized disclosure or modification, including:
      1. Where appropriate and feasible, employ OIS standard data encryption (see OIS for exception process).

2. Procedures, as appropriate, for transfer and receipt of information including, as required, notification and acknowledgment of receipt.
3. Protection from public/casual viewing.

The following are requirements that must be implemented to protect confidential/sensitive (critical or restricted as per DAS policy 107-004-050) information assets being transported.

3. Classification

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. Refer to DAS policy 107-004-050, Information Asset Classification.

4. Logging

a. At each point during transport, a log must be signed by the person releasing the information and the person receiving the package to maintain a chain of custody.
b. The log must include date and time picked up, number of packages, destination, etc.
c. The delivery driver must validate the information on the log and sign it.
d. Establish procedures for logging out information assets when being removed from the organization by employees.

5. Packaging

a. Use secure, legible and complete delivery and return address labeling.
b. Packaging must be sufficient to protect the contents from any physical damage likely to arise during transport 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.
c. Employ the use of tamper-evident packaging (which reveals any attempt to gain access).
d. The number, type and destination of media must be clearly delineated on a form inside the package.

6. Storage

a. Shipping
    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 must be stored in a secure location by receiving entity.
b. Maintaining Control
    1. When confidential information assets, in any medium, are removed from the worksite, they must be protected at all times. Examples of protection include, but are not limited to:
        i. Locked in vehicle trunk;
        ii. Hidden from site (if vehicle has no trunk);
        iii. Not left in vehicle overnight; and/or
        iv. Where possible, the person transporting the sensitive information should maintain physical possession.

7. Incident Reporting
All incidents involving loss or exposure of information assets should be reported as outlined in DHS-090-005-01: Privacy and Information Security Incident Reporting Procedure.

Procedure(s) that apply

DHS-090-005-01: Privacy and Information Security Incident Reporting Procedure

Form(s) that apply

DHS 3001: Privacy Incident Reporting Form

Reference(s)

DAS-107-004-100: Information Asset Classification
DAS-107-004-050: Transporting Information Assets
DHS-090-005: Privacy and Information Security Incident Response Policy
DHS Privacy Policies

Definition(s)

- See Privacy/Security Glossary of Common Terms
- See Common Terms for all department-wide support services policies

Contact(s)

Name: Kyle Miller **Phone:** 503-945-6812 **Email:** dhsinfo.security@state.or.us

Policy History

- **Version 1.0:**
  - 05/12/2008 - Initial Release