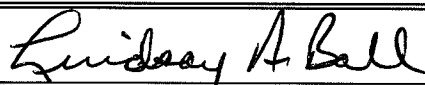


<b>SUBJECT:</b> Controlling Portable and Removable Storage Devices	<b>NUMBER:</b> 107-004-051
<b>DIVISION:</b> Enterprise Information Strategy and Policy	<b>EFFECTIVE DATE:</b> 07/30/07
<b>APPROVED:</b> 	

**POLICY/PURPOSE:**

**Purpose:** The purpose of this policy is to ensure the confidentiality, integrity, and availability of state information assets stored on portable or removable storage devices. Security controls are necessary to protect against theft of equipment, unauthorized disclosure of information, misuse of equipment, or unauthorized access to information assets.

**Policy:** Each agency will physically control and protect portable and removable storage devices, and protect and manage any sensitive information stored on them.

**Controlling Portable and Removable Devices**

Portable and removable storage devices may include, but are not limited to palmtops, laptops, mobile phones, flash drives, floppy diskettes, CDs, or DVDs.

Due to the portability of these devices, care needs to be taken to ensure the physical security of the device to prevent potential compromise through loss or theft of the device. To properly manage portable or removable storage devices agencies must know what devices they have, where they are, who has them, how they are being used, and what information is stored on them.

Each agency will adopt policy and procedures identifying types of approved devices, govern use of personally-owned devices, and establish methods for tracking the devices.

**Securing Information Stored on Portable and Removable Devices**

Each agency will adopt policies and procedures identifying what agency information assets may or may not be stored on portable or removable devices and approved methods for securing that information, as needed, appropriate to the information's sensitivity.

**Compliance**

Each agency may, based upon its individual business needs or legal requirements, exceed the security requirements put forth in this document but must, at a minimum, achieve the security objectives defined in this document.

State agencies have one (1) year from effective date of this policy to comply with this policy.

**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.

## Statewide Policy

**POLICY NAME:** Controlling Portable and Removable Storage Devices

**POLICY NUMBER:** 107-004-051

**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.

**Availability:** The reliability and accessibility of data and resources to authorized individuals in a timely manner.

**Confidentiality:** A security principle that works to ensure that information is not disclosed to unauthorized subjects.

**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.

**Integrity:** A security principle that makes sure that information and systems are not modified maliciously or accidentally.

**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.

**Sensitivity:** A measure of the importance assigned to information by its owner, for the purpose of denoting its need for protection.

**GUIDELINES:** Portable and Removable Storage Devices

State agencies should implement security controls in proportion with risk and exposure. These security controls are to protect against theft of enterprise equipment, unauthorized disclosure of information, misuse of equipment, or unauthorized access to information assets. Controls could include:

- Employees should only be given the necessary level of privileges for them to do their jobs.
- Equipment, information or software should not be taken off-site without prior authorization.
- Appropriate methods of transport should be implemented depending on the value of the information.

## Statewide Policy

**POLICY NAME:** Controlling Portable and Removable Storage Devices

**POLICY NUMBER:** 107-004-051

### Protect Information Assets

No portable storage device should store any sensitive information without suitable physical and technical protective measures in place. Access control mechanisms should provide appropriate safeguards to preserve the confidentiality, integrity, and availability of the information asset. Security mechanisms could include:

- Encryption
- Tamper evident packaging
- Stored in secure areas, for example, locked filing cabinets

### Disposal of Portable and Removable Storage Devices

There is risk of disclosure of sensitive information through careless disposal or reuse of equipment. Formal processes should be established to minimize this risk.

- The contents of removable media should be permanently destroyed or rendered unrecoverable in accordance with applicable state, federal or agency record retention requirements when no longer required.
- Storage devices such as hard disk drives and other media (tapes, diskettes, CDs, DVDs, Personal Electronic Devices (PEDs), or other devices that store information) containing sensitive information should be physically destroyed or securely overwritten to prevent the unauthorized disclosure of sensitive information. For disposal of electronic equipment, refer to the Statewide Policy 107-009-0050 on Sustainable Acquisition and Disposal of Electronic Equipment (E-Waste/Recovery Policy).