




# OREGON DEPARTMENT OF FISH AND WILDLIFE POLICY

## Information Services Division

<b>Title:</b>	<b>Portable Data Storage</b>	<b>ISD_630_02</b>
<b>Supersedes:</b>	None	
<b>Applicability:</b>	All state employees, volunteers, their agents, 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.	
<b>Reference:</b>	ISD_610_01 Acceptable Use of State Information Assets ISD_620_01 Information Asset Classification ISD_620_02 Transporting Information Assets DAS Statewide Policy 107-004-051 Controlling Portable and Removable Storage Devices	
<b>Effective Date:</b>	<b>December 1, 2014</b>	<b>Approved:</b> 

### I. PURPOSE

This policy establishes expectations of confidentiality, integrity, and availability of data (state information assets) that is stored or transported on portable data storage. The use of such items are a common practice in the course of agency business so security controls are necessary to protect the agency's data resources from unauthorized access, disclosure, theft, loss, or misuse.

### II. DEFINITIONS

A. **Asset Classification:** See policy ISD\_620\_01 'Information Asset Classification' for definitions and additional information

B. **Computing Device:** Any electronic hardware and its associated software used for some form of data processing. May be stationary or portable. Examples include, but are not limited to desktop computers, laptops, tablets, handheld devices, servers, data storage devices, network devices (routers, switches, hubs, etc.), operating systems, applications, programs, and utilities.

C. **Media:** Any form of product that stores data. Includes but not limited to USB keys, memory sticks, flash cards, magnetic tape, diskettes, CD, DVD, and Blu-ray.

D. **Personal Use:** Activity not considered essential or relevant to the daily business of the agency.

E. **Portable Data Storage:** A general term used to describe any device or media that is used to store data, is portable, and is not essential operational component part of a computing device or system. Can be easily removed or disconnected.

F. **User:** All state employees (and their agents), volunteers, 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. General

Today's portable data storage is small in size, easy to use, extremely portable and has capacity to store a large amount of data. The information they contain can be easily compromised when lost or stolen. Therefore caution needs to be taken to ensure the physical security from unauthorized access when in use, stored, in transit, or disposal.

Portable data storage is available in numerous forms and naming conventions such as, but not limited to:

- USB keys, Flash drive, Thumb drives
- Flash cards, compact flash (CF), Multimedia Card(MMC)
- Secure Digital (SD, mini SD, micro SD), xD Picture Card, Memory Stick, Memory Stick Duo
- CD, mini CD, DVD, Blu-ray disks
- Diskettes, cartridges

As with any technology, supervisors should set expectations and provide guidance to employees for the appropriate use, handling, and accountability of state assets.

#### B. Policy

The use of portable data storage is permitted for the purposes of temporarily storing state information assets (data) or to transfer such information for the purposes of conducting agency business. Portable data storage must not be used for long term storage that could compromise the availability, security, or integrity of agency data.

**C. Exclusions**

The following devices/media are considered large capacity storage technology for specific business applications. Use of these devices/media requires prior approval by the Information Systems Division and therefore not addressed by this policy.

- Portable disk drives
- External disk drives
- Large capacity drives and tape for data backup (DLT, LTO, DSS)

The following devices/media are also considered large capacity storage media designed to meet specific business functions. Use of these devices/media may be used for long term storage when viable alternatives have not been identified and the information stored is appropriate for the type of storage.

- Video (VHS, HD, DVR)
- Audio (cassette, digital audio)

**D. Owned by Other Agency or Organization**

Portable data storage owned by another agency, private company, or organization may be used for the purposes of transferring data to agency computers when there is a specific business purpose and the use of agency owned device/media is not readily available or practical.

**E. Personal Use of Agency Resources**

Portable data storage that is provided by the agency is for the exclusive purposes of conducting agency business and not intended for any personal use. As allowed by policy, use of agency resources to manage state provided benefits is considered business, not personal use.

**F. Personally Owned Devices or Media**

Personally owned portable data storage may not be connected to any agency computer, device, or network system for any purpose unless specifically allowed elsewhere in policy.

See policy ISD\_610\_02 'Bring Your own Device' for exceptions, if any.

**G. Security**

Users are responsible to ensure the security of any state information asset stored or transferred on any portable data storage. Reasonable and appropriate care must be taken that is conforming to the level of risk should the information be lost, stolen, or accessed inappropriately.

#### H. **Storing Devices and Media**

When not in use, store all portable data storage in a safe place that is likely to prevent loss, theft, damage, or unauthorized access. Storing out of sight in a desk drawer, file cabinet, or travel case may be sufficient. Never leave portable data storage unattended, unlocked in vehicle, exposed to direct sun, extreme heat/cold, or a place exposed to spills or moisture.

Also see section 'O. Restricted Use (Level 3 'Sensitive' or Level 4 'Restricted')' for additional information.

#### I. **Re-use**

Reasonable care must be taken to delete or erase any data from all portable data storage prior to re-use for another purpose or by use of another person. However the user must be aware that it may be possible to recover deleted information with enough knowledge and resources.

Also see section 'O. Restricted Use (Level 3 'Sensitive' or Level 4 'Restricted')' for additional information.

#### J. **Disposal**

Follow the agency disposal processes for other computer components or devices (including hard drives) based on the highest level of classification of data the device or media contains (or had previously contained).

- Level 1 '**Published**' - no additional disposal requirements are required.
- Level 2 '**Limited**' - follow instructions established by the information owner. If none stated, no additional disposal requirements are required.
- Level 3 'Sensitive' or Level 4 '**Restricted**' - see section 'O. Restricted Use' for additional information.

#### K. **Lost devices / Reporting**

Lost or stolen portable data storage must be reported to the immediate supervisor for further actions based on the potential risk to the agency considering any data the device may have contained and its asset classification.

Minimum reporting requirements by asset classification:

- Level 1 '**Published**' can be managed at the lowest level with immediate supervisor and there is no additional reporting requirement.
- Level 2 '**Limited**' is subject to the definitions and requirements set forth by the information owner(s) regarding the data loss. Reporting requirements are dependent on the business risk.

- Level 3 **'Sensitive'** or Level 4 **'Restricted'** - see section 'O. Restricted Use' for additional information.

**L. Data backup and retention**

ISD provides no mechanism for the retention or restoration of any data contained on a portable data storage device or media. Users must take appropriate care to ensure that all original data is safely retained on the agency's network system until no longer needed and has met policy and retention schedules.

Offline data should be 'synced' or copied to the agency's network system at the soonest possible opportunity, generally within 24 hrs. For extended field work, synchronization should not exceed 30 days to prevent substantial and possibly irrecoverable loss of data.

**M. Cloud Services**

Cloud or Internet based services are not to be used to store or transfer agency data as an alternative to agency owned portable data storage devices unless prior approved by the Information Systems Division.

Also see policy ISD\_610\_01 'Acceptable Use of State Information Assets' for additional information.

**N. Off-site Authorization**

Employees must have authorization by their supervisor to remove any state asset including portable data storage devices or media and the data it contains to any off-site location (including the employee's home) except when already defined as part of the employees work responsibilities or duties.

**O. Restricted Use (Level 3 'Sensitive' or Level 4 'Restricted')**

Portable data storage may contain data classified as Level 3 'Sensitive' or Level 4 'Restricted' ONLY as allowed by policy or clearly established in agency procedures.

Devices and media MUST be:

- Clearly marked and easily readable with the asset classification directly on the device or a permanently attached tag.
- AES 256bit encrypted (or stronger) to secure the data on the device at a hardware or software level. In addition, passwords or keys may also be used to prevent access to the device.
- Stored in secured areas or within locked cabinets when not in use.
- Used in a manner to prevent any casual or foreseeable attempt to access the information inappropriately. Access must be limited on a need to know basis.

- Transported with tamper evident packaging and whenever possible require the use of signed receipts.
- Used only for the designated purpose and not reused for other business functions. When no longer needed, destroy or erase with an ISD approved process designed to render any information unrecoverable.
- Disposed of in strict accordance to the disposal procedures of sensitive data to prevent the accidental or intentional discovery of sensitive information.
- Reported to ISD within one hour of discovery of loss. Notification is critical for risk containment and liability mitigation. If contact cannot be made, alternately report to ELT member.
- Used in accordance with all other policy.

#### **IV. PROCEDURES**

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'.