OREGON DEPARTMENT OF FISH AND WILDLIFE POLICY
Information Services Division

Title:	Portable Data Storage	ISD_630_02
Supersedes:	ISD_630_02 Portable Data Storage dated March 1, 2020	
Applicability:	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 objectives.	
Reference:	ISD_610_01 Acceptable Use of State Information Assets ISD_620_01 Information Asset Classification ISD_620_02 Transporting Information Assets ISD_630_01 Security of Information Systems DAS Statewide Policy 107-004-051 Controlling Portable and Removable Storage Devices	
Effective Date:	Jan 1, 2024	**Approved:** 

I. PURPOSE

This policy establishes expectations of confidentiality, integrity, and availability of data (as a state information asset) stored or transported on portable data storage devices. 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 an essential operational component part of a computing device or system. Can be easily removed or disconnected from another device or computer.

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. Acceptable Use

The use of portable data storage is permitted for **temporary** storing or transferring state information assets (data) while conducting agency business. Any use of portable data storage must not compromise the availability, security, or integrity of agency data or information assets.

B. Applicability

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

- USB keys, flash drive, and thumb drives.
- Flash cards, Compact Flash (CF), and MultiMedia Card (MMC).
- Secure Digital (SD, mini SD, micro SD), xD picture card, and memory stick,
- CD, mini CD, DVD, and Blu-ray disks.
- Diskettes and cartridges.

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).
- Storage Area Networks (SAN).

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).
- Microfiche.

D. **Devices 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, it connects only to an external data port, and the use of agency owned device/media is not readily available or practical.

E. **Personally Owned Devices or Media**

The use of personally owned portable data storage devices or media is prohibited from use or data transfer with any agency computer, device, or network system. No exceptions are allowed per state policy.

See policy ISD_610_02 'Bring Your own Device'.

F. **Personal Use of Agency Devices or Media**

Portable data storage provided by the agency is for the exclusive purpose of conducting agency business and is not for any personal use.

G. **Security**

Users are responsible to ensure the security of any portable storage device and the information it contains to prevent unauthorized access when in use, stored, in transit, or disposed. Reasonable and appropriate care must be taken conforming to the level of risk to prevent information from being lost, stolen, or accessed inappropriately anytime while the device is stored, in transit, or in use.

See section 'Restricted Use (Level 3 'Sensitive' or Level 4 'Restricted)' for additional security related information.

H. **Handling and Storing**

Portable storage devices must be adequately protected to prevent damage or loss as they are more likely to be broken, misplaced, or stolen while in use. When not in use, store all portable data storage in a safe place that is likely to prevent loss, theft, damage, or unauthorized access following clean desk practices as described in policy ISD_630_01 'Security of Information Systems'.

Never leave portable data storage unattended, unlocked in vehicle, exposed to direct sun, subject to extreme heat/cold, or in a location potentially exposed to spills or moisture.

I. **Data Backup and Retention**

Portable data storage is intended for temporary use only. Users must take appropriate care to ensure that all original data (authoritative source) is safely retained on the agency's network system or approved cloud services as required by policy until no longer needed and has met 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 where routine synchronization is not reasonably possible, a standard operating procedure must be established and approved to protect from irrecoverable loss of data until data synchronization can occur.

ISD provides no mechanism for the retention or restoration of any data contained on a portable data storage device or media.

J. **Cloud Services**

Cloud or Internet based services are not to be used to store or transfer agency data as an alternative to data storage on state owned systems unless prior approved by the Information Systems Division or established through an approved Cloud Workbook and vendor contract.

Also see policy ISD_610_01 'Acceptable Use of State Information Assets' for additional information.

K. **Off-site Use**

Users 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.

L. **Re-use of Devices**

Reasonable care must be taken to delete or erase any data from all portable data storage devices prior to re-use for another purpose or by use of another person. Alternative options include reformatting the device or resetting to factory settings. Be aware that it is possible to recover deleted information with enough knowledge and resources. If confidentiality or security is a concern thru the reuse of any portable storge, the device should be destroyed and disposed according to policy.

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

M. **Disposal**

Follow the agency disposal processes as 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 '**Restricted**' or Level 4 '**Critical**' – refer to section 'O. Restricted Use' for information.

N. **Reporting Lost or Stolen Devices**

Lost or stolen portable data storage devices must be reported to the immediate supervisor for further risk consideration and actions based on 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'** must be reported to the Information Systems Division in accordance with policy ISD_610_01 for 'Incident Reporting'.

O. **Use With Classification 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 and clearly established in agency procedures. Devices of this sensitivity/confidentiality must be:

- Clearly marked and easily readable with the asset classification directly on the device or a permanently attached tag.
- Encrypted to AES 256bit (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.
- Report immediately if the device is lost or stolen in accordance with policy ISD_610_01 for 'Incident Reporting' .
- Used in accordance with all other policy.

IV. POLICY GROUP

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'.