



OREGON YOUTH AUTHORITY
Policy Statement
Part I – Administrative Services



Subject:

Controlling Portable and Removable Storage Devices

Section – Policy Number:

C: Property Control – 1.1

Supersedes:

I-C-1.1 04/2009

Effective Date:

09/30/2011

Date of Last

Review/Revision:

None

Related Standards and References:

- ORS [164-377](#) (Computer Crime)
- [ORS 184.305 \(Oregon Department of Administrative Services\)](#)
- [ORS 184.340 \(Rules\)](#)
- [ORS 282.020 \(Control of state printing and printing purchases\)](#)
- [ORS 291.037 \(Legislative findings on information resources\)](#)
- Department of Administrative Services, Information Resources Management Division (DAS-IRMD), [Oregon Statewide IT Policies](#)
- Department of Administrative Services, Enterprise Information Strategy and Policy: [107-004-051](#) (Controlling Portable and Removable Storage Devices)
[107-009-0050](#) (Sustainable Acquisition and Disposal of Electronic Equipment)
- [OYA policy](#): 0-2.0 (Principles of Conduct)
 0-2.1 (Professional Standards)
 0-7.0 (Use of Electronic Information Assets and Systems)
 I-C-1.0 (Property Control Systems)
 I-C-9.0 (Use of State-owned Mobile Communication Devices)
 I-E-2.0 (Records Retention, Destruction and Archiving)
 I-E-2.3 (Requests for Offender Records, Reports, and Other Materials)
 I-E-3.2 (Information Asset Classification and Protection)
- [OYA form](#): YA 8021 (Employee Agreement on Electronic Communication and Information Assets)

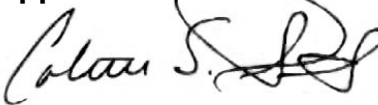
Related Procedures:

- Local protocols

Policy Owner:

Chief Information Officer

Approved:



Colette S. Peters, Director

I. PURPOSE:

This policy provides standards for OYA staff in protecting OYA information stored on portable and removable storage devices. These devices include diskettes, CDs, DVDs, laptops, backup tapes, smart phones, USB flash drives, or any kind of device that can store information.

II. POLICY DEFINITIONS:

Critical Information: Information that is deemed extremely sensitive and is intended for use by named individual(s) only. This information is typically exempt from public disclosure because, among other reasons, such disclosure would potentially cause major damage or injury up to and including death to the named individual(s), agency employees, clients, partners, or cause major harm to the agency.

Restricted Information: Restricted information intended for limited business use that may be exempt from public disclosure because, among other reasons, such disclosure will jeopardize the privacy or security of agency employees, clients, partners or individuals who otherwise qualify for an exemption. Information in this category may be accessed and used by internal parties only when specifically authorized to do so in the performance of their duties. External parties requesting this information for authorized agency business must be under contractual obligation of confidentiality with the agency prior to receiving it.

III. POLICY:

OYA physically controls and protects portable and removable storage devices, and protects and manages any information stored on them. The controls protect against theft of state-owned equipment, unauthorized disclosure of information, misuse of equipment or unauthorized access to information and devices.

Generally, critical and restricted information will be stored on the OYA network. Staff may load critical or restricted information onto OYA-authorized storage devices as needed to do their immediate work. Staff should only take the amount of critical or restricted information off site needed to perform their duties.

See OYA policy I-E-3.2 (Information Asset Classification and Protection) regarding what information is classified as “critical” or “restricted” and generally how these types of information must be protected.

IV. GENERAL STANDARDS:

A. OYA staff may temporarily store OYA information on authorized portable and removable storage devices when performing their work duties. Authorized devices are:

1. OYA-issued laptops;
2. Smart phones;

3. OYA-issued USB flash drives;
4. OYA-issued diskettes;
5. OYA-issued Compact Discs (CDs); and
6. OYA-issued Digital Versatile/Video Discs (DVDs).

B. Authorized devices must be controlled in the following manner.

1. Laptops must be –
 - a) OYA-issued;
 - b) password protected; and
 - c) stored in a locked cabinet or room when not in use.
2. Smart phones must be –
 - a) approved by the staff's supervisor;
 - b) compatible with Microsoft ActiveSync;
 - c) needed for state business;
 - d) only synchronized with the staff's OYA Outlook e-mail system; and
 - e) Password protected at sign-on.

See OYA policy I-C-9.0 (Use of State-owned Mobile Communication Devices) regarding acquisition and use of state-owned smart phones.

3. USB flash drives must be –
 - a) OYA-issued;
 - b) encrypted;
 - c) password protected; and
 - d) stored in a locked cabinet, drawer or room when not in use.
4. Diskettes, CDs, and DVDs must be –
 - a) OYA-issued; and
 - b) stored in a locked cabinet, drawer or room when not in use.

5. Assignment of laptops and USB flash drives

- a) Assignment of laptops and USB flash drives must be documented.
- b) The document must describe the device, who it is assigned to, the location of the worksite, the date assigned, and the supervisor responsible for the device.
- c) The assigned OYA staff's signature or office manager's signature must appear on the document.
- d) The documentation must be kept current and retained for two years after the laptop or flash drive is returned.

C. Transporting removable storage devices

- 1. Staff must have authorization to remove the storage device from the worksite. Authorization is contingent upon work assignment and local protocol.
- 2. Related protocols on logging removable storage devices must be followed (e.g. signing for a laptop or USB flash drive).
- 3. Transporting in vehicles
 - a) Staff will maintain physical control of the removable storage device throughout the transport and ensure protection from view by unauthorized people.
 - b) If the removable storage device must be left unattended in a vehicle, the vehicle must be locked and the device must be out of plain sight.

4. Shipping

Removable storage devices containing critical or restricted information may be shipped when the following conditions are met:

- a) Secure tape, sealant, or other tamper-evident material is used to identify a breach of the package; and
- b) The people who have a need to know of the shipment are identified.
 - (1) Pre-agreed receiving names are authorized for signature at the destination.
 - (2) Post-alert confirmation of delivery to recipient is ensured upon delivery (e.g. recipient contacts the sender upon the package's arrival).

- (3) Passwords are identified in a separate communication. Staff should not identify the related password in the same communication that mentions the specific removable storage device.

D. Intergovernmental agreements on sharing critical or restricted information on removable storage devices must be followed.

E. Disposal of portable and removable storage devices

1. Staff must deliver OYA laptops and removable storage devices to the OYA IS Service Desk for disposal.

Information Systems (IS) staff must follow the statewide policy on Sustainable Acquisition and Disposal of Electronic Equipment (DAS policy 107-009-0050).

2. Staff must mail or deliver OYA USB flash drives, CDs, DVDs, and diskettes to the Service Desk for disposal.
 - a) Staff will notify the Service Desk via e-mail of the number of devices and date shipped.
 - b) The Service Desk will confirm receipt and destruction of the devices.

3. Personal smart phones

OYA reserves the right to delete **all** information from a smart phone if a staff member's employment with OYA ends or the staff member's smart phone is lost, stolen, or replaced.

- a) Staff must notify the Business Services Assistant Director's executive support staff if the staff's smart phone is lost, stolen, replaced, or no longer needed for OYA business.
- b) Human Resources Section staff must notify the Business Services Assistant Director's executive support staff of an employee's separation from OYA on or before the staff member's separation.

F. Lost or stolen portable and removable storage devices

Staff must immediately notify their supervisor and the Technical Services Manager when a storage device containing OYA information is lost or stolen.

G. Personal portable and removable storage devices (not OYA-issued)

- a) Staff will not connect personal laptops, USB flash drives or diskettes to OYA computer systems or the OYA network without prior approval from Technical Services.
- b) Personal audio CDs and DVDs may be used for limited personal use as described in OYA policy 0-7.0 (Use of Electronic Information Assets and Systems).
- c) Staff will not store OYA information on personal DVDs, CDs, diskettes, USB flash drives or laptops.
- d) Only authorized personal smart phones may contain limited OYA information.

V. LOCAL OPERATING PROTOCOL REQUIRED: NO