



OREGON YOUTH AUTHORITY



Policy Statement

Part 0 – Mission, Values, Principles

Subject:

Use of Electronic Information Assets and Systems

Section – Policy Number:

0-7.0

Supersedes:

0-7.0 (04/09)
0-7.0 (12/06)
I-E-3.2 (12/02)

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: [107-004-110](#) (Acceptable Use of State Information Assets); [107-004-053](#) (Employee Security)
- [JJIS policy](#): Access to JJIS
User Security
Granting Access to JJIS and JJIS Data
- [JJIS forms](#): 2a (User Security Agreement)
3a (User Security Assignment)
- [OYA Style Guide](#)
- [OYA policy](#): 0-2.0 (Principles of Conduct)
0-2.1 (Professional Standards)
I-B-2.0 (Delegation for Expenditures)
I-C-1.1 (Controlling Portable and Removable Storage Devices)
I-E-2.0 (Records Retention, Destruction and Archiving)
I-E-2.3 (Requests for Offender Records, Reports, and Other Materials)
I-E-3.1 (Publications and OYA Forms)
I-E-3.2 (Information Asset Classification and Protection)
- [OYA forms](#): YA 1606 (Terminal Server Access Request)
YA 2502 (OYA Security Form Access to Other than OYA Systems)
YA 8021 (Employee Agreement on Electronic Communication and Information Assets)
- [Frequently Asked Questions](#) (FAQ) regarding this policy

Related Procedures:

- None

Policy Owner:

Chief Information Officer

Approved:

Colette S. Peters, Director

I. PURPOSE:

This policy provides security requirements and standards for OYA staff's acceptable staff use of electronic information, computer systems, and devices.

II. POLICY DEFINITIONS:

Control: Means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management or legal nature.

Encryption: Use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without the use of a confidential process or key.

Juvenile Justice Information System (JJIS): The Juvenile Justice Information System (JJIS) is a statewide-integrated electronic information system designed, developed, and implemented to support a continuum of services and shared responsibility among all members of the juvenile justice community. In a collaborative partnership between the Oregon Youth Authority (OYA) and Oregon's county juvenile departments, JJIS is administered by the State of Oregon through OYA.

Information Asset: Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics that has value to the organization.

Information System: Computers, hardware, software, storage media, networks, operational procedures and processes used in the collection, processing, storage, sharing or distribution of information within or with any access beyond ordinary public access to, the state's shared computing and network infrastructure.

User: All state employees, volunteers, their agents, 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:

Agency information, computer systems and devices are made available to authorized users to optimize the business processes of the State of Oregon. OYA will comply with statewide policy relating to acceptable use of state information assets as directed by the Department of Administrative Services (DAS), Enterprise Information Strategy and Policy Division. Any use of information, computer systems and devices must comply with this policy.

State information, computer systems and devices are provided for business purposes only and information on those systems are the sole property of the State of Oregon, subject to its sole control unless an overriding agreement or contract exists to the contrary. No part of state agency systems or information is,

or may become, the private property of any system user. The state owns all legal rights to control, transfer, or use all or any part or product of its systems. All uses must comply with this policy and any other applicable state policies and rules.

As a state agency, OYA is responsible for controlling and monitoring its systems and protecting its information assets. All information stored within applications, systems and networks are the property of the State of Oregon; therefore, users must comply with public retention laws and rules.

IV. GENERAL STANDARDS:

A. Security requirements

1. OYA Network and Intranet Security

- a) The agency Technical Services Manager oversees the general agency network information security and intranet practices.
- b) OYA Network administrators act as network security officers.

In this capacity, network security officers have the ability to create, delete and lock user accounts. They also may allow approved access to different folders on OYA servers.

- c) Security approval

Supervisors are responsible for approving their staff's access to the OYA network and intranet. The supervisor will indicate the type of clearance for each staff or work unit and notify the local network administrator by e-mail.

- d) All OYA staff must sign OYA form YA 8021 (Employee Agreement on Electronic Communication and Information Assets) prior to accessing the network, OYA intranet, or Web-based OYA e-mail, and annually thereafter.

2. Other Agency System Security

OYA staff duties may require access to systems outside of OYA such as the Customer Information Control System (CICS) and statewide financial management systems. These systems require agency security officers to oversee internal controls and authorize requests for security access to the systems.

- a) Customer Information Control System (CICS)

- (1) The OYA CICS Security Officer oversees OYA access to CICS. The CICS Security Officer may grant or revoke access as described herein.

(2) The OYA CICS Security Officer assures the YA 2502 (OYA Security Form Access to Other than OYA Systems) contains proper authorization and security clearances are accurately entered into the system.

b) Statewide Financial Management Systems

The OYA Accounting Security Officer maintains internal control for R*STARS (Relational Standard Accounting and Reporting System), ADPICS (Advanced Purchasing and Inventory System), Accounting Datamart, OSPA (Oregon State Payroll Application), and the Payroll Datamart. The Accounting Security Officer also authorizes all requests for security access to these systems.

See OYA policy I-B-2.0 (Delegation for Expenditures) for additional information.

3. Juvenile Justice Information System (JJIS) Security

See JJIS policies JJIS Security (Users) and Granting Access to JJIS and JJIS Data for guidelines on JJIS access authorization and revocation.

4. Security clearance

- a) Supervisors are responsible for approving security clearances to individuals or work units.
- b) The supervisor will indicate the type of clearance for each work unit or staff and notify the appropriate security officer or local network administrator.
- c) When a staff's work assignment or status changes, the supervisor must notify the appropriate security officer of any needed security changes or deletions.

B. Access and Control

OYA is responsible for granting and monitoring users' access to systems and information required to do their work, and for revoking user access in a timely manner. OYA may withdraw permission for any or all use of its systems at any time without cause or explanation.

- 1. All users must be properly authorized and authenticated to use state information assets.
- 2. Access to information on workstations and servers requires an individual sign-on that includes user identification and a password.

3. Passwords

Passwords must remain confidential and follow the minimum password requirements listed below.

Passwords must:

- a) Be a minimum length of eight characters on all systems;
- b) Meet these complexity requirements:
 - (1) Not contain the user's account name or parts of the user's full name that exceed two consecutive characters;
 - (2) Contain characters from **three** of the following four categories:
 - (i) English uppercase characters (A through Z);
 - (ii) English lowercase characters (a through z);
 - (iii) Base 10 digits (0 through 9); or
 - (iv) Non-alphabetic characters (e.g. !, \$, #, %).
- c) Expire within a maximum of 90 calendar days;
- d) Not be identical to the previous 10 passwords;
- e) Not be transmitted in the clear outside the secure location; and
- f) Not be displayed when entered.

4. Account Lockout

An account lockout occurs when the user fails to log on after a specified number of attempts. IS staff will enforce the following account lockout components:

- a) The account lockout threshold is set at three invalid logon attempts;
- b) Account lockout duration must be 30 minutes; and
- c) Account lockout must automatically reset after 30 minutes.

5. Workstation Security

Workstations must be locked or logged off when the user steps away from the terminal, or after a predetermined amount of inactivity. Password protecting the Windows screen saver is “locking” the workstation.

IS staff will ensure that workstations adhere to the workstation lock policy by –

- a) Setting the screen saver option to enabled and unchangeable by the user;
- b) Setting the screen saver password protection as enabled and unchangeable by the user; and
- c) Setting the screen saver timeout to 10 minutes with password protection enabled and unchangeable by the user.

6. Operation or use of information assets must be conducted in a manner that will not impair the availability, reliability or performance of state business processes and systems, or unduly contribute to system or network congestion.

7. Network and intranet user account revocation

Upon staff separation from OYA employment, Information Services (IS) will disable and delete user accounts according to IS procedures.

- a) Human Resources Section staff will notify IS of the staff’s separation from OYA employment on or before the staff’s separation date.
- b) IS staff will disable the user account.
- c) The account will be archived from all electronic systems (e.g. mail, home folders, roaming profiles) within 30 days after the user account has been disabled.

8. JJIS user account revocation

JJIS user accounts will be revoked when an employee separates from OYA employment or is no longer authorized to use JJIS.

See JJIS policy (JJIS Security (Users)) for guidelines on JJIS authorization and revocation.

C. Professional conduct related to use of information assets

1. Use of state information assets will not be false, unlawful, offensive, or disruptive.

State networks and systems **will not be used** to intentionally view, download, store, transmit, retrieve any information, communication or material which:

- a) is harassing or threatening;
 - b) is obscene, pornographic or sexually explicit;
 - c) is defamatory;
 - d) makes discriminatory reference to race, age, gender, sexual orientation, religious or political beliefs, national origin, health, or disability;
 - e) is untrue or fraudulent;
 - f) is illegal or promotes illegal activities;
 - g) is intended for personal profit;
 - h) condones to foster hate, bigotry, discrimination or prejudice;
 - i) facilitates Internet gaming or gambling; or
 - j) contains offensive humor.
2. Any use of state information systems will respect the confidentiality of other users' information and will not attempt to
 - a) access third party systems without prior authorization by the system owners;
 - b) obtain other users' login names or passwords;
 - c) attempt to defeat or breach computer or network security measures;
 - d) intercept, access or monitor electronic files or communications of other users or third parties without approval from the author or responsible business owners;
 - e) peruse the files or information of another user without specific business need to do so and prior approval from the author or responsible business owner; or
 - f) publish or disseminate confidential or unauthorized data.

D. Legal compliance

Use of state information systems must be in compliance with copyrights, licenses, contracts intellectual property rights and laws associated with data, software programs, and other materials made available through those systems.

E. Data integrity

Users will not knowingly destroy, misrepresent or otherwise change the data stored in state information systems.

F. Hardware installation

1. All hardware and software must be approved, purchased and installed by IS Technical Services staff.

Hardware devices that the user does not employ in the user's assigned work will not be attached to a state-provided computer.

2. Privately owned devices will not be connected to state networks, computers (including remotely used computers) or other equipment without Technical Services approval prior to connection.
3. All hardware attached to the state systems will be appropriately configured, protected and monitored so it will not compromise state information assets.

G. Downloads

Non-approved software will not be downloaded or installed from the Internet or other external sources (including portable computing and storage devices and e-mail attachments).

Any software that would result in copyright violations will not be downloaded or installed onto state systems.

H. Remote login

1. Access to OYA networks and intranet from remote locations is not allowed except through the use of OYA-approved or OYA-provided remote access systems or software.

Staff must sign OYA form YA 1606 (Terminal Server Access Request) prior to accessing the remote system or software.

2. OYA may allow remote access from non-state devices to access e-mail via a Web page.

I. Instant Messaging and audio/video streaming

1. Instant Messaging (IM) and other communications/messaging alternatives are for business purposes only and will be approved according to OYA IS procedure.
2. OYA allows for the use of streaming video/audio for business purposes only.
3. These uses will be approved, documented, adequately secured and comply with public records and archiving laws.

J. Use of e-mail

E-mail is intended to be used only for state-related business; however, OYA will allow employees limited, incidental personal use.

1. All e-mail will appear professional and follow style guidelines listed in the [OYA Style Guide](#).
2. Attachments to e-mail
 - a) State-related business attachments may be sent with state-related business e-mail.
 - b) Personal attachments may be sent with personal e-mails as long as they are limited in size and frequency.
3. Sending e-mail or other electronic communications that attempts to hide the identity of the user or represent the user as someone else is prohibited.
4. No use of scramblers, re-mailer services, drop-boxes or identity-stripping methods is permitted.
5. E-mail may be used for union business as authorized by the respective collective bargaining agreements.
6. E-mails are public record and OYA and all users are responsible for ensuring compliance with archiving and public records laws.
7. Confidential information transmitted externally must be appropriately protected according to OYA policy I-E-3.2 (Information Asset Classification and Protection).

K. Personal use of Internet, networks and services

Using the Internet increases the risk of exposing state information assets to security breaches. OYA will allow staff limited, incidental personal use as long as there is no or insignificant cost to the state and such use does not violate these guidelines.

State systems are capable of logging key strokes; therefore, users are strongly discouraged from conducting personal business requiring personally identifiable information. Examples include electronic banking and online shopping.

1. OYA has the sole discretion to determine if a staff's use is personal or business.
 2. Use in cases of emergency or to check weather conditions is acceptable.
 3. Use will not include playing computer games, whether Internet or personal, or those included with approved software applications.
 4. State systems will not be used for hosting or operating personal Web pages, or list serves; or creating, sending or forwarding chain e-mails.
 5. State systems will not be used with unauthorized proxy servers or any other means of bypassing OYA Internet monitoring systems.
- L. Business use of the Internet includes accessing information related to employment with the state, including all rights authorized by the respective collective bargaining agreements.

Approved sites for this purpose include but are not limited to PEBB, PERS, EAP, the Oregon JOBS page, Oregon Savings Growth Plan, and union contractual information.

M. Personal use of audio CDs/DVDs

OYA will allow staff users to play audio CDs/DVDs using state equipment provided it does not interfere with their or other's work, there are no licensing issues, and the material is appropriate.

OYA staff are not allowed to –

1. Transfer music from a CD/DVD to a workstation or laptop hard drive;
2. Play audio CDs/DVDs that require the user to install software on the workstation or laptop computer;
3. Make "compilation" CDs/DVDs or "burn" audio or video disks for personal use by using an OYA workstation or laptop computer;
4. Transfer music to portable music players through an OYA workstation or laptop computer;
5. Use peer-to-peer (P2P) file sharing on the state network.

N. Personal use of encryption

Personal hardware or software may not be used to encrypt any state or OYA-owned information so as to deny or restrict access to a public official who has a valid, job-related interest or purpose in the information, except in accordance with express or prior permission and direction from the OYA Director.

O. Personal solicitation

State information systems will not be used for personal solicitation. For example, systems will not be used to lobby, solicit, recruit, sell, or persuade for or against commercial ventures, products, religious or political causes or outside organizations.

P. Monitoring, control and compliance

State agencies are responsible for monitoring use of information systems and assets. OYA will, at a minimum, monitor on a random basis and for cause. The monitoring system is used to create usage reports that are reviewed by agency management for compliance.

Q. Violation

Violation of terms of this policy can result in limitation, suspension or revocation of access to state information assets and can lead to other disciplinary action up to and including dismissal from state service. Knowingly violating portions of this policy may also constitute "computer crime" under ORS 164.377.

V. LOCAL OPERATING PROTOCOL REQUIRED: NO