



OREGON YOUTH AUTHORITY

Policy Statement

Part 0 – Mission, Values, Principles



Subject:

Use of Electronic Information Assets and Systems

Section – Policy Number:

0: Mission, Values, Principles - 7.0

Supersedes:

- 0-7.0 (10/21)
- 0-7.0 (12/18)
- 0-7.0 (09/16)
- 0-7.0 (12/13)
- 0-7.0 (09/11)
- 0-7.0 (04/09)
- 0-7.0 (12/06)
- I-E-3.2 (12/02)

Effective Date:

12/20/2022

Date of Last

Revision/Review:

None

Related Standards and References:

- [ORS 164.377](#) (Computer Crime)
- [ORS 282.020](#) (Control of state printing and printing purchases)
- Enterprise Information Services [Cyber Security Services statewide policies](#)
- [OAR 416-040](#) (Offender Use of Electronic Networks within OYA Facilities)
- [JJIS policy](#): Security (Users)
Granting Access to JJIS and JJIS Data
- [JJIS](#) User Security Agreement
JJIS User Security Access Role Assignment
- [OYA policy](#): 0-2.0 (Principles of Conduct)
0-2.1 (Professional Standards)
I-B-2.0 (Delegation for Expenditures and Payment Obligation Approval)
I-C-9.0 (Mobile Communication Devices (Cell Phones) and Other Mobile Data Storage Devices)
I-E-1.4 (Public Records Management)
I-E-2.0 (Records Retention, Destruction and Archiving)
I-E-2.3 (Requests for Youth Information and Records)
I-E-3.1 (Publication Management)
I-E-3.2 (Information Asset Classification and Protection)
- [OYA forms](#):
YA 2502 (OYA Security Form Access to Other than OYA Systems)
YA 8021 (Employee Agreement on Electronic Communication and Information Assets)
[YA 8023](#) State Mobile Device User Agreement
- [Frequently Asked Questions](#) (FAQ) regarding this policy


Related Procedures:

- None

Policy Owner:

Chief Information Officer

Approved:



 Joseph O'Leary, 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.

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, printers, scanners, copiers, 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.

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.

Mobile Communication Device (MCD): A text messaging device or wireless, two-way communication device (cell phone) designed to receive and transmit voice or text communication, including mobile Global Positioning Systems (GPS), and smartphones and smartwatches.

Multifactor Authentication (MFA): An authentication method that requires the user to provide two or more verification factors to confirm their identity. These factors include:

- Something they know, such as a password, passphrase, or personal identification number (PIN);
- Something they have, such as a token (YubiKey) or smartcard; and
- Something they are, such as a biometric (e.g., fingerprint).

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 to accomplish the state's business objectives and processes.

YubiKey: A physical key used as a second factor in the multifactor authentication process.

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 regarding acceptable use of state information assets as directed by Enterprise Information Services. 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.

OYA staff must have access to information assets and systems equitably, according to their job requirements.

IV. GENERAL STANDARDS:

The OYA Technical Services manager is responsible for OYA's electronic information systems security.

A. Security Authorization

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. Staff are prohibited from allowing youth to use staff computers or electronic devices. OYA facilities have purpose-built computers for youth use (e.g., kiosks, Chrome books, school-designated computers).

Staff may allow a youth to use a state-owned mobile communication device when necessary to support the youth's case plan or goals. The staff must directly supervise the youth the entire time (see OYA policy I-C-9.0 Mobile Communication Devices (Cell Phones) and Other Mobile Data Storage Devices).

3. Access to state systems requires an individual logon that includes user identification, a password, and a second factor which is either a state-issued cell phone or YubiKey.
4. Security authorization approval
 - a) Supervisors are responsible for approving their staff's access to the OYA network, systems and data. The supervisor will indicate the type of clearance for each staff or work unit and notify the appropriate security officer, local network administrator, or the Information Services Service Desk.
 - b) 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. Passwords

1. Passwords must remain confidential and follow the minimum password requirements listed below:
 - a) Be a minimum length of 10 characters on all systems;
 - b) Not contain the user's account name or parts of the user's full name that exceed two consecutive characters;
 - c) Not contain spaces;
 - d) Contain characters from **three** of the following **four** categories:
 - (1) English uppercase characters (A through Z);
 - (2) English lowercase characters (a through z);
 - (3) Base 10 digits (0 - 9); or
 - (4) Non-alphabetic characters (e.g., !, \$, #, %);
 - e) Expire within a maximum of 90 calendar days;
 - f) Minimum password age is seven days;
 - g) Not be identical to the previous 10 passwords;
 - h) Be unique across different systems;
 - i) Not be transmitted in the clear outside the secure location;
and
 - j) Not be displayed when entered.

2. Browser password storage

Staff must not store passwords in web browsers, even when they are prompted by the browser.

C. Account Lockout

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

1. The account lockout threshold is set at five invalid logon attempts (three invalid log-in attempts for privilege access accounts);
2. Account lockout duration must be 30 minutes; and
3. Account lockout must automatically reset after 30 minutes.

D. User account revocation

1. Human Resources staff must notify IS of the staff member's employment status (e.g., separation, paid leave) on or before the date the staff member's account must be disabled.
2. Upon staff separation from OYA employment, IS staff must disable and delete user accounts according to IS procedures.
3. IS staff must archive the account from all electronic systems (e.g., mail, home folders) within 30 days after the user account has been disabled.

E. Hardware and software

1. All hardware and software must be approved, purchased, downloaded, and installed by IS staff.
2. Staff must not use personal computers, printers, or mobile devices (cell phones) for state business.
3. See OYA policy I-C-9.0 Mobile Communication Devices (Cell Phones) and Other Mobile Data Storage Devices for more information on this topic.

F. Use of information assets

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

3. State networks and systems must 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) Is harmful to OYA's reputation;
 - e) Makes discriminatory reference to race, age, gender, sexual orientation, religious or political beliefs, national origin, health, or disability;
 - f) Is untrue or fraudulent;
 - g) Is illegal or promotes illegal activities;
 - h) Is intended for personal profit;
 - i) Condone to foster hate, bigotry, discrimination or prejudice;
 - j) Facilitates Internet gaming or gambling; or
 - k) Contains offensive humor.

4. 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.

G. Network access

1. OYA's Technical Services manager oversees the general OYA network information security.
2. OYA Technical Services staff 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.
3. All OYA staff must sign a YA 8021 (Employee Agreement on Electronic Communication and Information Assets) form before receiving user credentials and annually thereafter.

H. Internet access

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

1. Since state systems are capable of logging keystrokes, users are strongly discouraged from conducting personal business requiring personally identifiable information (e.g., electronic banking, online shopping). Those who do this type of activity do so at their own risk.
2. OYA has the sole discretion to determine if a staff's use is personal or business.
3. Business use of the Internet includes accessing web hosted state systems, and 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.
4. State systems may not be used to play computer games, whether Internet or personal, or games included with approved software applications.
5. State systems may not be used for hosting or operating personal Web pages or list serves, or creating, sending, or forwarding chain e-mails.
6. State systems may not be used to log into personal e-mail or social media accounts.
7. State systems may not be used with unauthorized proxy servers or any other means of bypassing OYA Internet monitoring systems.
8. OYA allows for the use of streaming services for business purposes only.

9. State-owned devices may not be used to download, store, or retrieve any information or material for personal use.

I. Intranet access

OYA's intranet (OYANet) has a decentralized system of site owners who manage local site security. Each site owner must manage security and access to their assigned site.

J. Remote access

1. Staff may only access OYA networks and OYA's intranet from offsite locations with state-owned equipment provided by OYA's IS department.
2. Staff must use MFA to remotely access OYA systems and applications.
3. Staff must not take state-owned equipment outside the United States.

K. Wireless access

1. OYA wireless network

- a) Staff must connect to the secure OYA wireless access point when using state-owned equipment while in OYA offices.
- b) Staff may connect state-owned equipment to public wireless access points outside OYA offices.

2. Guest wireless network

- a) People who are guests to OYA offices may use the guest wireless network.
- b) The guest wireless network must be password protected. The password may be shared with guests. It can be found on OYA's intranet site home page.
- c) Staff may use the guest wireless network for incidental use as defined in this policy.
- d) State-owned equipment must not be connected to the guest wireless network.

L. Instant messaging (IM) and text messaging

1. Instant messaging (IM), text messaging, and other communications/messaging alternatives are intended for state-related business purposes.

However, OYA will allow staff limited, incidental personal use. The only approved solutions are Teams, Teams IM, and native texting application on state-provided cell phones. All communication transmitted through these services is discoverable.

2. Acceptable use

- a) Staff may use IM and text messaging to communicate factual and logistical information that is not a substantive part of official business; has been documented elsewhere; or will be captured, documented, and retained as a separate public record.
- b) In the absence of separate documentation, staff must not use IM or text messages for official purposes other than for routine communications that do not meet the definition of a “public record.”
- c) Text messages must not contain restricted or critical levels of information.
- d) Examples of IM and text messaging acceptable uses include:
 - (1) Scheduling;
 - (2) Requesting a call or e-mail on a matter, without substantive discussion;
 - (3) Requesting or offering logistical assistance (“Can you help me get these boxes to the warehouse?”);
 - (4) Forwarding any person’s contact information (“I’m at 503-123-4567”);
 - (5) Explaining your current whereabouts, or inquiring about someone else’s (“We’re at the meeting discussing this morning’s announcement. Are you around?”);
 - (6) Describing facts or events that do not relate to the substance of the agency’s work (“Spilled coffee all over myself right before the meeting!”), or that have been or necessarily will be separately recorded (“Mr. Jones just testified to the committee that our bill would cost taxpayers \$3 million”); and
 - (7) Inquiring about events like those above (“Has Mr. Jones testified in committee yet?”).

3. Unacceptable Use

- a) Staff must avoid substantive discussions of OYA business through IM and text messages. As noted above, substantive facts may be reported by IM or text message only if they will be, or are already, documented in a separate public record.
- b) If substantive discussion relating to OYA business occurs by IM or text message, such discussion must be immediately copied to a separate public record format (e.g., copying the relevant messages into an agency e-mail).

M. 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 must appear professional.
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. See OYA policy I-E-1.4 Public Records Management for e-mail record management.
7. Restricted and critical level information transmitted outside of OYA's e-mail system must be encrypted and appropriately protected according to OYA policy I-E-3.2 Information Asset Classification and Protection – Information Handling Guide.

N. State-owned devices

1. Workstations must be locked or logged off when the user steps away from it.

2. Staff must not connect personal mobile data storage devices (i.e., CDs, DVDs, Blu-Ray, flash drives) to state-owned devices.

O. Juvenile Justice Information System (JJIS)

JJIS contains restricted and confidential level information. See JJIS policies Security (Users) and Granting Access to JJIS and JJIS Data for guidelines on JJIS access authorization and revocation.

P. Other Agency System Security

OYA staff duties may require access to systems outside of OYA, such as the Customer Information Control System (CICS), Statewide Financial Management Systems (SFMS), Law Enforcement Data System (LEDS) and others. These systems require agency security officers to oversee internal controls and authorize requests for security access to the systems. Contact the appropriate security officer for access to these systems.

Q. Personal solicitation

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

R. 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.

S. Violation

Violation of the 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](#).

T. Monitoring, control and compliance

State agencies are responsible for monitoring the 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 agency management reviews for compliance.

V. LOCAL OPERATING PROTOCOL REQUIRED: NO

Frequently Asked Questions

1. Can a youth use an OYA staff computer?

No, youth are not allowed to use OYA staff computers. OYA staff computers are for official OYA business. Facility youth have access to other computers dedicated for their use.¹

Staff may allow a youth to use a state-owned MCD when necessary to support the youth's case plan or goals, and the staff must directly supervise the youth the entire time.

2. Is it okay to use a photo of my family as my background?

Yes. Staff may use personal photos as backgrounds. However, staff should e-mail the photos to their work e-mail address. This allows our e-mail system to scan the file for potential viruses. Staff should limit the number of personal photos saved on their computer.²

3. Can I use my personal USB thumb/flash drive or any other USB connectable information storage device on my workstation?

No. OYA cannot allow staff to connect any non-OYA removable media device that can store information to a state-owned computer or laptop. Only the OYA director may grant an exception to this standard.²

4. Can I use my personal computer at home to read my work e-mail?

No. Staff may only access state e-mail and other resources from state issued equipment. Staff are authorized to access Native Workday from a personal device.

5. Can I use graphics or animation in my e-mail signature line or background?

No. E-mail sent from the state system is representative of OYA and as such must be readable and professional. Staff are encouraged to include a signature block in their e-mail.

6. Can I listen to my favorite music radio station on my computer?

No. Streaming video and audio must only be for business use.²

7. Can I use a state laptop to check my personal e-mail when I am traveling?

No. Access to all non-OYA web-based e-mail is not allowed.²

8. Can I store personal music files on my computer or a network location or resource?

No. Personal music files must not be stored on state-owned computers.^{2,3}

9. Can I listen to music on my computer?

No. Staff must not connect personal mobile data storage devices (i.e. CDs, DVDs, Blu Ray, flash drives) to state-owned devices for personal use.⁴

10. What Internet categories are blocked on the OYA network?

- Abused Drugs
- Adults
- Command and Control
- Copyright Infringement
- Dating
- Gambling
- Hacking
- Malware
- Nudity
- Peer-to-Peer
- Phishing
- Proxy Avoidance and Anonymizers
- Weapons

The following categories are not blocked, but may be flagged with a warning that these site categories may only be used for authorized OYA business.

- Auctions
- Cryptocurrency
- Games
- Grayware
- Newly registered domains
- Questionable
- Swimsuits and intimate apparel

References:

1. OYA policy 0-7.0, IV.A.1
2. OYA policy 0-7.0, III, p.3
3. OYA policy I-C-9.0
4. OYA policy 0-7.0, IV.N.2