OREGON YOUTH AUTHORITY

Policy Statement

Part 0 – Mission, Values, Principles

Subject

Use of Electronic Information Systems

Section – Policy Number:	*Supersedes:*	*Effective Date:*	*Date of Last Review/Revision:*
0-7.0	**I-E-3.2 (12/02)**	**12/15/06**	**None**

Related Standards and References:

- 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
- JJIS policy: Access to JJIS
  User Security
- JJIS forms: 3 (User Security Agreement)
  4.3.3 (Security Access Role Assignment)
- OYA policy: 0-2.0 (Principles of Conduct)
  0-2.1 (Professional Standards)
  I-E-3.1(Publications)
  I-E-2.3 (Requests for Offender Records, Reports, and Other Materials)
- OYA form: YA 2502 (OYA Security Form Access to Other than OYA Systems)
  YA 8021 (OYA Employee Agreement on Electronic Communication)

Related Procedures:

- None

Interpretation: Information Systems

Approved:

Robert S. Jester, Director

I. PURPOSE:

This policy provides security requirements and guidelines for staff access and personal use of electronic information maintained by the OYA.

II. POLICY DEFINITIONS:

None

III. POLICY:

The OYA has a responsibility to establish specific security requirements and guidelines for access and personal use by staff of electronic information maintained by the OYA. All systems and information are, and will remain, the property of the OYA, subject to its sole control. No part of any system or piece of information is, or will become, the private property of any system user. The OYA owns all legal rights to control, transfer, or use all or any part or product of its systems. All uses must comply with OYA policy and other state policies and rules that apply.

All OYA electronic information systems will be used only for OYA business, as defined by the OYA, with minor exceptions.

IV. GENERAL STANDARDS:

A. Security requirements

1. Security Officer

a) The agency will appoint a Security Officer who has responsibility for approving security clearances.

b) The Security Officer must assure that the YA 2502 contains proper authorizations and that security clearances are entered accurately into the system.

2. Security clearance

a) Supervisors/Managers are responsible for assigning security clearances to individuals or work units.

b) The Supervisor/Manager will indicate the type of clearance for each work unit or staff and notify the central Security Officer on the appropriate form (JJIS form 4.3.3.)

c) When a staff's work assignment or status changes, the Supervisor/Manager must notify the central Security Officer of any needed security changes within one working day.

d) Supervisors/Managers must also assure that security clearances are assigned so that staff have an adequate separation of duties.

B. Access

1. Access to information on work stations requires an individual sign-on that includes user identification and a password.

2. Passwords are to remain confidential.

3. The OYA will use passwords, scramblers, encryption methods, re-mailer services, drop-boxes, or identity-stripping and control.

4. No user may attempt to access, copy, forward, delete, or alter the messages of any other user without OYA authorization.

C. Confidentiality of information

1. Computer files are subject to the same confidentiality as other case information.

2. Information on sensitive cases will be restricted to the Parole/Probation Officer, Supervisor/Manager, Parole/Probation Supervisor, and central Security Officer.

D. Retrieval of computer information from other agencies

1. Staff are allowed access to information from other agencies under the terms of Information-Sharing Agreements.

   a) Information from other agencies is confidential and will be used only for administering OYA programs.

   b) Procedures for accessing information from other agencies should be obtained from the Information Systems Help Desk.

2. An OYA system may not be used to attempt unauthorized access to any other information system.

3. Inquiries for non-official purposes may subject a staff to disciplinary action.

   Unauthorized release and use of information is a violation of federal regulations and Oregon statute and is subject to possible criminal and civil action.

E. Acceptable use of electronic systems

1. Control of electronic systems.

   The OYA:

   a) Reserves, and intends to exercise, all rights relating to information used in its systems.

b) Intends to trace, review, audit, access, intercept, block, restrict, screen, delete, recover, restore, publish, or disclose any information, at any time without notice.

c) Does not intend to tap phone conversations without notice or due process of law.

d) May authorize a party to any conversation to record it, as permitted by state law.

e) May withdraw permission for any or all personal or business uses of its systems at any time without cause or explanation.

2. Use of systems

Use of systems must be professional and reflect positively on the OYA's image.

a) E-mail must look like state e-mail, not the product of a pop culture.

b) Authors must not use CB handles or pen names.

c) Personal symbols, ornamental quotes, newsgroup or chat room slang are not allowed.

d) Use of systems must be lawful and inoffensive.

e) Use will not contain profanity, vulgarity, sexual content, or character slurs.

f) Use will not contain rude or hostile references to race, ethnicity, age, gender, sexual orientation, religious or political beliefs, national origin, health or disability.

3. Publishing

a) Publishing is restricted to state business as defined by the OYA and requires OYA authorization. See related policy, Publications (I-E-3.1).

b) The OYA may authorize a user to post queries or to represent it by posting professional comments to useful groups.

c) Comments will conform to this policy.

d) Content and frequency of posting will reflect the OYA's interests, not the user's.

4. Personal use

   a) The OYA will have sole discretion to decide whether a use is personal or business.

   b) Personal use must be at minimal cost to the state and the degree or extent must be petty or insignificant, compared to use for assigned work.

   c) Personal use must occur during meal or rest breaks only; not before, after or during work.

   d) Allowed personal use

      (1) A local call or long-distance call that is not charged to the state.

      (2) E-mail message.

      (3) Pager message.

      (4) A short toll-free FAX.

      (5) Limited use of a microcomputer.

      (6) Printing and copying a state job application, a resume, personnel and benefits papers, and necessary material of state-paid courses of study.

   e) Disallowed personal use

      (1) Use by, or on behalf of, any organization or third party.

      (2) Publishing where the content or purpose is personal.

      (3) Soliciting, lobbying, recruiting, selling, or persuading for or against commercial ventures, products, religious or political causes, or outside organizations.

      (4) Use of any system device that the user does not employ in his or her assigned work.

      (5) Connecting any privately owned device to state systems without OYA approval. System devices taken home remain subject to this policy.

   f) Games

      (1) Internet games and personal games will not be used by staff.

(2) Games that are part of the original software package may be used only with OYA permission and only during normal lunch breaks; not rest breaks.

(3) Games will be used without sound and only where not visible to the public.

(4) State-owned or licensed games created to teach necessary skills may be used.

V. LOCAL OPERATING PROCEDURE or PROTOCOL REQUIRED: NO