OREGON YOUTH AUTHORITY

Policy Statement

Part I – Administrative Services

Subject:

Information Security Incident Response

Section – Policy Number:	*Supersedes:*	*Effective Date:*	*Date of Last Revision:*
E: Information Management – 3.3	**I-E-3.3 (08/19)** **I-E-3.3 (12/14)** **I-E-3.3 (3/12)**	**10/29/2021**	**12/19/2022** (added Yubikey)

Related Standards and References:	▪ ORS 276A.300 (Information systems security in executive department; rules) ▪ DAS, Statewide Policy 107-004-120 Information Security Incident Response ▪ State of Oregon Information Security Incident Response Plan ▪ OYA policy: 0-7.0 Use of Electronic Information Assets and Systems I-C-9.0 Mobile Communication Devices (Cell Phones) and Other Mobile Data Storage Devices I-E-1.0 Director's Incident Notification and Report I-E-3.2 Information Asset Classification and Protection I-E-2.0 Records Retention, Destruction and Archiving I-E-2.1 Public Records Requests for Agency Records I-E-2.2 Youth Facility Case File and Medical File Protection and Transfer I-E-2.3 Requests for Youth Information and Records ▪ JJIS policy: Privacy and Protection of Confidential Information in JJIS ▪ OYA form: YA 1970 Information Security Incident Response ▪ OYA Information Asset Classification and Protection Matrix ▪ OYA Information Security Incident Response Plan
Related Procedures:	▪ TS I-E-3.3 Service Desk Information Security Incident Response

Policy Owner: Chief Information Officer	**Approved:** Joseph O'Leary, Director

I. PURPOSE:

This policy establishes OYA's information security incident response capabilities to provide a quick, effective and orderly response to information security incidents. Information security incidents range from unauthorized intrusions into OYA network systems to mishandling information in a way that may risk its confidentiality, integrity, or availability. The policy also ensures proper incident investigation of information asset loss, damage, misuse, or improper dissemination.

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.

Information: Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, including electronic, paper, and verbal communication.

Information security: Preservation of confidentiality, integrity and availability of information. Other properties such as authenticity, accountability, nonrepudiation, and reliability can also be involved.

Information security event: An observable, measurable occurrence in respect to an information asset that is a deviation from normal operations.

Information security incident (incident): A single or a series of unwanted or unexpected information security events that result in harm, or pose a significant threat of harm to information assets, OYA, or a third party and require non-routine preventive or corrective action.

Information Security Incident Response Plan: Written document that states the approach to addressing and managing information security incidents.

Information Security Team: OYA employees responsible for overseeing the agency's information security program to help ensure the security objectives are addressed. Team members include the OYA chief information officer, information services security officer, records management officer, and rules/policy coordinator. (See OYA's Information Security Plan for more information.)

Information Services Security Officer (ISSO): OYA employee who is responsible for managing the agency's policies and practices regarding electronic information asset security**.**

Restricted Information: Sensitive 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.

III. POLICY:

OYA has an incident response program to respond to electronic, paper, or verbal information security incidents. The program consists of the OYA Information Security Incident Response Plan, incident response procedures, this policy, staff awareness training, and ongoing review. Staff must follow the OYA Information

Security Incident Response Plan whenever an information security incident is suspected, or actually occurs.

All individuals granted access to OYA information or systems must comply with this policy and related policies, procedures, and guidelines. These individuals include OYA staff, volunteers, contractors, temporary workers, those employed by others to perform OYA work, and others authorized to access OYA information, networks, or systems.

Staff must immediately orally report information security events to their supervisors or the officer-of-the-day (OD), **and** the Information Services Service Desk (503) 378-4333. Voicemail is acceptable.

Verified information security incidents are considered significant incidents and require a Director's Incident Report pursuant to OYA policy I-E-1.0 (Director's Incident Notification and Report).

IV. GENERAL STANDARDS:

A. The Information Services security officer (ISSO) is the agency's information security incident point of contact (IPOC).

B. Information Security Incident Response Plan

OYA has an Incident Response Plan to respond to agency incidents. The plan includes roles, responsibilities, processes, and procedures for handling information security incidents.

C. Reporting Information Security Events

A reportable information security event involves information security (see definition); is unwanted, unexpected, or accidental; shows harm, intent to harm, or significant threat of harm; or the response requires nonroutine action.

1. Staff must immediately verbally report information security events to their supervisors or the officer-of-the-day (OD), and the Information Services Service Desk (503) 378-4333. Voicemail is acceptable.

   Staff must also report the event via email to IS.WorkOrder@oya.state.or.us, with "Information Security Event" as the subject.

2. Staff must include the following information in their reports:

   a) The nature of the event;

   b) What information is at risk;

   c) If there is any further risk; and

d) What mitigation efforts have been taken, if any.

3. Upon notification of an event, the Information Services Service Desk staff must immediately contact the IPOC.

4. The IPOC must assess the event for vulnerability, risk, and possible classification as an information security incident, according to the OYA Information Security Incident Response Plan.

   Possible information security incidents will be assessed using a YA 1970 Information Security Incident Response form.

5. If the event is classified as an information security incident, the IPOC must share the incident with Cyber Security Services and the OYA Information Security Team (IST) within 24 hours of occurrence.

   a) The IPOC must communicate with the IST to classify, triage and determine how to respond to the incident.

   b) The IPOC must follow OYA policy I-E-1.0 (Director's Incident Notification and Report).

   c) The IPOC must coordinate with CSS per the State of Oregon Information Security Incident Response Plan. They can be reached at (503) 378-5930 or ESO.SOC@oregon.gov.

   d) OYA Executive Team members must provide additional resources to mitigate and respond to an incident when necessary.

   e) At least once a year, the IST must present the Executive Team with information security incident and event data for awareness, review of trends, training, and policy issues.

D. Examples of reportable information security events include but are not limited to:

1. Personal information is accidentally or intentionally disclosed to unauthorized persons (e.g., first name or first initial and last name of person ***and*** Social Security number, identification number, account number, credit card number, debit card number);

2. An unauthorized person asks for or is given access to OYA systems;

3. Password or YubiKey for OYA networks, systems or JJIS access is compromised;

4. Unauthorized reproduction of information;

5. Unauthorized persons found in restricted area;

6. Restricted or critical information documents are not properly destroyed;

7. Loss or theft of physical or electronic data containing restricted or critical information;

8. Restricted or critical information is not properly protected or handled;

9. Mobile communication device or other data storage device (e.g., laptop, smart phone, flash drive, CD, desktop workstation) containing restricted or critical information is lost or stolen;

10. Data is defaced or destroyed;

11. Conversation about restricted or critical information overheard by an unauthorized person who discloses the information to the public;

12. Data is modified for unexplained reasons; or

13. Any violation of OYA information security policies.

E. Examples of nonreportable information security events include but are not limited to:

1. Criminal violations with no information security component such as theft of a car (no information security involved);

2. Network or intranet unavailable due to routine problem or maintenance (action required is routine);

3. Briefcase containing publicly disclosable information is lost (no harm, no intent to harm, or no significant threat of harm); or

4. Computer virus detected on a workstation that is successfully contained by anti-virus software (action required is routine).

5. If staff are unsure whether a situation is a reportable event, staff are encouraged to err on the side of caution and report it.

F. The OYA volunteer coordinator and contract administrators must ensure volunteers and contractors are aware of and follow this policy, when applicable.

G. The IST will ensure the reporting process is tested at least once per calendar year to evaluate staff awareness and agency vulnerability.

H. Information Services must have a written agencywide procedure that delineates how Service Desk staff will respond to and document staff-reported information security events and incidents.

V. LOCAL OPERATING PROTOCOL REQUIRED: NO