



# Oregon Juvenile Justice Information System



## Policy Statement

### Security (Users)

<b>Approved:</b>    <b>Jean Straight, Co-Chair JJIS Steering Committee</b>	<b>Effective Date:</b>	4/18/2012
	<b>JJIS Steering Committee Approval:</b>	1/18/2012
	<b>JJIS Policy &amp; Standards Committee Approval:</b>	8/24/2011
	<b>Supersedes:</b>	8/1/2010, 6/8/2009, 12/17/2008, 7/18/2007, 3/21/2007, 3/6/2006, 12/21/2005, 9/17/2003
<b>REFERENCE:</b>	OAR 416-180-0000, Administration of JJIS OAR 416-180-0050, Security of Information JJIS Policy - Workers JJIS Policy - Granting Access to JJIS and JJIS Data JJIS Policy - Privacy & Protection of Confidential Information in JJIS	

<b>PURPOSE:</b>	<ul style="list-style-type: none"> <li>■ <i>To articulate Security standards for access to JJIS and use of the Oregon Juvenile Justice Information System</i></li> <li>■ <i>To clarify standards for Authorization and Revocation of Access</i></li> <li>■ <i>To clarify consequences for Violations of Security</i></li> </ul>
-----------------	---

<b>DEFINITIONS:</b>	<p><u>JJIS User</u> – any individual who may be provided access to JJIS in order to view or enter information</p> <p><u>JJIS Youth Worker</u> – a JJIS User who has an assigned youth caseload</p> <p><u>Local Security Coordinator</u> – an OYA or county primary or back-up contact for administering and supporting JJIS security guidelines</p> <p><u>JJIS Security Officer</u> – OYA's Information Systems staff member who oversees JJIS security protocols consistent with JJIS policies and the direction of the JJIS Data Steward</p> <p><u>JJIS Data Steward</u> – OYA's Information Systems Chief Information Officer, responsible for the high-level administration and security of JJIS</p> <p><u>JJIS Internal Partners</u> - organizations whose employees will directly record data, report information, or manage youth offender caseloads using JJIS</p> <p><u>JJIS External Partners</u> - other public and private agencies that work with youth served by the county juvenile departments and the Oregon Youth Authority and have been authorized to have access to JJIS</p>
---------------------	---

<b>POLICY:</b>	<p><b><u>General Policy</u></b></p> <p>Information in JJIS is confidential unless considered public information pursuant to ORS 192.410 to 192.505; 419B.035; 419A.255.</p> <p>The JJIS system will comply with all federal, state, and local laws regarding public</p>
----------------	---



information and confidentiality, as well as information technology standards set forth by the Oregon Legislature, the Department of Administrative Services, and the Criminal Justice Information Standards.

To protect the integrity of the system, JJIS partners will conform to system security measures, as defined by JJIS policies and procedures and implemented at the local level through related procedures.

### **Access to Youth Records**

Workers who are assigned to work with a youth have access to the youth record consistent with the worker's security roles. Workers are considered assigned to a youth when they are recorded as an active worker on the youth record; they work in the office of the Primary Worker, Courtesy Supervision Worker, Referral Worker or JD Worker During OYA Commitment; or when they work in a facility in which the youth is currently admitted and they have a specific direct working relationship with that youth or an otherwise authorized work related reason to access that specific youth record or specific information on a youth's record.

Authorized work related reasons do not extend to all youth in the office or facility where a worker works. On-going auditing of a case in a facility where the worker does not have a direct relationship to work with that specific youth is not considered an authorized job task.

### **Temporary Assignment to Youth Records**

Workers who are not assigned to work with a youth may have a legitimate need to view and update youth information consistent with their security roles (e.g., Detention Intake Screening, Close Custody Transport, Training and Support). Workers who need access to the record of a youth to whom they are not assigned may grant themselves Temporary Assignment for 24 hours. All Temporary Assignments will be tracked.

### **Confidentiality and Appropriate Use**

JJIS information will be used only for legitimate law enforcement and juvenile justice purposes, or as otherwise allowed by state and federal statute. JJIS information should be conveyed only in a secure and appropriate manner.

No person is allowed to seek, obtain, use, or release information from JJIS for private or personal reasons.

Viewing information in JJIS is the equivalent of viewing information in a hard copy file. JJIS users will seek, obtain, and use only the minimum amount of information needed to accomplish an authorized job task.

Access to information protected by the Protection Indicator will be logged on an access log. See JJIS Policy on "Privacy and Protection of Confidential Information".

Employees seeking public information for uses other than an authorized job task should request and obtain the information from the local office Security Coordinator. The local Security Coordinator will review the request and respond consistent with local and JJIS policies on Public Information.

JJIS information can only be viewed and released subject to agency and JJIS policy. Unless otherwise provided by JJIS policy, information on youth with active cases should be released only by the agency with jurisdiction or physical custody, and in accordance with prevailing state and federal statutes. Disclosure of information on youth with a closed case is also subject to agency policy and must be in accordance with prevailing state and federal statutes. Unless otherwise provided by JJIS policy, confidential information should be released only by the agency that entered the



information into JJIS.

Any information in JJIS that relates to the past, present, or future physical or mental health condition of an individual, the provision of health care to an individual, or the payment for the provision of health care to an individual (known as “health information”) is considered confidential under the federal Health Insurance Portability and Accountability Act (45 CFR Parts 160 and 164) (HIPAA). Disclosure of health information which is not otherwise allowed or required by state or federal law may be a serious violation and subject to criminal investigation and prosecution by the State of Oregon and by the federal government.

### **Electronic Disclosure of JJIS Information**

Some JJIS features create automatic email notifications to designated users, such as Youth Incident Report notifications. JJIS users will adhere to JJIS and local agency policies regarding access, disclosure, confidentiality, and security when retrieving and disclosing any juvenile records contained in JJIS into a report, document, screen print, email, or other electronic format.

JJIS security protections that safeguard confidential juvenile records do not exist in various email and external electronic systems such as personal digital assistants (PDAs) and smartphones. Dissemination of these records by other electronic format increases a risk of inappropriate disclosure. In order to limit this risk, juvenile records referenced in an email or other electronic format will adhere to the following guidelines:

#### **Identity of the Recipients**

When an email contains youth information obtained from JJIS, whether or not it contains personally identifiable information about a youth, the names of sender and all recipients of the email must be clearly visible on the email. Any group distribution must clearly identify the members of the distribution group. The use of blind copy, generic group distribution, or any other means that masks the identity of a recipient is prohibited.

#### **Content Guidelines**

Confidential youth information will not be disclosed via text messaging.

Medical information will not be sent by email, text messaging, or any other electronic format unless that format adheres to federal and state requirements and includes adequate transmittal protections, such as encryption.

Local agency policy may have additional guidelines and may be more restrictive.

### **Conflict of Interest**

Persons are prohibited from using the JJIS system or data for their own interest, advantage, personal gain, or for any private purpose.

#### **Notification of Supervisor**

To support appropriate use and avoid potential conflicts of interest, employees with access to JJIS will notify their immediate supervisor if expected to work on a case where the employee has a close personal relationship with a youth or an associate of a youth in JJIS.

Examples of a close personal relationship include:

- a youth is a relative or close personal acquaintance; or
- the employee is the victim, or has a relative, spouse, or close personal acquaintance who is the victim of a crime committed by a youth.



### **Agency Director Commitment**

Each agency/department director will sign and submit to the JJIS Security Officer, an annual agreement reflecting an understanding and commitment that the agency/department:

- is responsible for the accuracy, timeliness, and completeness of any information that it enters into JJIS;
- will have a local primary Security Coordinator, and if appropriate, a back-up Security Coordinator;
- will provide the local Security Coordinator(s) with a description of the Security Coordinator's responsibilities;
- will keep JJIS workstations secure from unauthorized use or viewing;
- will release information only about youth within its jurisdiction or, when applicable, within its physical custody, and according to prevailing state and federal statutes or in accordance with JJIS policies.
- will comply with the JJIS "User Security" and "Granting Access to JJIS and JJIS Data" policies.

### **Local JJIS Security Coordinators**

Each JJIS Agency will have a local primary Security Coordinator, and if appropriate, a backup-up Security Coordinator, who is the primary contact for assigning and revoking security roles and distributing passwords.

Security Coordinators will sign an annual Security Coordinator Agreement that articulates their roles and responsibilities.

Local Security Coordinator responsibilities include:

- act as the primary or back up office contact person for security;
- assure that users understand JJIS security rules;
- obtain original and annual user agreements;
- maintain and archive original and/or copies of all local security forms, consistent with local agency directives and county and state retention schedules for information system related documents;
- maintain documented authorization for the agency's security templates;
- create user accounts, assign and change user security roles and/or templates, and grant custody unit log access, limited to the minimum amount of information needed to accomplish an authorized job task (OYA User Accounts are created centrally);
- unlock accounts, reset passwords, clear security and revoke user accounts when needed;
- provide access to JJIS instruction materials, including training updates, to each user;
- provide support to agency director regarding any security violations if requested;
- obtain and submit annual signed Agency/Department Director Security Agreement to the JJIS Security Officer by July 1 each year;
- submit annual Security Coordinator Roles and Responsibilities Agreement to the JJIS Security Officer by July 1 each year.



## **User Training**

Under ideal circumstances, user rights and security roles will not be issued, regardless of need, until the person has been adequately trained or trained commensurate with the level of security issued, or will be closely supervised.

Each user will have a record which tracks training. Each partner agency is responsible for determining responsibility for these records.

## **Adding Users and Creating User Accounts**

A JJIS User is any individual who may be provided access to JJIS in order to view or enter information.

Youth Workers are JJIS Users who have assigned youth caseloads.

Not all JJIS Users are Youth Workers. Not all Youth Workers will have JJIS access. A Youth Worker may be established in JJIS without access to JJIS (i.e., without a User Name and Password) in order to provide caseloads for organizational workers or units. (See JJIS "Worker" Policy).

Users will submit a signed User Security Agreement prior to gaining access to JJIS and a signed annual renewal by July 1 of each year to their local Security Coordinator. JJIS users will not give their User Name or Password to anyone. In order to protect confidentiality, JJIS users will not leave their JJIS screen accessible for unauthorized viewing or use by the public or any other unauthorized persons.

### **Adding Users**

OYA users will automatically be entered, updated, or terminated in JJIS the morning following any relevant entry in OYA's Human Resources information system. County Security Coordinators must manually add users in JJIS.

### **Creating Accounts**

A JJIS User must be provided with a unique User Name and Password in order to access JJIS. JJIS will automatically assign the next sequential and unique User Name and generate a Password; however, County Security Coordinators may create unique User Names for all county users and county-sponsored external partners, adhering to a standard naming convention using the assigned county code followed by any other locally defined naming conventions.

Security Coordinators will be able to re-issue a User Name for a previous User who has a prior JJIS account.

County

### **Single User / Multiple Job Assignments**

Users may have one or more Job Assignments; however, security is associated with the User, not a Job Assignment. Users with multiple job assignments must be provided with all the security roles needed to perform each job assignment.

Security Templates may be set up to provide easy assignment to authorized security roles for groups of designated staff. Only one Security Template can be assigned to a User. Security Coordinators will add additional Security roles to a user with multiple job assignments and will not remove a Security Template assigned by another Security Coordinator.

### **Single User / Multiple User Names**

Users who work in multiple work sites (e.g., workers who carry separate



caseloads, work for two county juvenile departments, or work for both OYA and a county juvenile department) may have two User Names in order to support accurate caseload, unit, and office statistics. Each account will be used only for the job for which the account was granted. Under some circumstances a worker with multiple jobs may need only one User Name.

- **Single User Name** - (e.g., multiple assignments or job rotation in the same agency) Instead of creating multiple User Names, Security Coordinators may create additional job assignments under a single User Name. When users with multiple job assignments under the same User Name log-on to JJIS, a screen with a list of assigned jobs will appear.

If necessary, users who work in multiple units can use the Switch Office feature to quickly move between their job assignments.

Users can have different default settings and notebook preferences for each of the offices they work in – when the User activates the Switch Office feature, the preferred settings for the selected office become effective..

- **Multiple User Names** - Individuals who work in more than one office may need different security and user settings depending on the job duties. Security is associated with the User and data are associated with the Worker or Worker's Office. This data affects a variety of functions in JJIS, including how statistics are computed. The following functions are affected by Worker Office:

- Default Settings & User Settings
- Access & Temporary Assignment to Cases
- Drop-Down List Visibility – such as Assessments, Documents, Programs, Services, Case Plan Interventions, Attendance Tracking, Population Groups, Decision Point Templates
- Unit Log Access for Workers in Facilities
- OYA Case Audit
- Worker Task List

Strong consideration should be given to having multiple User Names to obtain the correct options in drop-down lists (e.g., the user may be entering case plan interventions in multiple offices).

Users who work for more than one agency need multiple User Names and separate Security for each User Name. Examples when this might occur include:

- OYA employee works periodically at county juvenile department or detention facility
- County juvenile department employee works overtime periodically at an OYA facility
- County juvenile department employee works periodically at another county's detention center
- Approved External Partner (police officer) needs JJPS access for job and works relief at county detention facility
- County External Partner who works part-time or as a relief employee for OYA
- OYA External Partner who works part-time or as a relief employee for a county juvenile department



### **Granting Access and Assigning Security Roles**

Access to JJIS and JJIS data will only be granted consistent with the JJIS policy on “Granting Access to JJIS and JJIS Data”.

Security role authorization is to be issued only to those who are legally authorized to access information in JJIS.

Annual User Agreements will be maintained, filed, and archived locally consistent with local agency directives and county and state retention schedules for information system related documents.

Security roles will be granted to limit access to the minimum amount of information needed to accomplish an authorized job task.

Security roles will provide limits which prohibit creating, reading, updating or deleting information inconsistent with the user's role, agency policy, or that of other affected counties/departments (e.g., rights to create or delete a case or referral will be given to a limited number of people in most circumstances).

Each time a security role is changed, a JJIS User Security Access Role Assignment form will be signed and filed locally.

Security role authorizations will be reviewed and renewal User Agreements will be signed annually.

Security Templates may be authorized to efficiently assign multiple roles.

### **External Partner Access** (see “Granting Access to JJIS and JJIS Data” Policy)

External Partners may be granted access to JJIS only after approval from the JJIS Steering Committee. External Partners that have been approved to access JJIS will be authorized by a formal Memorandum of Understanding, if applicable, and a User Security Agreement for each employee accessing JJIS.

- External Partner User Agreements for new External Partner users will be sent to the JJIS Help Desk to obtain a User Name and Password.
- External Partner annual renewal agreements will be maintained locally.

These forms must be renewed annually and processed through the JJIS Security Officer.

### **Information Technology (IT) Developer Access**

Except for OYA's JJIS IT developers and Database Administrator approved by OYA's Chief Information Officer (CIO), security roles for IT developers who are granted access to JJIS will be limited to View Only. IT developers with JJIS access will work with the sponsoring agency's JJIS Security Coordinator to review and understand security issues and policies associated with JJIS data.

JJIS Partners who provide access to JJIS for IT developers will sign an annual agency agreement reflecting an understanding and commitment that the agency/department will assure that its IT developers:

- adhere to the policies and expectations of the JJIS partnership;
- agree to protect JJIS data from unauthorized viewing or use;
- agree to provide data obtained through JJIS or JJIS extracts or external applications to only those individuals who have security to access the information through the JJIS application itself or an approved research project;
- agree to not extract “Protected” information for use in local applications



unless specifically authorized by the OYA Chief Information Officer or designee;

- agree to not provide data from a “Restricted” notebook to anyone unless that person is authorized in JJIS to access the restricted notebook;
- agree to remove any identifying information about the youth from any external copies of JJIS or any local applications that have used JJIS data when a youth is expunged in JJIS.

IT Developers who are provided access to JJIS will sign an annual IT Developer User Agreement by July 1 of each year reflecting an understanding and commitment that they:

- are responsible for all transactions entered in JJIS under their User Name;
- will not give their User Name or password to anyone nor allow anyone to use their User Name;
- will protect their JJIS screen from unauthorized viewing or use by the public or any other unauthorized persons in order to protect confidentiality;
- will provide data obtained through data extracts or external applications only to those individuals who have security to access that data through the JJIS application or approved research access;
- will not extract “Protected” information for use in local applications unless specifically authorized by the OYA Chief Information Officer or designee. (See JJIS Policy on Privacy and Protection of Confidential Information in JJIS). When creating extracts that include case notes, programmers will access a special table that filters out protected case notes);
- will not provide data from a “Restricted” notebook to anyone unless the person is authorized in JJIS to access the restricted notebook;
- will remove all identifying information about a youth from any external copies of JJIS or any local applications that have used JJIS data when a youth is expunged in JJIS.

The OYA Database Administrator will monitor security roles assigned to these users.

### **Researcher Access**

Security roles for researchers who are granted access to JJIS will be limited to View Only. Researchers with JJIS access will work with the sponsoring agency’s JJIS Security Coordinator or appropriate business sponsor to review and understand security issues and policies associated with JJIS data. Access will be provided only to those employees or subcontractors who have a need in connection with performance of the activity for which the data is obtained. Such persons will be advised of and agree to comply with these regulations.

Researchers who are provided access to JJIS will sign an annual JJIS Research User Security Agreement by July 1 of each year reflecting an understanding and commitment that they will:

- adhere to the policies and expectations of the JJIS partnership;
- comply with their employer’s policy on appropriate use of computer equipment;
- not give their User Name or password to anyone nor allow anyone to use their User Name;
- protect their JJIS screen from unauthorized viewing or use by the public or any other unauthorized persons in order to protect confidentiality;
- understand that JJIS reports or extract files may contain data on youth whose records have been expunged subsequent to the preparation of the report or extract;



- agree to and understand the following standards regarding Confidentiality and Privacy of Identifiable Research and Statistical Information:
  - Information identifiable to a private person will be used only for research and statistical purposes.
  - Information identifiable to a private person will not be revealed to any person for any purpose except:
    - where the information has already been included in research findings (and/or databases); and is
    - revealed on a need-to-know basis for research or statistical purposes, provided that such transfer is approved by the person providing information under the agreement, or authorized.
  - Project plans will be designed to preserve anonymity of private persons to whom information relates, including, where appropriate, requirement name-stripping and/or coding of data or other similar procedures.
  - Project findings and reports prepared for dissemination will not contain information which can reasonably be expected to be identifiable to a private person.
  - Information identifiable to a private person (obtained in accordance with this agreement) will, unless otherwise agreed upon, be returned upon completion of the project for which obtained and no copies of that information retained.

Adequate administrative and physical precautions will be taken to assure security of information obtained for such purposes.

Knowingly and willfully using or disseminating information contrary to the provision of the agreement shall constitute a violation of these regulations and will result in termination of access, denial of future data access, and/or prohibition from publishing or presenting research findings, and possible disciplinary action up to and including dismissal.

### **Inactivity and Automatic Lock Out**

As a safeguard, after ten failed log-on attempts or after 60 days of inactivity on a JJIS account, the user's account will automatically lock. The local Security Coordinator will receive a warning email 7 days prior to the lock-out date and then forward the email to the JJIS user.

Once an account has been locked, the local Security Coordinator may unlock the account. If the user's account is locked because of failed log-ins, it may take up to 15 minutes before the Security Coordinator can unlock the account because of a JJIS system check. Once the account is unlocked, the user must log-in to reset the clock for inactivity.

Accounts will be revoked after 120 days of inactivity. The local Security Coordinator will receive a warning email 7 days prior the revocation date and then forward the email to the JJIS user. Another email will be sent to the Security Coordinator at the time of revocation (120 days) which can then be forwarded to the JJIS user.

If the account has been revoked for any reason, but the user's JJIS access is later approved to be reinstated, the Security Coordinator must create a new account for the user, using the same process as if requesting for a new user.

### **Revocation**

Access will be revoked when a user is no longer authorized to use JJIS (e.g., an employee is terminated from employment).

To initiate revocation of a user's access, JJIS Form 3d, User Security Revocation,



must be completed, signed and locally maintained, If there is a youth caseload, it must be transferred to other appropriate users and an End Date must be entered in the User Notebook; then the account can be revoked. Access to JJIS will be prevented immediately.

**Security Violations**

JJIS partners are responsible for monitoring appropriate use of JJIS and maintaining security standards. JJIS partners will follow local agency policy for investigating and responding to violations of security. JJIS partners will honor the confidentiality of local disciplinary measures regarding specific individuals.

The JJIS Steering Committee Chairperson will be notified of:

- any known security violation that is investigated and found to be true, including the resolution of the investigation;
- any suspected security violation requiring investigation assistance from the JJIS project;
- any suspected security violation in another internal partner or an external partner agency); and
- the resolution of the original reported suspected violation.

Inadvertent violations that do not require an investigation do not need to be reported.

The Chairperson will provide a quarterly report to the JJIS Steering Committee quantifying the number and types of security violations found to be true.

Suspected violations from another internal partner agency may also be reported to the director in the agency where the violation is suspected. In this case, the director of the agency where the violation is suspected will notify the JJIS Steering Committee consistent with this policy.

As soon as a security violation has been identified, the local agency will take immediate appropriate action. If necessary, the local agency will either suspend or terminate the employee’s access as soon as possible pending the investigation of the violation.

Resolutions will range from discipline to termination depending on the nature of the violation and local agency policy.

If the Security Violation involves suspected misuse of JJIS by one of the internal partner agency directors, the issue will immediately be brought to the attention of the JJIS Steering Committee to handle on a case-by-case basis.

JJIS tracks who makes changes and who has viewed specific screens and technical support is available to assist with the investigation of security violations. Any JJIS staff who receives information or provides investigative support regarding a security violation will maintain confidentiality.

**PROCEDURES:**

**A. Authorization of Access**

New Internal Partner employees:

1. Provide the new employee with access to adequate training and orientation to JJIS.
2. Obtain a signed copy of the JJIS User Security Agreement and create the new User Account. File the agreement locally according to local policy.
3. Complete or obtain from employee’s manager a JJIS Security Access Role Assignment form and maintain locally. Complete a new Role Assignment form every time an employee’s security roles change.



4. Assign and manage employee's security in JJIS consistent with security authorized on JJIS Access Role Assignment form.
5. Coordinate annual renewal signatures on JJIS User Security Agreements for each user by July 1 of each year and file locally.
6. Retain all forms consistent with the responsible agency's policies on file retention.

New authorized External Partner employees: (See "Granting Access to JJIS and JJIS Data" policy):

1. Following JJIS Steering Committee approval, obtain a signed JJIS User Security Agreement and submit to the JJIS Help Desk. File a copy of the agreement locally according to local policy.
2. Complete or obtain a JJIS Security Access Role Assignment form and maintain locally. The Security Roles must match the authorized access defined in appropriate authorization documentation (either an MOU or the JJIS Access policy). Complete a new Role Assignment form every time an employee's security roles change.
3. Provide the user with access to adequate training and orientation to JJIS.
4. Assign and manage user security in JJIS consistent with security authorized on JJIS Access Role Assignment form.
5. Coordinate annual renewal signatures on JJIS User Security Agreements for each user by July 1 of each year and file locally.
6. Retain all forms consistent with the responsible agency's policies on file retention.

#### **B. Revocation of Access**

When an employee terminates employment or is no longer authorized to use JJIS, unless revocation is automatically initiated by an OYA Personnel Action,

1. Obtain a signed JJIS User Security Revocation – JJIS Form 3d.
2. If there is a worker caseload, transfer it to another appropriate worker. Enter an End Date for the User in the JJIS User Notebook. This will immediately revoke access to the JJIS software and remove the person's name from the Office drop-down list in JJIS.
3. Revoke the Account.
4. Maintain appropriate copies of these forms locally.

#### **C. Inactivity and Automatic Lock Out/Revocation Procedures**

**53 days of user inactivity** = A lockout warning email that the user account will be locked in 7 days is sent to the local Security Coordinator(s) to forward to the user. The user will need to sign on to stop the lock out process.

**60 days of user inactivity** = The user account is locked and a lock out email is sent to the local Security Coordinator(s). The Security Coordinator will need to either revoke or unlock the account.

**113 days of user inactivity** = A revocation warning email that the user account is locked and will be revoked in 7 days is sent to the local Security Coordinator(s) to forward to the user. The Security Coordinator will need to unlock the account.

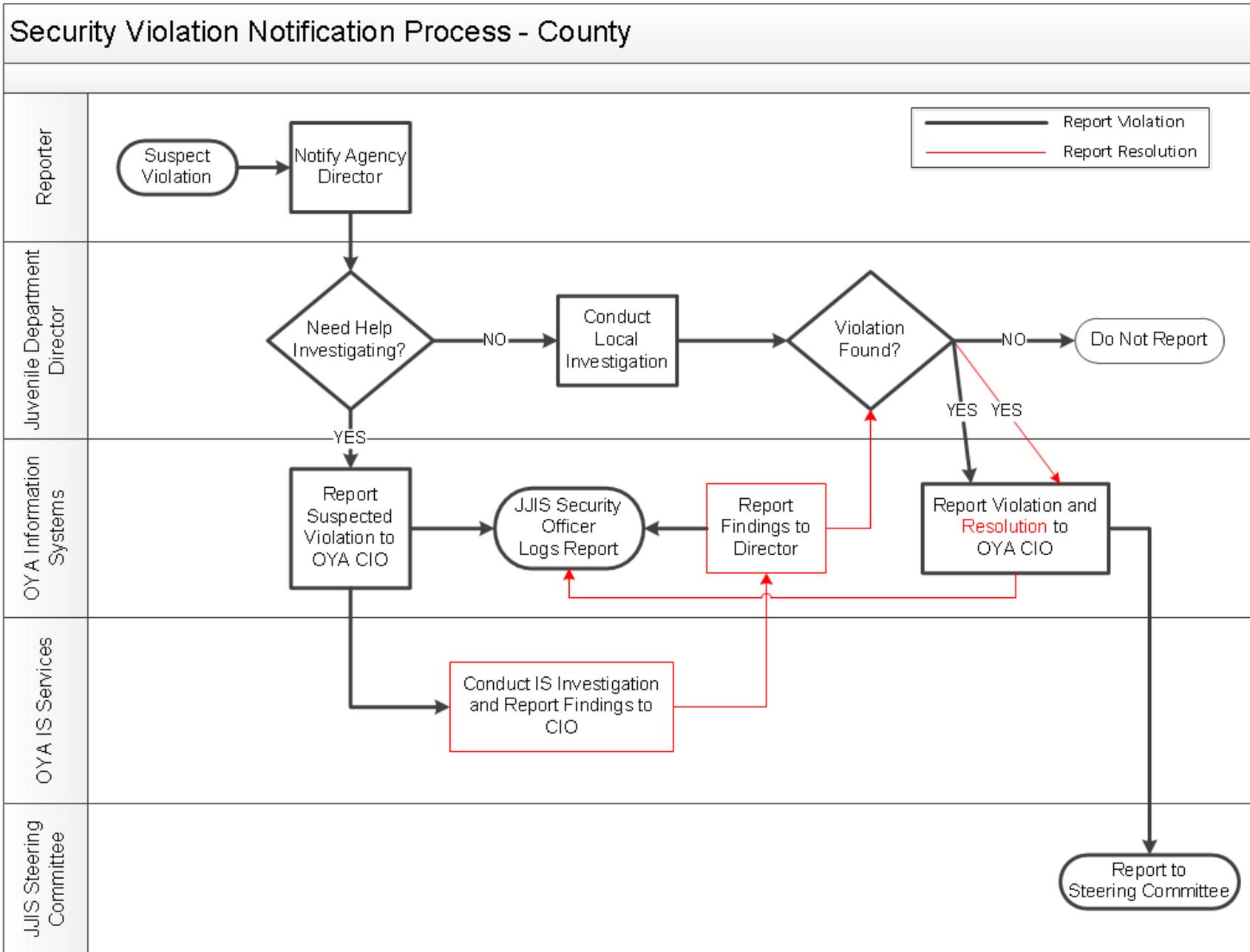
**120 days of user inactivity** = The account is revoked and an email is sent to the local Security Coordinator(s). The Security Coordinator will need to re-

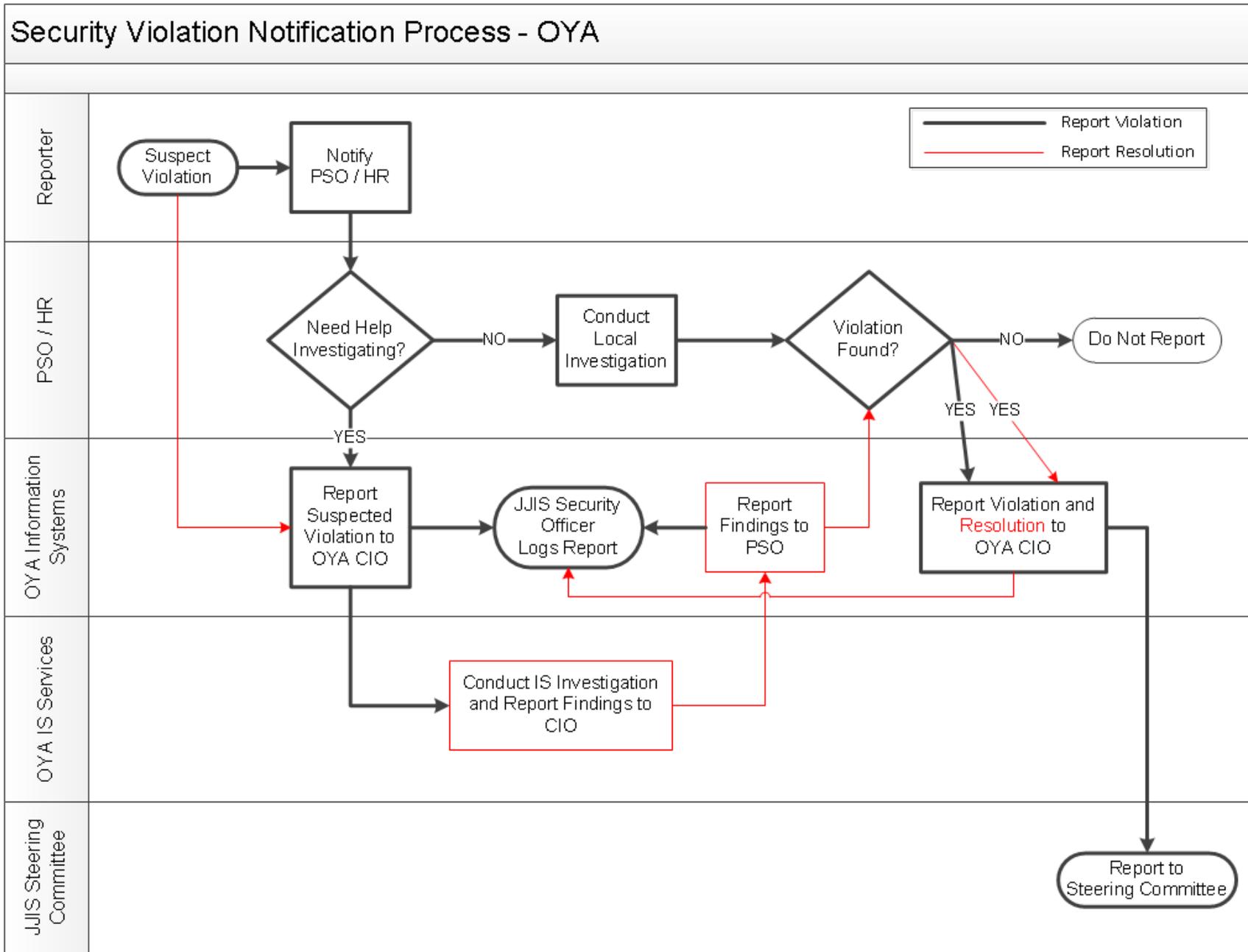


create the account.

#### **D. Security Violation Notification (JJIS Form 1d)**

- **Known Local Violation Resulting in an Investigation**
  - Agency/Office Director or authorized designee completes Sections I through IV of JJIS Security Violation Notification form and faxes it to the OYA Information Systems Chief Information Officer.
  - OYA Chief Information Officer notifies the chairperson of the JJIS Steering Committee.
  - JJIS Steering Committee chairperson notifies JJIS Steering Committee.
- **Suspected Violation Requiring JJIS Investigation Assistance**
  - Agency/Office Director or authorized designee completes Sections I through III of JJIS Security Violation Notification form and faxes it to the OYA Chief Information Officer.
  - OYA Chief Information Officer or designated staff contacts Agency/Office Director or authorized designee for additional details for investigation.
  - OYA Chief Information Officer communicates investigative findings to Agency/Office Director or authorized designee.
  - Agency/Office Director or authorized designee communicates resolution to JJIS to close investigation.
- **Suspected Violation in Another Internal Partner Agency/Office**
  - The Agency/Office Director or authorized designee completes Sections I through III of JJIS Security Violation Notification form and faxes it to the OYA Chief Information Officer.
  - Agency/Office Director or authorized designee notifies the director in the office where the violation is suspected.
  - The Director in the office where the violation is suspected completes Sections I through III of the JJIS Security Violation Notification Form and faxes it to the OYA Chief Information Officer.
  - OYA Chief Information Officer notifies Director of the other agency/office for action/resolution.
- **Suspected Violation in an External Partner Agency/Office**
  - Agency/Office Director or authorized designee of an agency who suspects a security violation in an external partner agency/office completes Sections I through III of the JJIS Security Violation Notification Form and faxes it to the OYA Chief Information Officer.
  - OYA Chief Information Officer notifies Director of the sponsoring internal partner agency for action/resolution.
- **Notification of Resolution of Suspected Violation**
  - Agency/Office Director or authorized designee completes Section I and IV of JJIS Security Violation Notification form and faxes it to OYA Chief Information Officer.
  - OYA Chief Information Officer notifies chairperson of JJIS Steering Committee if resolution involves disciplinary action.
  - JJIS Steering Committee chairperson notifies JJIS Steering Committee.







## JJIS Forms Distribution & Retention

(All JJIS Forms have a retention of three years.)

Form	Distribution for New Forms	Distribution for Annual Renewals
1a Agency/Department Director Security Agreement	<ul style="list-style-type: none"> <li>• JJIS Security Officer</li> <li>• Agency/Department Director</li> <li>• Site Security Coordinator files locally</li> </ul>	<ul style="list-style-type: none"> <li>• JJIS Security Officer</li> <li>• Agency/Department Director</li> <li>• Site Security Coordinator files locally</li> </ul>
1b Agency/Department Security Coordinator Security Agreement	<ul style="list-style-type: none"> <li>• JJIS Security Officer</li> <li>• Site Security Coordinator files locally</li> </ul>	<ul style="list-style-type: none"> <li>• JJIS Security Officer</li> <li>• Site Security Coordinator files locally</li> </ul>
1d Security Violation Notification	<ul style="list-style-type: none"> <li>• OYA Information Systems Chief Information Officer</li> </ul>	NA
1e External Partner Authorized Representative Security Agreement	<ul style="list-style-type: none"> <li>• JJIS Security Officer</li> <li>• External Partner Authorized Representative</li> <li>• Sponsoring Agency Security Coordinator files locally</li> </ul>	<ul style="list-style-type: none"> <li>• JJIS Security Officer</li> <li>• External Partner Authorized Representative</li> <li>• Sponsoring Agency Security Coordinator files locally</li> </ul>
2a User Security Agreement	<ul style="list-style-type: none"> <li>• Site Security Coordinator files locally</li> <li>• JJIS Help Desk – only non-employee OYA workers (e.g., interns, temporaries)</li> <li>• User</li> <li>• If External Partner, Authorized Agency representative</li> </ul>	<ul style="list-style-type: none"> <li>• Site Security Coordinator files locally</li> <li>• JJIS Help Desk – only non-employee OYA workers (e.g., interns, temporaries)</li> <li>• User</li> <li>• If External Partner, Authorized Agency representative</li> </ul>
2c Research Project User Security Agreement	<ul style="list-style-type: none"> <li>• JJIS Security Officer</li> <li>• Research Project User</li> <li>• Site Security Coordinator files locally</li> </ul>	<ul style="list-style-type: none"> <li>• JJIS Help Desk</li> <li>• User</li> <li>• Sponsoring Agency Security Coordinator files locally</li> </ul>
3a User Security Access Role Assignment	NA	NA
3b Notebook Restriction and Worker Authorization	<ul style="list-style-type: none"> <li>• Site Security Coordinator files locally</li> </ul>	NA
3d User Security Revocation	<ul style="list-style-type: none"> <li>• Site Security Coordinator files locally</li> </ul>	NA
4a External Partner / Research Access Request	<ul style="list-style-type: none"> <li>• JJIS Security Officer</li> <li>• Sponsoring Agency Security Coordinator files locally</li> </ul>	NA
4b Reports Access Request	<ul style="list-style-type: none"> <li>• JJIS Help Desk</li> <li>• User</li> <li>• Site Security Coordinator files locally</li> </ul>	NA



## JJIS Forms Distribution & Retention

(All JJIS Forms have a retention of three years.)

Form	Distribution for New Forms	Distribution for Annual Renewals
4c     Notification Form — External Partner Access	<ul style="list-style-type: none"> <li>• JJIS Security Officer (with a signed JJIS Form 2a for each user)</li> <li>• Sponsoring Agency Security Coordinator files locally</li> </ul>	NA
JJPS 1     JJPS Access Request/Notification	<ul style="list-style-type: none"> <li>• JJIS Security Officer (with a signed JJIS Form 2a for each user)</li> <li>• Sponsoring Agency Security Coordinator files locally</li> </ul>	NA
JJPS 2     JJPS Authorized Agency Representative Agreement	<ul style="list-style-type: none"> <li>• JJIS Security Officer</li> <li>• JJPS Agency Authorized Representative</li> <li>• Sponsoring Agency Security Coordinator files locally</li> </ul>	(Submit list of current JJPS users with renewal) <ul style="list-style-type: none"> <li>• JJIS Security Officer</li> <li>• Sponsoring Agency Security Coordinator files locally</li> </ul>
JJPS 4     JJPS User Security Revocation Form	<ul style="list-style-type: none"> <li>• JJIS Help Desk</li> <li>• JJPS Agency Authorized Representative</li> <li>• Sponsoring Agency Security Coordinator files locally</li> </ul>	NA
DEV1     Agency/Department IT Access Request	<ul style="list-style-type: none"> <li>• JJIS Security Officer</li> <li>• Requesting Agency Authorized Representative</li> <li>• Sponsoring Agency Security Coordinator files locally</li> </ul>	NA
DEV2     IT Developer Authorized Agency Agreement	<ul style="list-style-type: none"> <li>• JJIS Security Officer</li> <li>• Requesting Agency Authorized Representative</li> <li>• Sponsoring Agency Security Coordinator files locally</li> </ul>	<ul style="list-style-type: none"> <li>• JJIS Security Officer</li> <li>• Requesting Agency Authorized Representative</li> <li>• Sponsoring Agency Security Coordinator files locally</li> </ul>
DEV3     IT Developer Security Agreement	<ul style="list-style-type: none"> <li>• JJIS Security Officer</li> <li>• Requesting Agency Authorized Representative</li> <li>• User (Developer)</li> <li>• Sponsoring Agency Security Coordinator files locally</li> </ul>	<ul style="list-style-type: none"> <li>• JJIS Security Officer</li> <li>• Requesting Agency Authorized Representative</li> <li>• User (Developer)</li> <li>• Sponsoring Agency Security Coordinator files locally</li> </ul>