JJIS Security Review - Annual Renewal

About this presentation

The presentation does not automatically advance – use the keyboard Page Up/Down or arrow keys or the arrows in the lower right of the screen to move forward (or backward) in the presentation.

The presentation is not accompanied by audio or voiceover at this time.

Some slides include links to JJIS policy – for more information about your responsibilities as a JJIS user, click on the link to review the policy.

Juvenile Justice
JJIS
Information System

JJIS Security Review - Annual Renewal

Assurances and User Responsibilities

Annual Security Review

- Access and Use
- Security Tools
- Protecting Information

▶

Rev: 4/2021

JJIS Annual Review

Individuals who already have access to JJIS must complete a review process by July 1 of each year.

This brief presentation provides an overview of the expectations and requirements of JJIS users around security, appropriate access and use, and confidentiality.

By completing this review, users

1) demonstrate commitment to their ethical responsibility to the multiple jurisdictions whose data are contained in JJIS;
2) declare that they understand what is required of them to protect confidentiality and prevent any unintentional disclosure of information; and
3) acknowledge that JJIS may be used only for their approved purpose.

County and external partner users review this presentation provided by their local JJIS Security Coordinator.

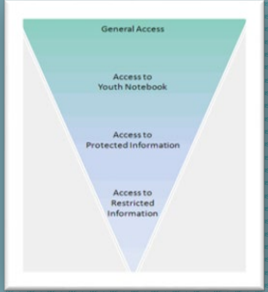
- Local JJIS Security Coordinators determine and coordinate the review process for their sites.
- Options are included at the of the presentation for completing a certificate, or completing a renewal of the JJIS User Security Agreement (JJIS Form 2a).

OYA users are assigned this mandatory review through the agency's online learning management system where it is tracked and recorded in their individual training record.

User Responsibilities

Appropriate Access & Use

- Understand appropriate use of a record
- Sharing information
- Investigation of suspected violations
- Violations vs. training issue


General Access
Access to Youth Notebook
Access to Protected Information
Access to Restricted Information

Security Tools

- Apply Temporary Assignment
- Understand Protected Information
- Understand Restricted Information
- Access logs

Protect Information

- Acquire the habit of locking workstations
- Recognize that shared log-ins inaccurately reflect case documentation
- Know how to change a password and the criteria for a strong password

Access

The JJIS system, its data, and any subsystems such as the Juvenile Justice Partner System (JJPS) or Juvenile Provider Access System (JPAS), are not to be used for a person's own interest, advantage, personal gain, or for any private purpose.

Users are expected to access only the minimum amount of information needed to accomplish their authorized job duties.

JJIS records should be accessed on a "need-to-know" basis by users to whom the youth is assigned.

Users are considered "workers" assigned to a youth if they:

1) are recorded as an active worker on the youth record;

2) work in the same office as an assigned worker*; or

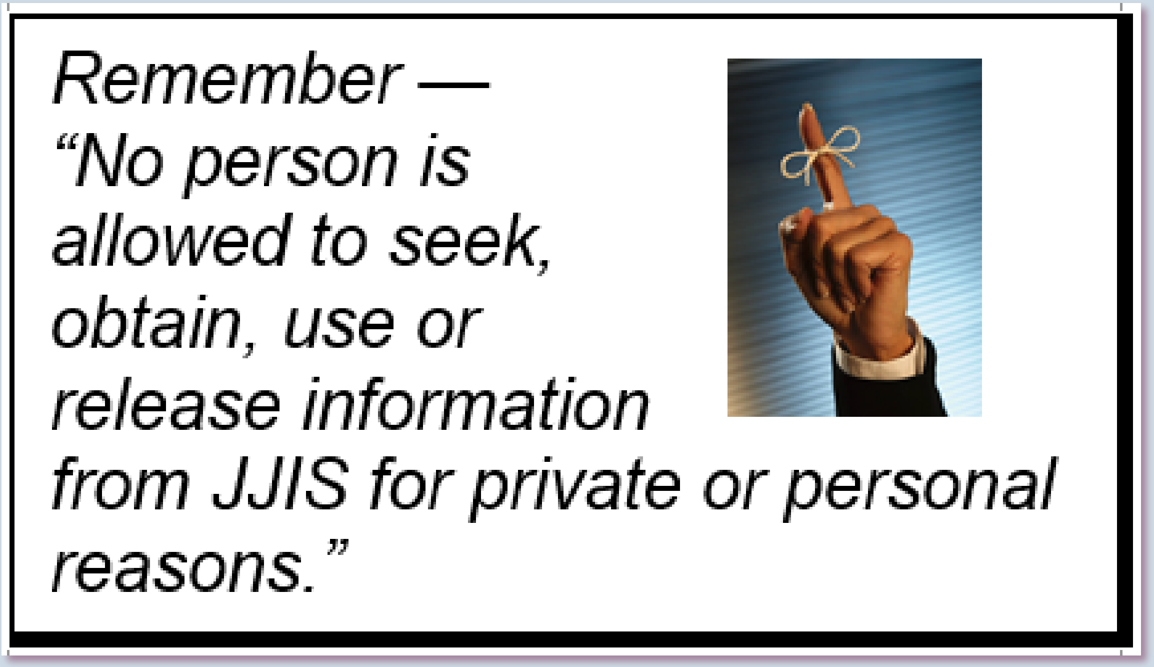
3) work in a facility in which the youth is currently admitted and they have a specific direct working relationship with the youth or other authorized work-related reason to access specific information in the youth record.

*Primary Worker, Courtesy Supervision Worker, Referral Worker, Juvenile Department Worker During OYA Commitment

Confidentiality

JJIS is a powerful tool and users have access to data, much of which is confidential and protected from public release by Oregon law.

All JJIS users should be alert to the necessity of protecting the integrity and confidentiality of the data in JJIS.



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

Security violations

Violations of the use of JJIS are taken very seriously.

If a known security violation is investigated and found to be true, users need to understand that they may be subject to discipline, up to and including dismissal.

Situations determined to be inadvertent and not in violation may be resolved through coaching and training, progressive discipline, or corrective action.

Remember how much trouble curiosity caused the cat!

Examples of security violations . . .

▶ Looking up one's own or co-workers' last names "just to see what comes up".

▶ Looking up names of co-workers and/or their family members and sharing information to intentionally cause conflict or distress for the co-worker.

▶ Looking up names of relatives, friends, or acquaintances.

▶ Looking up names of relatives, friends, or acquaintances to change or remove information in an existing JJIS record.

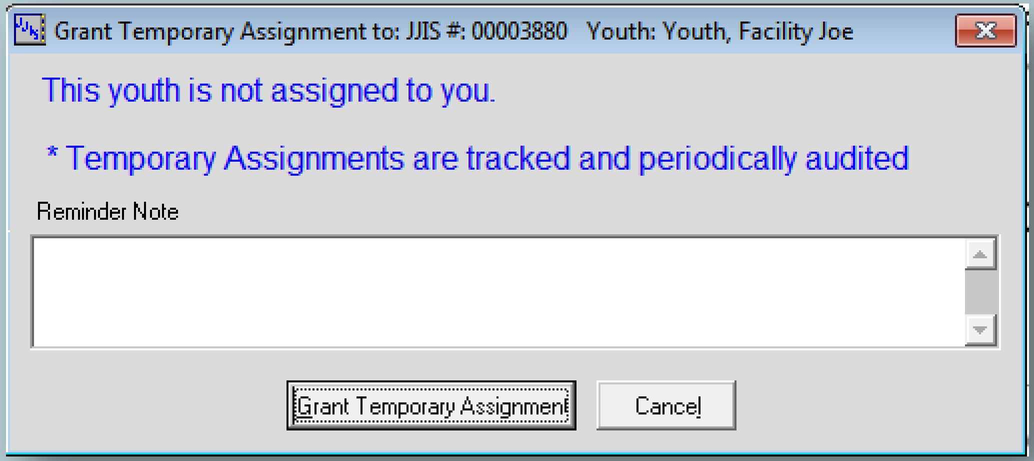
▶ Reviewing case notes of a youth not on one's caseload (for example, a high-profile or sensitive-designation youth).

Temporary Assignment

Users are expected to access only the minimum amount of information needed to accomplish their authorized job duties.

However, users not assigned to a youth may still have a legitimate need to view and update youth information consistent within their job duties.

If a user attempts to access information for a youth they are not assigned to, JJIS prompts with a screen to enter a note why the temporary access was needed.



Grant Temporary Assignment to: JJIS #: 00003880   Youth: Youth, Facility Joe

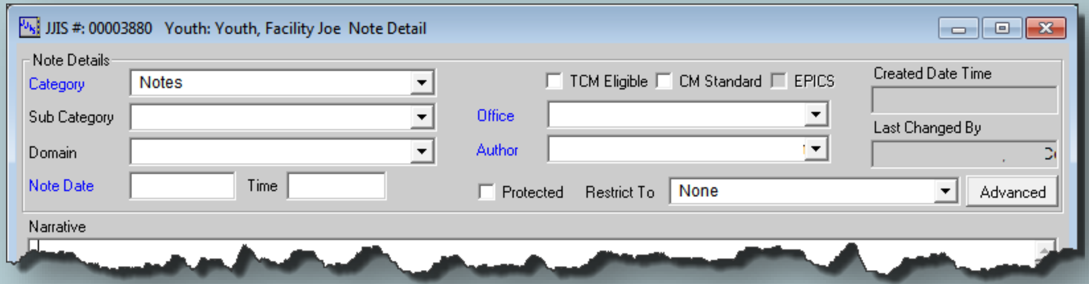
This youth is not assigned to you.

* Temporary Assignments are tracked and periodically audited

Reminder Note

Protected Information

The Protected Information feature allows a user to protect and/or restrict specific information such as notes, documents, assessments, and incidents to comply with HIPAA (Health Insurance Portability & Accountability Act) and 42CFR (Code of Federal Regulations) alcohol and drug confidentiality requirements. These features should only be used subject to local agency policy guidance.

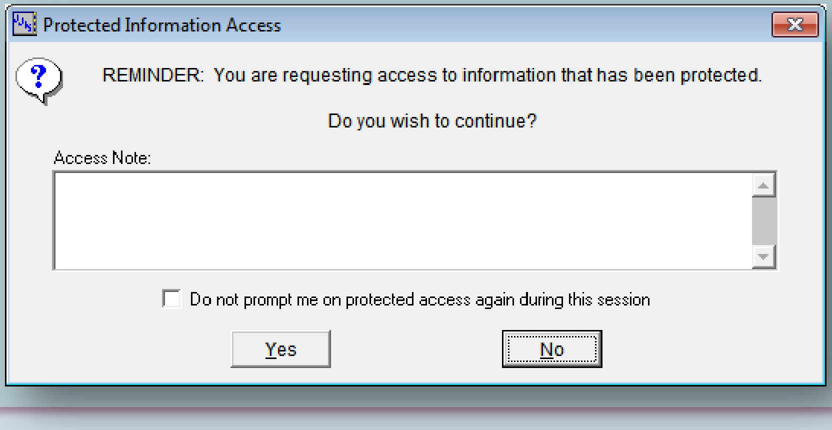


JJIS #: 00003880 Youth: Youth, Facility Joe Note Detail

Category: Notes

□ Protected Restrict To: None

When a user tries to access protected information in a case they are not assigned to, JJIS alerts them that the information is marked "protected" and provides an option to either proceed with accessing the information (including noting why they accessed the information) or decline. If the user proceeds, their access is logged.



Protected Information Access

REMINDER: You are requesting access to information that has been protected.

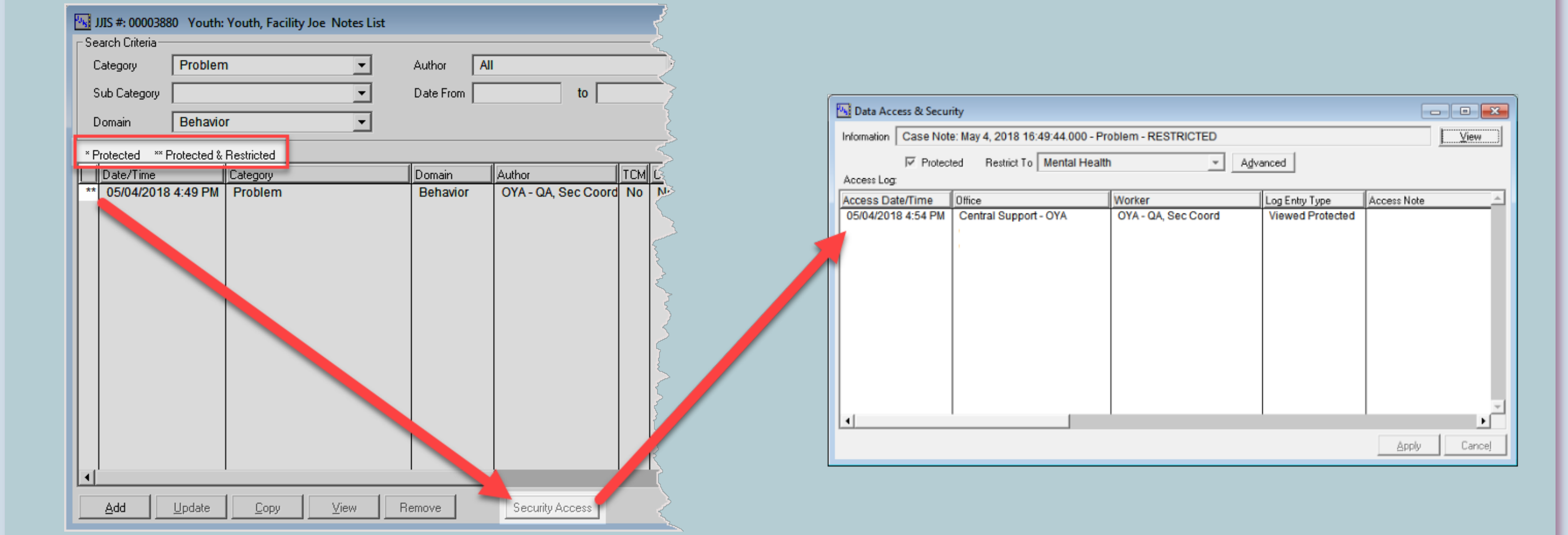
Do you wish to continue?

Access Note:
□ Do not prompt me on protected access again during this session
Yes
No

Restricted Information

Restricting information prevents individuals who are not part of a specified Security Group from accessing the information.

Only the individual who restricted the information can grant access to individuals outside of the Security Group.



JJIS #: 00003880 Youth: Youth, Facility Joe Notes List

Search Criteria

Category: Problem
Sub Category:
Domain: Behavior
Author: All
Date From: to

* Protected ** Protected & Restricted

	Date/Time	Category	Domain	Author	TCM	L
**	05/04/2018 4:49 PM	Problem	Behavior	OYA - QA, Sec Coord	No	N

Data Access & Security

Information: Case Note: May 4, 2018 16:49:44.000 - Problem - RESTRICTED

☑ Protected Restrict To: Mental Health

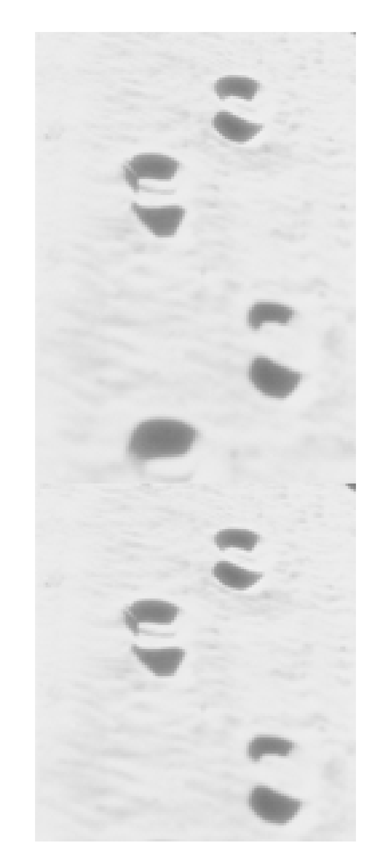
Access Log:

Access Date/Time	Office	Worker	Log Entry Type	Access Note
05/04/2018 4:54 PM	Central Support - OYA	OYA - QA, Sec Coord	Viewed Protected	

Workers assigned to a case can review a Data Access & Security Log that tracks by whom and when protected or restricted information was accessed.

This assists in supporting the HIPAA requirement of disclosing who has accessed certain information.

JJIS tracks "footprints"



JJIS tracks footprints?

Yes! In other words, JJIS knows where an individual has been in the system, who has viewed youth information, and who made a change to a record.

- Users are expected to access only the minimum amount of information needed to accomplish their authorized job duties.
- JJIS records should be accessed on a "need-to-know" basis by users to whom the youth is assigned.

◀ ▶

Secure your workstation

Users must comply with agency policy on appropriate use of computer equipment and information systems.

- Do not leave your workstation accessible for unauthorized viewing or use by the public or unauthorized persons.
- If you are working in a public setting (e.g., coffee shop), be aware of your surroundings and sit where your computer screen is not easily viewed.

TIP! Lock your computer when you step away from your workstation – use the Win+L keyboard shortcut.

Win (key) + L

Protect your log-in

You are responsible for all transactions entered into JJIS under your log-in.

- Do not allow anyone to use your User Name and Password.
- Keep your log-in information secure – for example, don't leave your log-in on a Post-It note next to the computer.
- If your work setting shares a common computer, do not share a single log-in.

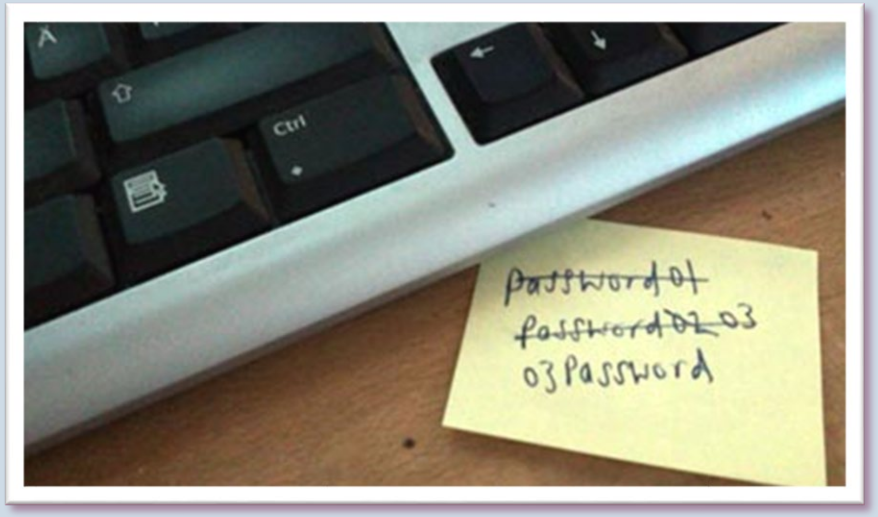


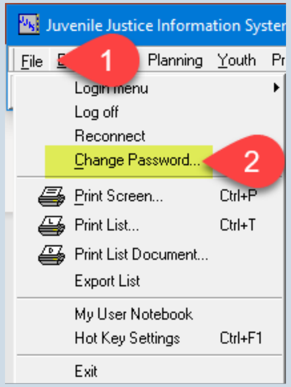
image licensed under Creative Commons

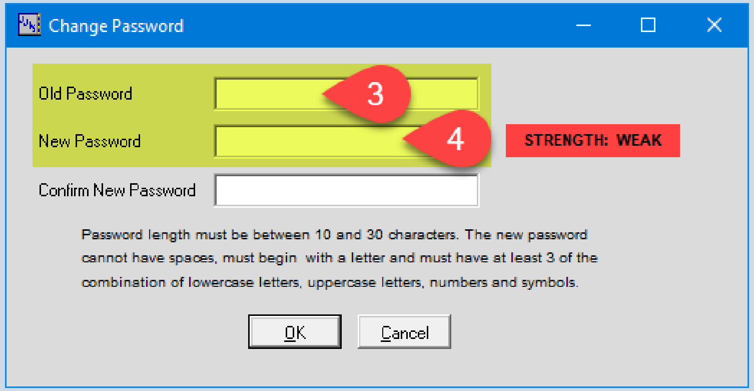
Change your password

When you are initially given access to JJIS, your local JJIS Security Coordinator provides your JJIS User Name and a temporary password that you change the first time you log on.

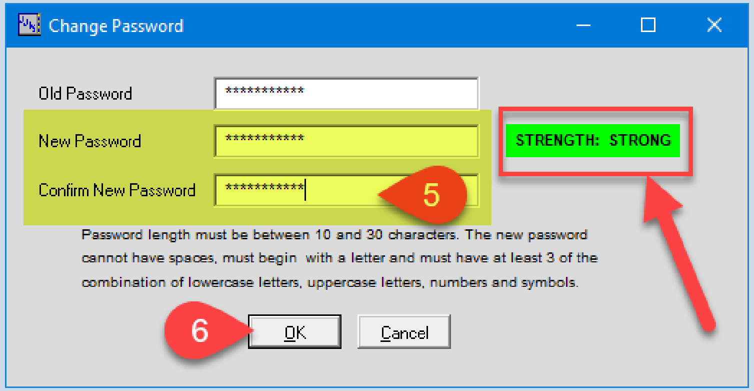
JJIS prompts you every 90 days to change your password, but you can change it at any time.

1. Select **File** from the JJIS Menu.
2. Select **Change Password** . . . a Change Password screen opens.
3. Enter your current password in the **Old Password** field.
4. Enter a new password in the **New Password** field.
5. Re-enter the new password in the **Confirm New Password** field.
6. Click **OK**.





Password length must be between 10 and 30 characters. The new password cannot have spaces, must begin with a letter and must have at least 3 of the combination of lowercase letters, uppercase letters, numbers and symbols.



Password length must be between 10 and 30 characters. The new password cannot have spaces, must begin with a letter and must have at least 3 of the combination of lowercase letters, uppercase letters, numbers and symbols.

JJIS enforces a "strong password" protocol.

As you enter your new password, a strength indicator changes from red to green when the password meets the criteria for a strong password.

JJIS Security Policies

The information in this presentation and applicable JJIS security policies must be reviewed by all new JJIS users and current JJIS users during the annual renewal process.

Click the links to the right to read the policies in their entirety.

JJIS Policy III-A-2 — JJIS User Security

JJIS Policy III-A-4 — Privacy & Protection of Confidential Information

◀
▶

Remember . . .

The JJIS system, its data, and any subsystems are not to be used for a person’s own interest, advantage, personal gain, or for any private purpose.

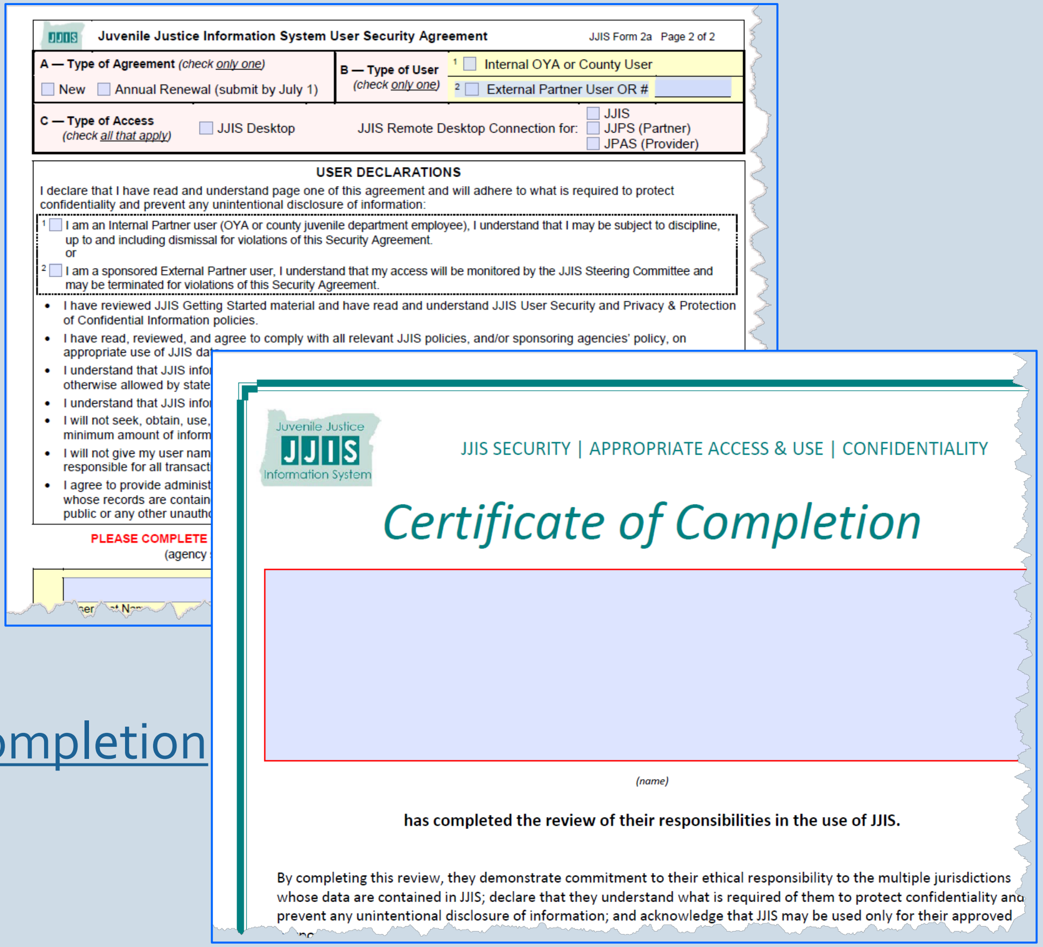
Form or Certificate?

The information in this presentation and applicable JJIS policies must be reviewed by new users and by all JJIS users annually.

Under the direction of their local JJIS Security Coordinator, users outside of OYA may complete JJIS Form 2a and/or add their name to a certificate of completion and submit to their local JJIS Security Coordinator for tracking.

OYA staff complete their renewal requirements through an online learning management system.

JJIS Form 2a — Individual User Security Agreement



JJIS **Juvenile Justice Information System User Security Agreement** JJIS Form 2a Page 2 of 2

A — Type of Agreement *(check only one)*

□ New □ Annual Renewal (submit by July 1)

B — Type of User *(check only one)*

[1] □ Internal OYA or County User

[2] □ External Partner User OR #

C — Type of Access *(check all that apply)* □ JJIS Desktop JJIS Remote Desktop Connection for: □ JJIS □ JJPS (Partner) □ JPAS (Provider)

USER DECLARATIONS

I declare that I have read and understand page one of this agreement and will adhere to what is required to protect confidentiality and prevent any unintentional disclosure of information:

[1] □ I am an Internal Partner user (OYA or county juvenile department employee), I understand that I may be subject to discipline, up to and including dismissal for violations of this Security Agreement.
or

[2] □ I am a sponsored External Partner user, I understand that my access will be monitored by the JJIS Steering Committee and may be terminated for violations of this Security Agreement.

- I have reviewed JJIS Getting Started material and have read and understand JJIS User Security and Privacy & Protection of Confidential Information policies.
- I have read, reviewed, and agree to comply with all relevant JJIS policies, and/or sponsoring agencies' policy, on appropriate use of JJIS da
- I understand that JJIS infor otherwise allowed by state
- I understand that JJIS infor
- I will not seek, obtain, use, minimum amount of inform
- I will not give my user nam responsible for all transact
- I agree to provide administ whose records are contain public or any other unautho

PLEASE COMPLETE
(agency

ser Nam

Juvenile Justice JJIS Information System

JJIS SECURITY | APPROPRIATE ACCESS & USE | CONFIDENTIALITY

Certificate of Completion

(name)

has completed the review of their responsibilities in the use of JJIS.

By completing this review, they demonstrate commitment to their ethical responsibility to the multiple jurisdictions whose data are contained in JJIS; declare that they understand what is required of them to protect confidentiality and prevent any unintentional disclosure of information; and acknowledge that JJIS may be used only for their approved

Certificate of Completion