FLORIDA DEPARTMENT OF JUVENILE JUSTICE PROCEDURE

Title: Provider Access to the Juvenile Justice Information System (JJIS) and JJIS Data Procedures

Related Policy: FDJJ – 1205.60

I. DEFINITIONS

Assistant Secretary – DJJ staff responsible for the operation of the applicable branch of the Department for which the Provider delivers services.

Chief of Information Technology (IT) – DJJ staff responsible for overseeing the IT Bureau within DJJ.

Confidential Information and/or Confidential Data – Information/Data exempted from disclosure requirements under the provisions of applicable state and federal law. Ensuring information and/or data is accessible only to those authorized to have access.

Confidentiality – Information is accessible only to those authorized.

Contract/Grant Manager – DJJ staff responsible for the monitoring and management of DJJ contracts, grants, and provider programs. The duties of Contract/Grant Managers may also be referred to as Contract Monitors, Grant Monitors, Grant Specialists, and Program Monitors.

Data Integrity Officer (DIO) – DJJ staff responsible for assisting users with maintaining integrity of the data entered in JJIS, creating JJIS user accounts, and assisting with training in use of JJIS.

DJJ Director – DJJ staff responsible for the operation of the applicable branch of the Department for which the provider delivers services.

Juvenile Justice Information System (JJIS) – An information system and database containing confidential data and information of youth under the care of the Department.

Provider – A contracted non-DJJ entity that provides a service for the Department

Provider Director – The person within the Provider's organization who is responsible for ensuring their organization is in compliance with the Department's contractual requirements.

Virtual Private Network (VPN) – A secure private network which allows Provider's access to the DJJ's internal network for accessing the Juvenile Justice Information Systems (JJIS) and sharing data.

II. STANDARDS/PROCEDURES

A. Requesting JJIS Access:

1. Each applicant (user) must read and sign the Provider Access User Agreement.
2. The Provider Director or designee will sign the Provider Access User Agreement, and submit it to the applicable DJJ staff (i.e. Contract/Grant Managers, etc.) who will review the form and then forward it to the applicable DIO, if access is to be granted.
3. The DIO will forward a copy of the Provider Access User Agreement form to the applicable IT staff allowing seven (7) business days from the receipt date for VPN account creation and notification.
4. The DIO will secure and retain completed Provider Access User Agreement forms in accordance with State of Florida guidelines for record retention.
5. The Chief of Information Technology (IT) will ensure the network account is created.
6. A notification will be sent to the applicable DIO after the network account has been created.

B. Terminating JJIS Access:

1. The Provider Director of each provider operation is responsible for notifying the Contract/Grant Manager in writing within 24 hours of staff terminations or when an employee's access to the system is no longer needed.
2. The Contract/Grant Manager will notify the applicable DIO of Provider staff terminations within 48 hours of receiving the notification from Provider Directors.
3. The DIO will delete applicable JJIS accounts and notify designated IT staff of terminations within 48 hours of receiving notification from the Contract/Grant Manager.
4. IT will terminate network accounts as requested by the DIOs and after more than 30 days of non-activity as outlined below.
5. Providers found in violation of the conditions of this policy and/or the Provider Access User Agreement form, are subject to immediate and permanent termination of network and JJIS access.

C. Non-Active Accounts:

1. IT will disable Provider network accounts after more than 30 days of non-activity.
2. IT will send monthly Non-Active reports to the Contract/Grant Managers which will list the Provider accounts that have been non-active for more than 30 days.
3. Contract/Grant Managers will contact the Provider Directors, using the monthly Non-Active reports to determine which accounts are valid or invalid.

4. Contract/Grant Managers will respond accordingly to Information Technology (IT) within 30 days of receiving the Non-Active report.

5. If the Contract/Grant Managers do not respond or request the accounts be re-enabled after 30 additional days (over 60 days of non-activity), the accounts will be deleted.

6. If a Provider network account is deleted due to non-activity, the Provider will have to submit a new Provider Access User Agreement form, reference Section II A, items 1 through 6.

D. Violations:

1. If a provider violates the conditions outlined in this policy and/or the Provider Access User Agreement form, immediate notification should be sent to the DJJ Information Security Manager, applicable DIO, and Contract/Grant Manager.

2. Violation of this policy may result in revocation of system access and/or disciplinary action, up to and including dismissal and/or potential criminal prosecution pursuant to Sections 815, Florida Statutes.

III. RESPONSIBILITY AND DUTIES

A. Providers:

1. The Provider is responsible for supplying computer related systems that comply with DJJ standards.

2. Providers will maintain their own computer equipment, except in those cases where DJJ owns the computer equipment and are located in a site owned and operated by DJJ.

3. The Provider Director of each provider's facility shall be responsible for the completion of the Provider Access User Agreement form for each new employee who needs access to the JJIS system. The Provider Director will sign the form, and when completed, will submit it to the Contract/Grant Manager.

4. The Provider Director of each provider's operation is responsible for notification, in writing, to the Contract/Grant Manager of staff termination of employment or when staff access to the system is no longer needed. This action is required within 24 hours of the earlier of either event.

5. When a user is locked out of his/her account, the user must contact the JJIS Help Desk for assistance. When a user needs his/her password reset, the user must contact their local Data Integrity Officer (DIO) or their supervisor who will submit a request to the JJIS Helpdesk to reset user password.

6. Every Provider requesting access to JJIS and JJIS data must read and comply with this policy (FDJJ-1205.60).

7. Every Provider requesting access to JJIS and JJIS data must read, complete, sign, and agree to the terms of the Provider Access User Agreement.

8. Providers are responsible for using all due diligence to protect confidential data and information. All confidential data information shall be secured in such a manner to prevent unauthorized access and/or disclosure.

9. The Provider Director or designee at each provider facility shall be responsible for maintaining up-to-date virus and security patches on all equipment, including laptops, that are used to access Agency resources, which includes access to JJIS and JJIS data.

B. Contract/Grant Managers:

1. Responsible for ensuring the Provider Director is knowledgeable of and understands agency policies and procedures.

2. Responsible for conveying all applicable, new and/or modified policies and procedures, which affect the Providers, to the Provider Director.

3. Will immediately contact the DIO if a Provider is observed violating the conditions outlined in the Provider Access User Agreement or any other related policies.

4. Upon receiving notification from a Provider Director of the termination of staff or that JJIS access is no longer needed, the Contract/Grant Manager will notify the applicable DIO.

5. Will contact the Provider Director or designee monthly to verify terminated employees.

6. Will use the monthly Non-Active reports to determine which accounts are valid or invalid and will respond to Information Technology (IT) accordingly.

C. DJJ Director or Assistant Secretary and/or designee:

1. Will review the Provider's request and sign the submitted Provider Access User Agreement form. The completed original form must be sent to the applicable DIO.

D. DJJ Bureau Chief of Information Technology (IT):

1. Will set the minimum computer system standards for Provider system configuration.

2. Will ensure new accounts are created and needed connections established.

3. Will ensure appropriate IT staff assists the DIOs in the process of timely termination of Provider's access.

E. Data Integrity Officers:

1. Assist with coordination of Provider connectivity.

2. Provide JJIS training to Provider staff.

3. Establish new JJIS accounts and assign appropriate user permissions.

4. Upon notification, will delete JJIS accounts.

5. Ensure Providers have read and understand this and related policies as referenced in the "Related References" section of this document prior to establishing JJIS accounts.

6. Ensure a signed Provider Access User Agreement has been completed and signed prior to establishing JJIS accounts.

7. When notified by applicable Contract/Grant Managers or Program Monitors that a Provider was observed violating the conditions outlined in the Provider Access User Agreement or any other related policies, the DIO will immediately terminate JJIS access, contact the appropriate IT staff to suspend the Provider's network account, and notify the DJJ Information Security Manager.

8. Shall be responsible for consulting with the Provider Director and Contract/Grant Managers to periodically review and reassign JJIS user permissions, as applicable, for Provider staff.

IV. ATTACHMENTS

Attachment 1 - Provider Access User Agreement