FLORIDA DEPARTMENT OF JUVENILE JUSTICE PROCEDURE

Title: Florida Crime Information Center (FCIC), National Crime Information Center (NCIC), Criminal Justice Network (CJNet), Judicial Inquiry System (JIS), and Driver and Vehicle Information Database (DAVID) Access and Use Procedures

Short Title: FCIC, NCIC, CJNet, JIS, and DAVID Access and Use Procedures

Related Policy: FCIC, NCIC, CJNet, JIS, and DAVID Access and Use (FDJJ-1805)

I. DEFINITIONS

Agency – Any state, local, or other entity user under the CJIS Agreement.

Agency Head – The Secretary of the Department of Juvenile Justice (DJJ).

Central Communication Center (CCC) – The unit within the Department that collects, retains, and disseminates information related to the care, safety, and humane treatment of youth served by the Department and its providers or grantees.

Computer Security Incident – Any event resulting in the Department's computer systems, networks or data being viewed, manipulated, damaged, destroyed, or made inaccessible by an unauthorized activity.

Criminal History Report Information – The national, state, and/or local agency report that identifies a person's crime or arrest information.

Criminal Justice Information Services (CJIS) – The central repository of criminal history records for the State of Florida. It provides criminal identification screening to criminal justice agencies, noncriminal justice agencies, and private citizens to identify persons with criminal warrants, arrests and convictions that impact employment, licensing, eligibility to purchase a firearm, and other criminal justice functions.

CJIS Agency Coordinator (CAC) – The central point of contact regarding all communications between Florida Department of Law Enforcement (FDLE) and the Department. This person helps FDLE facilitate discussions regarding CJIS matters with the Department and shall have Department authority to ensure all agency identified personnel, including those with decision-making authority, are made aware of and participate in FDLE CJIS discussions that may lead to Department business and policy changes.

CJIS Online Administrator – The person who maintains the CJIS Online System by: creating user accounts, tracking users' training, responding promptly to system-generated testing and expiration email notifications, and inactivating expired user accounts.

CJIS Online System – A system used by individuals who require Security Awareness Training because they have unescorted access to the agency's secured area and may encounter (hear or read) Criminal Justice Information.

CJIS Security Policy (CSP) – The resource that provides controls to protect the full lifecycle of Criminal Justice Information (CJI), whether at rest or in transit. It provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI. It applies to every individual contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity

with access to, or who operate in support of, criminal justice services and information. *(CSP-Website: http://www.flcjn.net/Information-Security/Documents/CJIS-Security-Policy_v5-7_20180816.aspx.)*

Criminal Justice Network (CJNet) – A secure, private, statewide intranet system managed and maintained by the Florida Department of Law Enforcement (FDLE) to connect Florida criminal justice agencies to various data sources provided by the criminal justice community.

Customer Support Center (CSC) – A FDLE support center that provides assistance to all CJIS users regarding questions about the CJIS systems, issuing and assigning trouble tickets, assisting with device malfunctions, computer line problems, and routing all terminal messages to the designated agencies or regions of the state. This service is available 24 hours a day, 365 days a year by calling toll free (800) 292-3242.

Driver and Vehicle Information Database – A web-based application that permits authorized users to query Florida driver and vehicle information.

Department – Refers to the Department of Juvenile Justice.

FALCON – The FDLE system for identifying criminals and reporting data.

FALCON Application Access Administrator (AAA) – The person who creates and manages users of the FALCON system, assigns devices, approves user's access, and provides roles and privileges to users who create and monitor Watch List records and who manage the agency's Retained Applicant Fingerprint Transactions.

FCIC Agency Coordinator (FAC) and Alternate FCIC Agency Coordinator (Alt-FAC) – The person who ensures compliance with the legal and policy requirements contained within the CJIS User Agreement and facilitates communication between FDLE CJIS and the Department regarding FCIC-related matters. The FAC should be the most knowledgeable agency personnel about the FCIC, NCIC, III, and Nlets systems and be available to respond during normal business hours.

Federal Bureau of Investigation (FBI) – An agency of the United States Department of Justice that serves as both a federal criminal investigative body and an internal intelligence agency.

Florida Crime Information Center (FCIC) – The State of Florida's primary law enforcement/criminal justice information system that provides agencies with access to Federal, State, and local criminal justice information.

Florida Department of Law Enforcement (FDLE) – An agency of the State of Florida that delivers investigative, forensic, and information system services to Florida's criminal justice community.

Information Delivery Team (IDT) – A team of FDLE trainers located throughout the state who assist criminal justice agencies with CJIS related issues.

Information Security Officer (ISO) – The individual within the Department who ensures compliance with the FBI - CJIS Security Policy and any other applicable security requirements. ISOs should be knowledgeable about technical aspects of the Department's network or be able to confirm information through local technical support.

International Justice and Public Safety Information Sharing Network (Nlets) – A computerized, high-speed message switching system created for and dedicated to the criminal justice community to provide interstate and/or interagency exchange of criminal justice and related information.

Interstate Identification Index (III) – The State of Florida's criminal justice information system that provides agencies with access to criminal records of all persons born in 1956 or later who have an FBI record, persons born prior to 1956 whose first arrest fingerprint card was submitted to the FBI on July 1, 1974 or later, and numerous older records converted to the automated system in the CJIS Division Manual Conversion Project, as well as certain fugitives and repeat offenders.

Judicial Inquiry System (JIS) – A web-based application that permits criminal justice entities and other government agencies access to multiple criminal justice data sources through a single point of entry.

Local Agency Instructor (LAI) – A CJIS certified instructor appointed by the agency head to provide CJIS certification/recertification training and testing to criminal justice users. The CJIS User Agreement does not require LAIs, but agencies may decide to assign an LAI.

Local Agency Security Officer (LASO) – The person responsible for the agency's technology compliance with the FBI CJIS Security Policy (CSP) and all applicable security requirements of the criminal justice information network and systems.

National Crime Information Center (NCIC) – The United States' central database for tracking crime-related information.

NexTEST – An on-line testing system that is available for CJIS certification via the CJNet.

NexTEST Administrator – The agency personnel responsible for creating user accounts, tracking user's training, responding promptly to system generated testing and expiration email notifications, properly marking user accounts inactive when a user leaves the agency or no longer needs access, and notifying the FDLE ID&T staff when an account needs to be moved to the correct agency list.

ORION (ORI Online) – A file that allows users to find the Original Agency Identifier (ORI) of agency when only the location (city and state) or federal agency (name of agency and state) is known. It also allows a user to gather information on the agency (such as address, phone, fax number) when only the ORI is known.

Public Key Infrastructure (PKI) Certificate – The digital certificate used for access to the Department of Highway Safety and Motor Vehicle's (DHSMV) Driver and Vehicle Information Database (DAVID).

Public Access System (PAS) – An Internet based application for use by the public to access certain FCIC records available via the FDLE website at www.fdle.state.fl.us. The public may conduct online queries for information regarding stolen property and wanted/missing persons. The response will provide status information only and will not include detailed information on the property or person. Inquiries resulting in a matching response will provide the inquirer the opportunity to send the entering agency tip information.

Public Access System (PAS) Contact – The person who serves as the agency liaison with FDLE regarding tips received via email or phone call.

Retention – The continued possession, use, or control of a document.

Secondary Dissemination – When a user within the Department shares any part of a criminal history with another authorized criminal justice agency either verbally or in writing. *(**NOTE:** See FDJJ-1800, Background Screening Policy and Procedure for details on sharing criminal history information.)*

Secondary Dissemination Log – Any agency that shares criminal history information with another entity must document whom they shared the information with and what information was shared. The dissemination

log must be maintained onsite for at least four (4) years. ***(NOTE:** See CJIS Certification Manual for details on the Secondary Dissemination Log.)*

Validations Administrator – The person who creates and maintains users who review and update the agency's FCIC and NCIC records each month and responds promptly to system-generated notifications and ensures all records are processed within the scheduled timeframe.

Validations System – The system used to validate records in FCIC and NCIC. ***NOTE:** Access to this system is granted to the agency that enters, uploads, or updates demographic and arrest data into FCIC and NCIC.*

II. STANDARDS/PROCEDURES

A. NCIC, FCIC, JIS and DAVID Use:

Use of the National Crime Information Center (NCIC), Florida Crime Information Center (FCIC), Judicial Inquiry System (JIS), or Driver and Vehicle Information Database (DAVID) and any system accessed via the CJNet is restricted to the administration of criminal justice or as otherwise specifically authorized or required by statute, policy, or user agreement.

1. Information obtained from NCIC, FCIC, JIS, and DAVID shall only be used for authorized purposes.

2. It is the responsibility of the Department to ensure access to CJNet and all CJIS systems are for authorized purposes only, and to regulate proper use of the network and information at all times.

3. Accessing information and CJIS systems or the CJNet for other than authorized purposes is deemed misuse.

4. The Department shall notify the Florida Department of Law Enforcement (FDLE), Florida Courts, and/or Department of Highway Safety and Motor Vehicles (HSMV) of any sustained or confirmed cases of misuse.

5. In cases of sustained or confirmed misuse, the Department shall identify disciplinary actions and the corrective actions taken to prevent future incidents.

6. FDLE, JIS, HSMV reserves the right to deny system access to any individual who has a sustained case of misuse.

B. Access to NCIC, FCIC, CJnet, JIS and DAVID and Dissemination of Criminal History Report Information:

1. The user is responsible for remaining current in the applications, procedures, and policies and in ensuring he/she attends training sessions to maintain appropriate certifications.

2. Only users who have successfully completed Criminal Justice Information Services (CJIS) certification shall be allowed to have unsupervised access to FCIC, NCIC, and CJNet Systems.

3. FCIC or NCIC users who are in their initial six (6) months of assignment may be permitted supervised access to FCIC or NCIC.

4. All personnel, who initiate a transaction to the FCIC message switch must successfully complete CJIS certification.

5. The Department shall remove from FCIC or NCIC access any user who fails to achieve required certification standards, whose certification has expired, whose certificate is otherwise rescinded or as directed by Florida Department of Law Enforcement (FDLE).

6. All Information Technology (IT) personnel, including any vendor who shall, during the course of their official duties initiate a transaction to the FCIC message switch, shall successfully complete CJIS certification.
7. All IT personnel, including any vendor, responsible for maintaining/supporting any IT component used to process, store or transmit any unencrypted information to or from the FCIC message switch, shall successfully complete the CJIS Online Security Training provided by FDLE.
    i. All FCIC data transmitted outside the boundary of a physically secure area shall be protected with a minimum of 128-bit encryption that meets FIPS 140-2 Standards (CSP 5.10.1.2). See the FBI CJIS Security Policy for encryption requirements.
8. Pursuant to a signed interagency agreement as authorized by Florida Statutes and/or federal regulations, the Department may share state Criminal History Report Information (CHRI).
9. Information obtained from the FCIC or NCIC "Hot Files," CJNet, JIS or computer interfaces to other state or federal systems, by mans of access granted pursuant to Section 943.0525, F.S., shall only be used for the administration of criminal justice. (i.e., criminal justice purposes).
10. Dissemination of CHR information requires compliance with all applicable statutes, FCIC, NCIC, and Interstate Identification Index (III) rules, regulations, and operating procedures, including logging.
11. The Department must maintain confidentiality of CHR information that is otherwise exempt from Section 119.07(1), F.S., as provided by law.
12. Criminal History Transmission:
    i. Any electronic device that uses wireless or radio technology to transmit voice data may be used for the transmission of CHR only when a law enforcement officer or authorized non-sworn user determines there is an **immediate** need for this information to further an investigation or to respond to a situation affecting the safety of an officer or the public.
    ii. A facsimile machine may be used to transmit criminal history information between criminal justice agencies, provided both agencies have an NCIC Originating Agency Identifier (ORI) and are authorized to receive criminal history information. Appropriate measures shall be taken to prevent unauthorized viewing or receipt by unauthorized persons.
13. Transaction Logging:
    i. Each interface agency accessing FCIC, NCIC, and III systems shall ensure that an automated transaction log is maintained. The FCIC, NCIC, and III portion of this log shall be maintained for a minimum of twelve months.
    ii. Automated transaction logging is a feature included in the application software provided by FDLE, and local agencies are encouraged to retain these logs for future reference. The Department purchasing or developing an interface to FCIC shall ensure transaction logging is an included feature.
    iii. The automated transaction log shall identify: the user on all transactions, the agency authorizing all transactions, the requester and secondary recipient for all criminal history

transactions. This information can be captured at log-on and may be a name, badge number, serial number, or other unique identifier.

iv. The Department shall only disseminate CHRI to another authorized recipient *(agency)* and shall maintain a record of any dissemination of state or federal criminal history information shared.

v. The dissemination record *(log)* shall reflect at a minimum: (1) Date of release; (2) to whom the information relates: (3) to whom the information was released; (4) the State Identification (SID) and/or the FBI number(s); (5) the purpose code and (6) the reason for which the information was requested.

a. The FAC and Alternate FAC are responsible for ensuring users at their location maintain and properly document any dissemination of state or federal criminal history information.

14. CHRI will be accessed, shared, and disseminated only as outlined in the FDLE CJIS Agency User Agreement and this Department's policy and procedure. Any unauthorized access, use, viewing or dissemination of CHRI or use that would violate the terms of the Department's user agreement with FDLE will result in disciplinary action up to and including immediate dismissal, and/or potential criminal prosecution.

15. Information Access:

i. The Department shall allow only properly screened *(pursuant to Section 9 of the CJIS Agency User Agreement Requirements Document - Personnel Background Screening)* authorized personnel performing a criminal justice function who have received proper security awareness training to have access to information contained within the CJNet, FCIC, NCIC, or other state or federal criminal justice information system accessed through the FCIC message switch, FBI CJIS Wide Area Network or Internet.

ii. The Department shall also assist other criminal justice agencies who are not equipped with direct FCIC access, in compliance with the legal and policy requirements, but only to the extent that such assistance is not otherwise prohibited.

iii. Users who access CJNet for purposes that are not authorized, disclose information to unauthorized individuals, or violate FCIC, NCIC, or III rules, regulations, or operating procedures are subject to disciplinary action, up to and including immediate dismissal, and/or potential criminal prosecution under Chapter 815, Florida Statutes, or other applicable federal, state, or local laws or policies.

16. Accessing information and CJIS Systems (NCIC or FCIC) or CJNet for other than authorized purposes is deemed unauthorized use.

i. The user shall notify his/her supervisor and the supervisor shall notify the local and Agency FCIC Agency Coordinator (FAC).

ii. The Agency FAC shall notify the CJIS systems Officer (CSO) of any sustained or confirmed cases of misuse by using the CJI Systems Misuse Reporting Form found on the CJNet CJIS Resource Center web page at *http://www.flcjn.net/Compliance-Resources/Compliance-Resources/Documents/Misuse_Form.aspx*.

iii. In cases of sustained or confirmed misuse, the Department shall identify disciplinary actions and the corrective actions taken to prevent future incidents.

iv. FDLE reserves the right to deny CJI access to any individual who has a sustained case of misuse.

17. If the Department provides an interface between FDLE and other criminal justice agencies, the serviced agency/agencies shall abide by all the provisions of the CJIS Agency User Agreement.

18. Serviced agencies that access CJNet, FCIC, NCIC, and/or related CJIS systems by interfacing through the Department shall, likewise, abide by all provisions of the CJIS Agency User Agreement. Additionally, the Department and the serviced agency shall enter into an interagency agreement when access to CJNet, FCIC, or NCIC is provided by the Department to a services agency.

19. For systems implemented after December 31, 2008, the Department shall ensure all automated interfaces that programmatically (i.e., without human intervention) generate transactions to the FCIC message switch are restricted to no more than one (1) transaction per second per interface.

20. **Messages:** Only law enforcement and other criminal justice messages shall be sent over and through the CJNet and FCIC or NCIC. The Department should be prudent in use of regional and statewide broadcast message requests. Plain English language shall be used in all the messages.

C. Access and Use of FDLE, JIS, and DAVID Computers and Networks:

1. Users shall always protect State of Florida property from loss or abuse and shall use state property, equipment, and personnel only in a manner that is beneficial to the Department.

2. Users utilizing FDLE, JIS, and DAVID computers or the FDLE, JIS or DAVID network are subject to monitoring of all access to the Internet and use of all FDLE, JIS, and DAVID administered information systems.

i. Users must affirmatively acknowledge this during their log-on to Department computers and networks by clicking "OK" to the following:

This is a Department of Juvenile Justice computer system that is for official use by authorized users only. Usage of this system indicates consent to monitoring and recording and may be subject to audit by the Bureau of Information Technology. Unauthorized or improper use of this system is a violation of Federal law and may be prosecuted resulting in criminal or administrative penalties including fines and/or imprisonment. If criminal activity is discovered, the information will be provided to the appropriate law enforcement officials. Suspected access violations or rule infractions should be reported to the Information Security Manager at (850) 717-2307.

D. Username and Password Authentication:

1. The Department shall ensure all personnel, including IT support and vendors, who initiate a transaction to the FCIC message switch have a separate and distinct username and password and/or authentication for the software and/or interface used to initiate the transactions.

2. Users having access to any FDLE, JIS, or DAVID administered system, including but not limited to those containing active criminal intelligence, criminal investigative information, or law enforcement sensitive information, must adhere to the operating guidelines associated with these respective systems.

3. Any misuse of an FDLE, JIS, or DAVID administered system or failure to comply with the system operating guidelines may result in an administrative, internal, and/or criminal investigation.

4. Misuse can include inappropriate access to or dissemination of any FDLE, JIS, or DAVID administered systems or data.

    i. Users shall refrain from sharing passwords and/or other authenticators, including but not limited to smart cards, tokens, public key infrastructure (PKI) certificates used to access CJI or CJNet-related systems.

    ii. Users shall refrain from using another individual's account or session to access CJI or other CJNet applications.

    iii. Users shall refrain from caching credentials/passwords for access to systems/applications used to process or store CJI.

    iv. Users with access to any system or application that processes or stores CJI for maintenance or administration purposes shall be uniquely identified.

5. Supervisors of users having access to FDLE, JIS, and DAVID administered systems shall conduct random "spot-check" reviews of their subordinates' use of these systems to ensure compliance with this and other applicable policies and procedures.

6. To obtain query reports associated with an authorized user's access to FDLE, JIS, and DAVID administered information systems, supervisors must obtain written approval through their chain of command.

7. Upon approval from the Assistant Secretary or his/her designee, the supervisor shall send a request specifying the user's name and time period for which a report is being sought to the Agency FAC and/or database administrator who shall forward the request to the FDLE, JIS, and/or DAVID System Administrator at TARRequest@fdle.state.fl.us, JIS_support@flcourts.org, and/or DAVIDsupport@flhsmv.gov.

8. Any Department user who becomes aware of or has knowledge regarding the possible misuse of any FDLE, JIS, or DAVID system or network shall immediately report it to their supervisor, or as appropriate, to the Central Communication Center (CCC) at 1-800-355-2280.

E. Deactivating User Access:

1. The Department shall deactivate user access to agent and/or other FCIC interfaces, other CJNet applications and other state/federal systems containing CJI, including but not limited to LEO and/or N-DEx, upon separation, reassignment, or termination of duties, provided user access is no longer required for the administration of criminal justice.

F. Computer Security Incidents:

1. In the event of a computer security incident, action shall be taken as outlined in the Department's Computer Security Incident Response Team, (C-SIRT) policy and procedure (FDJJ-1250).

2. The Department shall immediately notify FDLE, JIS, and/or DAVID system administrators of any suspected compromise of the FCIC, NCIC, CJNet, JIS, and/or DAVID system.

3. Suspected system compromise by unauthorized users or hackers shall be reported, by email, to the following agencies:

   i. FDLE system: Contact the FDLE CJIS Security Officer at CJISCSO@fdle.state.fl.us or CJIS Support at FDLECustomersupport@fdle.state.fl.us;

   ii. JIS system: Contact JIS support at the courts-JIS_support@flcourts.org,

   iii. DAVID system: Contact the Florida Department of Highway Safety and Motor Vehicles at DAVIDsupport@flhsmv.gov.

      a. *The e-mail should include the following information: date of the incident, locations of incident, systems affected, method of detection, nature of the incident, description of the incident, actions taken/resolution, date, and contact information for the agency.)*

4. The Department shall maintain a current diagram detailing network configuration of devices accessing FCIC/CJNet.

5. Devices accessing FCIC/CJNet include, but are not limited to: computers, interfaces, message switches, mobile laptops, servers, Computer Aided Dispatch (CAD), Jail Management Systems (JMS), Record Management Systems (RMS), routers, firewalls, or mobile handheld devices. Agencies are reminded that all requests for additional FCIC access must include an updated network diagram (CSP 5.7.1.2).

   i. The network diagram must detail the following:

      a. Existing FCIC access and mnemonics;

      b. Connections to other networks (city, county, etc.);

      c. All network components (e.g., firewalls routers, switches, hubs, servers, encryption devices);

      d. Wireless or mobile vendor (where FCIC passes over any wireless/mobile network);

      e. Devices which access FCIC, including interfaces, mobile computers, CAD, RMS, JMS, AFIS devices (including printers), or other servers;

      f. Routers, servers, or computers performing network address translation for access to FCIC/CJNet;

g. Other agencies receiving FCIC access through your agency's connection, including the agency name(s) and number of devices; and

h. The type and level of encryption being used where FCIC data passes outside the boundary of a physically secure area.

ii. Information received by FDLE regarding local agency network design is exempt from public records release and is for official use only. A request for network expansion cannot be processed until a network diagram is submitted, reviewed and confirmed to be following the FBI CJIS Security Policy. This process may take up to 90 days.

iii. Forward all request for new, additional or modifications for FCIC or CJNet access to: CjnetSrvRequest@fdle.state.fl.us.

G. Personnel Background Screening:

1. The Department, at a minimum, shall conduct a state and national fingerprint-based criminal history records check on:

   i. All personnel who are authorized to access state and/or national CJI data or systems;

   ii. IT personnel who maintain or support information technology components used to process, transmit, or store unencrypted CJI; and

   iii. Other personnel, including but not limited to support personnel, contractors and custodial staff, with unescorted physical or logical access to physically-secure locations, as defined in the FBI CJIS Security Policy (CSP), and/or to IT components used to process, transmit or store unencrypted CJI.

2. The Department is strongly encouraged to screen the applicant by other available means (e.g., local court records and local law enforcement agency records) in addition to the fingerprint-based record check.

3. The Department shall submit fingerprints of personnel for positive comparison against state and national criminal history records and for searching of the "Hot Files."

4. The results of the fingerprint-based record check shall be reviewed prior to granting access to CJI or components used to process or store CJI, including access for IT support.

5. The Department may conduct a preliminary online criminal justice employment check using Purpose code "J" for this purpose.

   i. If a record of any kind exists, the Department shall consult the FDLE Guidelines for CJIS Access and notify the CSO for review. *(**NOTE:** Complete the CJI Access Review Request form and submit it to FDLE. The link to the form is http://www.flcjn.net/Compliance-Resources/Documents/CJIS-Access-Review-Form.aspx.)*

ii. Upon notification from the Department, the CSO shall review the matter to determine if access is appropriate and officially notify the Department, in writing, of the CSO's decision regarding access.

iii. Once the original background screening has been completed, if the Department learns that an employee with access to CJI has a criminal history or pending charge(s), the Department shall consult the FDLE Guidelines for CJIS Access and notify the CSO.

a. The CSO shall review the facts and circumstances and notify the Department in writing regarding access to CJI.

iv. FDLE reserves the right to deny user access to any system or related program that is used to process, transmit, or store CJI based on valid, articulable concerns for the security and integrity of the information and/or related systems.

v. The Department shall ensure the appropriate ORI is used for submission of applicant fingerprints.

a. Fingerprints submitted for any other positions unrelated to the administration of criminal justice or required by the CSP, shall include the appropriate and approved noncriminal justice ORI.

b. Fingerprints submitted for positions associated with the administration of criminal justice, or as required by the CSP, shall include the Department's criminal justice ORI.

6. The user is responsible for the timely completion of training and/or certification required for FCIC, NCIC, CJNet, JIS, and/or DAVID use.

i. The Department is responsible for remaining current in the applications, procedures, and policies and ensuring personnel attend any required training sessions.

a. All personnel who access CJI for the administration of criminal justice shall complete CJIS security awareness training, including but not limited to criminal justice officials (e.g., Police Chiefs, Sheriffs, Judges, and State Attorneys).

b. Only users who have successfully completed CJIS certification shall be allowed to have unescorted access to the FCIC and NCIC system.

c. FCIC or NCIC users who are in their initial six (6) months of assignment may be permitted supervised access to FCIC and/or NCIC. Users shall successfully complete CJIS certification within six (6) months of appointment or assignment to duties requiring direct access to FCIC or NCIC.

ii. The Department shall deactivate user access to eAgent and/or other FCIC interfaces, other CJNet applications and other state/federal systems containing CJI *(e.g., JIS)*, upon separation, reassignment or termination of duties, provided user access is no longer required for the administration of criminal justice.

H. Physical Security:

1. The Department, or its designee, shall identify facilities, areas, rooms, where CJI is accessed, processed and/or stored to determine physical security requirements as identified in the CSP.

2. The Department may designate a facility, area, or room, either a physically-secure location or a controlled area, as defined in the CSP, provided the appropriate requirements are met. Access shall be limited to persons needing access for performance of required criminal justice duties.

    i. The Department shall have a written policy that ensures and implements security measures, secures devices that access FCIC, NCIC and CJNet, and prevents unauthorized use or viewing of information on these devices.

    ii. The use of password-protected screen-blanking softwTechare is required for devices that access FCIC or NCIC when the user may leave the computer unsupervised.

    iii. FDLE reserves the right to object to equipment location, security measures, qualifications, and number of personnel who will be accessing FCIC or NCIC and to suspend or withhold service until such matters are corrected to FDLE's reasonable satisfaction.

I. Retention and Storage of NCIC, FCIC, CJNet, and JIS Criminal History Report Information:

1. Retention of CHRI the Department maintains, whether retrieved from III or Florida's Criminal History Record system, shall be kept in a secure records environment to prevent unauthorized access. Retention of CHRI is governed by the record retention schedule for law enforcement, published by the Florida Department of State, GS2.

    i. Retention of criminal history records, whether retrieved from III or the state system, for extended periods may be appropriate when the status of the specific record at the time it was accessed is important.

    ii. When, in the sound judgement of the Department, retention of criminal history records, whether retrieved from III or the state system, is no longer required, final disposition will be accomplished in a secure manner in compliance with the legal and policy requirements to preclude unauthorized access.

    iii. When no longer usable, diskettes, tape cartridges, ribbons, hard copies, print-outs, and other similar items used to process or store FDLE, FBI, or CJI shall be destroyed by shredding, incineration, or method approved by the CJIS ISO, considering whichever method is available, appropriate, and cost effective. (This list is not all-inclusive.)

        a. In situations where an agency contracts for destruction of CJI, destruction must be observed by an authorized member of the criminal justice agency (CSP 5.8.4).

        b. IT systems that have processed or stored FDLE, FBI, or CJI shall not be released from control until the equipment is sanitized and all stored information has been cleared. The sanitization method shall be approved by the FDLE CJIS ISO.

c. IT storage media that will be reused by another entity shall be sanitized (This includes the hard drives in multifunctional copiers used by a criminal justice agency). The steps taken to sanitize shall be documented by the releasing agency. When possible, it is suggested that storage medium should be physically destroyed. Programs that perform complete overwrite are acceptable when the overwrite process is completed at least three (3) times; further overwrite process is encouraged (CSP 5.8.3).

J. Off-Site Storage/Processing of CJI:

1. The Department shall contact and receive approval from the CSO prior to entering into an agreement with a noncriminal justice governmental agency for off-site storage or processing of CJI (often referred to as cloud computing or cloud services).

K. Management Control Agreement:

1. In situations where data processing/information services, law enforcement dispatch functions or human resources functions are provided by a noncriminal justice governmental entity, the Department shall enter into a management control agreement as required by, and set out in, Appendix D.2, "Management Control Agreement" of the CSP.

2. In situations where governmental structure or hierarchy does not support or permit an agreement between the parties involved, a directive which includes all the provisions needed for a management control agreement identified in the CSP may be substituted.

L. Interagency Agreements:

1. The Department shall execute an Interagency Agreement with any other criminal justice agency to which criminal justice information services are outsourced, including but not limited to information technology-related functions.

2. The Department shall consult with FDLE to determine if a given function requires an Interagency Agreement.

M. Vendors/Contractors:

1. Private vendors which, under contract with the Department, are permitted access to information systems that process CJI, shall abide by all aspects of the FBI CJIS Security Addendum. *(Note the link to the FBI CJIS Security Addendum is http://www.flcjn.net/Falcon/Documents/CJIS-Security-Addendum.)*

   i. Any contract between the Department and a vendor that permits such access, shall incorporate the FBI CJIS Security Addendum to ensure adequate security of CJI.

   ii. The Department shall ensure all vendor employees who will or may have such access are appropriately screened prior to granting the vendor employees' access to CJI.

      a. Vendor employee fingerprints submitted by the Department to FDLE, as required by the CSP, shall be taken, rolled, and printed by a recognized law enforcement agency or

an FDLE-approved third-party vendor. ***NOTE:*** *A vendor may not fingerprint its own employees.*

iii. The Department shall maintain the Security Addendum Certification form for each member of the vendor staff with access to information systems that process CJI. *(**NOTE:** The link to the Security Addendum Certification form is http://www.flcjn.net/Information-Security/Documents/5-3SecurityAddendumCertification.)*

iv. The Department shall ensure all vendor employees with access to CJI have received the appropriate security awareness training, via the CJIS Online application, and are in status with respect to that training.

v. The Department shall ensure private vendors permitted such access are aware of the provisions of Section 501.171, F.S. regarding breach of security of personal information.

vi. The Department shall contact FDLE for review prior to entering into a contract or agreement with a private vendor during which CJI is processed, stored, or transferred from the Department's physically-secure location to a vendor-owned or operated facility/facilities (e.g., cloud services).

vii. The Department shall maintain and keep current a list of all vendor employees who have been authorized access to CJI.

N. Relocation:

1. Should the Department desire to relocate the data circuit(s) and/or equipment connected to CJNet, the Department shall provide FDLE written notice 90 days in advance of the projected move.

O. Audit Compliance:

1. The Department shall permit an FDLE, JIS, and/or DAVID appointed inspection team to conduct inquiries about any allegations of potential security violations, as well as for routine audits.

    i. FDLE conducts regularly-scheduled compliance and technical security audits of every agency accessing the CJNet to ensure network security, conformity with state law, and compliance with all applicable FDLE, CJNet, FCIC, NCIC, and III rules, regulations, FBI CJIS Security Policy and operating procedures. Compliance and technical security audits may be conducted at other than regularly-scheduled times.

P. Technical Security:

1. Remote access services to CJI, including, but not limited to, access to FCIC, NCIC, CJNet, and JIS via the Department's network, shall be permitted provided the Department establishes appropriate security measures to ensure compliance with the legal and policy requirements of FDLE.

2. All FCIC, NCIC, and III data transmitted over any public network segment shall be encrypted as required by the CSP. This requirement also applies to any private data circuit that is shared with noncriminal justice users and/or is not under the direct security control of a criminal justice agency.

3. The Department shall ensure only authorized criminal justice agencies or agencies authorized by FDLE are permitted access to the CJNet via the Department's CJNet connection.

4. The Department shall ensure all devices with connectivity to CJNet employ virus protection, anti-spam and anti-spyware software and such software shall be maintained in accordance with the software vendor's published updates. The Department shall not maintain unsupported software on their criminal justice network.

5. CJI, including but not limited to information obtained from the FCIC message switch and CJNet, may be accessed only via computers or interface devices owned by the Department or by the contracted entity, if applicable.

6. Vendors under contract with the Department to perform criminal justice functions may be allowed to use their own devices for access provided all requirements of the FBI CJIS Security Addendum are satisfied.

7. Provided appropriate security precautions are in place, and upon approval from the FDLE network Administration staff, the Department may employ wireless network connectivity (for example the 802.11 wireless networking protocol).

Q. Computer Security Incident Response Capability:

1. The Department shall have a written policy documenting the actions to be taken in response to a reported or possible security incident.

2. The policy shall include identifying, reporting, investigating, and recovery from any security incident.

3. The Department shall immediately notify the CSO of any known or suspected compromise of the CJNet. *(**NOTE:** The CJIS Security Incident Reporting Form link is http://www.flcjn.net/Information-Security/Documents/SecurityIncidentResponseForm-062018.aspx.)*

R. Security Authority:

1. The legal and policy requirements, are hereby incorporated into and made part of FDLE's agreement.

S. Client Software License:

1. The FCIC Client Software (eAgent) license from Diverse Computing, Inc., is located in the Help menu of the eAgent Client software and is made a part of and incorporated by reference into the User Agreement and shall be binding on the Department upon acceptance of the software.

2. The Department is allowed up to one hundred (100) eAgent sub-switch mnemonics.

3. The Department is not permitted to install eAgent, as provided by FDLE, on laptops for use in a mobile environment, including tablets, netbooks, and other "handheld" devices.

4. The Department is not permitted to use the eAgent client software as an interface to the FCIC message switch for another application.

III. RESPONSIBILITY AND DUTIES

A. Department of Juvenile Justice User Responsibilities

1. Users shall be held responsible for systems security and integrity, to the degree that his or her job requires the use of the FCIC, NCIC, CJNet, JIS, or DAVID. Fulfillment of these responsibilities shall be mandatory, and violation of security requirements or other provision of this policy may be cause for disciplinary action up to termination.

B. Agency Head or Agency Head Designee Responsibilities

1. The Agency Head or Designee shall:
   i. Designate an individual from its agency to function as the FCIC Agency Coordinator (FAC) and/or Point of Contact (POC). Agencies are strongly recommended to appoint an alternate FAC and/or POC to assist the primary FAC.
   ii. Designate an Information Security Officer (ISO) to ensure security of the FCIC, NCIC, JIS, and DAVID workstations, the connection to these systems, and any access to the information services provided on these systems to or by the Department. The Department's Bureau of Information Technology (IT) will appoint the ISO.
   iii. Designate a Point of Contact (POC) to receive and approve the issuance and revocation of Public Key Infrastructure (PKI) certificates for the Department's users. The POC for PKI will be the Agency FAC or his/her designee.
   iv. Designate a Public Access System (PAS) Contact. The PAS Contact is responsible for any follow-up activities deemed appropriate by the Department in response to tips resulting from the posting of records on the PAS.
   v. Ensure the Department maintains, in current status, and provides upon request by FDLE, Florida Courts, and/or Highway Safety and Motor Vehicles a complete topological drawing, which depicts the Department's network configuration as connected to the CJNet, JIS, and/or DAVID. This document must clearly indicate all network connections, service agencies, and interfaces to other information systems. The Department's Bureau of Information Technology will oversee this function.

C. Coordinator & Security Officer Responsibilities:

1. CJIS Agency Coordinator (CAC) shall:
   i. Be designated by the Department.
   ii. Act as the central point of contact regarding all communications between FDLE and the Department.
   iii. Help FDLE facilitate discussions regarding CJIS matters with the Department.
   iv. Ensure all agency-identified personnel, including those with decision making authority, are made aware and able to participate in all FDLE discussions that may lead to Department business and policy changes.

v. Appoint other Department personnel to serve in other designated CJIS positions and sign the agency contact form, once the CAC has been appointed by the Department chief executive officer.

2. FCIC Agency Coordinator (FAC) shall:

i. Be designated by the Department or the CAC.

ii. Ensure compliance with the legal and policy requirements.

iii. Facilitate communication between FDLE and the Department (and/or facility).
iv. Maintain a current CJIS Limited or Full Access Certification.
v. Attend FAC Training within six (6) months of being assigned to the position and as often as required by FDLE.
vi. Agencies may designate an Alt-FAC to assist with FAC duties.

3. Local Agency Security Officer (LASO) shall:

i. Be designated by the Department or the CAC.
ii. Ensure compliance with the CJIS Security Policy (CSP).
iii. Knowledgeable of the technical aspects of the agency's network and maintain an ongoing working relationship with the local technical staff as well as the FCIC Agency Coordinator (FAC/Alt-FAC).
iv. Provide the agency's network diagram and be responsible for the triennial CJIS Technical Audit.
v. Within six (6) months of assignment to the position, the LASO shall complete any appropriate LASO training made available by FDLE, including CJIS security awareness training.
vi. Maintain an active certification status of Level 4 Security Awareness Training.

4. Other Points of Contact and Positions:

i. Based on other services provided by FDLE, other points of contact and positions, in addition to CAC, FAC, and LASO, may be necessary to manage applications and facilitate communication between the Department and FDLE. These positions are identified on the Agency CJIS Contact Form, which may be found on the CJNet at the following link: *http://www.flcjn.net/CJIS-Resources/Resources/TAC-Toolbox/TAC-Resources/CJIS-Agency-Contact-Form*.

D. Agency Coordinators Duties:

1. Agency Coordinators shall:

i. Assist the agency head/designee with decisions regarding the FCIC/NCIC.

ii. Shall be CJIS certified and maintain current CJIS certification.

iii. Shall complete the FCIC Agency Coordinator (FAC) Training provided by FDLE within six (6) months of appointment.

iv. Shall ensure all records, warrants, and validations for the Department are in compliance with CJIS policies and procedures.

v. Serve as the liaison between the Department and FDLE, Florida Courts, and Highway Safety and Motor Vehicles.

vi. Serve as the liaison between office personnel and FDLE.

vii. Enforce CJIS, JIS, and DAVID policies and procedures.

viii. Ensure the Department is represented at the FDLE regional meetings.

ix. Ensure the Department and its users follow applicable state and national policies and procedures governing the use of the following: FCIC, NCIC, III, The International Justice and Public Safety Information Network (Nlets), the Criminal Justice Network (CJNet), and FBI CJIS Security Policy.

x. Ensure all personnel who have access to FCIC, NCIC, JIS, or DAVID data are appropriately trained and those who will have access to terminal areas have been properly fingerprinted and background checked.

xi. Ensure written policy is in place on validation procedures.

xii. Ensure User Agreements are up-to-date with current Department head's signature. These agreements include one (1) or more of the following as applicable:

i. Criminal Justice Agency User Agreement;

ii. CJNet Only Agency User Agreement;

iii. Noncriminal Justice Agency User Agreement;

iv. Other User Agreement;

v. JIS Interagency User Agreement; or

vi. HSMV-DAVID Memorandum of Understanding.

xiii. Ensure the Department is following proper validation procedures and the source documents for each record entered into the FCIC or NCIC system are reviewed.

xiv. Ensure written policy is in place for the penalties users shall receive for the misuse and abuse of the CJIS, JIS, and DAVID Systems.

xv. Ensure the following training classes are offered as appropriate:

i. CJIS Certification and CJIS Recertification (responsible for compliance if not designated as a Local Agency Instructor).

ii. On-the-Job Training (internal Computer Aided Dispatch (CAD) systems, jail management systems, records management and other systems utilizing the CJIS/CJNet applications).

xvi. Enter new users into the Training Information System (TIS) via eAgent message keys, update user information, and register users for classes.

xvii. Enter/modify users in eAgent's Client Manager (and/or other system interface).

xviii. Enter users into the nexTEST system for online CJIS certification/recertification testing (if designated by the Department as a nexTEST Administrator) or assist the Department's nexTEST administrator or Local Agency Instructor (LAI) in entering users.

xix. Enter users into CJIS Online Security Training (if designated by the Department as a CJIS Online Administrator).

xx. Ensure all Department FCIC or NCIC users are CJIS certified and they renew their certification every two (2) years as required.

xxi. Troubleshoot system problems as it relates to FCIC, NCIC, JIS, or DAVID.

xxii. Make deletions of personnel from the FCIC, NCIC, JIS, and DAVID systems upon termination of employment.

xxiii. Review operational issues, enhancements, or changes of FCIC, NCIC, the Nlets, JIS, or DAVID and make recommendations to appropriate agency/agencies.

xxiv. Monitor criminal history record dissemination and accuracy of dissemination log.

xxv. Ensure FCIC, NCIC, JIS, DAVID, and CJIS memos, emails and operating manuals are distributed to all users within the Department and new procedures and capabilities are used when made available.

xxvi. Ensure the Department's workstations are in a secure location, which prohibits unauthorized use or viewing.

xxvii. Ensure a secondary dissemination log is maintained for four (4) years because of criminal history information being disseminated to authorized individuals outside the Department either verbally or in writing.

xxviii. Ensure the Department's address is correct in the Nlets ORION file. If the information needs to be updated the CAC must contact the FDLE Customer Support Center (CSC).

xxix. Ensure the appropriate personnel within the Department knows the name(s) and phone number(s) of the CAC, FAC, and/or alternate CAC and/or FAC.

xxx. Ensure the Department's information is correctly entered and maintained in the Customer Information System (CIS) via eAgent message keys.

xxxi. Maintain the settings of the Department's workstations/devices in the eAgent station tables.

xxxii. Ensure changes in the CAC, FAC, and/or alternate CAC and/or FAC are communicated to FDLE headquarters via the designated CJIS Agency Contact Form within five (5) business days from the date of the change. The communication must be on Department letterhead.

xxxiii. Assist the Regional FDLE IDT representative(s) with issues pertaining specifically to the Department. (Example: obtaining signed agency user agreements).

xxxiv. Assist FDLE, JIS, DAVID auditors during the Department's audits to include, but not limited to on-site audits, correspondence audits and audits from the FBI.

xxxv. Ensure the Department adheres to the "hit" confirmation policy and that appropriate formats are used (NCIC formats are "YQ/YR"; the FCIC formats are "FYQ/FYR"). *(**NOTE:** A "Hit" is the positive response that is received when an agency inquires via FCIC/NCIC on a person or property. Details about the "Hit Confirmation" process can be found in the CJIS Manual on FDLE's website at:* http://www.flcjn.net/CJIS-Resources.aspx.)

IV. ATTACHMENTS N/A