STATE OF FLORIDA
DEPARTMENT OF
CHILDREN AND FAMILIES
TALLAHASSEE, June 27, 2022

CF OPERATING PROCEDURE
NO. 50-1

Systems Management

DEPARTMENT USE OF CRIMINAL JUSTICE INFORMATION SERVICES (CJIS) AND DRIVER AND VEHICLE INFORMATION DATABASE (DAVID)

This operating procedure provides requirements to ensure that criminal justice information, to include but not be limited to criminal history records, personal driver's license information, systems, and applications administered and regulated by the Federal Bureau of Investigations (FBI), Florida Department of Law Enforcement (FDLE) and Department of Highway Safety and Motor Vehicles (DHSMV), is accessed and queried by Department of Children and Families personnel only for authorized purposes and that information is protected in accordance with existing law, policy, and procedure.

This operating procedure is applicable to all Department of Children and Families employees with access to systems, applications, and information as authorized by the Department's user agreements with the Florida Department of Law Enforcement (FDLE), Department of Highway Safety and Motor Vehicles (DHSMV), and the Office of State Court Administrators (OSCA).

BY DIRECTION OF THE SECRETARY:

(Signed original copy on file)

COLE SOUSA
Chief Information Officer

SUMMARY OF REVISED, ADDED, OR DELETED MATERIAL

In Chapter 7, revised paragraph 7-13a(3) to change the timeframe for notifying the Region DAVID point of contact that an employee's account had not been logged into from 60 days to 90 days; and, revised paragraph 7-13a(4) to change the procedure for reactivating an employee's DAVID account.

This operating procedure supersedes CFOP 50-1 dated June 9, 2021.
OPR: Information Technology Services
DISTRIBUTION: General Counsel; Human Resources; Information Security Manager; Adult Protective Investigations; ESS Quality Management; ESS Public Benefits Integrity; Child Welfare including Florida Abuse Hotline; Background Screening; Sexually Violent Predator Program; and Region/Circuit Adult Protective Services, Child Welfare, Economic Self Sufficiency, and Substance Abuse/Mental Health staff.

TABLE OF CONTENTS

TABLE OF CONTENTS (continued)

Paragraph

TABLE OF CONTENTS (continued)

Chapter 1

GENERAL

1-1. Purpose. This chapter details general requirements for criminal justice information access; ethics and misuse; and confidentiality. Additionally, this chapter provides descriptions of in-state and out of state networks, user agreements, department CJIS roles and responsibilities, and definitions of terminology used throughout this operating procedure.

1-2. Scope. This chapter is applicable to all Department of Children and Families employees and Department contractors who are criminal justice information users and/or who are authorized for access to systems, applications, or devices containing criminal justice information.

1-3. Authorities and References. The following authorities and references apply throughout this operating procedure.

a. 28 Code of Federal Regulations (CFR), Subparts 20 (28CFR20), 50 (28CFR50), and 901 (28CFR901).

b. Public Law 109-248, The Adam Walsh Child Protection and Safety Act of 2006.

c. Driver's Privacy Protection Act of 1994, 18 U.S.C. § 2721 et. seq. (Public Law 103-322).

d. Section 119.071(5), Florida Statutes (F.S.); Section 322.142(4), F.S.; Section 943.045(10)(d), F.S.; Section 943.0525, F.S.; Section 943.053(3), F.S.; Section 943.055, F.S.; Section 943.056, F.S.; Section 943.0585(4)(a), F.S.; Section 943.059(4)(a)5, F.S.; Section 943.059(4)(c), F.S.; and Section 985.045(1), F.S.

e. CFOP 15-4, Records Management.

f. CFOP 50-2, Security of Data and Information Technology Resources.

g. CFOP 60-8, Chapter 1, Employee Personnel Records.

h. CFOP 60-12, Driver's License as a Condition of Employment.

i. CFOP 60-25, Chapter 2, Employee Security Background Screening.

j. U.S. Department of Justice, Federal Bureau of Investigations (FBI), Criminal Justice Information Services (CJIS) Security Policy 5.3.

k. Florida Department of Law Enforcement (FDLE) Criminal Justice Agency User Agreement with the Department of Children and Families (DCF).

l. Florida Department of Law Enforcement (FDLE) Non-Criminal Justice Agency User Agreement with the Department of Children and Families (DCF).

m. Florida Office of State Court Administrators (OSCA) user agreement with the Department of Children and Families (DCF).

n. Florida Department of Juvenile Justice (DJJ) user agreement with the Department of Children and Families (DCF).

o. Florida Department of Highway Safety and Motor Vehicle (DHSMV) Memorandum of Understanding and Data Exchange Agreement with the Department of Children and Families (DCF).

p. Florida Department of Law Enforcement (FDLE) Memorandum of Understanding with the Department of Children and Families (DCF) for the Department's Sexual Violent Predator Program.

1-4. Terminology and Definitions. The following terminology and definitions are used throughout this operating procedure.

a. Administration of Criminal Justice means criminal identification activities and associated tasks such as the collection, storage, and dissemination of criminal history record information and criminal justice employment.

b. Background Screening as used in this operating procedure refers to the processes and programs related to assessing the background of personnel for the purpose of making eligibility determinations. This may include, but is not limited to, F.S. 435 Level 2 screenings for the purposes of employment, as well as screenings for direct service providers, mental health personnel, service provider personnel, child care facility licensing, foster care and residential child-caring agencies, and consumer directed care.

c. Civil Workflow Control System (CWCS) (pronounced "QUICKS") is an automated system used to receive, process, and respond to electronic requests for applicant criminal history record checks via fingerprint submission by livescan device. CWCS allows different types of applicants to be scanned on a single device and allows input from a variety of livescan devices that adhere to FDLE and FBI standards and requirements.

d. CJIS Online Security Awareness Training is a course available online that addresses minimum topics for baseline security awareness training for all authorized personnel with access to CJI as required in the Federal CJIS Security Policy and user agreement with FDLE.

e. CJIS Personnel Background Screening refers to processes related to assessing the background of personnel to determine approval for access to CJI systems, information, and security at worksites as required in the user agreement with FDLE. Screenings may be conducted in conjunction with employment screenings but is a separate process and requirement. This screening may additionally be referred to as a requirement for the purpose of "criminal justice employment."

f. CJIS Security Policy (CSP) is the FBI's CJIS Security Policy document published by the FBI CJIS Information Security Officer. FDLE has adopted the FBI CSP as the foundations for FCIC, CJNET, and CCH related information security.

g. CJNet is a secure private statewide intranet system connecting Florida's criminal justice agencies that is managed and maintained by FDLE.

h. Computerized Criminal History (CCH) is a term used to describe criminal history records, more commonly known as rap sheets, which are maintained by the state where the offense occurred and contain identifying information on the individual as well as arrest, disposition, and incarceration information.

i. Criminal History Record or Criminal History Record Information (CHRI) is a subset of CJI and CCH. It means information collected by criminal justice agencies on persons, consisting of identifiable descriptions and notations of arrests, detentions, indictments, information, or other formal criminal charges and the dispositions thereof.

j. Criminal Justice Agency means (as stated in section 943.045(10)(d), F.S.).

(1) A Court.

(2) The Department.

(3) The Department of Juvenile Justice.

(4) The protective investigations component of the Department of Children and Families which investigates the crimes of abuse and neglect, and financial exploitation.

(5) Any other governmental agency or sub-unit thereof which performs the administration of criminal justice pursuant to a statute or rule of court and which allocates a substantial part of its annual budget to the administration of criminal justice.

k. Criminal Justice Information (CJI) is the abstract term used to refer to all CJIS provided data necessary for law enforcement agencies to perform their mission and enforce the laws and is often used in reference to National CCH and/or CHRI. For this operating procedure, CJI refers to any data obtained through the FCIC message switch or other systems accessed via the CJNet that contain the following: Florida or National CCH or Hot Files, driver's license/motor vehicle information, and/or an individual's Personally Identifiable Information.

l. Criminal Justice Information Access Program is the physical or logical (electronic) ability, right or privilege to view, modify or make use of Criminal Justice Information. It can also be referred to as Direct Access and is defined as:

(1) Having the authority to access systems whether by manual or automated methods, not requiring the assistance of, or intervention by, any other party or agency.

(2) Having the authority to query or update national databases maintained by the FBI including national queries and updates automatically or manually.

m. Criminal Justice Information Services (CJIS) refers to systems, equipment, facilities, procedures, agreements, and organizations thereof, used for the collection, processing, preservation, or dissemination of criminal justice information. Departmental service categories include but may not be limited to: ensuring compliance with Federal and State Law, Federal CJIS Security Policies, CJIS User agreements, and agency administrative code and operating procedures; coordinating activities and polices between agencies and programs; administering the agency CJIS information access program which includes criminal justice employment screening and user training and certifications; implementation of new CJIS policies; assisting programs with operationalizing practices and guidelines for the administration of criminal justice functions; ensuring CJIS security requirements and methods of access are integrated appropriately with programs business practices and operating procedures; and performing required compliance and technical audits.

n. Criminal Justice Information Access User means a person or group who has been properly vetted through a national fingerprint-based record check and have been certified when required prior to being granted access to CJI data or systems.

o. Criminal Justice Information Services (CJIS) Advisory Board (APB) is responsible for reviewing policy, technical, and operational issues related to the National Crime Information Center (NCIC). It meets minimally twice yearly and makes recommendations to the Director of the FBI for final approval.

p. CSP is the abbreviation for the U.S. Department of Justice, Federal Bureau of Investigation's (FBI), Criminal Justice Information Services (CJIS) Security Policy.

q. DataMotion SecureMail is a secure FDLE web mail application. When a fingerprint submission is completed using a livescan device, the results are posted to the appropriate DataMotion

SecureMail account. The results will include both state and national criminal history information, as well as any warrants and other information related to the individual.

r. Department of Corrections (DOC) is the department which is responsible for individuals and their records while incarcerated, on probation, parole, and up to the point of release.

s. Department of Highway Safety and Motor Vehicles (DHSMV) is the department which administers, maintains, and provides access to the Driver and Vehicle Information Database (DAVID).

t. Department of Juvenile Justice (DJJ) is the department which provides services to delinquent youth and families and is the administrator of the Juvenile Justice Information System (JJIS).

u. Dissemination means the transmission of information, by any means. Secondary dissemination of information to an authorized agency outside of the Department of Children and Families requires logging in the secondary dissemination log.

v. Driver and Vehicle Information Database (DAVID) is the database administered by the Florida Department of Highway Safety and Motor Vehicles where authorized individuals are able to search and obtain information on Florida driver licenses, identification cards, vehicle and boat registrations, and tags. Available information may include digitized driver license photos and driver history information.

w. Driver's Privacy Protection Act of 1994 (DPPA) is a federal act governing the privacy and disclosure of personal information gathered by state departments of Motor Vehicles.

x. e-Agent is a client application provided by FDLE that allows a user the ability and functionality to query, enter, modify, locate, clear, and cancel records in the FCIC and NCIC systems.

y. e-Agent Client Manager (ECM) is a system managed by FDLE that allows FCIC Coordinators (FC) the ability to create and manage user accounts for their own Agency staff that access FCIC AND/OR NCIC systems through the e-Agent browser-based application.

z. Expunged Record refers to a record that, pursuant to section 943.0585, F.S., no longer legally exists since the file and any reference to it is destroyed except for the reference contained in the FCIC database. EXPUNGED RECORDS ARE NOT PUBLIC RECORDS AND REQUIRE SPECIAL HANDLING.

aa. FALCON is a system available on the CJNet that provides registered users a method of developing and maintaining watch lists for the purpose of receiving notifications based on fingerprint identification. A watch list notification is based on a fingerprint match of incoming transactions against criminal fingerprints already on file with FDLE.

bb. FALCON Application Access Administrator (AAA) is responsible for the creation and management of the program members who are users of the FALCON system. The AAA approves user's access, provides roles and privileges, and monitors Watch List records.

cc. FALCON Watch List Supervisor is responsible for transferring watch list subjects when a watch list owner cannot or should no longer receive notifications on a subject.

dd. Federal Bureau of Investigation (FBI) investigates and tracks criminal activity for the United States and its territories.

ee. Florida Abuse Hotline is the Department's call center that operates twenty-four hours a day, seven days a week to accept and evaluate intakes alleging abuse, abandonment, neglect, self-neglect,

threatened harm, and exploitation of children and vulnerable adults; and Special Conditions Referrals. The Hotline and Forensic Unit areas at Department facilities are defined as CJIS Physically Secure Locations.

ff. Florida Crime Information Center (FCIC) is the primary information system on the CJNet and provides computerized State of Florida criminal history (CCH).

gg. Florida Department of Law Enforcement (FDLE) is Florida's CJIS System Agency and maintains the Criminal Justice Information Program pursuant to section 943.05, F.S. FDLE manages and maintains the FCIC system and CJNet intranet.

hh. FDLE refers to the Florida Department of Law Enforcement.

ii. Florida Safe Families Network (FSFN) is the Department's current Statewide Automated Child Welfare Information System (SACWIS) used by child and adult protective investigations and services. Additionally, this system is used to manage the Abuse Hotline's Crime Intel Units workload, provides protective investigators and case managers with functionality to submit record check requests and view results, and logs request and completion activities.

jj. Hot File is a record from the FCIC and/or NCIC database that may show that a subject is currently under an active criminal investigation, is a missing person, has an outstanding warrant, or is a status offender. These types of files can include but may not be limited to: Person Files such as warrant, missing person, or unidentified persons and/or Status Files such as a Sexual Offender/Predator, Probation/Supervised Release, Career Offender, Protection Order, and Federal Supervised Release.

kk. Inspection in Camera refers to a hearing or discussions with the judge in the privacy of his chambers (office rooms) or when spectators and those involved in the hearing have been excluded from the courtroom.

ll. Intake is the initial, supplemental, and/or additional instrument that Hotline staff generates in Florida Safe Families Network (FSFN) to document allegations of abuse, neglect, abandonment, self-neglect, and/or financial exploitation accepted for investigation and for Special Conditions Referrals.

mm. Judicial Inquiry System (JIS) is a web-based browser interface administered by the Office of State Court Administrators (OSCA) that provides the capability to query multiple Florida agency data sources. For the purposes of protective investigations, the Department has access to JIS to obtain driver's license as well as Department of Juvenile Justice, Department of Corrections, and Clerk of the Court information.

nn. Judicial Inquiry System (JIS) Point of Contact(s) is the individual(s) appointed by the Department as Point of Contact and FCIC Coordinator (FC) responsible for user account administration activities to include, but not limited to, approving account requests, notifying JIS for account deactivations, and assisting with troubleshooting issues. The Department has a JIS point of contact for the Hotline, CPI, and API programs. The data exchange agreement with the Office of State Court Administrators requires the completion of a JIS Point of Contact form, signed by the Agency head, identifying the agency's Point of Contact and FCIC Coordinator (FC).

oo. Livescan is a device used for the electronic submission of fingerprints.

pp. Local law enforcement refers to the local county and municipal law enforcement agencies (i.e., Sheriff or Police department).

qq. National Crime Information Center (NCIC) is operated and governed by the Federal Bureau of Investigation (FBI). It provides computerized criminal history for the United States and its territories.

rr. National Crime Prevention and Privacy Compact Council establishes the infrastructure and policy to exchange criminal history records for noncriminal justice purposes according to the law of the requesting state.

ss. NexTEST is an online testing system that is available for CJIS certification and recertification via the CJNet.

tt. Noncriminal Justice Agency (NCJA) is a governmental agency that provides services primarily for purposes other than the administration of criminal justice.

uu. Noncriminal Justice Purpose is the use of criminal history record information for purposes authorized by federal or state law other than purposes relating to the administration of criminal justice such as employment and licensing.

vv. OCA means the Originating Case Agency on a Live Scan submission. It is the identification number issued by the Background Screening office through the CSIS program. It is the key to identifying the provider/agency requesting the background screening or for whom the background screening is being completed. This is a unique number generated by the CSIS system or converted from a legacy system. For Live Scan submissions, the OCA is prefaced with the two-digit district number and ends with a “Z” (e.g., 03011234Z). This differs from an ORI, which is assigned to qualified governmental entities by the FBI.

ww. Office of State Court Administrators is the agency which administers, maintains, and provides access to the Judicial Inquiry System which has functionality to allow the querying of the DHSMV, DJJ, DOC, and Clerk of the Court databases.

xx. ORI means the Originating Agency Identifier. It is a nine-character identifier assigned by the FBI CJIS staff to an agency which has met the established qualifying criteria for ORI assignment. It identifies agencies in transactions on the NCIC system as well as for the submission of fingerprints.

yy. Personally Identifiable Information (PII) is information contained in CJI which can be used to distinguish or trace an individual’s identity, such as name, social security number, biometric records, alone or when combined with other personal information such as date and place of birth.

zz. Physically Secure Location (PSL) is a facility or area in a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems as defined in the Federal CSP. These are locations where CJI is accessed, processed, and stored such as at the Florida Abuse Hotline.

aaa. Purpose Code “C” is a code used in e-Agent to query the FCIC and NCIC system to obtain criminal history records from FCIC and NCIC on individuals involved in an investigation of abuse, abandonment, neglect, threatened harm, or exploitation. FCIC Purpose Code “C” records may contain a notice of expunged or sealed information and NCIC contains national information. Criminal history records generated using Purpose Code “C” are for criminal justice purposes only and may not be shared with other authorized individuals in or outside the Department, except for investigative units with Florida Sheriff Offices who have contracted with the Department to conduct child protective investigations.

bbb. Purpose Code “J” is a code used in e-Agent to query the FCIC and NCIC system to obtain criminal history records from FCIC and NCIC on individuals for the purpose of criminal justice employment.

ccc. Purpose Code "Q" is a code used in e-Agent to query the FCIC system to obtain criminal history records for child and adult protective investigations and on individuals in potential contact with children or vulnerable adults in need of placement. These records do not contain any expunged or sealed information.

ddd. Purpose Code "X" is a code used in e-Agent to query FCIC and NCIC system to obtain national (NCIC) criminal history records on individuals in potential contact with children in need of emergency placement in exigent circumstances with delayed fingerprint submission. These records do not contain expunged or sealed information. Criminal history records generated using Purpose Code "X" may not be shared with any non-governmental entity, including contracted child providers, except for investigative units with Florida Sheriff Offices who have contracted with the Department to conduct child protective investigations.

eee. Record means any and all documents, writings, computer memory, microfilm, or any other form in which facts are memorialized, irrespective of whether such record is an official record, public record, or admissible record or is merely a copy thereof.

fff. Secondary Dissemination is the dissemination of CJI from a releasing agency to an authorized recipient agency when the recipient agency has not been previously identified in a formal information exchange agreement.

ggg. Sealed Record is a record that has been sealed by the court, pursuant to section 943.059, F.S., and is not available to the general public. It can be opened for inspection by the individual, his/her attorney, a criminal justice agency and, in specific situations, a prospective employer. SEALED RECORDS ARE NOT PUBLIC RECORDS AND REQUIRE SPECIAL HANDLING.

hhh. Shadowing is term used at the Hotline to describe a visitor that will sit with a counselor or crime intelligence technician to observe work processes.

iii. User agreement is a written agreement between DHSMV or OSCA and the Department that includes the standards and sanctions governing use of driver and motor vehicle information and systems, as well as verbiage to allow audits. User agreements must be executed prior to the establishment of connectivity between organizations and may also be known and/or referred to as user agreements, memorandums of understanding, data exchange agreements, or data sharing agreements. The Department has both a Criminal Justice and Non-Criminal Justice agreement with FDLE.

jjj. Quarterly Quality Control Reviews are quarterly reviews required by the interagency agreement with DHSMV to review the Department's process for ensuring proper access and usage of driver and motor vehicle systems and information.

kkk. Visitor is a term used in reference to a person(s) who has not completed a CJIS Personnel Background Screening for unescorted access to a Physically Secure Location/worksite containing Criminal Justice Information such as criminal history records and/or systems. A visitor may be a Department or non-department person(s).

1-5. In-State and Out-of-State Networks.

a. FDLE manages and maintains the CJNet as a secure, private statewide intranet system connecting Florida's criminal justice agencies. The CJNet provides access to several state agency databases such as FDLE's Sex Offenders/Predators data base and the DOC Offender Information Network.

b. The Florida Crime Information Center (FCIC) is the primary information system on the CJNet.

(1) FCIC provides computerized criminal history (CCH) that contains identifying information on individuals as well as Florida arrest, disposition, and incarceration information.

(2) FCIC provides Hot Files, such as Person or Status files, such as missing person, outstanding warrant, protection order, and status offender files.

(3) E-Agent is a browser provided by FDLE that allows a user the ability and functionality to query, enter, modify, locate, clear, and cancel records in the FCIC system.

c. FALCON is a system available on the CJNet that provides registered users a method of developing and maintaining watch lists for the purpose of receiving notifications based on fingerprint identification. A watch list notification is based on a fingerprint match of incoming transactions against criminal fingerprints already on file with FDLE.

d. The nexTEST system is the online testing system that is available for CJIS certification and recertification via the CJNet.

(1) User will have access to FCIC AND/OR NCIC within a few business days after completing the course and passing the test.

(2) Limited Access Certification available via nextTest is required for staff who have access to the FCIC and/or NCIC systems.

e. Nlets is a computerized, high-speed message switching system created for and dedicated to the criminal justice community.

(1) The purpose is to provide for the interstate and/or inter-agency exchange of criminal justice and related criminal justice information.

(2) The system supports inquiries into each state’s motor vehicle, driver license, criminal history and other states databases.

f. The National Crime Information Center (NCIC) is the primary information system on Nlets.

(1) The Federal Bureau of Investigation (FBI) maintains stolen and recovered property as well as wanted and missing persons files for all 50 states, Canada, U.S. Virgin Islands, Puerto Rico, Guam, American Samoa, and Mariana Islands.

(2) All contributors to NCIC share these files.

(3) E-Agent is a browser provided by FDLE that allows a user the ability and functionality to query, enter, modify, locate, clear, and cancel records in the NCIC system.

g. The CJIS Online Security Awareness Training system is a training system made available for all personnel, to include contractors and vendors, which provides the minimum topics for baseline security awareness training for personnel with access to CJI as required in the Federal CJIS Security Policy and user agreement with FDLE.

(1) Level 1 security awareness training must be completed by personnel not performing a Criminal Justice function with unescorted access to a physically secure location.

(2) Level 2 security awareness training must be completed by personnel performing a Criminal Justice function with unescorted access to a physically secure location.

(3) Level 4 security awareness training is for personnel with information technology roles with unescorted access (physical or virtual) who work on an agency's computer or network that may store or process CJI.

h. The Judicial Inquiry System (JIS) is a web-based browser interface administered by the Office of State Court Administrators (OSCA) which provides the capability to query multiple Florida agency data sources for government agencies authorized for access to those data sources. For the purposes of protective investigations, the Department has access to JIS to obtain driver's license/motor vehicle as well as Department of Juvenile Justice, Department of Corrections, and Clerk of the Court information.

i. Civil Workflow Control System (CWCS) is an automated system used to receive, process, and respond to electronic requests for applicant criminal history record checks via fingerprint.

(1) Submissions to the CWCS are made by livescan devices that adhere to FDLE and FBI standards and requirements.

(2) Criminal history records resulting from these submissions are posted to the appropriate DataMotion SecureMail account.

1-6. General Requirements.

a. There are policies and procedures that govern all agencies and personnel using FCIC AND/OR NCIC /CJNet, criminal justice information, and/or criminal history records provided by FDLE and/or the FBI. CJIS Security Policy applies to the NCIC and criminal justice information obtained from that system.

(1) The CJIS Advisory Board (APB) is responsible for reviewing policy, technical, and operational issues related to the NCIC as well as additional systems and information administered by the FBI.

(2) The National Crime Prevention and Privacy Compact Council establishes policy specific to criminal history records and information obtained and used for noncriminal justice purposes.

b. Existing laws and our user agreement with FDLE establish what criminal justice information the Department may access, how the information can be accessed, how the information can be used, how the information can be shared, and how the information can be maintained. Department employees and designees or contractors must abide by the terms of these documents and maintain the confidentiality of the information obtained.

c. FCIC AND/OR NCIC /CJNet is provided to criminal justice and statutorily defined agencies for official criminal justice purposes. The term criminal justice purpose is defined in section 943.045, F.S., and 28 Code of Federal Regulations (CFR) Part 20.3.

d. Criminal justice information, to include criminal history records, may only be released to authorized criminal justice agencies and some non-criminal justice agencies for specific and limited purposes as defined in law and in the user agreement with the Florida Department of Law Enforcement (FDLE).

e. Information contained and accessed from other state computer files and records through FCIC AND/OR NCIC /CJNet devices cannot be used for non-criminal justice purposes or released to non-criminal justice personnel unless authorized by Florida Statute.

f. CJIS personnel background screenings, certifications, and trainings are required for CJIS information users. These requirements vary depending on the level and type of access. Successful completion of training and/or CJIS personnel background screening and/or certification may be required to perform duties for some position types.

g. The purpose of the request/access/query, not the requestor's job title/role, dictates what information can be accessed. Whether the staff member works for the Department or a contracted provider may additionally dictate what information can be disseminated and received.

h. Each program is responsible for establishing business practices and guidelines, in appropriate operating procedures, detailing what specific purpose information may be accessed, how the information can be shared, and how the information is to be used in accordance with this chapter, Federal and State laws, and the Department's user agreement with FDLE. To ensure compliance with Federal and State policies, such operating procedures should be reviewed by the Local Agency Security Officer (LASO) and FCIC Coordinator (FC).

1-7. CJIS User Agreements.

a. FDLE has entered into an agreement with the FBI regarding access to and use of the NCIC system.

b. In turn, FDLE has entered into an agreement with each Florida agency connected to CJNet and FCIC message switch.

(1) Agencies that participate must abide by all applicable Federal and State laws, regulations, policies, and procedures.

(2) Florida Statute authorizes termination of services to user agencies in cases of misuse or violation of law.

(3) Sanctions can include a warning of violation, restriction of service, discontinuance of service, or legal action.

c. A CJIS User Agreement is a binding agreement, signed by the agency head, that covers liability issues, outlines what is to be expected by each agency regarding proper use of systems and information, and for what purposes systems and information can be accessed.

(1) The Department and FDLE have a criminal justice inter-agency CJIS agreement for protective investigations and a non-criminal justice inter-agency CJIS user agreement for background screening for activities associated with making eligibility determinations for licensing, employment, etc.

(2) The Department and OSCA have a user agreement for access and usage of the Judicial Inquiry System (JIS) for the purpose of protective investigations.

(3) The Department and DJJ have a user agreement for access and usage of the Juvenile Justice Information System (JJIS) and related information just as juvenile delinquency records and dispositions.

(4) The Department may have additional user agreements with FDLE and OSCA for specific programs and purposes.

1-8. Security and Confidentiality.

a. Records containing criminal justice information (CJI) shall be held confidential and shall only be released to other parties who are allowed to view or have the records under Federal and/or State law and the Department's user agreement with FDLE.

b. FDLE has specific requirements regarding what CJI can and cannot be documented in case files and/or in a local system. Agencies must meet the FBI CSP requirements prior to cutting, copying, pasting, or scanning CJI which includes criminal history records into a local system. Examples of a local system include:

(1) Email;

(2) Department data bases;

(3) Flash Drives; and,

(4) Any type of electronic storage media that is accessed via a network connection.

c. It is the responsibility of each participating agency to ensure access to FCIC AND/OR NCIC /CJNet is for authorized criminal justice purposes only and to regulate proper use of the network and information at all times.

d. As appropriate, Circuits and/or programs shall be responsible for notifying appropriate personnel and/or changing a user's security level in appropriate Department systems if the user moves into a position for which they are not legally allowed access to certain criminal justice information. For example, if a protective investigator leaves the Department and is employed by a contracted provider as a case manager, their security level must be changed in the FSFN system to avoid any illegal access of information.

1-9. Ethics and Misuse.

a. All requests and system access must be for official state business purposes only. Improper use of any information obtained from FCIC AND/OR NCIC systems and devices may be unlawful or violate federal, state, and local policies, and could result in criminal prosecution.

b. All users requiring CJIS security awareness training and/or CJIS certification will be expected to successfully complete the training and testing on his/her own without the assistance of other individuals.

c. Criminal history checks shall **never** be requested or queried in the FCIC AND/OR NCIC system by Department staff for the purposes of diligent searches or efforts to locate persons, judicial reviews, adoptions, or respite.

d. Access of these systems and/or dissemination of information obtained from the FCIC and/or NCIC systems for non-criminal justice or unauthorized purposes is considered a misuse of the system.

e. The Department is required to establish appropriate written standards, which may be incorporated with existing codes of conduct, for disciplining violators of FCIC AND/OR NCIC /CJNet policy.

1-10. CJIS Roles and Responsibilities.

a. CJIS Agency Coordinator (CA). Acts as the point of contact regarding communications between FDLE and the user agency. The CAC has the authority to appoint other personnel to serve in other designated CJIS positions and ensures agency personnel are made aware of and able to participate in FDLE CJIS discussions that may lead to policy changes.

b. FCIC Coordinator (FC). Ensures compliance with the legal and policy requirements contained with the CJIS User Agreement and Requirements Document and communicates with FDLE regarding FCIC matters.

c. Local Agency Security Officer (LASO). This position is 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. The LASO should be knowledgeable of the technical aspects of the agency's network and maintain an ongoing working relationship with local technical staff as well as the FCIC COORDINATOR. The LASO is also required to provide the agency's network diagram upon request and be responsible for the triennial CJIS Technical Audit. The LASO must complete the online LASO training available on CJNet and complete and maintain an active certification status of Level 3 Security Awareness Training. A LASO is required at every agency that has direct access to FCIC AND/OR NCIC. The position is referenced and described in the FBI CJIS Security Policy and in FDLE's CJIS user agreement with DCF.

d. nexTEST Administrator. This position is responsible for maintaining the testing system of the agency's members who are Limited and/or Full Access FCIC AND/OR NCIC users. The nexTEST system is used for certification and recertification training by all operators who have direct access to FCIC AND/OR NCIC. The nexTEST administrator creates user accounts, system testing, receives/sends expiration notifications, edits active and expired user accounts, and notifies the FDLE IDT when an account needs to be moved.

e. Judicial Inquiry System (JIS) Point of Contact(s). The data exchange agreement with the Office of State Court Administrators requires the completion of a JIS Point of Contact form, signed by the Chief Executive or Agency Head, identifying the agency's Point of Contact and FCIC COORDINATOR. The Point of Contact is responsible for approving new user requests, determining the level of access, and submitting requests to deactivate JIS accounts. The Hotline, CPI, and API programs each have a JIS Point of Contact.

f. Information Security Manager (ISM). As defined in CFOP 50-2, the person designated by the Secretary of the Department to administer the Department's data and information technology resource security program.

Chapter 2

CRIMINAL JUSTICE INFORMATION ACCESS PROGRAM

2-1. Purpose. This chapter provides the personnel background screening, certification, training requirements for criminal justice information access and related internal business processes.

2-2. Scope. This chapter is applicable to all Department of Children and Families employees and Department contractors who are criminal justice information users and/or who are authorized for access to systems, applications, or devices containing criminal justice information.

2-3. CJIS Personnel Background Screenings.

a. Any Department employee requiring access to FCIC AND/OR NCIC /CJNet systems and/or workstations and/or unescorted access to CJIS Physically Secure Locations (PSL) must successfully complete a CJIS Personnel Background Screening.

(1) Screenings are conducted by electronic fingerprint submission to FDLE.

(2) Crime Intelligence staff located at the Hotline are designated as Criminal Justice Employee's for CJIS purposes. The FCIC COORDINATOR may conduct a preliminary criminal justice employment check using Purpose Code "J" for FCIC AND/OR NCIC system user applicants.

b. The FCIC COORDINATOR may designate a staff member responsible for completing these screenings for specific programs.

c. The FCIC COORDINATOR and/or the FCIC COORDINATOR's screening designee must refer an arrest record of any kind to the FDLE CJIS Systems Officer (CSO) for approval prior to access being granted.

(1) When there is an arrest record of any kind, a review letter approving access or deferring the decision must be received from FDLE prior to access being granted.

(2) Signed approval by the appropriate Program Office or Circuit leadership must be obtained prior to access when an FDLE review letter deferring the decision to the requesting agency is received.

(3) The FCIC COORDINATOR and/or screening designee must maintain copies of approval letters received from FDLE and/or the Program Office or Circuit leadership approval when the decision has been deferred.

2-4. CJIS Security Awareness Training.

a. All Department personnel who have access to criminal justice information, which includes criminal history records obtained from fingerprint submission, are required to complete CJIS Security Awareness Training within 6 months of initial assignment and biennially thereafter.

b. All Department personnel requiring access to a CJIS PSL, which includes the Hotline and Background Screening Program staff, are required to complete CJIS Security Awareness Training prior to unescorted access.

c. This security awareness training can be taken online and is available via the CJIS Online Security Awareness Training system website.

d. There are three levels of CJIS Security Awareness training. Which level is required depends on the position type and level of CJI access.

(1) Level 1 is for staff who need access to the PSL but not CJI or CJI systems such as custodial and maintenance workers.

(2) Level 2 is for non-IT personnel who require access to CJI, which includes criminal history records, and/or unescorted access to CJIS PSL.

(3) Level 3 is for IT personnel who will have access to systems/devices/servers/equipment containing CJI and/or require unescorted access to CJIS PSL.

2-5. CJIS Certification and Recertification.

a. Department personnel who use the FCIC AND/OR NCIC systems to only query and search for records must complete the Limited Access Online Certification training via the nexTEST training system available on the CJNet.

b. Department personnel needing certification must have a current CJIS personnel background screening completed prior to the FCIC COORDINATOR or nexTEST administrator initially creating a nexTEST training account.

c. Recertification is required biannually via the nexTEST system.

(1) Users will receive a notification from the FCIC system.

(2) The FCIC COORDINATOR or nexTEST administrator will notify users a minimum of 30 calendar days prior to the expiration date.

(3) It is recommended that users complete recertification at least 1 week prior to the expiration date to prevent a disruption to account access.

d. Certification is transferable to other Florida criminal justice agencies.

2-6. Contractor and Vendor Access.

a. All Contractor and Vendor personnel who require unescorted access to a CJIS PSL, which includes the crime intelligence areas of the Hotline, are required to complete a CJIS Personnel Background Screening and CJIS security Awareness Training.

(1) This same screening procedure shall be followed as described in paragraph 2-3 of this operating procedure for Department personnel.

(2) The same security awareness training is required as described in paragraph 2-4 of this operating procedure.

b. All Contractor and Vendor personnel who have or may have access to criminal justice information, which includes CJI stored or made available by Department systems or applications, are required to complete a CJIS Personnel Background Screening and CJIS Security Awareness Training.

(1) This same screening procedure shall be followed as described in paragraph 2-3 of this operating procedure for Department personnel.

(2) The same security awareness training is required as described in paragraph 2-4 of this operating procedure.

2-7. Tours and Shadowing.

a. The CJIS Security Policy (CSP) and our user agreement with FDLE both allow for visitors at CJIS Physically Secure Locations.

(1) Personnel visiting the PSL are required to be escorted and to sign a visitor log.

(2) A visitor log must be maintained for staff being provided escort which must be kept for a minimum of 4 years.

(3) Personnel visiting, including those participating in a tour shall be escorted at all times and their activity monitored while in the PSL.

(4) Public areas located outside the perimeter of the PSL do not require escort.

b. At a minimum, visitors who will be shadowing at the Hotline PSL shall additionally successfully complete a background screening and complete Level 1 CJIS Online Security Awareness Training prior to participation.

(1) For background screening, specifically for the purpose of shadowing and site security, the FCIC Coordinator is authorized to conduct a name-based check of the FCIC system using Purpose Code C.

(2) Personnel participating in a tour, but who are not shadowing, are not required to complete a background screening. However, personnel must be escorted at all times as detailed in paragraph 2-7a of this operating procedure.

2-8. Security Addendums.

a. The CJIS Security Addendum is a uniform addendum to an agreement between the government agency and a private contractor when authorized by federal law and state statue and approved by the Attorney General of the United States for access to CHRI. The Addendum limits the use of the information to the purposes for which it is provided, ensures the security and confidentiality of the information is consistent with existing regulations and CJIS security policy, and provides for sanctions. An example Security Addendum can be located on the Department's CJIS intranet page at http://eww.dcf.state.fl.us/cjis/.

b. Private contractors/vendors who perform administration of criminal justice and/or have access to criminal justice information:

(1) Shall meet the same training and certification criteria required by governmental agencies;

(2) Shall be subject to the same extent of audit review as are local user agencies; and,

(3) Shall acknowledge, via signing of the CJIS Security Addendum Certification page, and abide by all aspects of the CJIS Security Addendum.

Chapter 3

ACCOUNT ADMINISTRATION

3-1. Purpose. This chapter provides the responsibilities and related business processes for the administration of CJIS user and training accounts.

3-2. Scope. This chapter is applicable to all Department of Children and Families employees and Department contractors who are criminal justice information users and/or who are authorized for access to systems, applications, or devices containing criminal justice information.

3-3. CJIS Online Security Awareness Training System.

a. CJIS Online Security Awareness Training accounts are administered by the FCIC Coordinator for Hotline staff.

(1) Accounts can be created at the time of hire for Department personnel that are required to complete the training based on a requirement of the position like CPI and Hotline employees.

(2) For vendors and contractors, the FCIC COORDINATOR should be notified to create the account. A CJIS access request form can be completed and submitted for this purpose. A copy of the form is located on the Department's CJIS intranet page at http://eww.dcf.state.fl.us/cjis/.

b. The Agency CJIS Coordinator may designate a staff member responsible for administering these training accounts for a specific program office or area. CJIS Online Points of Contacts are designated in the background screening program, Sexually Violent Predator Program, the Office of Child Welfare and Adult Protective Services Program.

c. CJIS Online Security Awareness Training accounts should be deactivated when an employee separates from the Department or transfers to a position no longer authorized for access to CJI.

3-4. nexTEST.

a. nexTEST certification accounts are administered by the nexTEST administrator or the FCIC COORDINATOR.

(1) A CJIS personnel background screening must be successfully completed prior to the creation of the nexTEST training account in accordance with paragraph 2-1 of this operating procedure.

(2) A CJIS access request form must be completed and submitted by the requestor for this purpose and maintained by the FCIC COORDINATOR or nexTEST administrator. A copy of the form is located on the Department's CJIS intranet page at http://eww.dcf.state.fl.us/cjis/.

b. Users must take a recertification exam biannually.

c. nexTEST accounts should be deactivated within 5 business days when an employee separates from the Department or transfers to a position no longer authorized for access to CJI.

3-5. e-Agent.

a. e-Agent accounts are administered by the FCIC COORDINATOR or the FCIC COORDINATOR's designee.

(1) Accounts are managed using the e-Agent Client Manager.

(2) A CJIS personnel screening as detailed in paragraph 2-1 of this operating procedure and nexTEST certification as detailed in paragraph 2-3 of this operating procedure shall be completed prior to the creation of an e-Agent account.

b. nexTEST certification for Limited Access must be completed before e-Agent account can be used.

c. Each time a user transmits a message to FCIC AND/OR NCIC using the e-Agent browser his/her certification status is checked to ensure the user is actively certified. If the user is not an active certified user, the system will not allow the user to run transactions in FCIC AND/OR NCIC.

d. Each user shall be provided with the Department's policy for disciplining violators of FCIC AND/OR NCIC /CJNet policy and sign a copy of receipt. The receipt form shall be maintained by the FCIC COORDINATOR or the FCIC COORDINATOR's designee.

e. e-Agent accounts should be deactivated, in no more than 5 business days, when an employee separates from the Department or transfers to a position no longer authorized for access to CJI.

3-6. FALCON.

a. FDLE must approve an Agency and program prior to use of the FALCON system. A user agreement with the Department and program specific to its use may be required.

b. The Department's Sexual Violent Predator Program has a staff member designated as the FALCON Application Access Administrator (AAA). An Agency CJIS Contact Form must be completed for this purpose and signed by the Agency Head.

c. The AAA is responsible for the creation and management of the program members who are users of the FALCON system. The AAA approves user's access, provides roles and privileges, and monitors Watch List records.

d. A CJIS personnel screening as detailed in paragraph 2-1 of this operating procedure and nexTEST certification as detailed in paragraph 2-3 of this operating procedure shall be completed prior to the creation of an e-Agent and/or FALCON account.

e. The FCIC COORDINATOR is responsible for ensuring FALCON users have completed screening and certification requirements.

f. FALCON accounts should be deactivated and Watch Lists reassigned, in no more than 5 business days, when an employee separates from the Department or transfers to a position no longer authorized for access.

3-7. Judicial Inquiry System. Processes and procedures for Judicial Inquiry System (JIS) account administration to include user access requests are detailed in chapter 7 of this operating procedure.

3-8. DataMotion Secure Mail Accounts.

a. The DataMotion Secure Mail system is administered by FDLE.

b. These accounts are used by authorized staff to obtain access to the results of fingerprint submissions.

c. For assistance obtaining access to these mail accounts, the Department's Office of Child Welfare Operations – Background Screening Office should be contacted.

d. CJIS Security Awareness Training shall be completed prior to access to the Secure Mail Accounts.

Chapter 4

INFORMATION SECURITY

4-1. Purpose. This chapter provides requirements for the protection, proper usage, handling, documentation, dissemination, and storage of criminal justice information to include criminal history records.

4-2. Scope. This chapter is applicable to all Department of Children and Families employees and Department contractors who are criminal justice information users and/or who are authorized for access to systems, applications, or devices containing criminal justice information.

4-3. Criminal Justice and Personally Identifiable Information.

a. Criminal Justice Information (CJI), to include criminal history and Hot File records, obtained from FCIC, NCIC, CJNet, and from results received from fingerprint submissions are confidential and shall only be received and disseminated as prescribed in this Chapter. When creating and updating operating procedure and guidelines for their specific business practices, each program shall ensure that the policy and procedure detailed in this Chapter are incorporated.

b. Personally Identifiable Information (PII) is information which can be used to distinguish or trace an individual's identity, such as name, social security number, biometric records, alone or when combined with other personal information such as date and place of birth.

(1) A criminal history record inherently contains PII.

(2) PII shall be extracted from CJI for the purpose of official business only.

(3) To ensure appropriate controls are applied when handling PII, Department Administrative Code and Operating Procedures shall be followed, specific to the information type extracted from the CJI source.

4-4. Authorized Purposes.

a. The Department is authorized to access, receive, and/or disseminate criminal justice information to include criminal history and Hot File records for very specific purposes. Depending on the purpose, submission and access methods may vary.

b. Access to FCIC AND/OR NCIC /CJNet is restricted to those activities statutorily defined as criminal justice purposes:

(1) Protective Investigations;

(2) Criminal Justice Employment; and,

(3) CJIS PSL Work Site Security.

c. Access to FCIC AND/OR NCIC /CJNet is authorized for one specific non-criminal justice function for the Department: FCIC and NCIC for the purpose of Emergency Placements. Fingerprint submissions are still required unless a decision is made not to proceed with the placement.

d. Access for all other purposes by the Department are defined strictly as a non-criminal justice functions and Florida and National criminal history records are obtained by fingerprint submission. Examples of non-criminal justice include, but may not be limited to:

(1) Employment.

(2) Licensing.

(3) Adoption.

4-5. Physical Security. Sites containing FCIC AND/OR NCIC /CJNet workstations must meet the following criteria of a Physically Secure Location (PSL) as defined by Federal CJIS Security Policy (CSP) and the user agreement with FDLE:

a. Computers with access must be in a room that remains locked when unoccupied.

b. The monitor screens must face away from any open doors and not be visible from interior, ground floor, or cross-wing windows.

c. The perimeter of the physically secure location shall be prominently posted and separated from non-secure locations by physical controls.

d. Visitors shall be escorted at all times and their activity monitored.

e. A confidentiality acknowledgement form shall be signed by all visitors. The form shall reference CJIS policy and must be maintained for a minimum of four years.

f. Department personnel, contractors, and vendors requiring unescorted access must first complete the requirements as described in Chapter 2 of this operating procedure.

4-6. Documentation.

a. The FBI and FDLE have very specific guidelines regarding what CJI can and cannot be documented in case notes or in an agency's system of record such as the Florida Safe Families Network (FSFN). The primary issues are as follows:

(1) If written notes include specifics regarding sealed/expunged or National criminal history, a criminal history record is created that is not sanctioned by any statute.

(2) Contracted providers are prohibited from receiving or viewing Florida sealed and expunged information and National criminal history record information. If any written note or documentation (including information made available to a contracted provider) in FSFN contains this information, confidentiality of criminal history records has been violated.

(3) Criminal history obtained from FCIC, NCIC, and Hot File records must be protected from public record requests.

(4) The following standardized wording is recommended Purpose Code C, X, or N documentation in case notes for protective investigators: "The appropriate background checks were conducted on (date) for (individual's name). The Protective Investigator has evaluated the information and reviewed for patterns of behavior or domestic violence that may pose a potential safety concern or elevated risk to a (child or vulnerable adult). At this time, (there appears to be) or (there does not appear to be) an immediate negative impact on the victim's safety."

(5) Purpose Code Q Florida results do not contain sealed/expunged or National criminal history records. Florida Purpose Code Q information may be summarized in FSFN.

(6) CFOP 170-1, Chapter 3, contains additional procedures for Child Protective Investigators specific to the use of criminal history record information for the Family Functioning Assessment (FFA).

b. Criminal justice information to include criminal history and Hot File records must not be transmitted via unencrypted email. Agencies must meet the FBI CJIS Security Policy requirements prior to cutting, copying or pasting FCIC AND/OR NCIC response data into a local system for the purpose of documentation which includes email.

c. Each program office shall be responsible for establishing business practices and guidelines specific to CJI documentation in appropriate operating procedures for their program in compliance with this operating procedure, Federal and State laws, and the Department's user agreement with FDLE. To ensure compliance with Federal and State policies, such sections of operating procedures should be reviewed by the LASO and FCIC COORDINATOR.

4-7. Dissemination.

a. Criminal justice information obtained from FCIC, NCIC, and/or CJNet to include criminal history and Hot File records shall only be disseminated to and received by authorized agencies and personnel.

(1) Criminal justice information to include criminal history records obtained from FCIC that could contain a notice of sealed and/or expunged record, such as Purpose Code C, shall only be disseminated to and received by Department staff responsible for protective investigations, Sheriff Office units contracting with the Department to conduct child protective investigations, Department Children's Legal Services (CLS) attorneys, state attorneys, and to the court for an inspection in camera.

(2) NCIC information of any purpose code may not be shared with contracted providers including during case transfer of a protective investigation, except for investigative units with Florida Sheriff Offices who have contracted with the Department to conduct child protective investigations.

(3) Criminal history records obtained from FCIC and NCIC disseminated by the Hotline is available for view and print (if applicable) via the link located in Florida Safe Families Network (FSFN) for 72 hours from when the criminal history check is completed.

(4) Print function capability is disabled via the FSFN system for FCIC records containing sealed and expunged information and NCIC records.

b. Criminal justice information to include criminal history and Hot File records obtained from fingerprint submission results shall only be disseminated to and received by authorized agencies and personnel. Fingerprint results could contain notifications of Florida sealed and expunged information and national criminal history information.

(1) Florida and National criminal history record information may be accessed only as allowed by federal and state statutes, regulations, and guidelines.

(2) National criminal history information can only be received by the Department. Contracted providers cannot receive this information.

(3) All information obtained through the record check or background screening process is exempt from public disclosure and may not be used for any reason other than the purpose for which the individual was screened as provided in section 435.09, F.S.

(4) FDLE Florida criminal history public record information obtained through the background screening process for the purpose of employment or licensure is may only be disseminated to authorized agencies and personnel for those purposes.

4-8. Secondary Dissemination Logging.

a. There are secondary dissemination logging requirements for criminal justice information, to include criminal history and Hot File records, obtained from FCIC or NCIC.

b. All secondary dissemination of criminal justice information obtained from the FCIC and/or NCIC systems to authorized criminal justice or non-criminal justice agencies shall be recorded on the Secondary dissemination Log. A copy of a Secondary Dissemination Log can be found on the Department's CJIS intranet page located at http://eww.dcf.state.fl.us/cjis/.

(1) "Secondary dissemination" means the releasing of criminal justice information to include criminal history and Hot File records either by physically providing documents or verbally providing information from one authorized agency to another authorized agency.

(2) If the contracted provider initiates a request to the Hotline the provider is the requestor. FSFN electronically logs the request and transaction so there is no need to make a notation on an additional Secondary Dissemination Log. However, the contracted provider must record any secondary dissemination the provider makes to the court, state attorney, Department, etc. and the Department must additionally log any criminal history record disseminated to the provider that was obtained from the submission of fingerprints. Rules concerning what types of information can or cannot be disseminated to a contract provider still apply as detailed in paragraph 4-8 of this operating procedure.

(3) The Secondary Dissemination Log is used to document all authorized secondary disseminations of FCIC AND/OR NCIC information by staff in a unit, service center, agency, to personnel to other authorized agencies.

(4) Each entry on the Secondary Dissemination Log must be maintained for at least five (5) years.

(5) Circuits and contracted providers will determine how many Secondary Dissemination Logs are needed and where to maintain the Logs.

(6) When FDLE audits, the auditor will check to see that the Circuit or contracted agency is appropriately maintaining the Secondary Dissemination Log.

4-9. Storage and Destruction.

a. Criminal history records must be protected from public record requests. As such, criminal records must not be co-mingled with any file (hardcopy file or electronic) which is or may become a public record.

(1) Criminal History records obtained from FCIC and/or NCIC shall not be scanned into a local system unless approved as meeting CJIS Security Policy requirements for electronic storage of CJI. Example: These criminal history records shall not be scanned into the FSFN electronic file cabinet.

(2) Criminal history records obtained as a result of fingerprint submission shall not be scanned into a local system unless approved as meeting CJIS Security Policy requirements for electronic storage. These criminal history records shall not be scanned into the FSFN electronic file cabinet.

(3) Agencies must meet the CJIS Security Policy requirements prior to cutting, copying, or pasting FCIC and/or NCIC response data into a local system for the purpose of storage.

(4) NCIC criminal history and Hot File records received must not be printed or maintained in case files being sent to off-site storage facilities.

(5) Criminal history records to include National records obtained as a result of fingerprint submissions must not be included in files being sent to off-site storage facilities.

b. Criminal history information is constantly changing and should only be kept until the administrative value is lost.

c. Until disposal, criminal history records must be maintained in a secure location such as a locked file cabinet or file cabinet in a room with access limited to authorized staff.

(1) When criminal history records in a locked file cabinet is stored in a specific case file, the case file (and the criminal justice information therein) is retained until the retention period for the case file has been met.

(2) When criminal history records are filed in a separate file containing only criminal justice information from various cases, that file may be destroyed when the information therein no longer has any administrative value (per retention schedule GS1-SL, Item #2). Criminal justice records obtained from the FBA, NCIC or FCIC are “duplicates”; the record copy is held by the FBI or the Florida Department of Law Enforcement.

d. The Hotline is the only Department entity authorized to maintain electronic records of FCIC and NCIC information obtained from name-based checks.

e. An employee of the agency who has possession of the record must witness the destruction of criminal history records and files containing criminal history records. If a private vendor is used for record destruction, the record holder employee must remain with the record until it is destroyed.

f. Data sanitation must occur in compliance with CFOP 50-2 and CJIS Security Policy for all devices to include Department computer/printer/copier hard drives, hard drives on leased equipment, and servers that have been used to transmit, copy, print, or store criminal justice information.

4-10. Incident Reporting.

a. Incident reporting for misuse and/or abuse of systems, applications, and/or information must occur in accordance with CFOP 50-2, Chapter 3, Incident Reporting, which includes notifying the Department’s Information Security Manager (ISM).

b. Additionally, misuse of CJIS or JIS systems, applications, and/or information must be reported to the Department’s LASO and FCIC COORDINATOR.

c. Incidents must be reported to FDLE and/or OSCA in accordance with the Department’s user agreements.

d. Misuse of driver and motor vehicle systems or information, such as DAVID, via the JIS system, has additional reporting requirements to DHSMV as detailed in Chapter 7 of this operating procedure.

e. In the report to FDLE and/or OSCA the Department must include the following: a brief summary of the incident on agency letterhead, outcome of the review, number of records compromised, if owners of the compromised information were notified, what disciplinary action (if any) was taken, and corrective action plans to ensure misuse does not occur again.

f. The Department must immediately update user access permissions upon discovery of negligent use, improper use, unauthorized use, or unauthorized dissemination.

4-11. CJIS Disciplinary Policy. Agencies accessing FCIC AND/OR NCIC systems and/or criminal history records must establish appropriate written standards, which may be incorporated with existing codes of conduct, for disciplining violators of FCIC AND/OR NCIC /CJNet policy.

a. Department staff directly accessing FCIC AND/OR NCIC systems or CJNET must be provided with the Department's Criminal Justice Information (CJI) discipline policy and complete a receipt form.

b. Receipt forms shall be maintained by the FCIC COORDINATOR.

c. An electronic acknowledgement via the Department's Human Resources Tracking System (HRTS) is also an approved method for documenting receipt of the CJIS disciplinary policy.

Chapter 5

AUDITING AND ACCOUNTABILITY

5-1. Purpose. This chapter provides CJIS requirements for FDLE and FBI criminal justice compliance, technical, and non-criminal justice audits and related internal Department processes and responsibilities.

5-2. Scope. This chapter is applicable to all Department of Children and Families employees and Department contractors who are criminal justice information users and/or who are authorized for access to systems, applications, or devices containing criminal justice information.

5-3. Purpose Code X Reviews.

a. Every month, FDLE reviews the Purpose Code "X" checks completed by the Hotline and attempts to match them to fingerprint livescan submissions that are submitted by the Circuits.

b. FDLE creates a list of names it was unable to match and sends it to the FCIC COORDINATOR for a Department review.

(1) Each Circuit's NCIC Point of contact assists the FCIC COORDINATOR with completing the review, including obtaining information from child protective investigators and contract providers.

(2) For errors or violations, the FCIC COORDINATOR may be required to detail what corrective action took place.

c. FDLE may use the review results to determine when it will conduct on-site compliance audits. Failure to complete audits or audits that lack complete information may alert FDLE to the need for an on-site audit. FDLE reserves the right to conduct compliance audits at any time.

5-4. Criminal Justice Compliance Audits.

a. FDLE conducts regularly scheduled compliance audits of every agency accessing the FCIC AND/OR NCIC systems to ensure network security, conformity with state and federal law, compliance with CJIS Security Policy (CSP), CJIS Advisory Board (APB) policies, and requirements detailed in the Department's user agreement with FDLE.

b. FDLE and FBI compliance audits are normally scheduled triennially. However, compliance audits may be conducted at any time by FDLE or FBI CJIS audit staff.

c. These audits are conducted on-site at the Department's CJIS Physically Secure Locations.

d. The FCIC COORDINATOR is the Department's point of contact with FDLE concerning criminal justice compliance audits.

(1) Notification of the audit will be provided to the FCIC COORDINATOR in advance by FDLE or the FBI CJIS Audit Offices.

(2) A preliminary audit package will be sent to the FCIC COORDINATOR who will be required to complete and return by a specified date.

(3) Results of the audit will be provided by FDLE or the FBI in writing to the Department's agency head.

5-5. Non-Criminal Justice Compliance Audits.

a. FDLE conducts regularly scheduled compliance audits of every agency obtaining Florida and/or National criminal history records via the Civil Workflow Control System (CWCS) to ensure conformity with state and federal law, compliance with National Crime Prevention and Privacy Compact Council policies, and all applicable rules, regulations, and operating procedures.

b. These audits are conducted triennially in the Circuits and are scheduled by each Department non-criminal justice Originating Agency Identifier (ORI).

c. FCIC COORDINATOR should be notified by the Circuit when a non-criminal justice audit is scheduled by FDLE or the FBI.

d. The FBI may additionally conduct a non-criminal justice compliance audit which will include the Hotline triennially. This audit is separate from the criminal justice compliance audit.

5-6. Technical Audits.

a. FDLE and/or the FBI conducts regularly scheduled technical audits of every agency accessing the FCIC AND/OR NCIC systems to ensure technical compliance with the Federal CJIS Security Policy.

b. These audits are conducted triennially and may take place at the appropriate Department CJIS Physically Secure Locations.

c. The LASO is the Department's point of contact with FDLE and the FBI concerning technical audits.

5-7. Off-Line Searches.

a. FDLE and the FBI logs and archives information for completed transactions in the FCIC and NCIC systems. The archived information contained in these logs can be used for criminal investigations of suspected misuse, system compliance, public record requests, and administrative purposes.

b. Transaction Archive Reports (TAR) stores and logs the complete text of all FCIC AND/OR NCIC transactions to offline storage. Requests can be submitted via email to tarrequest@fdle.state.fl.us or contact the FCIC Coordinator for assistance.

5-8. DAVID Audits. Requirements for DAVID audits are detailed in chapter 7 of this operating procedure.

Chapter 6

AGENCY IDENTIFIER MANAGEMENT

6-1. Purpose. This chapter provides the requirements for agency identifier management for Originating Agency Identifier (ORI), terminal mnemonics, Originating Case Agency information and related internal Department processes and responsibilities.

6-2. Scope. This chapter is applicable to all Department of Children and Families employees and Department contractors who are criminal justice information users and/or who are authorized for access to systems, applications, or devices containing criminal justice information.

6-3. Originating Agency Identifier Administration.

a. An Originating Agency Identifier (ORI) is a nine-character identifier assigned by the FBI CJIS staff to an agency to identify agencies conducting transactions in the NCIC system. It is also used to identify agencies conducting transactions by submitting fingerprints via the Civil Workflow Control System (CWCS).

b. ORI's are assigned to each active computer terminal/workstation with access to FCIC and NCIC.

(1) These are considered criminal justice ORI's.

(2) The FCIC COORDINATOR with OITS Desktop support assistance is responsible for maintaining the Department's active listing of these ORI's to include computer terminal/workstation assignments.

(3) Additionally, the FCIC COORDINATOR is responsible for requests for additional ORI's, inactivating ORI's, and for ensuring agency information is updated in the FCIC system.

c. ORI's are assigned to each authorized livescan device for the purpose of submitting fingerprints.

(1) These are considered non-criminal justice ORI's.

(2) The Department's director of background screening is responsible for maintaining the Department's active listing of these ORI's.

(3) Additionally, the director of background screening is responsible for requests for additional ORI's.

6-4. Originating Case Agency Administration.

a. An Originating Case Agency (OCA) is a unique identification number issued by the Background Screening office generated by the CSIS system or converted from a legacy system.

(1) For Live Scan submissions, the OCA is prefaced with the two-digit district number and ends with a "Z" (e.g., 03011234Z).

(2) This differs from an ORI, which is assigned to qualified governmental entities by the FBI.

b. The Department's Office of Child Welfare Operations Director of Background Screening manages the Department's OCA process.

6-5. Mnemonic Administration.

a. In addition to the ORI each FCIC device has a unique, nine-character identifier called a mnemonic.

b. Mnemonics are issued by FDLE to identify specific agency devices and are structured into four fields.

(1) Agency Type;

(2) County Code;

(3) Agency Code; and,

(4) Device Number.

c. The FCIC COORDINATOR with OITS Desktop support assistance is responsible for maintaining the Department's active listing of these mnemonics to include computer terminal/workstation assignments.

d. Additionally, the FCIC COORDINATOR is responsible for requests for additional ORI's, inactivating ORI's, and for ensuring agency information is updated in the FCIC system.

6-6. Livescan Device Inventory.

a. Each Region shall be responsible for maintaining an up-to-date livescan inventory of Department devices located in their area that can be provided upon request. The inventory at a minimum shall include:

(1) Region;

(2) Device location and site name;

(3) Device ID;

(4) DCF contact;

(5) Primary assigned ORI;

(6) OS;

(7) Manufacturer;

(8) Scanner model; and,

(9) Scanner manufacturer.

b. Each Region shall notify the FCIC COORDINATOR and Background Screening Program Management when the DCF Contact for a specific device or ORI has changed to ensure that FDLE records are appropriately updated.

Chapter 7

DRIVER AND VEHICLE INFORMATION PROTECTION

7-1. Purpose. This chapter provides requirements to ensure that Florida Department of Highway Safety and Motor Vehicle (DHSMV) systems, applications, and information (to include, but not be limited to, personal driver's license and motor vehicle information) is accessed and queried by Department of Children and Families personnel only for authorized purposes, and that the results are protected in accordance with existing law, policy, and procedure.

7-2. Scope. This chapter is applicable to all Department of Children and Families employees authorized to access systems, applications, or information containing DHSMV and/or driver's license information or authorized to query such records.

7-3. General Requirements.

a. Access to driver's license information, to include photos and signatures, is limited to those purposes as defined in existing laws and the Department's memorandum of understanding with the Florida Department of Highway Safety and Motor Vehicles (DHSMV) and Office of State Court Administrators (OSCA).

b. The Department must establish what information may be accessed, for what purposes, Driver and Vehicle Information Database (DAVID) account roles for each system user, and information security procedures in accordance with existing laws and the memorandum of understanding with DHSMV and interagency agreement with OSCA.

c. The Department may not assign or sub-contract any rights or duties within the MOU without DHSMV consent.

d. Each program is responsible for establishing business practices, in appropriate operating procedures, detailing for what specific purpose information may be accessed, how the information can be shared, and how the information can be used in accordance with Florida Statute to include, but not limited to, Social Security Number (section 119.071, F.S.), Driver's License Photo (section 322.142, F.S.), Medical/Disability Information (section 322.125, F.S. and section 322.126, F.S.), this operating procedure, the Driver's Privacy Protection Act, and the Department's memorandum of understanding with DHSMV and interagency agreement with OSCA.

e. The purpose of the request and/or information access, not just the requestor's job title, dictates what information can be requested, queried, received, and/or viewed.

f. Department staff may be authorized to access DHSMV information by more than one system or application which includes, but may not limited to, DAVID and the Judicial Inquiry System (JIS).

g. Prior to accessing the DAVID data source via the Florida Department of Law Enforcement's CJNET or accessing driver's license/motor vehicle information from the Florida Crime Information Center (FCIC)/National Crime Information Center (NCIC), authorization must be obtained from the Department's FCIC Coordinator.

7-4. Security and Confidentiality.

a. Personal information, including restricted information as defined in 18 U.S.C section 2725, contained in a motor vehicle record is confidential pursuant to the federal Driver's Privacy Protection Act of 1994 (DPPA), 18 U.S.C. section 2721.

b. Such information may be released only as authorized by that act, Florida Statutes, and the interagency agreement with DHSMV.

c. Emergency contact information contained in a motor vehicle record is confidential and exempt from section 119.07(1), F.S., and section 24(a), Art. I of the State Constitution.

d. A person who knowingly violates the provisions of section 119.07(1), F.S., is subject to suspension and removal or impeachment and, in addition, commits a misdemeanor of the first degree, punishable as provided in section 775.082 or section 775.083, F.S.

e. A person who has been convicted of an offense other than a capital felony may be sentenced to pay a fine in addition to any punishment described in section 775.082, F.S. A person who has been convicted of a noncriminal violation may be sentenced to pay a fine. Fines for designated crimes and for noncriminal violations shall not exceed $1,000 (section 775.083(1)(d), F.S.) when the conviction is of a misdemeanor of the first degree.

f. DHSMV and OSCA logs and archives information for completed transactions in the DAVID and JIS systems. The archived information contained in these logs can be used for criminal investigations of suspected misuse, audits, quarterly quality control reviews, public record requests, and administrative purposes.

7-5. Driver's License Photo and Signature.

a. Access to personal driver's license photos and signatures is confidential and restricted to specific purposes as defined in section 322.142(4), F.S., and pursuant to the Department's memorandum of understanding with DHSMV and interagency agreement with OSCA.

b. Authorized Department purposes are:

(1) Protective investigations under Part III of Chapter 39 and Chapter 415, F.S.;

(2) For use as verification of identity to expedite the determination of eligibility for public assistance; and,

(3) For public assistance fraud investigations.

c. Access to DHSMV information for inspector general investigation purposes is detailed in and pursuant to the Department's Office of Inspector General's memorandum of understanding with DHSMV.

7-6. Emergency Contact Information (ECI) and Other Restricted Information Types.

a. Emergency contact information (ECI) contained in a motor vehicle record is confidential and exempt from section 119.07(1), F.S. and section 24(a), Art. I of the State Constitution.

(1) Emergency contact information contained in a motor vehicle record is restricted to law enforcement agencies. The Department is not authorized to access ECI.

(2) Roles allowing access to ECI shall not be provided by DCF DAVID Points of Contact to Department staff.

b. Extended timeout sessions are only authorized for law enforcement agencies. Department staff shall not be provided with extended time out sessions.

c. Additional information types that have restrictions include the following:

(1) Crash Reports (section 316.066, F.S.);

(2) Email Addresses (section 119.0712, F.S.);

(3) Voter Information (section 97.0585, F.S.); and,

(4) Deceased Dates (15 CFR 1110.102).

7-7. Roles and Responsibilities.

a. DAVID Point of Contact(s). Responsible for user account administration activities to include, but not be limited to, approving account requests, the creation/modification of user accounts, and password resets. DCF employees who do not know their DAVID Point of Contact(s) and have a need to know can email HQW.DCF.ISM.Team@myflfamilies.com to request information about their DAVID Point of Contact.

b. Information Security Manager (ISM). The person designated by the Secretary of the Department to administer the Department's data and information technology resource security program.

c. Judicial Inquiry System (JIS) Point of Contact(s). Responsible for user account administration activities to include, but not be limited to, approving account requests, notifying JIS for account deactivations, and assisting with troubleshooting issues.

d. FCIC Coordinator FC). Responsible for ensuring agency compliance with CJIS policies and procedures and acts as the agency liaison with FDLE's Criminal Justice Information Services (CJIS) staff. Also, ensures CJIS and DAVID audits are completed as required.

7-8. Account Access Requests.

a. DHSMV DAVID accounts are requested by completing the DCF Driver and Vehicle Information Database Access Authorization Request (form CF 140, available in DCF Forms). The request form can also be found on the Intranet at http://eww.dcf.state.fl.us/security/forms.shtml.

(1) The requestor's supervisor must approve access and sign the request form.

(2) Completed DAVID request forms should be submitted to the appropriate DAVID point of contact located within each Region's local security office via an IT Footprint ticket.

(3) When creating and/or modifying user accounts, the Department's DAVID Points of Contact shall follow access permissions and roles as detailed in the 2019 DCF DAVID Program Roles Reference form located at http://eww/cjis/policy.shtml.

(4) DAVID accounts may only be provided to direct employees and not contractors, sub-contractors, or any other non-employees.

(5) DAVID Access Authorization Request forms must be fully completed prior to providing an account. This includes but is not limited to: identifying requestor as direct employee by including his/her People's First ID, documenting the requestor's program/position, and signature approval by the requestor's supervisor.

(6) The DAVID Point of Contact list can be located on the Department's CJIS intranet page at http://eww.dcf.state.fl.us/cjis/.

(7) The Hotline and APS have selected to use the OSCA JIS interface to access DHSMV and should refer to section B for JIS access requests.

b. Judicial Inquiry System accounts are requested by completing the JIS Access Request. The request form is located on the Department's intranet page at http://eww.dcf.state.fl.us/cjis/.

(1) Completed JIS request forms are submitted to the Hotline, CPI, or API programs JIS point of contact as appropriate.

(2) Requests for CPI, API, and Background Screening staff can be submitted to HQW.OSCAJISRequest@myflfamilies.com.

(3) The JIS Point of Contact list is located on the Department's CJIS intranet page at http://eww.dcf.state.fl.us/cjis/.

(4) The JIS Point of Contact must approve access and level of access on the request form.

(5) Prior to approving access, the JIS Point of Contact shall validate that DAVID training and e-acknowledgements have been completed via People First.

(6) Any request for CJIS databases and/or information access must be approved by the FCIC COORDINATOR in addition to the JIS Point of Contact.

7-9. Dual Access Requests.

a. Each staff member's DAVID account is assigned to the appropriate Agency and sub-Agency (Region). If a user is dual employed by another agency and is authorized for access to DAVID at both agencies, then he/she needs to apply for Dual Access. Once Dual Access is obtained the user will need to select the appropriate agency during sign in.

b. Similarly, if a DCF staff member conducting the Quarterly Quality Control Review (QQCR) needs to audit users assigned to a different Region(s) as part of the QQCR process, then he/she will need to apply for Dual Access and select the appropriate sub-agency/Region during sign in.

c. Requests for Dual Access should be submitted to the DAVID point of contact in the requestor's Regional Security Office.

(1) The DAVID system requires a Dual Access request submission from the user's DAVID profile.

(2) Dual Access requires processing in the DAVID system by the user's primary Regional DAVID FCIC Coordinator and each Region's DAVID Point of Contact for which access is being requested.

d. Prior to the Region DAVID FCIC Coordinator providing Dual Access in the DAVID system, the user must additionally submit an IT Footprint Ticket attaching a new DCF Driver and Vehicle Information Database Access Authorization Request Form.

(1) The request form must be approved and signed by the user's supervisor as detailed in paragraph 7-8 of this operating procedure.

(2) Request forms must be signed by the Chief of Investigations for staff with the Office of Inspector General.

(3) To assist the DAVID POC with assigning appropriate roles in the user's DAVID account, both the IT Ticket and Request Form must detail the reason for the Dual Access such as conducting audits or Dual Employment.

(4) When submitting the IT Footprint Ticket, the user must copy the submission to the approving supervisor and the CJIS Coordinator.

(5) For Dual Employment, the other Agency name and contact information shall be included.

7-10. DAVID Transfer Requests. DAVID account transfer requests from other agencies are permissible and should be processed in accordance with SOP C-9, *DAVID Account Transfer Process*.

7-11. Training and Acknowledgements.

a. Department personnel are required to complete a DHSMV user training prior to accessing a DHSMV system or application. Users are required to take the training annually.

(1) The training is available through DAVID and new users are prompted to complete at initial sign in for that system.

(2) DAVID users are required to electronically sign a legal disclaimer acknowledging proper business usage and possible sanctions for misuse at each sign in.

b. The Judicial Inquiry System (JIS) does not contain a training module with the system itself.

(1) Training is available for JIS on People First for JIS users with the Hotline, CPI, and API programs.

(2) Department JIS users are required to complete the confidentiality and criminal sanctions acknowledgements via People First.

7-12. Password Resets.

a. Both the DAVID and JIS systems have available functionality for a user to set security questions to assist with password resets.

b. If the security questions have not been set, and a user needs assistance with a password:

(1) For DAVID, the appropriate Regional DAVID point of contact should be contacted for assistance. DHSMV customer support should not be contacted for a password reset.

(2) For JIS, the OSCA JIS support staff should be contacted for password resets for Judicial Inquiry System accounts by emailing JIS_Support@flcourts.org.

7-13. Account Deactivation.

a. DAVID Accounts.

(1) The DAVID point of contacts should be notified via the DCF Statewide Help Desk ticketing system when an employee with an active account separates from the Department, moves to position no longer requiring access, or moves to a position with a different level of access.

(2) User's access permissions must be updated immediately upon termination, reassignment, or upon discovery of negligent, improper, or unauthorized use or dissemination of

information in accordance with SOP S-2, DHSMV DAVID Related Event and Incident Reporting Procedure the process detailed in paragraph 7-14 of this operating procedure ("Incident Reporting").

(3) The appropriate Region DAVID point of contact should be notified if an employee's account has not been logged into for 90 days, and the DAVID point of contact shall inactivate the account.

(4) Employees needing account reactivation shall submit a DCF Statewide Help Desk ticket request.

(5) Account deactivations and modifications to permissions for OIG staff shall be submitted to the OIG DAVID Point of Contact.

b. JIS Accounts.

(1) The JIS point of contact should be notified when an employee with an active account separates from the Department or moves to position no longer requiring access or moves to a position with a different level of access.

(2) JIS accounts should be deactivated as soon as possible from the time of separation from the Department or assignment to a new position.

(3) The JIS point of contact should be notified if an employee's account has not been logged into for 60 days for account inactivation.

(4) Employees needing account reactivation shall submit a new JIS Access Request form following the procedure detailed in paragraph 7-8 of this operating procedure ("Account Access Requests").

7-14. Incident Reporting.

a. Incident reporting for misuse and/or abuse of DHSMV or OSCA systems, applications, and/or information must occur in accordance with CFOP 50-2, Chapter 3, Incident Reporting and SOP S-2, DHSMV DAVID Required Notifications Procedure.

(1) Requests for DAVID audits to investigate allegations or suspected misuse/abuse of DHSMV or OSCA systems shall be reported to the OIG and ISM by the Department's DAVID Administrator.

(2) Additionally, misuse of DHSMV or OSCA systems, applications, and/or information must be reported to DHSMV and/or OSCA as appropriate in accordance with the Department's interagency agreements.

b. When reporting an incident, DHSMV requires a brief summary of the incident on agency letterhead, the outcome of the review, the number of records compromised, if owners of the compromised information were notified, what disciplinary action (if any) was taken, and corrective action plans to ensure misuse does not occur again.

c. Additionally, DHSMV requires that owners of compromised information be provided notification. Documentation of the notice, to include the notification letters to DHSMV and owners of compromised information, shall be maintained by the appropriate program office QQCR staff and provided upon request by Department leadership/ISM/OIG, the Department's DAVID Administrator, and DHSMV to include during on-site audits.

d. The Department must immediately update user access permissions upon discovery of negligent use, improper use, unauthorized use, or unauthorized dissemination.

7-15. Dissemination of DAVID and JIS Information.

a. Personal driver and motor vehicle information, to include driver's license photos and signatures, obtained from DAVID and JIS systems are confidential and shall only be received and disseminated as prescribed in the Department's memorandum of understanding with DHSMV and interagency agreement with OSCA as well as Department operating procedures.

b. Personal driver and motor vehicle information, to include driver's license photos and signatures, may only be released or further disseminated to authorized personnel.

c. Driver's license photos and signatures shall only be received by Department staff directly responsible for performing tasks for purposes as defined in existing laws and the Department's memorandum of understanding with the Florida Department of Highway Safety and Motor Vehicles, including:

(1) Protective investigations;

(2) Identification verification for public assistance eligibility determinations; and,

(3) Fraud investigations.

d. Hard copies of the driver and motor vehicle information, including the driver's license photos and signatures, should not be disseminated to non-department staff such as case managers during case transfer from investigations. DAVID queries may not be requested or conducted for the purpose of protective services case management, home studies, or licensing.

7-16. Storage and Destruction.

a. Personal driver and motor vehicle information must be protected from access by unauthorized personnel. As such, information must not be co-mingled with any file (hardcopy file or electronic) or records scanned into a local database that may be accessed by personnel not authorized to view.

(1) Records obtained for the purpose of protective investigations from the DAVID system or JIS reports shall not be scanned into the Florida Safe Families Network (FSFN).

(2) Agencies must meet Driver's Privacy Protection Act and interagency agreement requirements prior to cutting, copying, or pasting response data into a local system for the purpose of transmittal or storage.

b. Driver and motor vehicle information and records are constantly changing and should only be kept until the administrative value is lost.

(1) DHSMV Information obtained through DAVID or the JIS system may be disposed via approved methods as described in this operating procedure when the information therein no longer has any administrative value (per retention schedule GS1-SL, Item #2, Administrative Convenience Records). The records obtained from DAVID or the JIS system are "duplicates"; the record copy is held by the Florida Department of Law Enforcement or the Department of Highway Safety and Motor Vehicles.

(2) Per our interagency agreement, DHSMV information may only be retained by Law Enforcement agencies.

c. Until disposal, driver license and motor vehicle records shall be maintained in a restricted location where only authorized personnel shall have access.

d. A staff member authorized to view the information must witness the destruction of driver's license and motor vehicle records and files containing such records. If a private vendor is used for record destruction, the record holder employee must remain with the record until it is destroyed.

7-17. Quarterly Quality Control Reviews.

a. The Department's interagency agreement with DHSMV requires the completion of Quarterly Quality Control Reviews (QQCR) to ensure proper access and usage of driver and motor vehicle systems and information.

b. Each program office that has staff authorized for access to DAVID is responsible for ensuring QQCR(s) audits are completed and the number of misuses documented.

c. A QQCR Manual and template for documenting the Quarterly Reviews can be located on the Department's CJIS intranet page at http://eww.dcf.state.fl.us/cjis/, then click on "Audit Resources."

d. DHSMV DAVID has functionality providing each user agency with the ability to run audit reports for Department users.

e. The Judicial Inquiry System (JIS) does not have audit functionality for user agencies. The appropriate JIS point of contact shall contact OSCA JIS Support for assistance with obtaining transaction information for audits of Department JIS users.

f. The QQCR should be completed and documented each quarter.

(1) Each program conducting the QQCR needs to determine the appropriate number of users and user transactions to query and review.

(2) Audit reports can be run for a randomly selected week or month in the quarter. Audit reports can be run by individual or by Region. If an audit report is run by Region rather than for a specific individual user, then users and transactions with other programs may be included in the results.

(3) The staff member conducting the QQCR shall look for any misuse, including but not limited to, reason codes, running siblings/spouses, running celebrities/political figures, repeated runs of the same subject, access to ECI information, and times of day that access occurred.

(4) The Department shall maintain an agency list identifying all staff with DAVID accounts. Each month a review of all program DAVID users shall be completed. This review shall include comparing the agency list to the DAVID active user report to ensure current users are appropriately authorized for access. If updates to user access permissions are identified, the DAVID point of contact in the appropriate Regional Security Office shall be immediately notified for completing appropriate account access permissions.

(5) The Department must keep records of new/inactivated users since the last QQCR. This shall include logging dates and reasons for any changes to user account permissions. When completing each QQCR review the number of active DAVID users should be recorded on the QQCR form.

(6) Programs conducting the QQCR shall provide a completed DAVID QQCR Report Summary form located at http://eww/cjis/audits.shtml to the Department's DAVID Administrator. The DAVID Administrator will collect each Program Area(s) summary form and complete the DAVID QQCR summary form for the Department.

(7) DHSMV requires each QQCR to be completed within 10 days from the end of the previous Quarter.

Chapter 8

BACKGROUND CHECKS FOR ADULT PROTECTIVE INVESTIGATIONS

8-1. Purpose. This chapter provides procedures for requesting and obtaining criminal history, delinquency, and Florida Safe Families Network (FSFN) records required for adult protective investigations. It also provides information regarding the procedures for the Adult Protective Investigator's (API) use of information provided by the Crime Intelligence Unit (CIU).

8-2. Scope. This chapter is applicable to all Department of Children and Families employees involved in the investigation of adult abuse, neglect, or exploitation.

8-3. Authority. The following authorities and references apply throughout this chapter.

a. Florida Department of Law Enforcement (FDLE) Criminal Justice Agency User Agreement with the Department of Children and Families (DCF).

b. 28 Code of Federal Regulations (CFR), Subparts 20 (28 CFR 20) and 50 (28 CFR 50).

c. Section 943.045(11), F.S., Section 943.056, F.S., Section 985.045(1), F.S., Section 415.104, F.S., and Section 415.1045(6), F.S.

d. Rule 11C-6.004, Florida Administrative Code (F.A.C.).

8-4. Definitions. Terminology and definitions can be found in Chapter 1, paragraph 1-4 of this operating procedure.

8-5. Requirements.

a. Background checks are conducted as a result of a call to the Florida Abuse Hotline having been "accepted" due to meeting the statutory requirements for an investigation of suspected adult abuse, neglect, or exploitation.

(1) The Adult Protective Investigations component of the Department is defined as a Criminal Justice Agency in section 943.045(11), F.S.

(2) The API is required to obtain specific record types for protective investigations.

(3) A Background Check Job Aid is located on the Department's CJIS Intranet at http://eww/cjis/.

b. The following record documents shall be provided by the CIU, for the purpose of adult protective investigations, when sufficient demographic information is available:

(1) Q Document: Florida criminal history Rap Sheet from the Florida Criminal Information Center (FCIC) for subjects/participants who are age 12 and older.

(2) C Document: Florida criminal history Rap Sheet from the Florida Criminal Information Center (FCIC) for subjects/participants who are age 12 and older. This document is provided only if sealed/expunged or Hot File information is located during the FCIC Query.

(3) J Document: Delinquency history from the Juvenile Justice Information System (JJIS) for subjects/participants who are age 12 to 26.

(4) J Document: Driver license or State ID information from the Department of Highway Safety Driver and Vehicle Information DAVID Database for subjects/participants who are age 18 and older.

c. The Department is not authorized to conduct National criminal history record checks for the purpose of adult protective investigations.

8-6. Obtaining Records.

a. CIU procedures for the Hotline intake process are detailed in CFOP 170-2, Chapter 8, paragraph 8-7.

(1) When sufficient demographic information is available at the time of intake, the CIU will provide the record and document types as detailed in paragraph 8-5 of this operating procedure.

(2) CIU documents are made available via a hyperlink in FSFN. The process for viewing record check documents is detailed in the FSFN Background Screening User Guide and How Do I Guides.

(3) The availability of demographic information at the time of intake may affect the accuracy of record results.

(4) The availability of data sources at the time of intake may affect the accuracy of record results.

(5) Data source downtimes to include scheduled and unscheduled maintenance can impact availability.

(6) The CIU will provide a summary in the Q document alerting the API to any data sources not checked.

b. The CIU is unable to provide local records for in state or out of state law enforcement agencies. Methods for obtaining these local records from law enforcement can vary by jurisdiction and agency.

8-7. Other Data Sources. API units have access to data sources that may assist the API for purposes of protective investigations. Examples include:

a. Individuals under DOC supervision which can be searched on the Florida DOC website for Offender Information Search.

b. FDLE Sexual Offender and Predator Public Website which provides public information and photos on individuals registered as Sexual Offenders or Predators in Florida.

c. Dru Sjodin National Sexual Offender Public Website which provides public information and photos on individuals registered as Sexual Offenders or Predators in States in addition to Florida.

d. Florida Office of State Court Administrator’s Judicial Inquiry System (JIS) which provides the ability to obtain records from the following data sources:

(1) Comprehensive Case Information System (CCIS) which provides Florida Clerk of Courts case information. CCIS Access Request Forms are located on the Department’s website for Security Forms.

(2) DHSMV DAVID for use in protective investigations. Details specific to the usage of DAVID and driver information is detailed in Chapter 7 of this operating procedure.

e. Additional information on these data sources to include the access request process (when applicable) can be found on the Department's Criminal Justice Information Services intranet page.

8-8. Recheck Procedure.

a. During an investigation, the API shall submit a "Recheck" when additional Florida criminal history records are required or the API determines new record checks should be completed.

b. The API shall submit a recheck request for additional focus household members:

(1) When records were not previously provided by the CIU during intake within 24 hours of the subject being made known to the API.

(2) When a household member's demographic information has been updated and the API determines a need for a new record check to ensure accuracy or to obtain updated results.

c. Recheck requests are submitted to the CIU via functionality available in FSFN. The process for requesting Background Checks is detailed in the FSFN Background Screening User Guide and How Do I Guides.

d. To ensure information is obtained only for authorized purposes, recheck requests shall only be submitted by APIs for the purpose of investigations.

8-9. Analyzing Results.

a. Background check records, to include state criminal history records, are types of information collected and reviewed during pre-commencement.

b. When reviewing background check records, the API should assess historical and/or current records for conditions or behavior that may place the child in danger.

(1) Assessment for worker safety.

(a) History of assault and battery on other persons; and,

(b) Determination if law enforcement should be contacted to accompany the API to the home.

(2) Historical criminal history records and/or current charges to assess for risks.

(a) Patterns of aggravated assault, domestic violence, substance abuse, sexual assault or violent crimes; and,

(b) Identification of Hot Files, to include Sexual Predator/Offense File, Probation File, and Protection Orders, contained in the criminal history documents provided by the CIU.

8-10. Information Security.

a. Chapter 4 of this operating procedure provides the core requirements for the protection, proper usage, handling, documentation, dissemination, and storage of criminal justice information (CJI) to include criminal history records.

b. Record check documents provided by the CIU for adult protective investigations, via hyperlink located in FSFN, have additional security protections to ensure compliance with CJIS policies and agreements with FDLE.

(1) Access to documents provided by the CIU are restricted by FSFN and are associated with a user's Login Profile.

(2) Documents provided by the CIU and available via the hyperlink in FSFN have a 72-hour availability for viewing after which they will no longer be viewable from the link within FSFN.

(3) The C document has security settings restricting an API from printing, saving, or forwarding.

c. Criminal Justice Information, to include State criminal history records, shall only be released to authorized agencies and personnel.

d. State criminal history records containing sealed or expunged records, to include the C Document provided by the CIU, cannot be disseminated to contracted providers to include protective services case managers.

e. There are logging requirements for the dissemination of Criminal Justice Information to include State criminal history records and information.

(1) Requests submitted to the CIU from an intake or investigation are recorded and logged in FSFN.

(2) The dissemination of criminal history records or information to other authorized agencies requires logging in a Secondary Dissemination log.

(a) Secondary dissemination logging is detailed in paragraph 4-8 of this operating procedure.

(b) A copy of a Secondary Dissemination Log can be found on the Department's CJIS intranet page located at http://eww.dcf.state.fl.us/cjis/.

f. Criminal history records shall only be used for the reason they were obtained. The API will not use criminal history records obtained for an adult protective investigation for other purposes.

g. There are several improper uses of criminal justice information. Examples include, but are not limited to:

(1) Submitting a request to the CIU for State criminal history for unauthorized purposes.

(2) Querying systems to include but not limited to the Judicial Inquiry System (JIS) for other than authorized business purposes.

(3) Distributing information to unauthorized persons or agencies.

8-11. Documentation.

a. The FBI and FDLE have very specific guidelines regarding what criminal justice information can and cannot be documented in case notes or an agency's data base. Core requirements for criminal justice information documentation are detail in paragraph 4-6 of this operating procedure.

b. The following standardized wording is recommended when documenting results of “C” documents provided by the CIU in case notes for protective investigators: “The appropriate background checks were conducted on (date) for (individual’s name). The Protective Investigator has evaluated the information and reviewed for patterns of behavior or domestic violence that may pose a potential safety concern or elevated risk to a (child or vulnerable adult). At this time, (there appears to be) or (there does not appear to be) an immediate negative impact on the victim’s safety.”

Chapter 9

FINGERPRINT APPLICANT NOTIFICATION AND ACKNOWLEDGEMENT

9-1. Purpose. This chapter provides guidance to ensure that the Florida Department of Law Enforcement (FDLE) and Federal Bureau of Investigations (FBI) privacy act notification is provided to applicants submitting fingerprints and that acknowledgement forms are maintained for federal audits.

9-2. Scope. This chapter is applicable to all Department of Children and Families employees involved in tasks related to the submission of fingerprints by applicants for background screening purposes.

9-3. General Requirements. The Department is required to provide applicants, submitting fingerprints for the purpose of searching Florida and national criminal history records, with a notification specific to the retention of fingerprints, privacy policy, and the right to challenge an incorrect criminal history record.

9-4. Notification and Acknowledgement Procedure.

a. The Agency for HealthCare Administration's (AHCA) Clearinghouse has functionality that provides these notifications for screenings conducted using that system.

b. For screenings not conducted using the AHCA Clearinghouse, FDLE provides a notification and applicant notification form located in Attachments 1 and 2 to this chapter. Screenings by the Department not currently conducted using the AHCA Clearinghouse include employment by the Department and relative/non-relative placement for children in out-of-home care.

c. Where fingerprints are submitted via electronic fingerprint submission and how appointments are scheduled for the purposes of Department employment and relative/non-relative placement screenings can vary by region and/or circuit.

(1) To ensure compliance with federal and state policies, each region is responsible for establishing a process for providing the FDLE/FBI notification and acknowledgement form (Attachments 1 and 2 to this chapter) to fingerprint applicants, to include obtaining the applicants signature and acknowledgement, prior to or at the time of the electronic submission of fingerprints.

(2) When applicable, regions will need to consider if electronic fingerprinting vendors are used in the fingerprint submission process and how the notification and acknowledgement procedure might work in this instance.

9-5. Documentation Procedure. Each region is responsible for establishing a process for storing acknowledgement forms signed and completed by fingerprint applicants.

a. When applicable, regions will need to consider how completed acknowledgement forms will be obtained from electronic fingerprinting vendors.

b. Each region's CJIS Circuit Point of Contact shall be responsible for providing completed acknowledgement forms when requested during FDLE and/or FBI audits.

9-6. Applicant's Right to Challenge a Criminal History Record.

a. Any applicant has the right to receive Florida and national criminal record information obtained via fingerprint submission. This applies only to results obtained for non-criminal justice purposes via fingerprint submission and does not apply to criminal justice name-based checks of FCIC/NCIC. Name based results may not be released. Applicants requesting a copy of his/her Florida

criminal history record shall be referred to FDLE and/or a copy of his/her national criminal history record to the FBI for assistance.

b. An applicant may conduct a personal review of his/her criminal history record as provided in section 943.056, F.S., and Rule 11C-8.001, F.A.C., by contacting FDLE at (850) 410-7898. If an applicant believes the Florida criminal history record is in error, the applicant may contact FDLE to challenge the record at (850) 410-7898.

c. Applicants may receive any national criminal history record that pertains to him/her directly from the FBI pursuant to 28 CFR Sections 16.30-16.34. If a fingerprint applicant believes the national criminal history record is in error, he/she may contact the FBI at (304) 625-2000.

State of Florida
Department of Children and Families

Ron DeSantis
Governor

Shevaun L. Harris
Secretary

NOTICE FOR APPLICANTS SUBMITTING FINGERPRINTS FOR A CRIMINAL HISTORY RECORD CHECK

NOTICE OF:

- **RETENTION OF FINGERPRINTS,**
- **PRIVACY POLICY, AND**
- **RIGHT TO CHALLENGE AN INCORRECT CRIMINAL HISTORY RECORD**

This notice is to inform you when you submit a set of fingerprints to the Florida Department of Law Enforcement (FDLE) for the purpose of conducting a search for any Florida and national criminal history records that may pertain to you, the results of the search are returned to the authorized agency ORI indicated in the transaction. By submitting fingerprints, you are authorizing the dissemination of any state and national criminal history record that may pertain to you to the agency from which you are seeking approval to be employed, licensed, or have access to their facility. The fingerprints submitted are retained by FDLE and the Federal Bureau of Investigation (FBI), and FDLE will notify the agency of any subsequent arrests.

Your Social Security Account Number (SSAN) is needed to keep records accurate because other people may have the same name and birth date. Pursuant to the Federal Privacy Act of 1974 (5 U.S.C. § 552a), FDLE is responsible for informing you whether disclosure is mandatory or voluntary, by what statutory or other authority your SSAN is solicited, and what uses will be made of it. FDLE does not require a SSAN but it could cause a delay in processing your criminal record check.

Authorized agencies are allowed to release a copy of the state and national criminal record information to a person who requests a copy of his or her own record if the identification of the record was based on submission of the person's fingerprints. Therefore, if you wish to review your record, you may request a copy of your record from the screening agency. After you have reviewed the criminal history record, if you believe it is incomplete or inaccurate, you may conduct a personal review as provided in section 943.056, F.S., and Rule 11C-8.001, F.A.C., by calling FDLE at (850) 410-7898. If you believe the national information is in error, you may contact the FBI at (304) 625-2000. You can receive any national criminal history record that may pertain to you directly from the FBI, pursuant to 28 CFR Sections 16.30-16.34. You have the right to a reasonable time to obtain a determination as to the validity of your challenge before a final decision is made about your status as an employee, volunteer, contractor, or subcontractor.

The FBI's Privacy Statement follows on the next page and contains additional information.

PRIVACY ACT STATEMENT

Authority: The FBI's acquisition, preservation, and exchange of fingerprints and associated information is generally authorized under 28 U.S.C. 534. Depending on the nature of your application, supplemental authorities include Federal statutes, State statutes pursuant to Public Law 92-544, Presidential Executive Orders, and federal. Providing your fingerprints and associated information is voluntary; however, failure to do so may affect completion or approval of your application.

Social Security Account Number (SSAN): Your SSAN is needed to keep records accurate because other people may have the same name and birth date. Pursuant to the Federal Privacy Act of 1974 (5 USC 552a), the requesting agency is responsible for informing you whether disclosure is mandatory or voluntary, by what statutory or other authority your SSAN is solicited, and what uses will be made of it. Executive Order 9397 also asks Federal agencies to use this number to help identify individuals in agency records.

Principal Purpose: Certain determinations, such as employment, licensing, and security clearances, may be predicated on fingerprint-based record checks. Your fingerprints and associated information/biometrics may be provided to the employing, investigating, or otherwise responsible agency, and/or the FBI for the purpose of comparing your fingerprints to other fingerprints in the FBI's Next Generation Identification (NGI) system or its successor systems (including civil, criminal, and latent fingerprint repositories) or other available records of the employing, investigating, or otherwise responsible agency. The FBI may retain your fingerprints and associated information/biometrics in NGI after the completion of this application and, while retained, your fingerprints may continue to be compared against other fingerprints submitted to or retained by NGI.

Routine Uses: During the processing of this application and for as long thereafter as your fingerprints and associated information/biometrics are retained in NGI, your information may be disclosed pursuant to your consent, and may be disclosed without your consent as permitted by the Privacy Act of 1974 and all applicable Routine Uses as may be published at any time in the Federal Register, including the Routine Uses for the NGI system and the FBI's Blanket Routine Uses. Routine uses include, but are not limited to, disclosures to: employing, governmental or authorized non-governmental agencies responsible for employment, contracting licensing, security clearances, and other suitability determinations; local, state, tribal, or federal law enforcement agencies; criminal justice agencies; and agencies responsible for national security or public safety.

Additional Information: The requesting agency and/or the agency conducting the application investigation will provide you additional information pertinent to the specific circumstances of this application, which may include identification of other authorities, purposes, uses, and consequences of not providing requested information. In addition, any such agency in the Federal Executive Branch has also published notice in the Federal Register describing any systems(s) of records in which that agency may also maintain your records, including the authorities, purposes, and routine uses for the system(s).

APPLICANT NOTIFICATION AND ACKNOWLEDGEMENT

This form shall be completed and signed by every applicant for background screening purposes.

I hereby authorize the Florida Department of Law Enforcement (FDLE) to process a set of my fingerprints for the purpose of accessing and reviewing Florida and national criminal history records that may pertain to me to determine eligibility for employment.

I understand the following:

- My fingerprints may be retained at FDLE and the Federal Bureau of Investigation (FBI) for the purpose of providing notice of any subsequent arrests.
- FDLE will use local, state, and national law enforcement databases to conduct the criminal justice employment check.
- Upon request, FDLE may provide a copy of my criminal history record to me.
- A copy of any national criminal history record that may pertain to me can be obtained directly from the FBI.
- I am entitled to challenge the accuracy and completeness of any information contained in any such criminal history record pursuant to section 943.056, F.S., and Title 28 CFR Sections 16.30-16.34.
- I may obtain a prompt determination as to the validity of my challenge before a final decision is made regarding my status as an employee, volunteer, contractor, or subcontractor if it is the sole factor precluding my employment or unescorted access to the secure facility.

Signature:_____

Date:_____

Printed Name: _____ Date of Birth: _____

Chapter 10

CARETAKER SCREENING

10-1. Purpose. This operating procedure establishes standards and procedures for screening and re-screening of persons in positions designated by law to be screened as caretakers pursuant to Chapter 435, Florida Statutes (F.S.), Chapter 39, F.S., Chapter 110, F.S., Chapter 393, F.S., Chapter 394, F.S., Chapter 397, F.S., Chapter 402, F.S., Chapter 408, F.S., and Chapter 409, F.S.

10-2. Definitions. For the purposes of this operating procedure, the following definitions apply:

a. APD means the Agency for Persons with Disabilities.

b. Applicant, as used in this operating procedure, refers to the person being screened for employment, volunteer work, registration, or licensure.

c. Care Provider Background Screening Clearinghouse, known as “Clearinghouse” (CLH), is a web-based application and single data source that allows providers and state agencies to access Level 2 background screening information. The Clearinghouse is used to retrieve background screening results for persons screened for employment by or licensure of providers/facilities that provide services to children, the elderly, or disabled individuals. The Agency for Health Care Administration (AHCA) is charged with maintaining the Clearinghouse.

d. Caretaker Screening Information System (CSIS) refers to the statewide computer program utilized by the Department’s Background Screening Program and other background screening entities within the Department to track screenings for persons required to be screened pursuant to Chapter 435, Florida Statutes (F.S.), Chapter 39, F.S., Chapter 110, F.S., Chapter 393, F.S., Chapter 394, F.S., Chapter 397, F.S., Chapter 402, F.S., Chapter 408, F.S., and Chapter 409, F.S.. Only results received by the Background Screening Program are entered into the system. This system will become obsolete when the new workforce management system is completed.

e. Child Care refers to the provider/facility type that includes all owners, operators/directors, designated representatives, employees, or volunteers working with children’s programs. This does not include individuals who work in the facility after hours when children are not present or the parents/guardians of children in Head Start. The following also operate within the same statutes and are considered Child Care facilities:

(1) Family Day Care Homes include operators, substitutes, employees, and every household member over the age of 12 years old.

(2) Religious Exempt facilities include owners, operators/directors, employees, and volunteers who serve 10 hours or more per month. This does not include individuals who work in the facility after hours when children are not present.

(3) Enrichment Programs refer to individuals who provide language training, music instruction, educational instruction, and other experiences to specific children during a specific time that is not part of the regular program in a Child Care facility.

(4) Afterschool refers to a program that is operated and staffed directly by that school or through a formal agreement, such as a contract, between the school and a provider which names the school/school district as the responsible party for the operation of the program.

f. Child Welfare refers to the provider/facility type that includes residential Child-Caring Agencies, Child-Placing Agencies and Foster/Shelter-Group Homes (licensed out-of-home care).

Individuals screened includes directors and employees who have direct contact with clients and every household member aged 12 years and older residing in the home.

g. Clerk of the Court Websites, as used in this operating procedure, refers to online public record systems, by county, that allow for the search of a specific court case or individual.

h. Comprehensive Case Information System (CCIS), as used in this operating procedure, refers to a web-based information system that allows Background Screening personnel access to view Florida criminal records in reference to an individual or specific case search.

i. Department means Department of Children and Families (DCF).

j. FBI means Federal Bureau of Investigation.

k. Florida Crime Information Center (FCIC) refers to the State of Florida criminal history results retained by the Florida Department of Law Enforcement. In reference to this operation, Background Screening personnel review the FCIC, as obtained through the Level 2 screening, to determine employment eligibility.

l. FDLE means Florida Department of Law Enforcement.

m. Florida Safe Families Network (FSFN) refers to is the Department's current Comprehensive Child Welfare Information System (CCWIS) used by child and adult protective investigations and services. The Background Screening Program uses this application to perform child abuse and neglect checks prior to an individual's eligibility determination.

n. Illegible/Rejected Prints refers to FBI criminal history results indicating that the applicants' fingerprints were illegible due to low quality of fingerprints or a scanning error. A Transaction Control Reference (TCR) number is provided by the FBI with the rejected fingerprint response, allowing the applicant to submit a second set of fingerprints within 180 days without incurring a second screening charge.

o. Initial Screening ("Primary Screening") refers to the first screening completed as an act of original employment, hiring, licensing or contracting, prior to starting employment, licensure, or contracting. An initial screening may also occur following a 90-day break in employment from a position for which an individual acquired an initial screening. An approved leave of absence does not constitute a break in employment.

(1) "Level 1 Screening" refers to a screening required by law for all individuals to complete the Level 1 screening requirements. These are name-based screenings requested through FDLE.

(a) Level 1 screenings completed pursuant to section 435.03, F.S. are also granted for adult household members who have a physical, developmental, or cognitive disability that prevents that person from safely submitting fingerprints.

(b) All exempted individuals must submit a Request for Fingerprint Exemptions and be approved by the Department. Screening requests are submitted manually or electronically.

(2) "Level 2 Screening" refers to a screening required by law for employment, licensure, volunteers, and registration as directed by Florida Statutes. A Level 2 screening differs from a Level 1 screening in that it is fingerprint based and a national criminal history check is required.

(3) A program may have additional screening requirements as identified in program specific statutes or rules (e.g., local criminal history, employment history, references, etc.).

p. Judicial Information System (JIS) is a web-based browser interface administered by the Office of State Court Administrators (OSCA) that provides the capability to query multiple Florida agency data sources. For the purposes of this operation, the Background Screening Program has access to JIS to view criminal history records for individuals being screened for employment or licensure.

q. Licensing Entity refers to the government entity responsible for issuance of a license.

r. Licensing Agency refers to the entity, government, or non-government, responsible for training prospective licensees and submitting all necessary documentation to the Licensing Entity or Regulatory Authority.

(1) Some counties have their own “Local Licensing Agency.”

(2) These agencies serve to license local Child Care facilities and homes whose licensing standards meet or exceed state minimum standards within that specific county.

s. Live Scan is a device used for the electronic submission of fingerprints.

t. Medicaid Waiver System refers to a Medicaid program that provides home and community-based supports and services to eligible persons with developmental disabilities living at home or in a home-like setting. This system is maintained by APD under the authorization of the Agency for Healthcare Administration, Division of Medicaid.

u. National Crime Information Center (NCIC) refers to the national criminal history results from all states and territories retained by the FBI and/or other state repositories. In reference to this operating procedure, Background Screening personnel review the NCIC, as obtained through the Level 2 screening, to determine employment eligibility. Such records are confidential except to other governmental agencies under specific circumstance and must not be shared outside of the Department.

v. Name Check Only (NCO), or “Name Search” refers to a request sent to the FBI to conduct a search for criminal history results using only the person’s government-recognized name. For the purposes of this operating procedure, the Background Screening Program utilizes this type of search when an applicant’s Live Scan fingerprinting has resulted in two sets of illegible fingerprints.

w. National Fingerprint File (NFF) refers to the program in which duplicate criminal history record searches for states participating in the program are eliminated. Child Care providers/facilities can utilize the national criminal history results obtained through the Level 2 screening to satisfy the out-of-state criminal history requirement for applicants who have retained residency in a participating state within the past five years.

x. Originating Case Agency Number (OCA) refers to the identification number issued by the Background Screening Program through the CSIS program. It is the key to identifying the provider/agency requesting the background screening or for whom the background screening is being completed. This is a unique number generated by the CSIS system or converted from a legacy system. When registered with FDLE for Live Scan submissions, the OCA is prefaced with the two-digit district number and ends with a “Z” (e.g., 03011234Z). This differs from an ORI, which is assigned to qualified governmental entities by the FBI.

y. Originating Agency Identifier (ORI) refers to the nine-character identifier assigned by the FBI Criminal Justice Information Services (CJIS) staff to an agency which has met the established

qualifying criteria for ORI assignment. It identifies agencies in transactions on the NCIC system as well as for the submission of fingerprints:

(1) EDCFGN10Z – Child Placing and Residential Child Care Agencies, Chapter 39 Subcontracted Providers who Tutor and Mentor.

(2) EDCFGN10Z – Child Care Facilities, Family Day Care Homes, Religious Exempt, After School Programs, Child Enrichment Programs, Membership Organizations, Registered Family Day Care Homes, Private Charter Schools.

(3) EDCFGN10Z – Substance Abuse (Adults Only) determination based on MH criteria.

(4) EDCFMH20Z –Substance Abuse and Mental Health, Substance Abuse (Adults and Children), Mental Health Only, Chapter 39 Subcontracted Facilities who provide Psychological, Mental Health Counseling, Assessment, Therapy, and Behavioral Counseling.

(5) EDCFSC30Z – Summer Camp.

(6) EAPDGN10Z – APD General, Group Homes, Medicaid Wavier.

(7) EAPDFC20Z – APD CDC Plus Programs.

(8) EAPDDD30Z – APD Developmental Disability Centers.

(9) FL9XXXX5Z – Caretaker State Employees.

z. Re-Arrest refers to an automatic notification received by the Clearinghouse through FDLE. This notification references the recent arrest of an applicant who is on a provider/facility's employee roster in CLH. The Background Screening Program utilizes this notification to determine necessary updates made to the applicant's eligibility within the Clearinghouse.

aa. Regulatory Authority refers to the government entity responsible for the oversight of a service provider/facility.

bb. Membership Organizations, as used in this operating procedure, refers to providers/facilities affiliated with national organizations which do not provide Child Care, whose primary purpose is providing activities that contribute to the development of minors in this state. These organizations charge only a nominal annual membership fee, are not for profit; and are certified by their national associations as following the association's minimum standards and procedures.

cc. Mental Health refers to the provider/facility type that includes all program directors, professional clinicians, employees, and volunteers working in public or private mental health programs and facilities who have direct contact with individuals held for examination or admitted for mental health treatment where the primary purpose of the facility is the treatment of minors.

dd. Peer Specialist refers to a person who:

(1) Has been in recovery from a substance-use disorder or mental illness for at least two years, who uses his or her personal experience to provide services in behavioral health settings to support others in their recovery; or,

(2) Has at least two years of experience as a family member or caregiver of an individual who has a substance-use disorder or mental illness.

ee. Recovery Residence/Sober Home refers to a residential dwelling unit, the community housing component of a licensed day or night treatment facility with community housing, or other form of group housing, which is offered or advertised through any means, including oral, written, electronic, or printed means, by any person or entity as a residence that provides a peer-supported, alcohol-free, and drug-free living environment.

ff. Renewal, as used in this operating procedure, refers to the initiation within the Clearinghouse to renew an applicant's retained fingerprints. This must happen every five years to maintain eligibility for employment. The employer must request a Renewal prior to the retained print's expiration date.

gg. Re-screening refers to the initiation of a Level 2 screening for the continued employment, licensure, or contracted status of an applicant within the Clearinghouse. Everyone is required to be re-screened at five-year intervals following the completion of his or her initial screening. The five-year re-screen is also required for juveniles.

hh. Resubmission, as used in this operating procedure, refers to a type of screening initiated in the Clearinghouse that resubmits an applicant's retained fingerprints to generate new FDLE and FBI criminal history results. This is typically conducted when there has been a lapse in an applicant's employment for greater than 90 days.

ii. Sealed Record, as used in this operating procedure, refers to a record that has been sealed by the court, pursuant to section 943.059, F.S., and is not available to the general public. It can be opened for inspection by the individual, his/her attorney, a criminal justice agency, and those entities set forth in section 943.059(4)(a)5., F.S., for their perspective licensing and employment purposes. Sealed records are not public records and require special handling.

jj. Shelter Homes (Homeless) refers to services provided to individuals who lack a fixed, regular, and adequate nighttime residence or those living in shelters and temporary housing, or public and private places not designed for sleeping accommodations (e.g., on the street, in cars or parks, etc.).

kk. Volunteer refers to an unpaid helper who assists on an intermittent basis for less than 10 hours per month in most programs, or 40 hours per month in substance abuse programs. This individual is not considered a caretaker, provided the individual is under direct and constant supervision of/by persons who meet Level 2 screening requirements. At no time may any child or developmentally disabled adult be left alone with a volunteer unless the volunteer has met Level 2 screening requirements. Level 2 screening requirements are based on fingerprints submitted under a government issued Social Security Number or government issued Individual Taxpayer Identification Number (ITIN) for international volunteers.

ll. Voluntary Pre-Kindergarten (VPK) refers to a pre-kindergarten program, established by the 2005 Legislature, with special funding for providers and available to all children within the state who will attain the age of 4 on or before September 1 of the school year, allowing them to attend either a private or public pre-kindergarten program. This group includes individuals already required to be screened as employees working in programs in private schools with children under the age of 5, facilities exempt from licensure, and licensed childcare centers.

10-3. Scope. This chapter applies to state employees, personnel in child care, contracted children's programs, mental health programs, substance abuse service provider personnel, those working with children and the developmentally disabled, child foster care, and residential child-caring and child-placing agencies, Shelter Homes, Recovery Residences, Membership Organizations, Summer Camps, and direct service providers of the Agency for Persons with Disabilities. All the above are subject to

Level 2 screening. This chapter also applies to volunteers in programs where volunteers are required to be screened.

10-4. Screening Procedure.

a. Establishing a Facility OCA (Identification Number).

(1) The Background Screening Program receives a request or inquiry for an OCA number from the licensing entity or regulatory authority. The Background Screening Program will assist individuals as needed in identifying the regulatory authority and the appropriate program office.

(2) If it is determined that the provider is eligible for a Facility OCA, a search of CSIS should be conducted to ensure the provider does not have an existing Facility OCA.

b. Submission of Information for Initial Screening.

(1) The applicant will complete a notarized Affidavit/Attestation of Good Moral Character attesting to their eligibility and submit it to his or her employer, licensing entity, or regulatory authority in accordance with program specific rules or policies.

(2) The employer, licensing entity, or regulatory authority must ensure that the applicant submits fingerprints and any additional required information necessary for the Background Screening Program to determine eligibility prior to employment or access/contact with any vulnerable person.

(3) The request for local criminal history is the responsibility of the licensing entity, regulatory authority, or provider, if applicable. The Background Screening Program may aid with interpretation as requested.

c. Completion of Background Screening for Child Welfare. All background screenings for child welfare purposes, including the placement of children, must be completed within 14 business days after receiving a person's criminal history results, unless additional information is required to complete the screening.

d. Evaluation of Criminal History Results and Determining Eligibility.

(1) Criminal History results received from FDLE and the FBI, as well as any action taken and/or final eligibility determinations made, are required to be recorded, updated, and maintained in the Clearinghouse and the CSIS database by the Background Screening Program.

(2) If the Department receives a result from FDLE and/or the FBI that identifies any criminal history, the Background Screening Program will determine eligibility pursuant to the applicable criteria required by law. It is the Background Screening Program's responsibility to verify eligibility based on resources such as CCIS, JIS, Clerk of the Court Websites, CSIS, and any available internal resources.

(3) If an applicant is determined "Eligible," the Background Screening Program will update the eligibility status in the Clearinghouse. This sends an automatic notification to the provider/facility notifying them that they may retrieve the applicant's results. This determination does not imply a recommendation for or against employment or licensure. Employment eligibility is made solely by the provider/facility.

(4) If the applicant is determined "Not Eligible" based on the criminal history results received, the Background Screening Program will notify the applicant in writing. If the applicant is

determined “Not Eligible” based on results from a Re-Arrest notification, the Background Screening Program will notify the applicant in writing and the licensing program by email.

(5) If additional information is received by the Background Screening Program, an electronic file in CSIS will be created. The electronic file will be retained by the Background Screening Program which can include, but is not limited to, the following:

(a) Criminal history results;

(b) Correspondence; and,

(c) Other miscellaneous documents submitted by the applicant.

(6) If the applicant does not provide requested documentation within 30 calendar days of the date of the letter for additional information, the applicant will be determined “Not Eligible” until the documentation is received, and a determination is able to be made.

e. Confidentiality and Sharing of Screening Information.

(1) All information obtained through the screening process is exempt from public disclosure and may not be used for any purpose other than determining whether the person meets the minimum standards for the required screening process as outlined in section 119.07(1), F.S.

(2) The sharing of FDLE criminal history information obtained through the screening process is restricted to employment or licensure purposes.

(a) Sealed and expunged information is privileged information and cannot be shared with providers.

(b) Any national information obtained by the Background Screening Program cannot be shared with providers. This includes any national information obtained from FDLE.

(c) As per section 435.10, F.S., any background screening information obtained by providers can be shared with other providers or the Department only for employment or licensure purposes.

f. Records Management. Records shall be retained in accordance with the Department’s Records Management Procedure.

Chapter 11

EXEMPTION FROM DISQUALIFICATION

11-1. Purpose. This chapter provides guidance to process exemption requests for persons disqualified pursuant to Chapter 435, Florida Statutes (F.S.).

11-2. Definitions. For the purposes of this operating procedure, the following definitions apply:

a. “APD” means the Agency for Persons with Disabilities.

b. “Applicant” means the person requesting an exemption from disqualification from employment, volunteering, registration, or licensure.

c. “Care Provider Background Screening Clearinghouse”, known as “Clearinghouse,” is an information system that the Background Screening Program utilizes to document screenings completed by the Department for care providers.

d. “Clear and Convincing Evidence” is a heavier burden than the preponderance of the evidence standard but less than beyond a reasonable doubt. It means that the evidence presented is credible and verifiable, and that the memories of witnesses are clear and without confusion. The evidence must create a firm belief and conviction of the truth of the facts presented and, considered as a whole, must convince the Department representatives, without hesitancy, that the requester will not pose a threat if allowed to hold a position of special trust relative to children, vulnerable adults, or to developmentally disabled individuals.

e. “Department” means the Department of Children and Families.

f. “FDLE” means the Florida Department of Law Enforcement.

g. “FBI” means the Federal Bureau of Investigation.

h. “Verifiable” means that the documentation contains enough information to contact the issuing person/entity should any reviewer wish to substantiate the document or obtain additional information.

11-3. Disqualifying Screenings Results.

a. The Department shall have Background Screening Coordinators that are responsible for reviewing and determining disqualifying criminal history pursuant to sections 435.04 and 408.809, 39.0138, 402.302 and/or 393.0655, F.S.

(1) The Background Screening Coordinator will prepare a disqualification letter to the applicant detailing the criminal offense(s) that render him or her not eligible under section 435.04, F.S.

(2) The Background Screening Coordinator will update the applicant profile to indicate a status of “Not Eligible” in the Clearinghouse as a notification to the employer.

b. If a disqualifying offense is identified for which an exemption is statutorily permitted, the Background Screening Coordinator will notify the applicant of the opportunity to request an exemption from disqualification. If the offense is permanently disqualifying, the Background Screening Coordinator will prepare a letter that notifies the applicant that he or she is not eligible to request an exemption from disqualification.

c. All letters sent to the applicant regarding permanent disqualification from employment, licensure, or registration must be sent by certified mail, return receipt requested with a notice that he or she has the right to appeal the Department's decision.

11-4. Eligibility to Request.

a. An applicant that has received a notice of disqualification or termination from employment based on criteria in sections 435.03, 435.04, 408.809, or 393.0655, F.S., may apply for an exemption from such disqualification, in writing, if the offense is one for which an exemption may be granted pursuant to section 435.07, F.S. The provisions of that section are to be strictly construed when considering a request for exemption from disqualification.

b. The three-year waiting period related to the commission of a felony begins after the applicant has completed or been lawfully released from confinement, supervision, or nonmonetary condition for the disqualifying felony.

c. For a disqualifying felony offense committed as a juvenile and for which the applicant was adjudicated delinquent, an exemption may not be granted until at least three years after the completion of confinement, supervision, or nonmonetary condition for the offense.

d. An individual who has committed a misdemeanor is eligible for consideration for an exemption after the applicant has completed or been lawfully released from confinement, supervision, or nonmonetary sanction for the disqualifying offense.

e. An individual that has committed a felony that has since been reclassified and is now considered to be a misdemeanor is eligible to apply for an exemption after the applicant has completed or been lawfully released from confinement, supervision, or nonmonetary sanction for the disqualifying offense.

f. An individual that was ordered to pay any amount for any fee, fine, fund, lien, civil judgment, application, costs of prosecution, trust, or restitution as part of the judgment and sentence for any disqualifying felony or misdemeanor must pay the court-ordered amount in full before he or she is eligible for the exemption.

g. A person employed or applicants for employment, by treatment providers who treat adolescents 13 years of age and older who are disqualified from employment solely because of crimes under sections 796.07(2)(e), 810.02(4), 812.014(2)(c), 817.563, 831.01, 831.02, 893.13, or 893.147, F.S., or any related criminal attempt, solicitation or conspiracy under section 777.04, F.S., may request an Exemption from Disqualification without applying the waiting period.

h. An individual designated as a sexual predator, career offender, or sexual offender is not eligible for an Exemption from Disqualification, unless the requirement to register as a sexual offender has been removed pursuant to section 943.04354, F.S.

i. Any individual identified as Child Care Personnel who has a permanent disqualifying offense as outlined in section 435.07(4)(c), F.S., is not eligible for an Exemption from Disqualification.

j. If 5 years or more, or 3 years or more for any certified peer specialist or an individual seeking certification as a peer specialist, have elapsed since an applicant for an exemption from disqualification has completed or been lawfully released from confinement, supervision or a nonmonetary condition from the applicant's most recent disqualifying offense, the applicant may work with adults with substance use disorders or co-occurring disorder under the supervision of persons who meet all personnel requirements outlined in section 397.4073, F.S., for up to 90 days while applying for the Exemption from Disqualification.

k. For Substance Abuse service providers that treat adolescents 13 years of age and older, service provider personnel whose background checks indicate crimes under sections 796.07(2)(e), 810.02(4), 812.014(2)(c), 817.563, 831.01, 831.02, 893.13, or 893.147, F.S., and any related criminal attempt, solicitation or conspiracy under section 777.04, F.S., **shall** be exempted from disqualification for those offenses if:

(1) At least 5 years, or at least 3 years in the case of an individual seeking certification as a peer specialist under section 397.417, F.S., have elapsed since the applicant requesting an exemption has completed or has been lawfully released from any confinement, supervision, or nonmonetary condition imposed by a court for the applicant's most recent disqualifying offense; and,

(2) The applicant has not been arrested for **any** offense during the 5 years, or 3 years in the case of a peer specialist, before the request for exemption.

11-5. Exemption Request Requirements.

a. It is the responsibility of the applicant to present clear and convincing evidence that he or she should be exempted from disqualification.

b. In order to be considered for an exemption from disqualification, the applicant must meet the burden of clear and convincing evidence that he or she should be exempted from disqualification. Evidence that may support a decision to grant an exemption includes, but is not limited to:

(1) Personal reference(s). The person reviewing the request for exemption should consider whether the reference document includes a date, original signature, an indication of how the applicant is known to the writer, the time lapse from the date of the recommendation and the date of the application, and a telephone number for contact, if needed;

(2) Letters from employers or other professionals. The person reviewing the request for exemption should consider whether employer or professional reference letters are provided on business letterhead, are relevant, and provide an original signature, signature date, and telephone number for contact, if needed;

(3) Evidence of rehabilitation, including documentation of successful participation in a rehabilitation program;

(4) Evidence of further education or training;

(5) Evidence of community involvement (examples include documentation of involvement in a civic organization, volunteer activities, church, etc.);

(6) Evidence of special awards or recognition;

(7) Evidence of military service, including whether such service is documented by Department of Defense Form 214; and,

(8) Parenting or other caregiver experiences.

c. Each person reviewing the request for exemption should carefully consider whether each evidentiary item provided in support of the request for exemption is verifiable.

d. Other factors to consider when determining whether to grant the exemption include, but are not limited to, the following:

(1) All available criminal history background information, including records, if available, from FDLE, the FBI, local police, or sheriff's offense incident reports and arrest affidavits, and pertinent court documents including case disposition and the applicant's plea. For disqualifying offenses, if the criminal history information is no longer available, the applicant will submit a notarized statement outlining the circumstances of the offense and any probation or other sanctions ordered and the status of the sanctions.

(2) Any information provided by the applicant regarding how he or she became involved in the incident and assurances that such an incident could not recur. Information may include:

(a) Documentation as to the status of any imposed conditions as a result of the applicant's offense or subsequent offenses;

(b) The length of time between the disqualifying event and the request for exemption, and any subsequent law violations, whether disqualifying or not;

(c) The severity of the harm or risk of harm to the victim or victims, including the degree of harm caused, any permanent or temporary injuries suffered, and restitution made as result of the applicant's actions; or,

(d) Any other history or circumstances indicating that employment can be continued without risk of harm.

(3) In the case of applicants seeking exemptions from disqualification from employment, licensure or registration for child welfare and child care programs, the person reviewing the request for exemption may include the use of any verified abuse reports where the applicant was identified as the person responsible or when the applicant is a subject in three or more abuse reports within a five-year period. For programs other than child welfare and childcare, verified reports can be used to evaluate the appropriateness of granting an exemption.

11-6. DCF Exemption Requests. If an applicant requests an exemption that is statutorily permitted, the Exemption Coordinator shall forward the following necessary forms to the applicant requesting an exemption review:

a. Request for Exemption form;

b. Exemption Application form;

c. Checklist form for materials needed for exemption consideration which will include directions for submitting the requested documents; and,

d. Employment History form.

11-7. Additional Required Documents.

a. Certified court dispositions for all disqualifying offenses and non-disqualifying offenses less than 10 years old.

b. Arrest report, charging affidavit, or citation for all disqualifying offenses and non-disqualifying offenses less than 10 years old.

c. Non-disqualifying offenses 10 years old or greater do not need court dispositions or arrest reports; however, they must be addressed by the applicant in the Exemption application.

d. Any required court disposition(s) or arrest documentation that is no longer available, a statement from the court of jurisdiction or law enforcement agency that the record does not exist or has been destroyed is acceptable.

11-8. Completion of Application.

a. After receipt of the exemption request package from the applicant, the Exemption Coordinator will, using due diligence, review the documents for completion. If information is missing, the Exemption Coordinator will notify the applicant in writing by mail and email.

b. The Exemption Coordinator will also search available data, including, but not limited to, a review of records from FDLE, the court system data base, the FBI, local police or sheriff's offense incident reports, and pertinent court documents including case disposition and the applicant's plea in order to determine the appropriateness of granting the applicant an exemption. These materials, in addition to the information provided by the applicant, will form the basis for a recommendation as to whether the exemption should be granted.

c. The Exemption Coordinator shall search the Caretaker Screening Information System (CSIS) to determine prior licensure or other caregiver positions and gather information that may be pertinent to the issue of rehabilitation from the disqualifying offense. The search of CSIS shall include a determination whether the applicant has ever been considered for an exemption prior to the current application, and the results of any previous applications.

d. After all available evidence is gathered and the exemption packet is complete, the Exemption Coordinator shall forward the exemption file to the General Counsel's Office for review by the Agency Clerk or designee.

e. The exemption request file shall be reviewed by the General Counsel's office to determine legal sufficiency.

f. The exemption request file will be prepared for review by a panel to make an initial recommendation to grant or deny the exemption. The panel consists of the Background Screening Assistant Director, a representative from Human Resources, and a representative from the Substance Abuse and Mental Health Program Office.

g. After the panel makes a recommendation, the exemption summary and recommendation shall be prepared for the Chief of Staff or the Secretary's Designee for final determination.

h. Whether the exemption is granted or denied, the decision must be documented in the applicant's exemption request file by copy of the decision letter and completion of the Exemption Review Report Routing Sheet. The Routing Sheet will contain dates and signatures of the review. The Exemption Coordinators are responsible for maintaining the exemption files.

i. At no point during the evaluation process shall an evaluator rely on state or federal criminal history reports with an effective date that is more than 60 days old. If the most recent criminal history report, state or federal, is more than 60 days old at the time of review, new criminal history reports must be generated prior to the final decision being made.

j. After an exemption request decision is final, the Exemption Coordinator will provide a written response to the applicant. The letter will be prepared with the Secretary's signature.

(1) If the exemption is granted, the applicant shall be notified of the decision by regular mail. The Exemption Coordinator will update CSIS and the Clearinghouse. The facility or employer will obtain the updated eligibility through the Clearinghouse.

(2) If the request is denied, in whole or in part, notification of the decision shall be sent by certified mail, return receipt requested, to the applicant, addressed to the last known address.

k. Notification to the applicant of the Department's decision shall be made no later than 30 days following the receipt of the complete exemption request package from the applicant, all requested missing documentation from the applicant, or the new criminal history report(s) if required as provided in paragraph i above, whichever is the latest.

11-9. Exemption Transferability. If an individual who has been granted an exemption by APD or any other agency applies to the Department for an exemption, the Department shall consider the prior grant of an exemption but is not bound by any previous exemption pursuant to DCF's obligations to review disqualifications from employment.

11-10. Limitations of an Exemption. The Department has the authority to grant exemptions from disqualification to work solely in mental health treatment facilities, or in programs or facilities that treat co-occurring substance use and mental health disorders. No other limitations are permitted.

11-11. APD Exemption Requests.

a. If an applicant requests an exemption that is statutorily permitted, the Exemption Coordinator shall forward the necessary forms to the applicant requesting an exemption review:

(1) APD Request for Exemption form;

(2) Checklist form for materials needed for exemption consideration which shall include directions for submitting the Exemption Request Package;

(3) Employment History form;

(4) APD Affidavit of Good Moral Character; and,

(5) Certified Court Dispositions and Arrest Reports or Charging Affidavits for all disqualifying criminal offenses.

(6) Court Dispositions and Arrest Reports or Charging Affidavits for all offenses charged after the first disqualifying offense, however, they are not required to be certified.

(7) For criminal offenses prior to the first disqualifying offense, no documentation will be required.

b. After receipt of the exemption request package from the applicant, the Exemption Coordinator will, using due diligence, review the documents for completion. If information is missing, the Exemption Coordinator will notify the applicant in writing by mail or email. The Exemption Coordinator will also search available data, including, but not limited to, a review of records from FDLE, the court system data base, the FBI, local police or sheriff's offense incident reports, and pertinent court documents including case disposition and the applicant's plea in order to determine the appropriateness of granting the applicant an exemption. These materials, in addition to the information

provided by the applicant, will form the basis for a recommendation as to whether the exemption should be granted.

c. The Exemption Coordinator shall search CSIS to determine prior licensure or other caregiver positions and gather information that may be pertinent to the issue of rehabilitation from the disqualifying offense. The search of CSIS shall include a determination whether the applicant has ever been considered for an exemption prior to the current application, and the results of any previous applications.

d. After all reasonable evidence is gathered during the exemption review, the Exemption Coordinator shall upload the file into CSIS and notify APD that the file is complete and ready for their review.

e. The Exemption Coordinator will notify the applicant when the exemption has been transferred to APD for determination.

f. The exemption request file shall be reviewed by APD's General Counsel's Office to determine legal sufficiency. Such review and determination shall not be done by the Department, unless otherwise agreed to by the Department and APD.

g. The Department's reviewers are not involved in the APD exemption request review process.

h. If APD determines that the exemption should not be granted, the Exemption Coordinator shall be informed, and the denial shall be communicated in writing to the applicant and the employer by APD.

i. If APD determines that the exemption should be granted, the applicant will be notified in writing by APD, and the Exemption Coordinator shall be informed, and the determination documentation returned to the Exemption Coordinator.

j. Whether the exemption is granted or denied, the decision must be documented in the applicant's exemption request file. The Exemption Coordinators are responsible for maintaining the exemption files.

11-12. Exemption Duration. If an exemption is granted, there shall be no limitation in the duration of the exemption except as provided by statute.

11-13. Subsequent Disqualification. If an employee for whom an exemption has been granted is subsequently arrested for or found guilty of, regardless of adjudication, or entered a plea of nolo contendere or guilty to any new disqualifying offense as provided in Chapters 393, 408. and 435, F.S., the employee is disqualified from employment. The employee must, if he or she wishes to again become employed and is otherwise eligible to seek an exemption, seek a new exemption from disqualification. The previously granted exemption must be identified as no longer being valid due to a subsequent disqualification in any Department maintained computer system that tracks exemptions or identifies persons with currently valid exemptions.

11-14. Security of Criminal History Records. All records of criminal background information gathered for the process of determining whether an exemption should be granted must be maintained in strict compliance with the Interagency Agreement between the Department and FDLE. This Agreement requires, among other things, that the records be maintained separately from any other departmental records, including personnel records, and that they be kept in a secure environment.

11-15. Right to Administrative Hearing (section 120.57, F.S.). The denial letter will include standard language notifying the applicant of his or her right to an administrative hearing and the requirement to submit the request to the Agency Clerk within 21 days from the date of receipt of the denial letter.

Chapter 12

CRIMINAL BACKGROUND CHECKS FOR CHILD CARE PERSONNEL

12-1. Purpose, Scope and Authority. This chapter provides guidance for caretakers subject to Level 2 screening under the following sections of Florida Statutes (F.S.):

a. Section 402.301, F.S. relating to national membership organizations.

b. Section 402.302, F.S. relating to transient establishments.

c. Section 402.305, F.S., relating to child care facilities and specialized child care facilities for the care of mildly ill children.

d. Section 402.3025, F.S., relating to nonpublic schools.

e. Section 402.3131, F.S., relating to licensed large family child care homes.

f. Section 402.313, F.S., relating to registered and licensed family day care homes.

g. Section 402.3054, F.S., relating to child enrichment service providers.

h. Section 402.316, F.S., relating to religious exempt child care programs.

i. Section 409.175, F.S., relating to summer day camps and summer 24-hour camps.

j. Section 1002.88, F.S., relating to informal child care providers participating in the school readiness program.

12-2. Definitions. See Attachment 1 to this chapter.

12-3. Required Components of Screening. Pursuant to section 402.302, F.S., the Department will determine screening eligibility for licensure, registration, employment, and/or volunteer service based on results of the following:

a. Employment history checks for the previous 5 years of employment;

b. A search of the criminal history records, sexual predator, and sexual offender registry of any state in which the applicant resided during the preceding 5 years, and child abuse and neglect registry; and,

c. A Child Care Affidavit of Good Moral Character (form CF 1649A, available in DCF Forms).

12-4. Establishing a Facility Originating Case Agency Number (Facility OCA). The Background Screening Program obtains information and determines if the provider is one whose employees must be screened in accordance to law, and, if so, which program and statute listed in paragraph 12-1 of this operating procedure governs the provider. This will include a written description from the appropriate licensing entity or regulatory authority. If the provider is eligible for a Facility OCA, a search of the Caretaker Screening Information System (CSIS) should be conducted to ensure the provider does not have an existing Facility OCA. The Facility OCA will be issued or reactivated by the Background Screening Program and email notification send to provider and copying licensing entity.

12-5. Initial Screening Procedure.

a. Fingerprint Submission. A full set of fingerprints must be submitted to the Department or to a vendor, entity, or agency authorized in section 943.053(13), F.S. The fingerprint submission must comply with the requirements of section 435.12, F.S., relating to the Clearinghouse. Visit www.myflfamilies.com/backgroundscreening for training materials on how to use the Agency for Health Care's Clearinghouse system. The provider must initiate the screening in the Clearinghouse prior to the applicant's arrival at a live scan vendor location. Failure to do so may result in the Department's inability to determine eligibility for child care programs.

(1) The vendor, entity, or agency shall forward the fingerprints to the Department of Law Enforcement for state processing.

(2) The Department of Law Enforcement shall forward the fingerprints to the Federal Bureau of Investigation for national processing.

(3) After processing by the Federal Bureau of Investigation, the Department of Law Enforcement shall forward the results to the Department.

b. Other States of Residence. If an applicant has lived outside of Florida in the last five years, a request for a state criminal history is required.

(1) If applicant has lived outside the state of Florida in the last five years as indicated during the initiation of the screening, a request to each state for a state criminal history check must be initiated by the provider or applicant. Information for obtaining out of state criminal history is found at www.myflfamilies.com/backgroundscreening. The Background Screening Program will document the screening is in process while awaiting out of state criminal history results in the criminal history tab of the Clearinghouse. The documentation will identify the state or territory required. The provider must provide the results of the out of state searches to the Department for completion of the background screening process.

(2) If the applicant lived outside the state of Florida in the last five years, review of the Florida's Level 2 requirements will occur.

c. Abuse and Neglect Search.

(1) The background screening unit will conduct a child abuse and neglect search in the Florida Safe Families Network system (FSFN) for the State of Florida. The FSFN search is conducted using the following demographic fields: applicant's last name, first name, date of birth and Social Security number (SSN). DO NOT enter the applicant's middle initial in the search string, as this may limit results. Instead, cross-reference the middle initial with the search results. The following search string combinations must be conducted:

(a) Each field must be completed for a combined search;

(b) Name (first and last) and date of birth without social security number; and,

(c) Social security number only. (The SSN field will dominate the search and could cause a subject to be overlooked if SSN was entered incorrectly or no SSN was entered for subject.)

(2) If the applicant has a prior name, each of the above searches must also be conducted for each prior name.

(3) The findings of the search of FSFN will be noted on the individual's profile page in the Clearinghouse.

(4) The employer/owner/operator must send a request for a search of each state's child abuse and neglect registry for each individual that has lived outside the state of Florida in the preceding five years. Instructions can be found at http://www.myflfamilies.com/backgroundscreening, Out of State Abuse Registry Check link. The results will be maintained in the employee personnel file.

d. Employment History Check. The employer must conduct an employment history check, including, at a minimum, three documented attempts to contact each prior employer of the applicant within the preceding 5 years, including employment outside the State of Florida. Contact attempts and the findings must be documented in writing and maintained in the employee personnel file.

e. Affidavit of Good Moral Character. The applicant must complete a notarized Child Care Affidavit of Good Moral Character (form CF 1649A, available in DCF Forms) attesting to his/her eligibility and submit it to the employer, licensing entity or regulatory authority.

f. Sexual Offender Registry Check. The employer must complete a sexual offender and sexual predator check for each state for which the applicant has resided within the previous 5 years. The results will be maintained in the employee personnel file. The Florida Sexual Offender Registry Check is included in the state's criminal history records search completed by FDLE.

12-6. Rescreening Procedure. A new Level 2 screening, according to the procedures of the preceding section, must be conducted every 5 years, upon a break in service of 90 days or more, or if verification of the original screening cannot be obtained.

a. If the individuals' fingerprints are found during a search of the Clearinghouse, the provider will initiate a resubmission in the Clearinghouse.

b. Rescreening will be initiated in the Clearinghouse by the provider prior to the employee's arrival at a live scan vendor location if the individual is not found to exist in the Clearinghouse. Failure to do so may result in the Department's inability to determine eligibility for child care programs.

12-7. Analyzing Results.

a. Once results have been received via the Clearinghouse and from other states of residency (if applicable), background screening staff will review all results to determine if any disqualifying criminal offenses, pursuant to section 435.04, F.S., have been committed. Any out-of-state criminal offense which, if committed in Florida, would constitute a disqualifying offense, will be treated as a disqualifying offense.

b. The Background screening unit will review FSFN for reports of abuse, neglect, abandonment or exploitation of a child or vulnerable adult.

(1) If a search of FSFN does NOT reveal the applicant is a caregiver responsible in a report of abuse, neglect or abandonment, background screening staff will provide notification to the employer. The individual's profile in the Clearinghouse will be updated to advise the provider that the Department has reviewed child welfare records and there is no record of the applicant being the caregiver responsible for a verified finding of abuse or neglect of a child or vulnerable adult.

(2) If a search of FSFN does reveal the applicant is a caregiver responsible in a verified report of abuse, neglect or abandonment, the background screening staff will provide notification to the employer. The individual's profile in the Clearinghouse will be updated to advise the provider that the

Department has reviewed child welfare records and additional information may be available pursuant to Chapter 119, F.S., at the request of the individual applicant.

c. Out-of-state abuse and neglect registry searches, once requested and obtained by the provider, will be reviewed and applied solely on the provider's discretion.

12-8. Documenting Results.

a. FBI and FDLE Criminal History Results. Documentation of receipt and action taken based on the criminal history check will be documented in the Clearinghouse under the criminal history tab.

b. Out-of-State Criminal History Results.

(1) Documentation of receipt and action taken based on the out-of-state criminal history check will be documented in the Clearinghouse under the criminal history tab.

(2) If the results of out-of-state requests are not received within 45-business days after the request was sent, background screening staff will determine the applicant "Not-Eligible" in the Clearinghouse for DCF Child Care. If results are received within 90-days from the date of screening, background screening unit will review the results to determine continued eligibility to work in child care.

c. Out-of-State Abuse and Neglect Registry Results.

(1) Documentation of the date the search was requested, and the date the results were received, must be maintained in the employee's file for review by the licensing authority.

(2) If the Department receives verified findings of abuse or neglect, the report number will be documented in the Clearinghouse on the criminal history tab. Documentation should include search date, report number, date, and findings.

12-9. Determining Eligibility. Eligibility determinations by the Department shall be based on Level 2 criteria, including sealed and expunged records, and out-of-state criminal history results. If necessary, the background screening unit may request additional documentation from the applicant such as police reports, arrest, or probable cause affidavits, charging documents, final court dispositions, and sworn complaints. If the applicant refuses or does not respond to the request for additional documentation within 30 calendar days of the receipt of the Request to Applicant for additional Information, the applicant will be ineligible for employment pursuant to sections 435.05(1)(d) and 435.06(3), F.S. Based on the results of the screening and any supplemental information, background screening staff will take the following action and document in the Clearinghouse:

a. No criminal history. Applicant shall be determined eligible.

b. No criminal history, with no out-of-state residency in the previous 5 years. Applicant shall be determined eligible.

c. No criminal history, with pending out-of-state residency in the previous 5 years searches. Once it has been determined that an applicant is clear of any disqualifying offenses (Level 2- Florida Standard, Chapter 435, F.S.), the applicant will be deemed authorized for provisional hire for a period of 45-days while awaiting out-of-state criminal history results.

d. No disqualifying criminal history. Applicant shall be determined eligible.

e. No disqualifying criminal history (Level 2 Florida Standard, Chapter 435, F.S.), with out-of-state residency in the previous 5 years pending. Once it has been determined that an applicant is clear

of any disqualifying offenses, the applicant will be deemed authorized for provisional hire for a period of 45-businessdays while awaiting out-of-state criminal history results.

f. Disqualifying offense(s) eligible for consideration of an exemption. Provided that all criteria included in section 435.07, F.S., are met, the applicant will be notified that he or she is not eligible and notified of the next steps for requesting an exemption.

g. Disqualifying offense(s) not eligible for exemption. If applicant is found to have a disqualifying offense that is not eligible for an exemption pursuant to section 435.07, F.S., the applicant will be notified that he or she is not eligible to work in child care and is not eligible for an exemption at the time of review.

h. If, upon screening, it is determined that an exemption had been previously granted, the exemption will continue only if the disqualifying offense is not a permanent disqualifier under Chapter 435, F.S.

12-10. Confidentiality and Sharing of Screening Information.

a. All information obtained through the screening process is exempt from public disclosure and may not be used for any reason other than the purpose for which the individual was screened as provided in section 435.09, F.S. An exception exists under section 435.10, F.S., for the sharing of personnel information among employers.

b. Details regarding findings may not be shared with anyone other than the applicant.

c. FDLE and FBI criminal history record information is restricted to those personnel designated by the Department to perform this function and may be accessed only as allowed by federal and state statutes, regulations and guidelines. The Department has instituted security precautions and standard operating procedures, in compliance with provisions established within User Agreements, pertaining to information access (see Chapter 4, Information Security, of this operating procedure).

d. Pursuant to CFOP 50-1, Chapter 1 and Chapter 4, a violation of access restrictions may result in termination of the User Agreement and cessation of Department access to FDLE and FBI databases and may result in fines and penalties being assessed against the Department and/or responsible employees. Personnel found in violation of FDLE and FBI access restrictions will be subject to disciplinary action, which may include, but is not limited to:

(1) Oral reprimand;

(2) Written reprimand;

(3) Suspension from employment;

(4) Termination from employment;

(5) Legal action; and/or,

(6) Criminal liability.

12-11. Records Management.

a. If a disqualification action is issued and/or additional information and documents were requested by the Background Screening Unit in order for an eligibility determination to be made, a file

will be created that will be retained by the Background Screening Unit and will include criminal history results, all correspondence, and any documents submitted by the applicant.

b. Background screening records used to evaluate criminal history results and determine eligibility for employment or licensure shall be retained in the Clearinghouse by the Department for 20 fiscal years. Upon storage of records, this section will be referenced within the records storage request as justification for storage and retention.

c. The employer/owner/operator must maintain on-site at the program copies/documentation of completion of all applicable elements in the screening process for an individual in the personnel file for review by the licensing authority.

Definition of Terms

Background Screening Staff – the group of individuals employed by the Department's Background Screening Program. Staff include:

Background Screening Coordinators are responsible for reviewing screenings with criminal history, including exemptions.

Call Center Specialists process calls and emails from providers and applicants to the Department's Background Screening Program via the Background Screening Helpdesk.

Technicians complete abuse history checks in FSFN.

Caretaker – Refers to the individual required to be screened.

A **volunteer** who assists on an intermittent basis for less than 10hours per month is not considered a caretaker, provided the volunteer is under direct and constant supervision of/by persons who meet Level 2 screening requirements.

In **Child Care Facilities, Nonpublic schools pursuant to section 402.3025(2), F.S., National Membership Organizations,** and **Specialized Child Care Facilites for the Care of Mildly Ill Children,** this term includes: owners, operators/directors, employees, and volunteers who serve 10 hours or more per month, but does not include individuals who work in the facility after hours when children are not present or the parents of children in Head Start.

In a **Family Day Care Home or Large Family Child Care Home,** this term includes: operators, substitutes, employees, and every household member over the age of 12.

In **Religious Exempt** Child Care Providers, this term includes: owners, operators/directors, employees, and volunteers who serve 10 hours or more per month, but does not include individuals who work in the facility after hours when children are not present.

In **Summer Camps** (day and 24 hour), this term includes: owners, operators, employees, and volunteers who serve 10 hours or more per month.

In **Child Enrichment Service Providers**, this term includes: directors, owners, employees, and volunteers who serve 10 hours or more per month.

Care Provider Background Screening Clearinghouse (Clearinghouse) – The purpose of the Clearinghouse is to provide a single data source for background screening results of persons required to be screened by law for employment in positions that provide services to children, the elderly, and disabled individuals. The Clearinghouse allows criminal history results to be shared among specified agencies when a person has applied to volunteer, be employed, be licensed, or entered into a contract that requires a state and national fingerprint-based criminal history check. (Section 435.12, F.S.)

Caretaker Screening Information System (CSIS) – CSIS is a statewide computer program utilized by the Department's Background Screening Program and other background screening entities within the Department to track screenings for persons required to be screened pursuant to Chapter 435, F.S. Only results received by the Background Screening Program are entered into the system.

Expunged Record – Any criminal record of a minor or an adult which is ordered expunged by a court of competent jurisdiction pursuant to section 943.0585, F.S., is physically destroyed or obliterated by any criminal justice agency having custody of such record and is not available to any person or entity except upon order of a court of competent jurisdiction.

A person who is the subject of an expunged criminal record may lawfully deny or fail to acknowledge the arrests covered by the expunged record, except in certain circumstances including seeking employment or licensing by or to contract with the DCF in a position having direct contact with children or the developmentally disabled, as outlined in section 943.0585(4)(a)5., F.S.

FSFN (Florida Safe Families Network) – The state's official case file record for each investigation and case, and the official record for all homes and facilities licensed by the state or approved for adoption placement. All pertinent information about every intake, investigation and case management function must be entered into FSFN, including the Child's Resource Record. The FSFN electronic case file is the primary record for each investigation, case, and placement provider. Please reference Rule 65C-30.001(12) and Rule 65C-30.001(113), Florida Administrative Code.

Initial Screening – The first screening completed as an act of original employment and/or hiring, and/or licensing or contracting, initiated prior to starting employment or prior to licensure/contracting or following a 90-day break in employment from a position for which an individual acquired an initial screening.

Licensing Entity – The government entity responsible for issuance of a license.

Licensing Agency – The entity, government, or non-government, responsible for training prospective licensees and submitting all necessary documentation to the Licensing Entity or Regulatory Authority.

Live Scan – The electronic submission of fingerprints to FDLE for acquisition of state and national criminal history information/checks.

Local Licensing Agency – A county whose licensing standards meet or exceed state minimum standards and has been designated as a local licensing agency to license child care facilities and homes in the county.

National Results – Criminal history from all states and territories retained by the Federal Bureau of Investigation (FBI) and/or other state repositories.

OCA – Originating Case Agency on a Live Scan submission is the identification number issued by the Background Screening Program through the CSIS program. It is the key to identifying the provider/agency requesting the background screening or for whom the background screening is being completed. This is a unique number generated by the CSIS system or converted from a legacy system. For Live Scan submissions, the OCA is prefaced with the two-digit district number and ends with a "Z" (e.g., 03011234Z). This differs from an ORI, which is assigned to qualified governmental entities by the FBI.

ORI – Originating Agency Identifier is a unique identifier assigned to qualified governmental entities by the FBI for submission and processing of fingerprint results. Clearinghouse ORIs are as follows:

DCF General: EDCFGN10Z

DCF Mental Health: EDCFMH20Z

DCF Summer Camp: DCFSC30Z

Regulatory Authority – The government entity responsible for oversight of a service provider.

Re-Screening – For continued employment, licensure, or contracted status, each individual is required to be re-screened at 5-year intervals following the completion of his or her initial screening. The re-screening shall include Level 2 fingerprint screening.

Sealed Record – Any criminal history record of a minor or an adult which is ordered sealed by a court of competent jurisdiction pursuant to section 943.059, F.S., is confidential and exempt from provisions of section 119.07(1), F.S. and s. 24(a), Constitution of the State of Florida, and is available only to the person who is the subject of the record, to the subject's attorney, to criminal justice agencies for criminal justice purposes, or to those entities set forth in section 943.059(4)(a)5., F.S., for their respective licensing and employment purposes.

> A person who is the subject of a sealed criminal record may lawfully deny or fail to acknowledge the arrests covered by the sealed record, except in certain circumstance including seeking employment or licensing by or to contract with the Department of Children and Families in a position having direct contact with children or the developmentally disabled, as outlined in section 943.059(4)(a)5., F.S.

Voluntary Pre-Kindergarten – A pre-kindergarten program established by the 2005 Legislature with special funding for providers and available to all children within the state who will attain the age of 4 on or before September 1 of the school year, allowing them to attend either a private or public pre-kindergarten program. This group includes individuals already required to be screened as employees working in programs in private schools with children under the age of 5, facilities exempt from licensure, and licensed childcare centers.