INDIANA DEPARTMENT OF CHILD SERVICES ADMINISTRATIVE POLICIES AND PROCEDURES		
Policy Number: GA-23	Effective Date: July 1, 2022	Version: 2.0

POLICY TITLE: CRIMINAL JUSTICE INFORMATION SYSTEM

OVERVIEW: The Indiana Department of Child Services (DCS) has established this policy to address the appropriate use and disclosure of information contained within the criminal history records obtained through records released by the Federal Bureau of Investigations (FBI) via the Indiana State Police (ISP). It incorporates the regulations, DCS policies and laws from Indiana DCS, Adam Walsh Act, Criminal Justice Information System (CJIS) Policy Council Act, Criminal Justice Information Systems (CJIS) Security Policy, and CJIS addendum.

I. DEFINITIONS

A. Authorized Access Escort: An authorized user who always accompanies a visitor while the visitor is within a physically secure location to ensure the protection and integrity of the physically secure location and any Criminal Justice Information (CJI).
B. Authorized Requestor: An individual granted permission by policy and law to request criminal history information from ISP. This includes Child Protective Service (CPS), Child Support Bureau (CSB), and Juvenile Justice workers; contract staff, and DCS embedded State Personnel Department (SPD) staff.
C. Authorized User: An individual/group of individuals authorized to access CJI, as required by policy and permitted access by law. This includes CPS, CSB, and Juvenile Justice workers; contract staff, and DCS embedded SPD staff.
D. Central Office Agency Security Officer (Security Officer): An individual designated by DCS to ensure DCS compliance with CJIS and Indiana Data and Communication System (IDACS) requirements.
E. Criminal History Record (CHR): A non-public record entered by ISP Criminal Justice Information Center and contains information about a person's criminal history.
F. Criminal History Record Information (CHRI): Background information obtained from the criminal history record.
G. Criminal Justice Agency (CJA): An agency that is either a court, governmental agency, or a subunit of a governmental agency that performs administrative activities of criminal justice pursuant to a statute or executive order and allocates a substantial part of its annual budget to the administration of criminal justice.
H. Criminal Justice Information (CJI): Data (electronic or hardcopy) collected by criminal justice agencies for the purpose authorized or required by law.
I. Criminal Justice Information System (CJIS): The FBI's Criminal Justice Information Services Division, being the repository for criminal justice information services in the FBI. The National Crime Information Center (NCIC) and Interstate Identification Index (III/Triple I) are systems managed by CJIS.
J. CJIS System Agency (CSA): The state organization responsible for connecting agencies and users within the state systems managed by CJIS. ISP is the CSA for the State of Indiana.
K. Dependent Agency: The agency utilizing CJIS is the dependent agency which in this instance is DCS.

L. Interstate Identification Index (III/Triple I): A cooperative state-federal system for the electronic exchange of criminal history record information for authorized purposes, as specified by local, state, and federal laws.
M. National Crime Information Center (NCIC): A nationwide computerized information system that helps the criminal justice community perform its duties by providing accurate and timely documented criminal justice information, which includes restricted and non-restricted interface files. Restricted and non-restricted files are differentiated by the policies governing their access and use.
N. Noncriminal Justice Agency (NCJA): Any court, governmental agency, or a subunit of a government agency that performs administrative activities other than the administration of criminal justice.
O. Originating Agency Identifier (ORI): Provided to a governmental agency or subunit defined as either a CJA or NCJA to identify each unit/agency. Each transaction made from that unit/agency includes the assigned ORI.
P. Person Query (III/Triple I name-based check): A way to look up criminal justice information available using non-Fingerprint-Based Checks. Queried information requires the same privacy and protections outlined in this policy and the Criminal Justice Information Systems (CJIS) Security Policy.
Q. Terminal Agency: For this policy, the ISP is the terminal agency.

II. REFERENCES

- IC 10-13-3-27.5: Record check by department of child services under exigent circumstances; transmittal of report copy; providing fingerprints; removal of child for failure to provide fingerprints; compliance with federal law; contesting denial of placement; fee
- IC 10-13-3-35: Indiana data and communication system; national crime information center's missing, wanted, and unidentified person files; entry or deletion of information
- 28 CFR 20: Criminal Justice Information Systems
- 240 IAC 5-1-1: General policy; restrictions on use
- 240 IAC 5-1-2: Audit of system transactions
- 240 IAC 5-2-9: User agreement
- 34 USC 20961: Access to national crime information databases
- Criminal Justice Information Systems (CJIS) Security Policy
- DCS Policy Chapter 13- Background Checks

III. STATEMENTS OF PURPOSE

A. Each agency or subunit that has an assigned ORI must appoint selected staff to serve as a Central Office Agency Security Officer (Security Officer).
B. The Security Officer serves as a compliance expert and helps to ensure the physical security, software compliance, and physical security screening requirements are adhered to and immediately reports any breaches.
C. An authorized requestor should be knowledgeable about DCS policies that address criminal history background checks (see Chapter 13- Background Checks). The authorized requestor must be associated with an individual through the requestor's

assigned workload to obtain criminal history record information regarding that individual.

D. Proper access and dissemination of data from restricted NCIC files must be consistent with the access and dissemination policies for the III/Triple I, as described in 28 CFR 20. As described in 34 USC 20961, state access is authorized for NCIC and III/Triple I files for the purpose of obtaining national criminal history information on a person involved in cases of child abuse and/or neglect (CA/N).

E. DCS has access and exposure with the ability to receive and/or review CJI, without direct access. Authorized users who have indirect access include any agency staff who may be required to review and interpret CHRI as a part of their job duties. This may also include private contractors/vendors, custodial workers, or others with access to physically secure locations or controlled areas in which criminal history may be present electronically or in hard copy.

F. To access and view CJI, a physically secure location is required. This may be an area, room, or a group of rooms within a facility with both physical and personnel security controls that are sufficient to protect the CJI and associated systems. The perimeter of the physically secure location should be noticeably identifiable and separated from non-secure locations by physical controls that define the security perimeters as controlled and secured. The restricted, nonpublic area should be identified with a sign at the entrance.

G. Visitors to a DCS office must have an authorized access escort with them at all times to access physically secure locations where CJI and associated information systems are located (the use of cameras or other electronic means used to monitor a physically secure location does not constitute an escort).

H. A DCS authorized user may be granted authorized offsite access, which allows the authorized user to access CJI from a location outside of the employee's assigned office (e.g., the employee's home or a non-assigned office). The employee must not access CJI using a public connection (e.g., at a coffee shop).

I. A violation of any requirement in this policy by:
   1. An authorized user will result in disciplinary action, up to and including loss of access privileges, civil and/or criminal prosecution, and/or termination; and
   2. A visitor may result in similar disciplinary action against the sponsoring employee (i.e., the employee who invited the visitor into the secured area but failed to continue escorting the visitor).

J. Any suspected violation of the CJIS policy pertaining to unauthorized access, use, or disclosure should be reported immediately to the Background Check Program Manager. CJI may only be requested by DCS requestors who are authorized users.

IV. PROCEDURE

A. The Security Officer must:
   1. Identify who is using the approved hardware, software, and firmware to ensure only authorized individuals have access;
   2. Ensure the upholding of personnel security-screening procedures, as outlined in this policy;

3. Ensure the approved and appropriate security measures are in place and working as expected; and
4. Support policy compliance and promptly inform the CSA Information Security Officer (ISO) of security incidents.

B. An authorized user is responsible for interpreting the criminal history information obtained from ISP.
C. Authorized users, as defined in (I)(C), shall:
   1. Pass a state and federal fingerprint-based criminal history background check per evaluation standards outlined in the Criminal Justice Information Systems (CJIS) Security Policy and:
      a. Shall be disqualified for any felony conviction,
      b. May be disqualified for any misdemeanor conviction. Factors that will be considered include, but are not limited to the conviction type, number of convictions, time that has passed since the conviction, and other arrests/convictions,
      c. May be disqualified if the staff is a fugitive or has an excessive arrest history without convictions, or
      d. May be disqualified due to an arrest or pending conviction.

Note: All State staff, contractors, custodians, or others that have unescorted physical access will undergo fingerprint-based criminal history background checks every five (5) years.

   2. Complete CJIS training and pass the test/certification with no less than a 70% within the first 60 days of hire and then no less than annually.

D. The following steps will be taken to ensure controlled areas, which are configured workstations assigned to staff for the purpose of processing CJI, are secure:
   1. Monitors used to view CJI should be positioned away from doorway/entry of a cubicle/office;
   2. Any physical media is to be locked;
   3. Computers will be restarted and locked at the end of the business day;
   4. Computers will be locked during working hours when employees are away from their desk;
   5. The lock function will be used when printing CJI on a shared printer to ensure the CJI does not print until the authorized person is at the printer;
   6. Appropriate action will be taken to protect all confidential data;
   7. Staff will not share individually issued keys, access cards, or computer log-in information, including passwords;
   8. Computers will be protected from viruses, worms, trojan horses, and other malicious code;
   9. Web usage will be protected;
   10. Staff will ensure secure dissemination of CHRI when sending or receiving the information by phone, fax, or e-mail for review;

11. Any physical security incidents will be reported to the Background Check Program Manager;
12. CJI will be properly released only to authorized personnel, and when the CJI is no longer needed, printouts will be crosscut shredded; and
13. Staff will ensure the perimeter security door securely locks after entry and departure.

E. DCS will ensure visitors:
   1. Check-in before entering a physically secure location; and
   2. Are accompanied by a DCS authorized access escort at all times.

F. When accessing CJI using authorized offsite access, the authorized user will:
   1. Always connect to the Virtual Private Network (VPN) before logging into and accessing CJI;
   2. Refrain from printing CJI on a public or home printer; and
   3. Adhere to all CJIS security policies.

G. A violation of CJIS policy may result in the following as outlined in the Criminal Justice Information Systems (CJIS) Security Policy and applies for a person who intentionally uses or discloses non-public information for personal gain or in a manner that is not authorized by law or rule:
   1. A first offense is a misdemeanor, which is punishable by imprisonment, a $500 fine, or both;
   2. A second offense is a felony, which is punishable by not more than four (4) years imprisonment, a $2,000 fine, or both; and
   3. Staff found to have misused CJI are subject to disciplinary action, up to and including dismissal.

V. FORMS AND OTHER DOCUMENTS

N/A

Date: June 29, 2022

Donald Travis, Deputy Director of Juvenile Justice Initiatives and Support
Department of Child Services