TITLE	POLICY NUMBER	
Criminal Records Requests	DCS 02-45	
RESPONSIBLE AREA	EFFECTIVE DATE	REVISION
Business Operations	March 7, 2024	

I. POLICY STATEMENT

The Arizona Department of Child Safety (DCS, Department) is responsible for ensuring that personnel are compliant with all applicable laws, rules, regulations, policies, and procedures governing access to criminal justice information system (CJIS) networks. This policy is designed to ensure the completeness, integrity, accuracy, and security of data that is transmitted between the Department and CJIS networks.

II. APPLICABILITY

This policy applies to all Department personnel.

III. AUTHORITY

A.A.C. Title 13, Chapter1, Article 2	ACJIS Network
A.R.S. § 8-451	Department; purpose
A.R.S. § 8-514.02	Placement of a child
A.R.S. § 8-514.03	Kinship foster care; requirements; investigation

A.R.S. § 8-807	DCS information; public record; use; confidentiality; violation; classification; definition
A.R.S. § 41-1750	Central state repository; department of public safety; duties; funds; accounts
CFR Title 28 Part 20	Criminal Justice Information Systems (CJIS)
CJIS Security Policy	US Department of Justice, Federal Bureau of Investigation

IV. DEFINITIONS

Arizona Criminal Justice Information System (ACJIS): A network maintained by the Arizona Department of Public Safety that is available to authorized local, state, and federal criminal justice agencies and serves as a conduit to the National Criminal Information Center (NCIC).

Authorized users: Department employees permitted to receive information directly via the ACJIS network who handle/view information received but do not require terminal operator certification.

Criminal justice agency: a government agency or any subunit thereof which performs the administration of criminal justice pursuant to a statue or executive order, and which allocates a substantial part of its annual budget to the administration of criminal justice.

Criminal justice information (CJI): The information that is collected by criminal justice agencies and that is needed for the performance of their legally authorized and required functions, such as criminal history record information, citation information, stolen property information, traffic accident reports, wanted persons information, and system network log searches.

Criminal justice information system (CJIS): An information system that collects, processes, preserves, disseminates, and exchanges criminal justice information (including criminal history, motor vehicle division records, booking data, and missing and wanted persons, etc.) and includes the electronic equipment, facilities, procedures, and agreements necessary to exchange this information. Records from the

State of Arizona are housed in the Arizona Criminal Justice Information System (ACJIS).

Department or DCS: The Arizona Department of Child Safety.

Justice Web Interface (JWI): A law enforcement and criminal justice portal developed and owned by Maricopa County. Interconnected with ACJIS, JWI provides access to legacy and integrated data sources.

National Crime Information Center (NCIC): The computerized information system, which includes telecommunications lines and any message switching facilities that are authorized by law, regulation, or policy approved by the Attorney General of the United States to link local, state, tribal, federal, foreign, and international criminal justice agencies for the purpose of exchanging NCIC related information.

System Security Officer (SSO): The Department employee designated to serve as the liaison between DCS and a CJIS whose duties are enumerated in section V. Various units within the department (e.g., Human Resources, Learning and Development) will collaborate and liaise with the SSO regarding security requirements.

Unauthorized Access: Gaining logical or physical access without permission to a network, system, application, data, or other resource, or any access that violates a stated security policy.

V. POLICY

A. Information Access

1. Use of A/CJIS information systems must be for a valid purpose only. Within the Department's investigative scope, the only valid purpose pertains to open reports of child abuse/neglect.

2. Every incident of misuse, deliberate or unintentional, of the A/CJIS system shall be evaluated and addressed independently based on the situation and circumstances.

B. System Security Officer

1. The System Security Officer (SSO) shall follow the guidelines and policies set forth by both the ACJIS and SSO manual.

2. SSO duties include:

    a. quality control matters, including internal auditing of the system;

    b. security matters;

    c. agency personnel authorization/training/certification;

    d. maintaining authorized user lists;

    e. maintaining training records;

    f. maintaining fingerprint card records;

    g. notifying the Federal Bureau of Investigation (FBI) and Arizona Department of Public Safety (DPS) of any cyber-attack incidents and coordinating/communicating, as necessary.

C. Department Personnel Background Checks

1. All Department personnel who have contact with children shall undergo pre-employment Level One Fingerprint Clearance Card fingerprinting. A user's Level One Fingerprint Clearance Card must be current/valid prior to accessing A/CJIS and having contact with children.

2. If a criminal record of any kind exists, access to CJI shall not be granted until the SSO or designee reviews the matter to determine if access is appropriate.

    a. If a felony conviction of any kind exists, the Department shall deny access to CJI. However, the SSO may consider extenuating circumstances where the severity of the offense and the time that has passed would support a possible variance.

    b. Applicants with a record of misdemeanor offense(s) may be granted access if the SSO, or designee, determines the nature or severity of the misdemeanor offense(s) do not warrant

disqualification. This same procedure applies if the person is found to be a fugitive or has an arrest history without conviction.

c. If a record of any kind is found on a contractor, the Department shall delay access to CJI pending review of the criminal history record information. The Department shall notify the contractor's security officer.

d. If a person already has access to CJI and is subsequently arrested and or convicted, continued access to CJI shall be determined by the SSO (refer to *Duty to Advise of Arrests, Prosecutions, and Convictions* (DCS 04-50) policy for further information). For offenses other than felonies, the SSO has the latitude to delegate continued access determinations to their designee.

e. The SSO shall maintain a list of personnel who have been authorized unescorted access to unencrypted CJI and shall, upon request, provide a current copy of the access list to the DPS Access Integrity Unit.

D. Department Authorized User Training

1. All Department personnel shall obtain a Level One Fingerprint Clearance Card from DPS and complete the following training:

a. DPS CJIS Security computer-based training (CBT) within 6 weeks of hire and biannually thereafter;

b. DPS Criminal Background Checks classroom training during DCS Specialist Core;

c. Information Security Awareness and Privacy CBT within 30 days of hire and annually thereafter;

d. Kevin Mitnick Security CBT within 30 days of hiring and annually thereafter.

2. After initial certification, all certified DCS personnel shall recertify annually.

VI. PROCEDURES

A. Information Access and Dissemination

1. A/CJIS shall only be accessed via the DCS JWI Portal for:

   a. an open DCS Assessment or Case;

   b. the purpose of evaluating the fitness of custodians or prospective custodians of juveniles, including parents, relatives and prospective guardians (A.R.S. § 41-1750 (G) (13);

   c. the purpose of investigating or responding to reports of child abuse, neglect or exploitation (A.R.S. § 41-1750 (G) (22).

2. All queries shall be documented in the corresponding Guardian Assessment or Case via a case note.

3. The case note shall document:

   a. the date and time of the query;

   b. what query was run (see VI.A.1, above);

   c. what person(s) were run, and why;

   d. how the person(s) are involved in the Assessment or Case.

4. A/CJIS information may **not** be:

   a. disseminated outside of DCS;

   b. given, shown, or communicated to the person of record or any other persons who are not authorized to view CJI;

   c. sent via a device not issued by the Department;

   d. sent via a method other than AZDCS domain email or monitored fax;

e. scanned into a case file or maintained as hard copy;

f. used for curiosity or other personal purposes;

5. Authorized users shall restrict their monitor view while conducting criminal background checks.

6. Any individual who wishes to review and challenge the results of a DPS criminal records check shall be referred to the DPS Criminal History Records Section at 602-223-2222. The individual may request a Record Review Packet for an arrest, conviction, or indictment by a law enforcement jurisdiction in Arizona. If the criminal record concerns an arrest, conviction, or indictment outside Arizona, the individual must contact the applicable law enforcement jurisdiction in that state.

B. Noncompliance

1. If a Department employee becomes aware of or suspects misuse, deliberate or unintentional, of the A/CJIS system, they shall notify the System Security Officer as soon as possible. Pursuant to A.R.S. § 41-1756, it is considered a Class 6 felony to misuse the ACJIS.

2. Notification may be verbal or in writing and shall include:

a. involved personnel;

b. date(s) and time(s) of misuse; and

c. nature of misuse.

3. The SSO shall:

a. document the incident as reported;

b. contact the involved employee’s manager or direct supervisor;

c. notify the Department of Public Safety Access Integrity Unit as necessary.

4. Individual users and/or the agency may be sanctioned for noncompliance including but not limited to:

    a. discipline up to and including termination;

    b. civil and/or criminal prosecution;

    c. discontinuance of system access for the user; and/or

    d. discontinuance of system access for the Department.

C. Information Destruction

1. Printed A/CJIS information shall be immediately placed in a designated, secured shred bin when it is no longer required for investigative or placement purposes.

2. Printed A/CJIS information shall not be retained indefinitely in a case folder, hard file, or any other form of storage.

3. Digitally stored A/CJIS information shall be immediately erased from any forms of storage, including email, when it is no longer required for investigative or placement purposes.

VII. FORMS INDEX

N/A