ARIZONA DEPARTMENT OF CHILD SAFETY

TITLE	POLICY NUMBER	
Criminal Justice Information System (CJIS)	DCS 13-02	
RESPONSIBLE AREA	EFFECTIVE DATE	REVISION
Office of Child Welfare Investigations (OCWI)	09/19/19	2

I. POLICY STATEMENT

The Office of Child Welfare Investigations (OCWI) is responsible for ensuring that OCWI personnel are in compliance 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 OCWI and CJIS networks.

II. APPLICABILITY

This policy applies to all OCWI personnel.

III. AUTHORITY

A.A.C. Title 13, Chapter1, Article 2	ACJIS Network
A.R.S. § 8-807	DCS information; public record; use; confidentiality; violation; classification; definition
A.R.S. § 41-1750 (G) (22)	Central state repository; department of public safety; duties; funds; accounts
CFR Title 28 Part 20	Criminal Justice Information Systems

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: OCWI employees who are permitted to receive information directly or indirectly via the ACJIS network and have completed the Arizona Terminal Operator Certification (TOC) program, and OCWI employees identified as criminal justice practitioners who handle/view information received via the ACJIS network 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 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.

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.

Office of Child Welfare Investigations (OCWI): A criminal justice agency within the Arizona Department of Child Safety (DCS) that has investigative authority when criminal conduct is alleged. As a designated criminal justice agency, OCWI is assigned an Originating Agency Identifier (ORI) by the Federal Bureau of Investigation; this number pertains specifically to OCWI, not to DCS as a whole.

System Security Officer (SSO): The OCWI employee designated to serve as the liaison between OCWI and a CJIS.

Terminal Operator Certification (TOC) Program: A state and federally mandated program that requires knowledge and proficiency testing concerning the ACJIS network. The "Level B" certification referenced in this policy requires successful completion of an on-line certification test consisting of 25 questions. This level is for ACJIS operators who inquire into the ACJIS network and interpret responses; it is not for entering or updating records.

V. POLICY

A. Information Access

1. Use of A/CJIS information, systems, and any resources restricted to designated criminal justice agencies must be for a valid criminal justice purpose only. Within OCWI's investigative scope, the only valid criminal justice purpose is a criminal conduct report 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/Assistant System Security Officer

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

2. SSO duties include:

a. quality control matters;

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 Investigations and Arizona Department of Public Safety of any cyber-attack incidents and

coordinating/communicating, as necessary.

C. OCWI Personnel Background Checks

All OCWI personnel shall undergo pre-employment fingerprinting and criminal history background checks prior to employment. Updated fingerprinting and criminal history checks shall be completed quinquennially, from the date of the original fingerprinting.

D. OCWI Authorized User Training

1. All OCWI personnel shall complete the following training within six months of employment:

   a. ACJIS Privacy and Security Training;

   b. Security Awareness;

   c. ACJIS Level B TOC exam (direct access users only);

   d. An OCWI Criminal Justice User Agreement shall be completed for each authorized user at the completion of training.

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

E. Terminal Security

OCWI A/CJIS terminals shall be housed so only authorized personnel can view information on the monitor or printer.

F. Direct Network Access

Direct access of the ACJIS network shall be limited to Analyst Unit personnel who are “level B” TOC-authorized users, as defined by the ACJIS rules and regulations.

G. Indirect Network Access

Indirect access of the ACJIS network shall be limited to OCWI personnel. Information sent to indirect users is for their investigative use only.

VI. PROCEDURES

A. Information Access and Dissemination

1. Prior to accessing A/CJIS systems, the following information shall be obtained and documented:

   a. Guardian Assessment Number;

   b. reason for the request; and

   c. requestor, if other than the direct user.

2. A/CJIS information may be disseminated to authorized users via:

   a. email: requires encryption ([secure]) added to the subject line;

   b. fax, if the recipient is authorized to receive the information and can confirm they are monitoring the fax to collect the information to prevent any unauthorized viewing.

3. A/CJIS information may not be:

   a. disseminated outside of OCWI; all forms of secondary dissemination are prohibited;

   b. sent via a device not issued by the agency;

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

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

   e. given to the person of record;

   f. used for curiosity or other personal purposes;

   g. given, shown, or told to unauthorized personnel.

B. Noncompliance

1. If an OCWI employee becomes aware of or suspects misuse, deliberate or unintentional, of the A/CJIS system, the OCWI System Security Officer ("SSO") or an Assistant SSO ("ASSO") shall be notified as soon as possible. If an ASSO is notified, the ASSO shall notify the SSO.

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.

2. The SSO shall:

a. document the incident as reported;

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

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

3. 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 agency.

C. System Security Officer/Assistant System Security Officer

OCWI process standard work and position standard work are established for SSO duties and are available on SharePoint.

1. Standard work for the SSO position shall be reviewed annually for accuracy and modification.

D. OCWI Personnel Background Checks

1. Fingerprint cards shall be stored and archived for active TOC-certified OCWI employees if the employee was not digitally fingerprinted. Upon competition of digital fingerprinting, the physical fingerprint card shall be destroyed via shredding.

2. Employees shall complete electronic/digital fingerprinting at the time their level-one fingerprint card expires using the OCWI fingerprinting code.

3. Pre-employment background checks shall follow the OCWI standard work process located on SharePoint.

E. Terminal Security

1. Access at 3003 N. Central Ave, 22nd floor is currently restricted to authorized personnel only via cipher locks installed on each office occupied by direct network users.

2. Manuals, training materials, and other related documents, publications, and printouts must be maintained in a restricted area.

3. All visitors to A/CJIS terminal areas must be escorted by OCWI personnel at all times.

F. Direct Network Access

1. Analyst Unit members shall only access ACJIS via authorized equipment issued by the department using a secured connection.

2. The ACJIS Network shall only be used if access and viewing is limited to authorized users (e.g. blinds are closed, doors are shut and locked). The ACJIS Network shall not be accessed to in publicly accessible buildings and facilities (e.g. a Starbucks or local library).

3. ACJIS Network access shall be limited via JWI roles as defined by ACJIS training and position standard work.

4. Transactions shall be logged in the Analyst Unit member's respective database for auditing purposes. Logging shall include:

   a. criminal conduct status;

   b. Guardian assessment number/ID number;

   c. requestor; and

   d. systems accessed.

5. Other criminal justice databases accessed shall follow the access and logging procedures as detained in this section.

G. Indirect Network Access

1. Indirect access users shall obtain ACJIS network information via a request to Analyst Unit members.

2. Requests sent to the OCWI Analyst Unit for ACJIS/NCIC data shall include:

    a. Guardian criminal conduct assessment number/ID;

    b. name of the person requesting the information;

    c. information of the persons being queried; and

    d. reason for the request (existence of a report is not justification).

H. 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 purposes.

2. Digitally stored A/CJIS information shall be immediately erased from any forms of storage, including email, when it is no longer required for investigative purposes. If saved to portable media, such as a USB drive, the portable media shall be formatted a minimum of two times, with the "quick format" feature of Windows formatting unchecked.

VII. FORMS INDEX

N/A