Example Noncriminal Justice Agency Policies and Procedures

Revised June 20, 2018

Note: Please read these policies in their entirety. You cannot simply copy and paste your agency name on these policies for them to be complete or accurate. You must also customize these policies to reflect your agency-specific procedures. Everything listed here will be verified during the audit process.

As a guideline, text that is highlighted in yellow is where you enter your agency name.

Text that is highlighted in green is either instructions for you or a decision that you must make to reflect your policies. Remove/modify the applicable text from the final document as needed.

GENERAL ADMINSTRATION

I. Purpose

Agency Name may use the Criminal Justice Information (CJI) or Criminal History Record information (CHRI) obtained from the Arizona Department of Public Safety (DPS) only for the specific purpose of evaluating **(state the purpose from your user agreement - i.e. employees, volunteers, contractors, licenses, etc.)**. CJI/CHRI may not be reused for any other purpose.

II. Authority

Agency Name has the authorization to submit fingerprints to the Arizona Department of Public Safety for Fee-Based State and Federal Criminal History Checks pursuant to **(list your authority here (i.e. specific Arizona state law, executive order, local ordinance, tribal resolution, etc.))**. The authority is listed in the Noncriminal Justice User Agreement between the Arizona Department of Public Safety and **Agency Name**.

III. Agency Security Contact (Primary Liaison)

Agency Name's Agency Security Contact (ASC) is the point of contact with DPS through which all communication with DPS regarding audits, agency/personnel information changes and training and security are conducted. The ASC will maintain all authorized personnel training on the NCJA Training Documentation Form (or similar document). This information will be available at time of audit. The ASC can receive and disseminate communication updates from DPS. For the responsibilities of the ASC, refer to the Agency Security Contact Basic Responsibility worksheet in the training handouts.

IV. Authorized Personnel

Agency Name's Human Resources (HR) staff may encounter CJI/CHRI. Authorized personnel will be given access to view and handle the CJI/CHRI after completing the required training (CJIS Online Security & Awareness training and reading our agency-specific policies and procedures) and the one-time signing of an acknowledgement statement. The Authorized Personnel consists of **(list specific job titles or departments here as needed),** and designated Agency Security Contact (ASC). Refer to the Authorized Personnel List for the most current authorized personnel. The authorized personnel are aware of the other personnel on this list. Upon termination of authorized personnel, the ASC will update the Authorized Personnel List with DPS as soon as possible.

The personnel listed on the current Authorized Personnel List on file with the DPS Access Integrity Unity (AIU) are the only personnel authorized to access, discuss, use, handle, disseminate, file, log and destroy the CJI/CHRI. To prevent tampering, all terminated personnel, the public, all outside persons and entities are prohibited from handling or having any access to CJI/CHRI for any reason. Secondary dissemination to an outside agency is prohibited.

If your agency does not store CJI/CHRI electronically then remove this entire highlighted paragraph. Only authorized personnel have access to the electronic secured and encrypted database where brief information of the CJI/CHRI are electronically stored. To prevent tampering or unauthorized access, once the authorized personnel is done entering or reviewing information, they must lock the database and log off the computer. Refer to the Storage of CJI/CHRI section below for more information regarding electronic storage. **Remove the previous sentence if you do not list more information in the Storage of CJI/CHRI section.**

Agency Name does not store CJI/CHRI electronically.

To prevent unauthorized access or tampering, the fingerprint filing cabinet and drawers are locked throughout the day and one key is secured with the ASC and one other key is secured with the designated authorized personnel. All visitors to the area where CJI/CHRI are kept are accompanied by authorized staff personnel as well.

The Non-Criminal Justice Applicant Fingerprint Card Inventory Sheet(s) must be retained for auditing purposes. The Arizona Department of Public Safety is on a three-year auditing cycle and can request to see the previous year's inventory sheets. For example, if the audit is being conducted in 2018, the inventory sheets from 2017 must be made available if requested.

Where possible, have personnel on the Authorized Personnel List been fingerprinted? As there is no Arizona state law existing as a specific authorization, this is not currently required. State if you are able to do this however. For example, many agencies in this program have a user agreement that states the purpose is for employment. In this example you could fingerprint the personnel on your list. If your purpose is adoption certification, then obviously you could not fingerprint the personnel on your list. Personnel with a felony conviction should not have access to CJI/CHRI.

FINGERPRINT SUBMISSIONS

V. Fingerprint Card Processing

Agency Name requires that all applicants must provide a valid, unexpired form of government-issued photo identification during the application process and prior to fingerprinting to verify their identity. Accepted forms of primary and secondary identification have been approved through the National Crime Prevention and Privacy Compact Council Identity Verification Program Guide.

A copy of the applicant's FBI Privacy Rights Notification will be provided to the applicant prior to fingerprinting.

Agency Name requires that all applicants must be fingerprinted if they are **(state the purpose from your user agreement - i.e. employees, volunteers, contractors, licenses, etc.)**. Applicants that have disclosed a conviction will be fingerprinted as well. **Applicants are fingerprinted on-site at the Agency Name's HR office or the fingerprint card is given/mailed to the applicant to take to their local police department to get fingerprinted.**

If you mail fingerprint cards to applicants you need to include a chain of custody form so that the fingerprinter can verify the applicant's identity at the time of fingerprinting. A sample form can be found in the NCJ Agency Guide Appendix A. The fingerprinter should be sealing the envelope the fingerprints are mailed in so that the applicant cannot tamper with them. State here if you are doing this and how.

Agency's Name designated HR staff takes possession of the fingerprint card and will ensure the correct purpose and authority (see above) are written on the fingerprint card in the "reason fingerprinted" box. Once the fingerprint card is completed and at no point in time is the fingerprint card to be returned to the applicant. Chain of custody procedures are maintained to protect the integrity of the applicant's fingerprints prior to submission to DPS and/or the FBI.

The fingerprint cards are then placed in a manila folder and then into a locked drawer to be mailed with the inventory sheet to DPS. Only authorized personnel have access to this locked drawer and the key is stored in the ASC's office.

When a fingerprint card is mailed or provided to the applicant, authorized personnel or designated HR staff will provide a packet that contains the following:

- Pre-filled fingerprint card with the employer's address, reason for fingerprint (authorization and purpose) and OCA number.
- A sealable envelope pre-labeled with the employer's address and a space marked with an X on the back of this envelope for the fingerprint technician to sign on the line provided.
- Applicant FBI Privacy Rights Notification.
- Instructions for the applicant on how to handle and return the fingerprint card in the provided envelope.
- Fingerprint technician instructions.

If the envelope shows evidence of opening or tampering, the applicant will be asked to provide another fingerprint card and authorized personnel will repeat the procedures to issue a new fingerprint card.

If your agency performs its own fingerprinting then delete this paragraph. If your agency sends applicants off-site to be fingerprinted, ensure you state here what your procedures are for ensuring the fingerprinter is verifying the identity of the applicant and how the fingerprints are being safeguarded until they are returned to your agency prior to submission to DPS. Does the fingerprinter mail the fingerprints to you agency or do they give them back to the applicant?

PRIVACY & SECURITY

VI. Handling/Retention of CJI/CHRI

The fingerprint results from DPS are delivered in a sealed envelope clearly labelled "Arizona Department of Public Safety". This mail should be considered to contain CJI/CHRI and should only be provided directly to authorized personnel or the ASC. Only authorized personnel will open mail that contains the CJI/CHRI.

During the course of suitability determination, here are the steps that authorized personnel will follow:

- **If your agency does not store CJI/CHRI electronically then remove this bullet point.** A summary of the CJI/CHRI are stored electronically on the Human Resources secured and encrypted drive with only authorized personnel having access.
- Before suitability is determined, the CJI/CHRI is stored in a locked drawer for the authorized personnel to review and make a suitability determination.
- After suitability is determined, the CJI/CHRI is stored in a separate employee fingerprinting file. These records cannot be released for any public records request and are not archived with the Arizona State Library, Archives and Public Records.
- After the final determination is rendered, the CJI/CHRI are filed in the fingerprint filing cabinet which is locked throughout the day and all visitors to the area are accompanied by designated HR staff or authorized personnel.

State here if your agency retains CJI/CHRI and for how long. If you are not retaining CJI/CHRI state that it is destroyed after a hiring decision or after any appeals process has been completed.

VII. Communication

Authorized Personnel may discuss the contents of the CJI/CHRI with the applicant in a private secure place and extreme care should be taken to prevent overhearing, eavesdropping or interception of communication. The applicant may not be given a copy of the record or allowed to take a picture of it with an electronic device. The record is for **Agency Name's** use only. Employees will not confirm the existence or non-existence of an individual's criminal history record to the public or to any unauthorized individual. The applicant should be informed that if he/she wishes to challenge the content of the record, they can contact:

- For a copy of an Arizona criminal history record contact the DPS Criminal History Records Unit at 602-223-2222 to obtain the fingerprint card and a review and challenge packet.
- For a copy of an FBI criminal history record contact the FBI at 304-625-5590. More information can be found at https://www.fbi.gov/services/cjis/identity-history-summary-checks

Agency Name provides all applicants the right to review and challenge his/her criminal history record if they deem the information has been inaccurately reported. Each applicant will be provided **(let applicants know how many days you are providing them to challenge their record)** upon notification to provide **Agency Name** authentic documentation that reports the criminal history information accurately and completely. This information must be provided prior to determination of suitability for **(state the purpose from your user agreement - i.e. employees, volunteers, contractors, licenses, etc.)**.

CJI/CHRI shall not be copied, emailed, faxed or scanned nor disseminated to secondary parties or the employee. Any casual unauthorized release of information is not allowed (i.e. social media, discussion with friends or family members). CJI/CHRI shall only be discussed (written or verbally) between the authorized personnel as necessary to carry out the specific purpose for which the information was requested and all verbal discussions take place in private.

If the fingerprint-based check has a disqualifying factor, the authorized personnel who opened and reviewed the record will hand-carry the record to the ASC or occasionally other authorized personnel, to determine the next steps. The ASC or authorized personnel will discuss the contents of the record with the applicant in a private and secure manner to obtain any additional information.

If your agency does not have an appeals process for an initial denial of employment, etc. then remove this paragraph. **Agency Name** will provide applicants with an appeals process. The appeals process can take place when the applicant challenges his/her suitability determination made by those on the authorized personnel list. This process concludes with the **(title of individual)** making the final suitability determination.

VIII. Storage of CJI/CHRI

Once the CJI/CHRI has met its purpose, it is filed by authorized personnel in a secured locked filing cabinet in the HR office in a secure location. CJI/CHRI are retained in accordance with **Agency Name's** record retention policy. This CJI/CHRI filing cabinet does not contain any other employment records or any files which may be considered public record to prevent unauthorized access or dissemination. The filing cabinet is locked throughout the day to prevent unauthorized access by non-authorized personnel. The keys to the filing cabinet are kept secure by the ASC and another back-up key is kept secure with other authorized personnel. Only authorized personnel are allowed access to the filing cabinets that contain the CJI/CHRI. If a key to the filing cabinet that contains the records is lost, the filing cabinet will be re-keyed to prevent unauthorized access. Authorized personnel are responsible for safeguarding the confidentiality of the information at all times and may not disclose or allow access to the information to anyone except authorized personnel. CJI/CHRI is always secured and never left unattended.

If your agency does not store CJI/CHRI electronically then remove this paragraph. The actual copy of the CJI/CHRI results are not electronically stored, but as mentioned above in section VI. Handling/Retention of CJI/CHRI, some essential information is entered for reference and tracking purposes and electronically stored. Physical protection of CJI/CHRI as well as a physically secure location for CJI/CHRI will be shared and verified with the DPS. The database where the CJI/CHRI is stored is in the **Agency Name** Human Resources server which is secure, encrypted and controlled directly by **Agency Name**. No other organization has access to this database. All visitors to the area where CJI/CHRI are stored electronically are accompanied by authorized personnel.

IX. FBI notifications

The authorized personnel will provide a copy of the FBI Applicant's Privacy Rights Notification to the applicant when they arrive to be fingerprinted. Copies of the FBI Applicant's Privacy Rights Notification are available at the front desk and it will contain the following information:

- Your fingerprints will be used to check the criminal history records of the FBI. If you have a criminal history record, the officials making a determination of your suitability for the job, license, or other benefits must provide you the opportunity to complete or challenge the accuracy of the information in the record. You should be afforded a reasonable amount of time **(your agency must define what reasonable means, i.e. 5 days, etc.)** to correct or complete the record (or decline to do so) before officials deny you the job, license, or other benefits based on information in the criminal history record.
- The procedures for obtaining a change, correction or updating of your FBI criminal history record are set forth in Title 28 Code of Federal Regulations, section 16.30 through 16.34. Information on how to review and challenge your FBI criminal record can be found at www.fbi.gov under Identity History Summary Checks or by calling 304-625-5590.
- To obtain a copy of your Arizona criminal history in order to review, update or correct the record, you can contact the Arizona Department of Public Safety Criminal History Records Unit at 602-223-2222 and to obtain a fingerprint card and review and challenge packet. Information on the review and challenge process can be found on the DPS webpage at www.azdps.gov.

X. Disposal of CJI/CHRI

When the CJI/CHRI has met the destruction date in accordance with **Agency Name's** record retention policy, authorized personnel will destroy the CJI/CHRI. **State how you destroy CJI/CHRI (either shredding or burning).**

In the event of a third-party contractor that performs the shredding, authorized personnel will accompany the vendor to oversee the shredding and handling of the CJI/CHRI. The authorized personnel, will observe the contractor from the time the shredding receptacle is picked up through the complete destruction of the CJI/CHRI.

XI. Misuse of CJI/CHRI

In the event of deliberate, reckless or unintentional misuse of CJI/CHRI, the employee will be disciplined in accordance with the signed acknowledgement statement and **Agency Name's Human Resources** policy which can include termination.

XII. Training and Acknowledgement Statements

All authorized personnel must be trained in the online security awareness (CJIS Online) training within six months of hire (or upon being added to the Authorized Personnel List) and then every two years thereafter.

All authorized personnel must be trained in all in-house privacy and security training on the access, use, handling, dissemination and destruction procedures regarding CJI/CHRI within six months of hire (or upon being added to the Authorized Personnel List) and then every two years thereafter.

All authorized personnel will sign an acknowledgement statement regarding the notification of the penalties for misuse of CJI/CHRI. It is a class 6 felony in Arizona for a person to misuse CJI/CHRI per Arizona Revised Statues (A.R.S. § 41-1756).

All training and acknowledgement statements will be recorded on a training documentation log. This log is reviewed during audits by DPS.