

# NONCRIMINAL JUSTICE COMPLIANCE WORKSHEET

## PART 1 - POLICIES AND PROCEDURES

Use the Arizona Noncriminal Justice Agency Guide and "NCJA Compliance Training" class materials as resources. Some categories below have verbiage examples which are adapted from policies/procedures used by other agencies. You are under no obligation to use the wording of the examples or to adopt the examples as part of your processes. The examples are not intended to be legal advice on how to write your agency's policies and procedures; each agency is encouraged to consult its legal advisor for wording and policies appropriate for its own type of organization.

### USE

#### How does the agency ensure CHRI is only used for the purpose for which it was requested?

Points to consider:

- Do you state the purpose for which CHRI is requested? (If you don't state what it is used for, then how are people supposed to know what the use is limited to?)
- What does your agency's authorization say about your agency's use/purpose?
- Are there any additional laws/regulations which apply to your agency as far as criminal history results are concerned?

References to review: NCJA Guide Section 3, NCJA Guide Section 5.2.3

#### **Examples**

"Criminal history information is only to be used for the specific purpose for which it was requested (employment)."

"The school district completes fingerprint-based criminal history checks for paid and unpaid personnel under the authorization of Arizona Revised Statutes 15-512 and District Governing Board policy."

"CJI/CHRI shall only be used for the specific purpose for which it was requested, which is for employing paid sworn firefighters, reserve firefighters or volunteer firefighters (ARS 48-805)."

### ACCESS

#### Who is authorized to access/view the CHRI?

Points to consider:

- Consider categories of people or people with certain job duties - not names of individuals.
- What are the criteria to be part of the Authorized Personnel?
- Do you have procedures for when/how Authorized Personnel receive the agency's privacy and security training?

References to review: NCJA Guide Section 3, NCJA Guide Section 4.1.2, NCJA Guide Section 5.2.1 (#2) & 5.2.3

#### **Examples**

"Human Resources (HR) staff that may possibly come in contact with criminal history information will be given access to view/handle criminal history information. These individuals include the HR director, HR specialist, HR secretary, and HR receptionist. Upon termination of authorized personnel, HR will update its list with DPS within 48 hours of termination."

"District authorized personnel are Human Resources employees."

"The Human Resources Department will manage the fingerprint checks for paid city employees, excluding the Police Department. The Community & Recreation Services Department will manage the checks for volunteers, part-time, and contract employees. The Authorized Personnel List shall contain the minimum number of employees necessary, but will include all personnel who may possibly come into contact with CJI/CHRI. "

## How does the agency restrict access to only Authorized Personnel?

Points to consider:

- Do you need to consider key access/room access to the storage area?
- Communication about CHRI can only be among Authorized Personnel. How large is your agency - do the Authorized Personnel know who the other Authorized Personnel are or how to authenticate the other person's access?
- Do you store CHRI electronically - who has access to the online files? (see also Technical/Digital Security)

References to review: NCJA Guide Section 3

### **Examples**

"CJI/CHRI shall be stored in a locked drawer/cabinet located in the office of the ASC. Only Authorized Personnel will be issued a key."

"The only personnel authorized to access, discuss, use, handle, disseminate, file and destroy CJI/CHRI are the persons listed on the most current Authorized Personnel List (List) on file with the Arizona Department of Public Safety (DPS) Access Integrity Unit (AIU). The public, all outside persons and entities, terminated personnel and personnel not listed on the most current Authorized Personnel List are prohibited from handing or having any access to CJI/CHRI for any reason."

## HANDLING

### General Considerations

Points to Consider

- Consider and document the process for CHRI from its receiving point to its destruction. (You don't need to be unnecessarily restrictive, but the Authorized Personnel should have enough information to know what to do with the CHRI at each step.)
- What is your agency's specific authorization for fingerprint criminal history checks and does it have any additional requirements you must consider?
- Are there any additional laws/regulations which apply to your agency as far as criminal history results are concerned?

References to review: NCJA Guide Section 3, NCJA Guide Section 5.2.3

## What happens to the CHRI when it arrives?

Points to consider:

- Where is it received? By whom?
- Where does it go from the receiving point?
- Who processes it?

References to review: NCJA Guide Section 3, NCJA Guide Section 5.2.3

### **Examples**

"Results of the fingerprint criminal history check will be sent to the District Office. All criminal history checks that are returned with a disqualifying factor will be handled and housed by the approved personnel at the District office."

"Fingerprint results from DPS are only opened by Authorized Personnel in Human Resources"

"All criminal history results go to the Director's office to be opened and reviewed".

## What happens to the CHRI after it is opened?

Points to consider:

- How is it reviewed/documented?
- Who discusses it with the applicant and what are the procedures for doing that?
- Have you taken into account privacy during conversations and communication among necessary personnel?
- Who can see/handle/review it?
- What happens to it when the processing is done?
- Are all the people involved in this process part of the Authorized Personnel?

References to review: NCJA Guide Section 3, NCJA Guide Section 5.2.3

### **Examples**

"Authorized personnel may discuss the contents of the criminal history record with the applicant in a private and secure place. The applicant may not be given a copy of the record; the record is for district use only. The applicant should be informed that if he/she wishes to challenge the content of the record, a Review and Challenge packet for Arizona criminal history can be obtained from DPS Criminal History Records. Information on challenging a FBI record can be obtained by contacting the FBI (current phone numbers and more information is available on the FBI website)."

"Verbal or written communications regarding criminal history may only occur between personnel authorized to view the information and only if necessary to carry out the specific purpose for which the information was requested. Care should be taken to prevent overhearing, eavesdropping, or interception of communication. Criminal history cannot be emailed or sent electronically via cell phone or other handheld device. Casual unauthorized release of information is not allowed, i.e., social networks, discussions with friends and family members. Criminal history cannot be further disseminated to any other agency or individual."

"CJI/CHRI received is not shared nor is it released in any form to the public. Employees will not confirm or deny the existence of an individual's criminal history record to the public or to any unauthorized individual or agency."

"CJI/CHRI shall NOT be copied, emailed, faxed, scanned or stored electronically. CJI/CHRI shall NOT be disseminated to secondary parties. CJI/CHRI shall NOT be discussed other than:

- a. Between Authorized Personnel as necessary to carry out the specific purpose for which the information was requested. Personnel will ensure that verbal discussions take place in private, so as to not be overheard.
- b. With an applicant, as outlined in the Applicant Process/Fingerprint Submittals section of this procedure."

"If the fingerprint-based check has a disqualifying factor, the technician will discuss the record with the Director to determine the next steps. The designated technician will discuss the contents of the record with the applicant in a private and secure manner to obtain any needed additional information. The copy of the criminal history check will not be provided to the applicant."

"All fingerprint-based criminal history check results are accessed only by Authorized District Personnel."

## How does the agency store CHRI?

Points to consider:

- Do you have a locked room or locked cabinet?
- If you are storing electronically, what are your rules for access, physical and technical safeguards of the computer and server, and reporting possible breaches? (If there is no electronic storage allowed, do you say so?)

References to review: NCJA Guide Section 3, NCJA Guide Section 5.2.3  
Electronic storage - FBI CJIS Security Policy Part 5

### **Examples**

"The results of state and FBI record searches are stored in the office inside of a locked filing cabinet in the Human Resources department. Only authorized personnel have a key to the office and filing cabinet. Authorized personnel must accompany all visitors to this area."

"All CJ/CHRI received by the district office is stored in a locked filing cabinet. Only Authorized Personnel may have access to this information. CJ/CHRI information is not stored electronically. "

## How does the agency prevent unauthorized access?

Points to consider:

- Are you limiting access to the storage?
- How are unauthorized personnel prevented access (unauthorized personnel in agency, terminated/formerly authorized personnel)?
- Do you have rules for not leaving CHRI unattended when it's not in secure storage?
- Do you have precautions regarding issues like overhearing and casual disclosures?

References to review: NCJA Guide Section 3, NCJA Guide Section 5.2.3

### **Examples**

"Only Authorized Personnel are permitted access to the locked filing cabinet where CHRI is stored."

"Upon termination of authorized personnel, that employee's final paycheck will be held until the keys have been returned. If a key is lost then HR will have the office and filing cabinet re-keyed to prevent unauthorized access."

"Authorized personnel may discuss the contents of the criminal history record with the individual in a private and secure place, but authorized personnel may not give a copy of the criminal history to the individual."

"Employees with access to criminal history information are responsible for safeguarding the confidentiality of the information at all time and may not disclose or allow access to the information to anyone except authorized individuals."

"All criminal history results are stored in the locked filing room separate from any file which may be released as public record. Only Authorized Personnel will be granted unsupervised access to the filing room. All other personnel must be accompanied by an Authorized Person."

"The filing cabinet for the CHRI is maintained in the Director's office. The door to the office will stay locked any time the room is empty."

## Is secondary dissemination allowed at the agency?

Points to consider:

- Secondary dissemination is only allowed if authorized by law - an agency cannot authorize itself to disseminate. If this is allowed, what are your procedures for sending the CHRI and protecting it enroute?
- How do you authenticate the recipient?
- What are your logging/tracking procedures?

References: NCJA Guide Section 3

## How long does the agency retain CHRI?

Points to consider:

- CHRI should be destroyed when your agency no longer needs it. Define when your agency is done with the CHRI. (Keep in mind that the longer you have it, the more you risk unauthorized access/dissemination.)
- When is your suitability determination done? Have any appeals been exhausted? You can't use CHRI for any other purpose, so when can you destroy it?
- Do you have retention guidelines or other regulatory guidelines which apply?

References to review: NCJA Guide Section 3, your agency's retention guidelines, your agency's appeals process

### **Examples**

"CHRI must be destroyed when the purpose for which it was requested has been fulfilled."

"When the department is notified that that the applicant's appeals hearing is completed and the final disposition determined, Authorized Personnel will shred the criminal history information and document the destruction on the tracking log."

## What are the procedures for destroying CHRI?

Points to consider:

- You can shred it or burn it - which is your agency doing?
- Are you limiting the destruction to Authorized Personnel?
- Do you have a contracted shredding company - if so, what are your procedures for witnessed destruction?

References to review: NCJA Guide Section 3

### **Examples**

"Records are to be shredded by authorized personnel only."

"CJI/CHRI must be completely destroyed when no longer needed to minimize the risk of unauthorized access and distribution. The information will be shredded by authorized District employees."

"When no longer needed for its original purpose, CJI/CHRI must be completely destroyed in the shredder. Originals and any copies must be destroyed by personnel who are authorized to access/handle CJI/CHRI."

"The contracted shredder arrives the first week of every month. The contractor will be accompanying by one of the Authorized Personnel, who will observe the contractor from the time the shredding receptacle is picked up through the complete destruction of the criminal history. This observation duty will rotate among those on the Authorized Personnel List."

## FINGERPRINT SUBMISSIONS

### What is the agency process for giving FBI notifications to the applicant?

Points to Consider:

- When and how do the applicants get the required notifications? Are you providing them in writing?
- Do your employees know that the applicant has to be able to take the notifications with them if they want to?
- What defines the "reasonable opportunity" for an applicant to review and challenge a criminal history record? Is it one standard amount of time, or does it vary on a case by case basis?
- Do you have an appeals process? How is the applicant notified of the appeals process?

References to review: NCJA Guide Section 2.5, NCJA Guide Section 5.2.2 (#5), your agency's appeals process

#### **Example**

"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 benefit must provide you the opportunity to complete or challenge the accuracy of the information in the record. You will be afforded a reasonable amount of time to correct or complete the record (or decline to do so) before officials deny you the job, license, or other benefit 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 (CFR), Section 16.30 through 16.34. Information on how to review and challenge your FBI criminal history record can be found at [www.fbi.gov](http://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/correct the record, you can contact the Arizona Department of Public Safety Criminal History Records Unit at (602) 223-2222 to obtain a fingerprint card and a Review and Challenge packet. Information on the review and challenge process can be found on the DPS website ([www.dps.gov](http://www.dps.gov))."

### How does the agency verify the identity of the applicant being fingerprinted?

Points to consider:

- *We fingerprint on-site.*
  - Find ideas for your process by reviewing the references. There are different ways to formulate your procedures.
  - Does your fingerprint technician ask for photo identification? What types of ID do you accept?
  - Is there any process to verify that the technician asked for ID - a tracking sheet or a log?
- *We sent applicants elsewhere to be fingerprinted.*
  - Find ideas for your process by reviewing the references. There are different ways to formulate your procedures.
  - Are you sending instructions and/or a verification form with the applicant? Or do you have an agreement or contract with the fingerprinting agency to abide by procedures to identify your applicants?

References to review: NCJA Guide Section 2.2  
NCJA Guide Section 5.2.2,  
NCJA Guide Appendix G  
*Compact Council Identity Verification Program Guide* (found on [www.fbi.gov](http://www.fbi.gov))

(See examples under fingerprint tampering section.)

## How does the agency prevent fingerprint card tampering?

Points to consider:

- *We fingerprint on-site.*
  - Find ideas for your process by reviewing the references. There are different ways to formulate your procedures.
  - Does your procedure say employees should retain the card and not give it back to the applicant?
  - Do you have any tracking of who fingerprinted a particular applicant?
  
- *We sent applicants elsewhere to be fingerprinted.*
  - Find ideas for your process by reviewing the references. There are different ways to formulate your procedures.
  - Are you sending instructions and/or a tracking verification form with the applicant?
  - Do you use a sealed envelope system where the technician at the fingerprinting agency seals the fingerprint card inside an envelope before giving it to the applicant, or do you have a pickup or mailing agreement with the fingerprinting site?
  - Do you reject "open" prints and/or those which appear to be tampered with?

References to review: NCJA Guide Section 2.3  
NCJA Guide Section 5.2.2  
NCJA Guide Appendix G  
*Compact Council Identity Verification Program Guide* (found on [www.fbi.gov](http://www.fbi.gov))

### ***Examples (Identity Verification and Tampering Prevention)***

"Individuals are fingerprinted at the City's Community and Recreation Services (CRS) office by CRS staff. Individuals are required to present photo identification to verify identity. Once the fingerprints are on the card, the card remains in the possession of CRS staff and the card is not returned to the individual. CRS staff hand-carry the cards and the COS Fingerprint Log for employee or volunteers as defined above to the Human Resources Office in confidential envelopes."

"Give the applicant the fingerprint card and the instruction/verification sheet in a brown envelope. The applicant should be told to be fingerprinted at the police department or [REDACTED]. The applicant can only hand-carry the fingerprint card back to the front counter if the fingerprint technician has sealed the fingerprint card and verification sheet inside the envelope. The envelope cannot show any signs of opening or tampering."

"Fingerprinting will be conducted by the [REDACTED] Police Department, who will confirm the identity of the applicant by current state-issued identification card (other forms of identification will not be accepted). The fingerprint card shall not be given back to the applicant. The [REDACTED] Police Department will hold the card in a secure location until it is retrieved, in person, by Authorized Personnel of the [REDACTED] District. Authorized Personnel will secure the card in a locked filing cabinet until it is submitted."

## MISUSE

### What is the agency disciplinary policy for misuse of CHRI?

Points to consider:

- What is your agency policy for steps to be taken in the event of misuse of criminal history?
- What are applicable disciplinary actions or what employee misconduct policy does this fall under?
- When you are training your employees on privacy and security, what do you need to say about the following to be sure they are fully informed about what constitutes misuse and what the consequences are?
  - Arizona laws/regulations
  - federal law/regulations
  - applicant privacy and due process
  - civil liability for violations

References: NCJA Guide Section 3, NCJA Guide Section 5.2.3 (#4), Your agency's misconduct policies

#### **Examples**

"In the event of deliberate, reckless or unintentional misuse of CJI/CHRI, the employee will be written up following the school's disciplinary policy."

"Misuse of criminal history information falls under the Staff Ethics and Staff Conduct policies and is subject to disciplinary action under the district disciplinary procedure."

"In the event of deliberate, reckless or unintentional misuse of CJI/CHRI, the employees will be subject to disciplinary action, up to and including termination, as outlined in the Corrective Action/Disciplinary Process of the Personnel Policies."

## MISCELLANEOUS QUESTIONS/NOTES

Points to consider:

- Have you reviewed your agency's policies to see if you have existing policies already covering these issues?
- Do you have an administrative code which applies to your agency which may already have processes which apply?
- Have you reviewed your fingerprinting authorization (statutes, ordinance, etc.) to make sure that your processes do not conflict with specific provisions in your authorization?
- Do you have oversight entities which may have policies you need to consider when formulating your processes? Examples:
  - State oversight agencies (Dept of Education, Board for Charter Schools)
  - Governing boards (district boards)
  - Administrative agencies (state oversight boards, auditing entities, Administration of Courts)
- Have you consulted your agency's legal advisor?
- Did you ask the DPS AIU Noncriminal Justice Compliance Team for clarification if needed?

# NONCRIMINAL JUSTICE COMPLIANCE

## PART 2 - TRAINING AND ACKNOWLEDGEMENT STATEMENTS

### REQUIRED TRAINING FOR THE AGENCY'S AUTHORIZED PERSONNEL

#### Part 1 - CJIS Online

*"How do I do this?"*

To comply with the CJIS Online Training component:

1. Have personnel go to [www.CJISOnline.com](http://www.CJISOnline.com)
2. Log in information is on the CJIS Online Noncriminal Justice Agency Supplement.
3. Instruct personnel to review the supplement and the applicable CJIS Online sections.
4. When they have finished viewing the training, Document each person's completion on the Training Documentation Form.

*"Where do I find the documents I need?"*

Forms and documents can be downloaded from the NCJA Fingerprint Compliance section of the DPS website ([www.azdps.gov/Services/NCJA](http://www.azdps.gov/Services/NCJA)). If you're having trouble locating what you need, call or email the Noncriminal Justice Compliance Team. Authorized Personnel training is discussed in sections 4.2 and 5.2.4 of the NCJA Guide.

#### Part 2 - Internal Agency Training

*"How do I do this?"*

##### Task 1

Draft a training outline which lists the contents of the agency's privacy and security training for Authorized Personnel. The training outline can be as simple or elaborate as it needs to be to suit your agency's needs. It should serve two main functions:

- Personnel at your agency are aware of which policies/procedures apply to criminal history handling and what they are responsible for.
- Based on your training outline, an auditor should be able to identify the content of the training presented to Authorized Personnel. During an audit interview, the auditor will need to review applicable policies.

The training outline can be as simple as matching the required policy/procedure categories (Use, Access, Handling, etc.) to the policy number or written procedure section which covers that process, or you can add detail and training notes if you desire. Authorized Personnel training is discussed in sections 4.2 and 5.2.4 of the NCJA Guide.

##### Example

##### Training Outline

Use, Access - Dept Policy 2.1 - 2.2  
Handling - Dept Policies 2.3 through 5.6  
Fingerprint Submissions - see office procedure dated 2/13/2014  
Misuse - the Employee Misconduct Policy and Policy 6 Consequences

##### Task 2

1. Use whatever training method works best for your agency to present the material. Some agencies add the training to an online learning system the agency already uses. Some hold an in-service meeting and train all employees at once. Some compile all the applicable policies into a training notebook or an online file for employees to review and indicate they have read and understood. Determine what method suits your agency and implement the training.
2. Once all personnel have completed the training, document the completion date on the Training Documentation Form.

## ACKNOWLEDGEMENT STATEMENTS

Each person on your agency's Authorized Personnel List must sign a statement acknowledging notification of penalties for misuse, including agency disciplinary actions. There is no standard form for this; your agency makes the agency's standard acknowledgement statement that meets its needs depending on its format for training.

*"What are the minimum requirements for the Acknowledgement Statement?"*

1. At a minimum, the statement must include something similar to "I acknowledge notification of the penalties for misuse of criminal history". It can contain whatever other language the agency deems is necessary. (Some agencies choose to put the training outline on the Acknowledgement Statement and add language acknowledging the training as well.)
2. It must have a place for the authorized person to sign.

References to review: NCJA Guide Section 3.7, NCJA Guide Section 4.2.2, NCJA Guide Section 5.2.4, your agency's misconduct policies

### **Examples**

The next pages have examples of Acknowledgement Statements drafted by various agencies.

## **EXAMPLES**

### ACKNOWLEDGEMENT STATEMENT

All Authorized Personnel are made aware of the guidelines, consequences and liabilities that could occur from unauthorized use of criminal justice information and criminal history record information. Employees are advised of the following:

- It is a class 6 felony in Arizona for a person to:
  - Give criminal history record information (CHRI) to someone who is not authorized to receive it.
  - Allow unauthorized access to criminal history information (CHI).
  - Use criminal history record information (CHRI) for any other purpose other than those provided for in ARS 41-1750.
- Other federal and/or state penalties may apply depending upon the circumstances of the release.
- Unauthorized release could also potentially expose the District to civil liability.
- Access to criminal justice information (CJI) and CHRI via submitted fingerprints could be suspended or cancelled for violations of security and/or violations of the Terms and Conditions in the User Agreement.
- Misuse subjects an employee to discipline under the District Employee Misconduct policy.

I acknowledge that I have been advised of the consequences of misuse of criminal justice and criminal history record information.

\_\_\_\_\_  
Employee Name (Print)

\_\_\_\_\_  
Employee Signature

\_\_\_\_\_  
Date

**Acknowledgement Statement**

**For Authorized Personnel Regarding Privacy and Security of Criminal Justice Information (CJI) and Criminal History Record Information (CHRI)**

All Authorized Personnel are trained on the authorized use, access, handling, destruction, privacy and security of criminal history information (CJI) and criminal history record information (CHRI) and [REDACTED] District’s Fingerprinting and Criminal Background Check SOG. Authorized Personnel are also informed of the possible consequences of misuse of CJI/CHRI. Consequences may include:

- **Internal.** In the event of deliberate, reckless or unintentional misuse of CJI/CHRI, the employees will be subject to disciplinary action, up to and including termination, as outlined in the Corrective Action/Disciplinary Process of the Personnel Policies.
- **Arizona Revised Statutes (ARS).** ARS §41-1756 states it is a class 6 felony in Arizona for a person to:
  - Give criminal history record information to someone who is not authorized to receive it.
  - Allow unauthorized access to criminal history Information.
  - Use criminal history record information for any other purpose than those provided in ARS.
  - Other state penalties may apply depending upon the circumstances.
- **Federal Statutes.** Federal statutes states that access to CJI/CHRI is subject to cancellation for dissemination outside the authorized recipients(s) (Title 28 USC §534 and Title 28 CFR §20.33). Other federal penalties may apply depending upon the circumstances.
- **Civil Liability.** Unauthorized release could also potentially expose the employee and/or District to civil liability.
- **Other Consequences.** The District’s access to CJI/CHRI may be suspended or cancelled according to the terms and conditions of the user agreement with DPS.

By signing below, I acknowledge that I have received training on the [REDACTED] District’s Fingerprinting and Criminal Background Check SOG, including procedures for privacy and security of criminal history information. I further acknowledge that I have been advised of the consequences of misuse of CJI/CHRI.

\_\_\_\_\_  
Employee Signature

\_\_\_\_\_  
Date

\_\_\_\_\_  
Employee Name (Print)

**POLICIES/PROCEDURES SIGN OFF**

Criminal justice information (CJI) and criminal history record information (CHRI) is only used for valid employment (paid and unpaid) purposes only. Only authorized employees are allowed to view CJI/CHRI. I have been informed of the privacy and security policies/procedures regarding use, release, physical security, and destruction of CJI/CHRI.

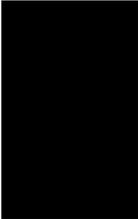
I understand that violations of these policies/procedures will result in disciplinary action under the employee code of conduct and may constitute violations of law which could result in criminal prosecution or civil liability.

\_\_\_\_\_  
Employee Name (Print)

\_\_\_\_\_  
Employee Signature

\_\_\_\_\_  
Date

**Training Outline**

POLICY		AUTHORIZED PERSONNEL AND ACCESS
POLICY		USE/HANDLING OF INFORMATION
POLICY		COMMUNICATIONS/DISSEMINATION
POLICY		PHYSICAL SECURITY
POLICY		RETENTION/DESTRUCTION
POLICY		CONSEQUENCES OF MISUSE

**Acknowledgement Statement**

I acknowledge that I have received training regarding the procedures for privacy and security of criminal history information and I have been advised of the consequences of misuse of criminal justice and criminal history record information.

\_\_\_\_\_  
Employee Signature

\_\_\_\_\_  
Date

\_\_\_\_\_  
Date Training Conducted

\_\_\_\_\_  
Trainer

