SAMPLE POLICY INSTRUCTIONS

This document is a sample policy outlining the requirements needed in order to obtain compliance. Each section of the policy highlights a general overview of the procedures each agency should have in place. In order to be accepted, this document must be updated to include each agency's specific procedures currently in place.

As mentioned above, this is a sample policy and should be updated. Anywhere <Agency> is found must be updated with each unique agency's name. Throughout the policy there are also additional fill-ins formatted in the same manner that must be updated.

Adopting this sample policy without updating the document to reflect your agency's procedures will result in non-compliance.

<Agency>

POLICY GOVERNING
FINGERPRINT-BASED CRIMINAL HISTORY RECORD INFORMATION (CHRI)
CHECKS MADE FOR NON-CRIMINAL JUSTICE PURPOSES

This policy is applicable to any fingerprint-based state and national criminal history record check made for non-criminal justice purposes and requested under applicable federal authority and/or state statute authorizing such checks for <update with your agency's purpose for receiving CHRI (ex. licensing/employment> purposes. Where such checks are allowable by law, the following practices and procedures will be followed.

Requesting CHRI checks

Fingerprint-based CHRI checks will only be conducted as authorized by the FBI and LSP, in accordance with all applicable state and federal rules and regulations. If an applicant or employee is required to submit to a fingerprint-based state and national criminal history record check, they shall be informed of this requirement and instructed on how to comply with the law. Such instruction will include information on the procedure for submitting fingerprints. In addition, the applicant or employee will be provided with all information needed to successfully register for a fingerprinting appointment.

Acceptable Use

All CHRI is subject to strict state and federal rules and regulations. CHRI is used only for the official purpose for which it was requested, and CHRI cannot be shared with other entities for any purpose, including subsequent hiring determinations. All receiving entities are subject to audit by the Louisiana State Police (LSP) and the FBI, and failure to comply with such rules and regulations could lead to sanctions. Furthermore, an entity can be charged with federal and state crimes for the willful, unauthorized disclosure of CHRI.

CHRI Training

An informed review of a criminal record requires training. Accordingly, all personnel authorized to receive and/or review CHRI at <Agency> will review and become familiar with the educational and relevant training materials regarding CHRI laws and regulations made available by the appropriate agencies.

In addition to the above, all personnel authorized to receive and/or review CHRI must undergo Security Awareness Training on an annual basis. This training will be accomplished using the training provided by CJIS Online.

Adverse Decisions Based on CHRI

If inclined to make an adverse decision based on an individual's CHRI, <Agency> will take the following steps prior to making a final adverse determination:

- Provide the individual the opportunity to complete or challenge the accuracy of his/her CHRI; and
- Provide the individual with information on the process for updating, changing, or correcting CHRI.

A final adverse decision based on an individual's CHRI will not be made until the individual has been afforded a reasonable time of <time period (ex. 15 days, 30 days, etc)> to correct or complete the CHRI.

Non-Criminal Agency Coordinator (NAC)

The <Agency> NAC is <Name>. The NAC is responsible for the following:

- Maintaining an updated Authorized Personnel List on file with the LSP Bureau.
    - Ensuring everyone included on this list must undergo the appropriate level of CJIS Security Awareness Training
- Inform the LSP Bureau of changes in the agency head or any relevant business information (agency name changes, mailing/physical address changes, etc.).
    - Contact the LSP Bureau immediately to update the User Agreement and, if necessary, submit the new authorization to the LSP Bureau.
    - Submit a NAC change form to the LSP Bureau in the event of a change in roles.

Local Agency Security Officer (LASO)

The <Agency> LASO is <Name>. The LASO is responsible for the following:

- Identifying who is using or accessing CHRI and/or systems with access to CHRI.
- Ensuring that personnel security screening procedures are being followed as stated in this policy.
- Ensuring the approved and appropriate security measures are in place and working as expected.

When changes in the LASO appointment occur, <Agency> shall notify the Louisiana State Police of the change.

Personnel Security

All Personnel

All personnel requiring access to CHRI must first be deemed "Authorized Personnel." The LSP will review and determine if access is appropriate. Access is denied if the individual has ever had a felony conviction, of any kind, no matter when it occurred. Access may be denied if the individual has one or more recent misdemeanor convictions.

In addition to the above, an individual believed to be a fugitive from justice, or having an arrest history without convictions, will be reviewed to determine if access to CHRI is appropriate. The LSP will take into consideration extenuating circumstances where the severity of the offense and the time that has passed would support a possible variance.

Persons already having access to CHRI and who are subsequently arrested and/or convicted of a crime will:

- Have their access to CHRI suspended until the outcome of an arrest is determined and reviewed by the LSP in order to determine if continued access is appropriate.
- Have their access suspended indefinitely if a conviction results in a felony of any kind.
- Have their access denied by the LSP where it is determined that access to CHRI by the person would not be in the public's best interest.

All access to CHRI by support personnel, contractors, and custodial workers will be denied. If a need arises for such persons to be in an area(s) where CHRI is maintained or processed (at rest or in transit); they will be escorted by, or be under the supervision of, authorized personnel at all times while in these area(s).

Personnel Termination

The LASO shall terminate access to CHRI immediately upon notification of an individual's termination of employment.

<Agency> CHRI access termination process:

- Notification will be sent via email to the LSP
- This is to be done within 24 hours of receiving notification of termination
- All keys, email accounts, etc. will be obtained/disabled from the user within 24 hours

Storage of CHRI

CHRI shall only be stored for extended periods of time when needed for the integrity and/or utility of an individual's personnel file. Administrative, technical, and physical safeguards, which are in compliance with the most recent LSP and FBI Security Policy, have been implemented to ensure the security and confidentiality of CHRI. Each individual involved in the handling of CHRI is to familiarize himself/herself with these safeguards.

In addition to the above, each individual involved in the handling of CHRI will strictly adhere to the policy on the storage and destruction of CHRI.

Media/Physical Protection

All media containing CHRI is to be protected and secured at all times. The following is established and to be implemented to ensure the appropriate security, handling, transporting, and storing of CHRI media in all its forms.

Physical Storage and Access
Physical CHRI media shall be securely stored within physically secured locations or controlled areas. Access to such media is restricted to authorized personnel only and shall be secured at all times when not in use or under the supervision of an authorized individual.

Physical CHRI media:

- Is to be stored within employee records when feasible or by itself when necessary

- Is to be maintained within a lockable filing cabinet, drawer, closet, office, safe, vault, or other secure container

Media Storage and Access

<Include details on where your agency maintains electronic CHRI and how it is secured>

Electronic CHRI media shall be securely stored within physically secured locations or controlled areas. Access to such media is restricted to authorized personnel only and shall be secured at all times when not in use or under the supervision of an authorized individual.

Electronic CHRI media:

- Is to be stored on secure servers within a physically secure location when feasible
- <Include details on how electronic CHRI is secured>

Destruction of CHRI

Disposal of Physical Media

Once physical CHRI media (paper/hard copies) is determined to be no longer needed by <Agency>, it shall be destroyed and disposed of appropriately. Physical CHRI media shall be destroyed by shredding, cross-cut shredding, or incineration. <Agency> will ensure such destruction is witnessed or carried out by authorized personnel:

- The LASO shall witness or conduct disposal.
- Cross-cut shredding will be the method of destruction used by <Agency>.

Media Sanitization and Disposal (Disposal of Electronic Media)

To compliantly destroy and sanitize electronic CHRI, a NCJA has three options. The NCJA must choose one of these options to destroy the electronic CHRI and ensure it is properly documented in the agency policies.

Once electronic CHRI media (data stored on computers) is determined to be no longer needed by <Agency>, it shall be destroyed and disposed of appropriately.

*Agency must choose one option below to use in this policy

Option 1: The NCJA will sanitize the electronic CHRI by overwriting the data at least three times prior to disposing of or reusing the computer/device/system the electronic CHRI was stored on.

Overwriting the CHRI data must be completed or witnessed by authorized personnel within the agency.

Option 2: The NCJA will degauss the electronic CHRI prior to disposing of or reusing the computer/device/system the electronic CHRI was stored on. Degaussing the CHRI data must be completed or witnessed by authorized personnel within the agency. (Degaussing is neutralizing a magnetic field to erase information from a magnetic disk or other storage device).

Option 3: If the computer/device that the CHRI data is stored on is no longer operational, the NCJA must physically destroy the device. Destruction of the device containing electronic CHRI must be completed or witnessed by authorized personnel within the agency.

Retention of CHRI

Federal law prohibits the repurposing or dissemination of CHRI beyond its initial requested purpose. Once an individual's CHRI is received, it will be securely retained in internal agency documents for the following purposes only:

- Historical reference and/or comparison with future CHRI requests
- Dispute of the accuracy of the record
- Evidence for any subsequent proceedings based on information contained in the CHRI.

CHRI will be kept for the above purposes in:

- Hard copy form in personnel files located in the locked filing cabinet located in the locked filing room
    - CHRI will be maintained for <**Add retention timeframe here**>. At the end of this term, the CHRI will be disposed of according to the Disposal of Physical Media policy.

Disciplinary

If an individual at <Agency> has misused or is currently misusing CHRI, the following requirements will be adhered to.

- Using CHRI for any purpose other than what is allowed by state statute or Federal code is considered misuse.
- The specific steps your agency will take in the event intentional misuse is discovered.

- Misuse of CHRI can result in loss of access to CHRI, loss of employment and/or criminal prosecution.
- Misuse of CHRI shall be reported to the state.

Incident Response

The security of information and systems in general, and of CHRI in particular, is a top priority for <Agency>. Therefore, we have established appropriate operational incident handling procedures for instances of an information security breach. It is each individual's responsibility to adhere to established security guidelines and policies and to be attentive to situations and incidents which pose risks to security. Furthermore, it is each individual's responsibility to immediately report potential or actual security incidents to minimize any breach of security or loss of information. The following security incident handling procedures must be followed by each individual:

- All incidents will be reported directly to the LASO.
- If any records were stolen, the incident will also be reported to appropriate authorities.
- Once the cause of the breach has been determined, disciplinary measures will be taken in accordance with the disciplinary policy.

In addition to the above, the LASO shall report all security-related incidents to the LSP within 24 hours.

All agency personnel with access to FBI and/or LSP CHRI have a duty to protect the system and related systems from physical and environmental damage and are responsible for correct use, operation, care and maintenance of the information. All existing laws and <Agency> regulations and policies apply, including those that may apply to personal conduct. Misuse or failure to secure any information resources may result in temporary or permanent restriction of all privileges up to employment termination.