**Local CJIS Security Policy for ENTER AGENCY NAME HERE**

## I. Purpose

The Agency Name may use Criminal History Record Information (CHRI) obtained from the Kentucky State Police (KSP) for fitness determination of applicants and for authorizing personnel who will make fitness determinations. CHRI may not be used for any other purpose.

## II. Authority

Agency Name has the authorization to submit fingerprints to KSP for a fee-based state and federal background check pursuant to Kentucky Revised Statute (KRS) ENTER KRS NUMBER HERE.

## III. Noncriminal Justice Agency Contact (NAC) & Local Agency Security Officer (LASO)

The NAC and LASO are the points of contact with KSP through which all communication regarding audits, agency personnel changes, training, and security are conducted. The NAC and LASO will receive and disseminate communication from KSP to all authorized agency personnel. Additionally, the LASO shall where applicable:

1. Identify who is using the CSA approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.
2. Identify and document how the equipment is connected to the state system.
3. Ensure that personnel security screening procedures are being followed as stated in Policy.
4. Ensure approved and appropriate security measures are in place and working as expected.
5. Support policy compliance and ensure the CSA ISO is promptly informed of security incidents.

## IV. Authorized Personnel

Authorized personnel will be given access to view and handle CHRI after completing the required Security and Privacy Training.

Training, and any additional training required by KSP. Only authorized personnel may access, discuss, use, possess, disseminate, or destroy CHRI.

Agency Name will keep an updated list of authorized personnel that will be available to KSP Auditor during the audit process.

## V. Training of Authorized Personnel

The Agency Name will ensure all persons authorized to have CHRI access will complete Security and Privacy Training via CJIS Online immediately upon hire or appointment to access CHRI. The NAC will keep on file the Security and Privacy Training certificate on all authorized personnel.

The Agency Name will ensure authorized users’ complete recertification of Security and Privacy Training every twelve (12) months.

Authorized personnel will review the KSP website Noncriminal Justice Agency (NCJA) section for policies, procedures, and forms necessary for CHRI handling and fitness determination.

## VI. Fingerprint 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.

A copy of the applicant’s FBI Privacy Rights Notification will be provided to the applicant prior to fingerprinting. Applicant will also be advised of the process regarding a challenge of the criminal history record.

Agency Name requires that all applicants must be fingerprinted if they are an employee accessing CHRI. Applicants that have disclosed a conviction must still be fingerprinted as well.

Proper reason for fingerprinting must be documented in the “Reason for Fingerprinting” box. *(i.e. KRS recommended)*

Proper chain of custody procedures must protect the integrity of the applicant’s fingerprints. This includes maintaining fingerprint results in a secure environment.

## VII. Communication with Applicant

Authorized personnel may discuss the CHRI results with the applicant in a secure, private area. Extreme care will be taken to prevent overhearing, eavesdropping, or interception of communication.

Agency Name will not allow an applicant to have a copy of their record or take a picture of it with an electronic device.

Agency Name will provide applicant with required forms and options to obtain their record if a record is to be challenged.

**VIII. Physical Security**

Agency Name will ensure that information system hardware, software, and media are physically protected through access control measures by ensuring the perimeter of a physically secured location shall be prominently posted and separated from non-secure locations by physical controls. Agency Name will control all access points (except for those areas within the facility officially designated as publicly accessible) and will verify individual access authorizations before granting access. Agency Name will control physical access to information system distribution and transmission lines within the physically secure location. Agency Name will control physical access to information system devices that display CJI and will position information system devices in such a way as to prevent unauthorized individuals from accessing and viewing CJI. Agency Name will monitor physical access to the information system to detect and respond to physical security incidents. Agency Name will control physical access by authenticating visitors before authorizing escorted access to the physically secure location (except for those areas designated as publicly accessible) and will escort visitors in a secured location.

## IX. Storage and Retention of CHRI

The fingerprint results from KSP should only be handled by authorized personnel.

During the fitness determination:

CHRI will be stored in a locked drawer/container (name location) only accessible to authorized personnel.

CHRI will only be accessible to authorized personnel for the sole purpose needed.

CHRI will be stored in a separate file that cannot be released for any public records request and will not be archived in a publicly accessible location.

CHRI results will be stored electronically the agency using proper security and encryption methods. (remove statement if not applicable)

If stored electronically, Agency Name will ensure compliance of CJIS Security Policy for the Network Infrastructure to include the following:

1. Network Configuration
2. Personally Owned Information Systems
3. Publicly Accessible Computers
4. System Use Notification
5. Identification/User ID
6. Authentication
7. Session Lock
8. Event Logging
9. Advance Authentication
10. Encryption
11. Dial-up Access
12. Mobile Devices
13. Personal Firewalls
14. Bluetooth Access
15. Wireless (802.11x) Access
16. Boundary Protection
17. Intrusion Detection Tools and Techniques
18. Malicious Code Protection
19. Spam and Spyware Protection
20. Security Alerts and Advisories
21. Patch Management
22. Voice over Internet Protocol (VoIP)
23. Partitioning and Virtualization
24. Cloud Computing DC

Agency Name will store CHRI results for XX (specify timeframe) before disposal of CHRI.

**X. Media Protection**

Agency Name will ensure that access to digital and physical media in all forms is restricted to authorized individuals. (Agency needs to list procedures for securely handling, transporting and Media storage)

**XI. Media Transport**

Agency Name will protect and control digital and physical media during transport outside of controlled areas and will restrict the activities associated with transport of such media to authorized personnel (If digital media containing CJI is moved from one location to another list how your agency will prevent compromise of data)

**XII. Disposal of Media CHRI**

Agency Name will properly sanitize or destroy Physical or Electronic CHRI by (name method of destruction and list if Physical or Electronic Media). (If a third party performs the destruction, such a Shred-it, requires an authorized person to accompany the CHRI through the destruction process)(For electronic media agency shall overwrite three times or degauss digital media prior to disposal or release, inoperable digital media shall be destroyed; cut up, shredded, etc. Agency shall ensure the sanitation or destruction is witnessed or carried out by authorized personnel.)

Agency Name will store CHRI results for XX (specify timeframe) before disposal of CHRI.

**XIII. Standards of Discipline**

In the event of deliberate or unintentional misuse of CHRI, the Agency Name will employ formal sanctions process for personnel failing to comply with established information security policies and procedures by (employee will be disciplined in the following manner agency should outline steps of discipline including escalation to termination or request for criminal investigation/charges).