EASTCONN
Where Learning Comes to Life

PERSONNEL
Series 4000
Policy #4010.2.1

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

Purpose

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 employees, contractors, and volunteers. Where such checks are allowable by law, the following practices and procedures will be followed.

The following policies were developed using the FBI's Criminal Justice Information Services (CJIS) Security Policy. The EASTCONN Board of Directors may complement this policy with other local policy; however, the CJIS Security Policy shall always be of the minimum standard. The local policy may augment, or increase the standards, but shall not detract from the CJIS Security Policy standards.

Criminal Justice Information (CJI) and Criminal History Record Information (CHRI)

CJI is the term used to refer to all of the FBI CJIS provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to biometric, identity history, biographic, property, and case/incident history data.

CHRI, is a subset of CJI and for the purposes of this document is considered interchangeable. Due to its comparatively sensitive nature, additional controls are required for the access, use and dissemination of CHRI. In addition to the dissemination restrictions outlined below, Title 28, Part 20, Code of Federal Regulations (CFR), defines CHRI and provides the regulatory guidance for dissemination of CHRI.

Requesting CHRI checks

Fingerprint-based CHRI checks will only be conducted as authorized by the FBI and the Connecticut Department of Emergency Services and Public Protection - COLLECT CJBAU, 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.

376 Hartford Turnpike • Hampton, CT, 06247
Phone: (860) 455-0707 • Fax: (860) 455-0691
www.eastconn.org

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 COLLECT CJBAU 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.

Personnel Training

An informed review of a criminal record requires training. Accordingly, all personnel authorized to receive and/or review CHRI at EASTCONN 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 a biennial basis. This training will be accomplished using the training provided by CJIS Online.

Personnel Security

All Personnel

All personnel requiring access to CHRI must first be deemed "Authorized Personnel." The COLLECT CJBAU 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 COLLECT CJBAU 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 COLLECT CJBAU, 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 COLLECT CJBAU where it is determined that access to CHRI by the person would not be in the public's best interest.

376 Hartford Turnpike • Hampton, CT, 06247
Phone: (860) 455-0707 • Fax: (860) 455-0691
www.eastconn.org

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.

EASTCONN CHRI access termination process:

- Notification will be sent via email to the COLLECT CJBAU
- 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.

Adverse Decisions Based on CHRI

If inclined to make an adverse decision based on an individual's CHRI, EASTCONN 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 15 days to correct or complete the CHRI.

Non-Criminal Agency Coordinator (TAC)
The EASTCONN TAC is Andrew DePalma. The TAC is responsible for the following:

- Maintaining an updated Authorized Personnel List on file with the COLLECT CJBAU.
    - Ensuring everyone included on this list must undergo the appropriate level of CJIS Security Awareness Training.
    - Ensuring everyone included on the list has appropriate access based on job functions and a need-to-know basis.

- Inform the COLLECT CJBAU of changes in the agency head or any relevant business information (agency name changes, mailing/physical address changes, etc.).

376 Hartford Turnpike • Hampton, CT, 06247
Phone: (860) 455-0707 • Fax: (860) 455-0691
www.eastconn.org

- Contact the COLLECT CJBAU immediately to update the User Agreement and, if necessary, submit the new authorization to the COLLECT CJBAU
- Submit a TAC change form to the COLLECT CJBAU in the event of a change in roles.

Local Agency Security Officer (LASO)
The EASTCONN LASO is Andrew DePalma. 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, EASTCONN shall notify the COLLECT CJBAU of the change.

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 comply with the most recent COLLECT CJBAU 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.

Controls shall be in place to protect electronic and physical media containing CHRI while at rest, stored, or actively being accessed. "Electronic media" includes memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, backup medium, optical disk, flash drives, external hard drives, or digital memory card. "Physical media" includes printed documents and imagery that contain CHRI.

The agency shall securely store electronic and physical media within physically secure locations or controlled areas. The agency shall restrict access to electronic and physical media to authorized

376 Hartford Turnpike • Hampton, CT, 06247
Phone: (860) 455-0707 • Fax: (860) 455-0691
www.eastconn.org

individuals. If physical and personnel restrictions are not feasible then the data shall be encrypted per Section 5.10.1.2.

Physical Storage and Access

Physical CHRI media shall be securely stored within physically secured locations or controlled areas. A physically secure location is a facility or an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect the FBI CJI and associated information systems. The perimeter of the physically secure location shall be prominently posted and separated from non-secure locations by physical controls. 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.

Only authorized personnel will have access to physically secure non-public locations. EASTCONN will maintain and keep a list of authorized personnel. All physical access points into the agency's secure areas will be authorized before granting access. The agency will implement access controls and monitoring of physically secure areas for protecting all transmission and display mediums of CJI.

Authorized personnel will take necessary steps to prevent and protect the agency from physical, logical and electronic breaches.

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.

Electronic CHRI media:

The LIVESCAN system incorporates several security measures to protect electronic Criminal History Record Information (CHRI) media:

- Secure data transmission: Fingerprint data and associated CHRI are transmitted electronically using encrypted channels to authorized state repositories or the FBI's Automated Fingerprint Identification System (AFIS).
- Access control: The system requires authorized operators who are trained and certified to use the LIVESCAN equipment and software. This helps prevent unauthorized access to sensitive data.
- Two-factor authentication: the LIVESCAN system implements two-factor authentication for operator access, adding an extra layer of security.
- Real-time image quality checks: The software performs quality checks on captured fingerprint images to ensure accuracy and completeness, reducing the risk of errors in CHRI.

376 Hartford Turnpike • Hampton, CT, 06247
Phone: (860) 455-0707 • Fax: (860) 455-0691
www.eastconn.org

- Secure storage: storage of CHRI on the LIVESCAN system is encrypted and access-restricted.
- Compliance with CJIS Security Policy: LIVESCAN systems handling CHRI must adhere to the FBI's Criminal Justice Information Services (CJIS) Security Policy, which outlines strict guidelines for protecting criminal justice information.
- Physical security: The LIVESCAN equipment itself is located in a physically secure area with controlled access, monitoring, and visitor restrictions.
- Secure workstation: The computer workstation used to operate the LIVESCAN system has additional security measures such as firewalls, antivirus software, and regular security updates.
- Audit trails: LIVESCAN system maintains logs of all access and transactions for accountability and security auditing purposes.

These security measures work together to ensure that electronic CHRI media captured and processed through the LIVESCAN system remains protected from unauthorized access, tampering, or disclosure throughout its lifecycle

Destruction of CHRI

Disposal of Physical Media

Once physical CHRI media (paper/hard copies) is determined to be no longer needed by EASTCONN, it shall be destroyed and disposed of appropriately. Physical CHRI media shall be destroyed by shredding, cross-cut shredding, or incineration. EASTCONN 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 EASTCONN.

Media Sanitization and Disposal (Disposal of Electronic Media)

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

Overwriting:

As the name implies, overwriting uses a program to write (1s, 0s, or a combination of both) onto the location of the media where the file to be sanitized is located.

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.

376 Hartford Turnpike • Hampton, CT, 06247
Phone: (860) 455-0707 • Fax: (860) 455-0691
www.eastconn.org

Remote Access

EASTCONN shall authorize, monitor, and control all methods of remote access to the information systems that can access, process, transmit, and/or store FBI CJI. Remote access is any temporary access to an agency's information system by a user (or an information system) communicating temporarily through an external, non-agency-controlled network (e.g., the Internet).

The EASTCONN shall employ automated mechanisms to facilitate the monitoring and control of remote access methods. EASTCONN shall control all remote access through managed access control points. EASTCONN may permit remote access for privileged functions only for compelling operational needs but shall document the rationale for such access in the security plan for the information system.

Utilizing publicly accessible computers to access, process, store or transmit CJI is prohibited. Publicly accessible computers include but are not limited to hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.

Personally Owned Information Systems

A personally owned information system shall not be authorized to access, process, store or transmit CJI unless the agency has established and documented the specific terms and conditions for personally owned information system usage. A personal device includes any portable technology like camera, USB flash drives, USB thumb drives, DVDs, CDs, air cards and mobile wireless devices such as Androids, Blackberry OS, Apple iOS, Windows Mobile, Symbian, tablets, laptops or any personal desktop computer. When bringing your own devices (BYOD) are authorized, they shall be controlled using the requirements in Section 5.13 of the CJIS Security Policy.

Disciplinary

If an individual at EASTCONN 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.

376 Hartford Turnpike • Hampton, CT, 06247
Phone: (860) 455-0707 • Fax: (860) 455-0691
www.eastconn.org

Incident Response

The security of information and systems in general, and of CHRI in particular, is a top priority for EASTCONN. 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 COLLECT CJBAU within 24 hours.

All agency personnel with access to FBI and/or COLLECT CJBAU 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 EASTCONN 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.
(cf. 4112.5/4212.5 - Security Check/Fingerprinting)
(cf. 4112.51/4212.51 - Employment/Reference Checks)

Legal Reference: Connecticut General Statutes

> 10-221d Criminal history records checks of school personnel. Fingerprinting. Termination or dismissed. (as amended by PA 01-173, PA 04-181 and June 19 Special Session, PA 09-1, PA 11-93 and PA 16-67)
>
> 29-17a Criminal history checks. Procedure. Fees.
>
> PA 16-67 An Act Concerning the Disclosure of Certain Education Personnel Records
>
> Criminal Justice Information Services (CJIS) Security Policy, Version 5.4, U.S. Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services Division, October 6, 2015.

376 Hartford Turnpike • Hampton, CT, 06247
Phone: (860) 455-0707 • Fax: (860) 455-0691
www.eastconn.org

CJIS Security Policy

Title 28 C.F.R. Part 20

Adopted: September 24, 2024
Revised:
Replaces:

376 Hartford Turnpike • Hampton, CT, 06247
Phone: (860) 455-0707 • Fax: (860) 455-0691
www.eastconn.org