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

The Board is committed to ensuring the protection of the Criminal Justice Information (CJI) and its subset of Criminal History Record Information (CHRI) until the information is purged or destroyed in accordance with applicable record retention rules.

Accordingly, this policy applies to any electronic or physical media containing Federal Bureau of Investigation (FBI) or Colorado Bureau of Investigation (CBI) CJI while being stored, accessed, or physically moved from a secure location within Centennial BOCES. This policy also applies to any authorized person who accesses, stores, and/or transports electronic or physical media containing criminal history record information.

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 licensing or employment purposes. Where such checks are allowable by law, the following practices and procedures will be followed.

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

CJI refers to all of the FBI Criminal Justice Information Services (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 means information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, information, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, and release. The term does not include identification information such as fingerprint records if such information does not indicate the individual's involvement with the criminal justice system. 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.

Requesting CHRI checks

Fingerprint-based CHRI checks will only be conducted as authorized by the FBI and CBI, 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, he/she 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.

Proper Access, Use, and Dissemination of CHRI

All CHRI is subject to strict state and federal rules and regulations. CHRI must only be used for an authorized purpose consistent with the purpose for which it was accessed or requested and

cannot be disseminated outside the receiving departments, related agencies, or other authorized entities. Dissemination to another agency is authorized if (a) the other agency is an Authorized Recipient of such information and is being serviced by the accessing agency, or (b) the other agency is performing noncriminal justice administrative functions on behalf of the authorized recipient and the outsourcing of said functions has been approved by Colorado Bureau of Investigation (CBI) officials with applicable agreements in place. All receiving entities are subject to audit by the CBI (Colorado Bureau of Investigations) 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.

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 CBI 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.

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***:

a. Historical reference and/or comparison with future CHRI requests
b. Dispute of the accuracy of the record
c. Evidence for any subsequent proceedings based on information contained in the CHRI.
d. CHRI will be kept for the above purposes in:
    i. hard copy form in personnel files located in the locked filing cabinet located in the locked filing room

Security Awareness CHRI Training

An informed review of a criminal record requires training. Accordingly, all personnel authorized to receive and/or review CHRI at Centennial BOCES will review and become familiar with the educational and relevant training materials regarding CHRI laws and regulations made available by the appropriate agencies. Authorized personnel is defined as an individual, or group of individuals, who have completed security awareness training and have been granted access to CJI data.

In addition to the above, all personnel authorized to receive and/or review CHRI must undergo Security Awareness Training within six month of initial assignment, and on a biennial basis thereafter. This training will be accomplished using the training materials made available by the CBI.

Adverse Decisions Based on CHRI

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

a) Provide the individual the opportunity to complete or challenge the accuracy of his/her CHRI; and
b) 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 to correct or complete the CHRI.

Physical Security

All CJI and CHRI information must be securely stored. Centennial BOCES will maintain a current list of authorized personnel. Authorized personnel will take necessary steps to prevent and protect Centennial BOCES from physical, logical, and electronic breaches.

Local Agency Security Officer

Each NCJA receiving CHRI is required to designate a Local Agency Security Officer (LASO). An individual designated as LASO is:

a) An individual who will be considered part of the NCJA's "authorized personnel" group.
b) An individual that has completed a fingerprint-based background check and found appropriate to have access to CHRI.
c) An employee directly involved in evaluating an individual's qualifications for employment or assignment.

The Centennial BOCES LASO is responsible for the following:

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

When changes in the LASO appointment occur, Centennial BOCES shall complete and return a new LASO appointment form. The most current copy of the LASO appointment form will be maintained on file indefinitely by the agency.

Personnel Security

All Personnel

Access to CJI and/or CHRI is restricted to authorized personnel. Authorized personnel is defined as an individual, or group of individuals, who have completed security awareness training and have been granted access to CJI data.

The CBI 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 CBI 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:

a) Have their access to CHRI suspended until the outcome of an arrest is determined and reviewed by the CBI in order to determine if continued access is appropriate.
b) Have their access suspended indefinitely if a conviction results in a felony of any kind.
c) Have their access denied by the CBI 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 should arise 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:

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

Media Protection, Storage and Access

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 must be in place to protect CHRI electronic and physical media containing CJI 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 CJI.

Centennial BOCES must securely store CHRI electronic and physical media within physically secure locations or controlled areas. Centennial BOCES restricts access to electronic and physical media to authorized individuals. If physical and personnel restrictions are not feasible then the data must be encrypted. When no longer usable, information and related processing items must be properly disposed of to ensure confidentiality.

Physical CHRI media:

a) Is to be stored within employee records when feasible or by itself when necessary.
b) Is to be maintained within a lockable filling cabinet, drawer, closet, office, safe, vault, or other secure container.

Media Sanitization and Disposal

When no longer usable, hard drives, diskettes, tape cartridges, CDs, ribbons, hard copies, print-outs, and other similar items used to process, store, and/or transmit FBI or CBI CJI must be properly disposed of in accordance with measures established by Centennial BOCES.

Physical media (print-outs and other physical media) must be disposed of by the following method:

a) shredding using Centennial BOCES-issued shredders by the Centennial BOCES TAC observed by the Centennial BOCES LASO

Centennial BOCES will ensure such destruction is witnessed or carried out by authorized personnel:

a) The LASO shall witness or conduct disposal.
b) Cross-cut shredding will be the method of destruction will be used.
c) This will occur at the end of each school year (May/June).

Electronic media (hard-drives, tape cartridge, CDs, printer ribbons, flash drives, printer and copier hard-drives, etc.) must be disposed of by one of the following methods:

a) Overwriting (at least 3 times) - an effective method of clearing data from magnetic media. 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.
b) Degaussing - a method to magnetically erase data from magnetic media. Two types of degaussing exist: strong magnets and electric degausses. Note that common magnets (e.g., those used to hang a picture on a wall) are fairly weak and cannot effectively degauss magnetic media.
c) Destruction – a method of destroying magnetic media. As the name implies, destruction of magnetic media is to physically dismantle by methods of crushing, disassembling, etc., ensuring that the platters have been physically destroyed so that no data can be pulled.

IT systems that have been used to process, store, or transmit FBI or CBI CJI and/or sensitive and classified information must not be released from Centennial BOCES's control until the equipment has been sanitized and all stored information has been cleared using one of the above methods.

Account Management

Centennial BOCES must manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. Centennial BOCES must validate information systems accounts at least annually and must document the validation process.

All accounts must be reviewed at least annually by the designated CJIS point of contact or their designee to ensure that access and account privileges commensurate with job functions, need-to-know, and employment status on systems that contain CJI. The CJIS point of contact may also conduct periodic reviews.

Reporting Information Security Events/Incident and Disciplinary Response

The security of information and systems in general, and of CHRI in particular, is a top priority for Centennial BOCES. 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:

a) All incidents will be reported directly to the LASO.
b) If any records were stolen, the incident will also be reported to appropriate authorities.
c) 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 CBI within 24 hours.

All Centennial BOCES personnel with access to FBI and/or CBI CHRI has 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 Centennial BOCES 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.

All employees, contractors, and third party users must be made aware of the procedures for reporting the different types of event and weakness that might have an impact on the security of Centennial BOCES assets and are required to report any information security events and weaknesses as quickly as possible to the designated point of contact.

Policy Violation/Misuse Notification

Violation of this policy or misuse of CHRI by any personnel can result in significant disciplinary action, up to and including loss of access privileges, civil and criminal prosecution, and/or termination.

Likewise, violation of this policy or misuse of CHRI by any visitor can result in similar disciplinary action against the sponsoring employee, and can also result in termination of services with any associated consulting organization or prosecution in the case of criminal activity.

LEGAL REFS.: P.L. 92-544 (authorizes the FBI to exchange CHRI with officials of state and local governmental agencies for licensing and employment purposes)
28 C.F.R. 20.33 (b) (limited dissemination of criminal history record information)
28 C.F.R. 50.12 (b) (notification requirements regarding fingerprints)
C.R.S. 22-2-119.3 (6)(d) (name-based criminal history record check – definition)
C.R.S. 22-32-109.8 (non-licensed personnel – submittal of fingerprints and name-based criminal history record check)
C.R.S. 22-32-109.9 (licensed personnel – submittal of fingerprints and name-based criminal history record check)
C.R.S. 24-72-302 (definition of criminal justice information)
CJISD-ITS DOC-08140-5.9 Section 5.8.4 Disposal of Physical Media
CJISD-ITS DOC-08140-5.9 Section 5.12.4 Personnel Sanctions
CJISD-ITS DOC-08140-5.9 Section 5.3 Incident Response

CROSS REFS.: GBEB, Staff Conduct (and Responsibilities)
GCE/GCF, Professional Staff Recruiting/Hiring
GDE/GDF, Support Staff Recruiting/Hiring

Revised June 2021
Adopted: January 21, 2021
Centennial BOCES