NOTE: Colorado BOCES that operate a school or educational program for K-12 students and/or employ staff who work with students are required by law to adopt a policy on this subject and the law contains some specific direction as to the content or language. This sample contains the content/language that CASB believes best meets the intent of the law. However, the BOCES should consult with its own legal counsel to determine appropriate language that meets local circumstances and needs.

Criminal History Record Information

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 the BOCES. This policy also applies to any authorized person who accesses, stores, and/or transports electronic or physical media containing criminal history record information.

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, informations, 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.

Proper access, use, and dissemination of CHRI

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.

Personnel security screening

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.

Security awareness training

Basic security awareness training is required within six months of initial assignment, and biennially thereafter, for all personnel with access to said confidential information.

Physical security

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

Media protection

Controls must be in place to protect 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.

The BOCES must securely store electronic and physical media within physically secure locations. The 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.

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 the BOCES.

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

1) shredding using BOCES-issued shredders; or

2) placed in locked shredding bins for a private contractor to come on-site and shred, witnessed by BOCES personnel throughout the entire process.

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:

1) 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.

2) 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.

3) 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 the BOCES's control until the equipment has been sanitized and all stored information has been cleared using one of the above methods.

Account management

The BOCES must manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The 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

The BOCES must promptly report incident information to appropriate authorities to include the CBI's Information Security Officer (ISO). Information security events and weaknesses associated with information systems must be communicated in a manner allowing timely corrective action to be taken. Formal event reporting and escalation procedures must be in

place. Wherever feasible, the BOCES must employ automated mechanisms to assist in the reporting of security incidents.

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 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.

August 11, 2021

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)*

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