Board Member Fingerprint Policy

SkyView Academy utilized the Colorado Bureau of Investigations (CBI) to conduct fingerprint background checks on all employees and board members. This policy applies 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.

I. 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 must 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 instructions will include information on the procedure for submitting fingerprints. In addition, the applicant or employee will be provided with all information required to register for a fingerprinting appointment successfully.

II. Access to CHRI

All CHRI is subject to strict state and federal rules and regulations. CHRI cannot be shared with other entities for any purpose, including subsequent hiring determinations. 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 CHRI's willful, unauthorized disclosure.

III. 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 CBI and FBI security policies, 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 handling CHRI will strictly adhere to the policy on its storage and destruction.

IV. 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 SVA Fingerprint Based CHRI Checks for Non-Criminal 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 following purposes:

- A Hard copy form in personnel files is located in the locked filing cabinet located in the locked filing room.

V. CHRI Training

An informed review of a criminal record requires training. Accordingly, all personnel authorized to receive and/or review CHRI at the 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 biennially. This training will be accomplished using the training materials made available by the CBI.

VI. Adverse Decisions Based on CHRI

If inclined to make an adverse decision based on an individual's CHRI, the Agency will take the following steps before 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 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.

VII. Local Agency Security Officer

Each NCJA receiving CHRI is required to designate a Local Agency Security Officer (LASO).

An individual designated as LASO is:

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

The Agency LASO is the Head of Operations. 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 the LASO appointment changes, the Agency shall complete and return a new LASO appointment form. The agency will maintain the most current copy of the LASO appointment form on file indefinitely.

VIII. Personnel Security

All Personnel:

All personnel requiring access to CHRI must first be deemed “Authorized Personnel.” 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 also 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 consider 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 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.

Support personnel, contractors, and custodial workers will be denied all access to CHRI. 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 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

XI. Media Protection

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

Media 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:

A. It is to be stored within employee records when feasible or by itself when necessary.
B. Is to be maintained within a lockable filing cabinet, drawer, closet, office, safe, vault, or other secure container.

Disposal of Physical Media

Once physical CHRI media (paper/hard copies) is determined to be no longer needed by the agency, it shall be destroyed and disposed of appropriately. Physical CHRI media shall be destroyed by shredding, cross-cut shredding, or incineration. The agency 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 by the agency.
C. This will occur at the end of each school year (May/June).

X. Incident and Disciplinary Response

The security of information and systems in general, and of CHRI in particular, is a top priority for the 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 that 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 are stolen, the incident will also be reported to the 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 agency personnel with access to FBI and/or CBI CHRI must protect the system and related systems from physical and environmental damage and are responsible for correctly using, operating, caring for, and maintaining the information. All existing laws, 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.