

**NONCRIMINAL JUSTICE AGENCY (NCJA)  
CRIMINAL HISTORY RECORD INFORMATION (CHRI)**

**Requirement**

Pursuant to federal requirements, a Noncriminal Justice Agency (NCJA) with access to Criminal History Record Information (CHRI) is required to have an information security policy and procedure in place. Access to CHRI is directed through a series of memoranda, policies, regulations, and federal laws. Agencies that have access and use of CHRI share a responsibility in creating appropriate administrative, technical, and physical safeguards to ensure the security, confidentiality, and integrity of CHRI in all its forms.

**Instructions**

The Information Security Policy template is provided in a Word format. This template is to provide your agency with the framework for creating your agency's individual policy. The template alone will not make your agency compliant. Your agency will be required to provide agency specific procedures for areas identified on how your agency will carry out the policy. Points have been noted as applicable to assist you in creating your agency specific procedures. Starting at first page to last page:

**Agency Name:** Michigan Virtual Charter Academy ("MVCA")

NCJA means-A noncriminal justice governmental agency authorized by federal statute, executive order, or state statute and approved by the U.S. Attorney General to be able to receive state and federal fingerprint based CHRI, directly or indirectly from the Michigan State Police (MPS). Examples of services include, but are not limited to, employment suitability, licensing determination, immigration and naturalization matters, and national security clearances.

POLICY: MICHIGAN VIRTUAL CHARTER ACADEMY – INFORMATION SECURITY POLICY  
SUBJECT: CRIMINAL HISTORY RECORD INFORMATION (CHRI)  
DATE: DECEMBER 17, 2018 ADOPTED BY BOARD

---

Pursuant to Michigan Compiled Law (MCL) 380.1230a, Michigan Virtual Charter Academy (“MVCA” or “Academy”), is considered a Noncriminal Justice Agency (NCJA) and is an Authorized Recipient (AR), wherein certain Authorized Personnel can request and receive fingerprint-based Criminal History Record Information (CHRI) checks. Authorization for ARs to receive CHRI is for the purpose of employment of staff by the Academy’s Educational Products and Services Provider, K12 Virtual Schools, LL (“K12”) or volunteer determinations. Therefore, Michigan Virtual Charter Academy is to ensure compliance with applicable state and federal laws, applicable rules and regulations, and the most current version of the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy, in addition to Michigan Virtual Charter Academy’s policies, procedures, and processes. This Information Security Policy provides the appropriate access, maintenance, security, confidentiality, dissemination, integrity, and audit requirements of CHRI in all its forms, whether at rest or in transit.

The most stringent requirement shall prevail if conflict(s) is/are found between agency policies, state or federal laws, with the most current version of the FBI CJIS Security Policy, and corresponding rules or regulations.

As used in this Policy:

(a) Authorized Recipients:

- (1) A criminal justice agency or federal agency authorized to receive CHRI pursuant to federal statute or executive order;
- (2) A nongovernmental entity authorized by federal statute or executive order to receive CHRI for noncriminal justice purposes; or
- (3) A government agency authorized by federal statute, executive order, or state statute which has been approved by the United States Attorney General to receive CHRI for noncriminal justice purposes.

(b) Authorized User/Personnel-An individual, or group of individuals, who have been appropriately vetted through a national fingerprint-based background check, where required, and have been granted access to CJI data, wherein access is only for the purpose of evaluating an individual’s qualifications for employment or assignment to work at or on behalf of the Academy.

## **USER AGREEMENT**

Michigan Virtual Charter Academy shall complete and maintain a Noncriminal Justice Agency User Agreement for Release of Criminal History Record Information (RI-087) provided by the Michigan State Police (MSP). Agreements are in place to provide for data ownership, individual roles, responsibilities, etc. Michigan Virtual Charter Academy shall complete and return a new user agreement when changes in contact information (physical address, e-mail address, contact name, etc.) occur. The most current copy of this user agreement will be maintained on file at the agency indefinitely.

## **LOCAL AGENCY SECURITY OFFICER (LASO)**

The MVCA Head of School will designate a LASO by means of completing and returning to the MSP, Security & Access Section (SAS), a Noncriminal Justice Agency Local Agency Security Officer Appointment (CJIS-015). An individual designated as the LASO is:

- An "authorized user/personnel."
- An individual that has completed a fingerprint-based background check, where required, and found appropriate to have access to CHRI.
- If a school, the LASO is an employee of the Educational Products and Services Provider, in this case K12, who is directly involved in evaluating an individual's qualifications for employment or assignment.

A LASO is responsible for the following:

- Identifying who is using or accessing CHRI and/or systems with access to CHRI.
- Identifying and documenting any equipment connected to the state system.
- Ensuring personnel security screening procedures are being followed as stated in this policy.
- Confirming the approved and appropriate security measures are in place and working as expected.
- Supporting policy compliance and ensuring the MSP Information Security Officer (ISO) is promptly informed of security incidents.

When changes in the LASO appointment occur, Michigan Virtual Charter Academy shall complete and return a new LASO appointment form. The most current copy of the LASO appointment form will be kept on file indefinitely by the agency (CJIS-015).

All MSP fingerprint account changes are to be made by the LASO.

## **PERSONNEL SECURITY**

### **ALL PERSONNEL**

All personnel requiring access to CHRI must first be deemed "Authorized Personnel." Prior to access of CHRI, such individuals shall complete a fingerprint-based CHRI background check. The LASO or authorized designee will review and determine if access is appropriate. Access is denied if:

- a. The law prohibits the individual from working in or with Michigan Virtual Charter Academy
- b. The individual has ever had a felony, of any kind, no matter when it occurred.

If a record of any other kind is found, the LASO or authorized designee will review if access is appropriate. Persons believed to be a fugitive, or having an arrest history without conviction must be reviewed to determine if access to CHRI is appropriate. The LASO or authorized designee may ask for a review by the CJIS Systems Officer (CSO) of the MSP in extenuating circumstances where the severity of the offense and the time that has passed would support a possible variance.

Access will be granted upon determination by the LASO or authorized designee, so long as providing such access would not be detrimental to the agency or the individual for which the record pertains.

Persons with access to CHRI that 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 LASO or authorized designee in order to determine if continued access is appropriate.
- b. Have their access to CHRI suspended indefinitely if a conviction results in a felony of any kind.
- c. Have their access to CHRI denied by the LASO or authorized designee where she/he determines that access to CHRI by the person would not be in the public's best interest.

Whenever possible, access to CHRI by support personnel, contractors, and custodial workers will be denied. If a need should arise for such individuals to be in an area(s) where CHRI is maintained or processed (at rest or in transit); persons will be escorted by or under the supervision of authorized personnel at all times while in these area(s).

NCJAs that do not have passed and federally approved legislation authorizing or requiring the civil fingerprint-based background checks are exempt from this requirement until such a time as appropriate legislation has been written into law.

## **PERSONNEL SCREENING FOR CONTRACTORS AND VENDORS**

In addition to the screening requirements provided in the immediate preceding areas, contractors and vendors (persons with access to agency system hardware or software) shall meet the following requirements:

- a. Have completed a state and federal fingerprint-based CHRI background check.
- b. If a record of any kind is found, delay access until the LASO or authorized designee can review the record and determine whether such access to CHRI is appropriate.
- c. If a felony record of any kind is found, access to CHRI will be denied.
- d. If a confirmed outstanding arrest warrant is found, access to CHRI will be denied.

Michigan Virtual Charter Academy will retain and keep current a list of K12 personnel who have been given authorized access to CHRI, and make this list available to the MSP upon request.

NCJAs that do not have passed and federally approved legislation authorizing or requiring the civil fingerprint-based background checks are exempt from this requirement until such a time as appropriate legislation has been written into law.

## **PERSONNEL TERMINATION**

The LASO or authorized designee shall terminate access to CHRI immediately, which is within 24 hours of a notification that an individual's termination of employment with the Educational Products and Services Provider, K12, has occurred.

Michigan Virtual Charter Academy, through its Educational Products and Services Provider, K12, will take the following steps when terminating the LASO or authorized designee:

- a. The LASO is the only individual who has access to CHRI. If the LASO is being terminated, the MVCA Head of School will immediately notify the MSP-CJIC to terminate access to the LASO.
- b. The MVCA Head of School will also immediately notify MSP-CJIC of changes to sections I and III on the Agency User Agreement (Form RI-087) by completing a new form and identifying the new authorized personnel to receive CHRI (the LASO).
- c. The MVCA Head of School will also assign a new LASO by completing the Non-Criminal Justice Agency Local Agency Security Officer Appointment form (Form CJIS-015) immediately.
- d. The MVCA Head of School will notify the MVCA Board of Directors and the K12 Regional Operations Manager.
- e. Within a 24-hour period, the LASO will no longer have access to CHRI and will relinquish keys to the Head of School at Michigan Virtual Charter Academy. The LASO will turn over all keys to the building, office, desk, and/or file drawers.
- f. The LASO's email account and all K12 accounts will be deactivated by the Regional Operations Manager through K12's ServiceNow.

## **PERSONNEL TRANSFER**

Individuals with access to CHRI, and where the individual has been reassigned or transferred, shall have his or her access reviewed by the LASO or authorized designee to ensure access is still appropriate. Currently, only one (1) individual has access to CHRI at Michigan Virtual Charter Academy; the Operations Manager/LASO. If access is determined to be suspended, the individual shall be restricted from access to CHRI within the immediate 24 hours of transfer or reassignment and the following steps shall be taken by Michigan Virtual Charter Academy immediately:

- a. The LASO is the only person that has access to CHRI. If the LASO accepts a new personnel transfer, the MVCA Head of School will immediately notify the MSP-CJIC to terminate access to the LASO.
- b. The MVCA Head of School will also immediately notify MSP-CJIC of changes to sections I and III on the Agency User Agreement (Form RI-087) by completing a new form and identifying the new authorized personnel to receive CHRI (the LASO).
- c. The MVCA Head of School will also assign a new LASO by completing the Non-Criminal Justice Agency Local Agency Security Officer Appointment form (Form CJIS-015) immediately and submit to [msp-cjic-ats@michigan.gov](mailto:msp-cjic-ats@michigan.gov)

- d. The newly appointed Operations Manager/LASO will receive access to CHRI upon appropriate training and CHRI check.
- e. The former LASO will turn in their keys to the MVCA Head of School who will lock the keys in the Operations Manager/LASO office drawer with the Office Administrator as a witness. The MVCA Head of School will release the keys to the new Operations Manager/LASO upon arrival.

## **SANCTIONS**

Persons found noncompliant with state or federal laws, current FBI CJIS Security Policy, rules or regulations, including Michigan Virtual Charter Academy Information Security Policy, will be formally disciplined. Discipline can be, but not limited to, counseling, the reassignment of CHRI responsibilities, dismissal, or prosecution. Discipline will be based on the severity of the infraction and at the discretion of the Educational Products and Services Provider, K12, who is the employer.

## **MEDIA PROTECTION**

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

## **MEDIA STORAGE & ACCESS**

Digital and physical CHRI media shall be securely stored within physically secured locations or controlled areas, and within the Academy's facility unless otherwise permitted. Access to such media is restricted to authorized personnel only and secured at all times when not in use or under the supervision of an authorized individual.

Physical CHRI media:

Is to be maintained within a lockable filing cabinet drawer located in the locked Michigan Virtual Charter Academy Operations Manager's office.

Digital CHRI media:

- a. Digital CHRI media is not stored on any electronic devices at Michigan Virtual Charter Academy.
- b. All digital communications sent via email will be sent directly to the LASO's secured email address on the computer solely designated for CHRI and Board information.

## **MEDIA TRANSPORT (DIGITAL AND/OR PHYSICAL)**

Should the need arise to move CHRI media outside of the secured location or controlled area, the LASO and the Head of School shall establish and implement appropriate security controls to prevent compromise of the data while transporting. The transport of CHRI media will be conducted by authorized personnel.

CHRI media includes:

- Physical CHRI media such as paper/hard copies.
- Digital CHRI media such as laptops; computer hard drives; and any removable, transportable digital memory media, such as magnetic tape or disk, optical disk, flash drives, external hard drives, or digital memory card(s).

If Michigan Virtual Charter Academy needs to transport CHRI, the following procedures will be used:

- a. The LASO will handle and transport all CHRI media.
- b. The LASO will transport all materials from one office directly to the new location during the work hours of 8:00 am to 5:00 pm. Transportation will occur only upon justification and approval by the MVCA Board of Directors.
- c. The LASO will transfer the CHRI in a locked, rolling container. The container shall have a built in lock that only the LASO has access to by key.
- d. The CHRI is to remain in the physical possession of the LASO until the CHRI media is delivered to its intended destination.

## **DIGITAL MEDIA SANITIZATION AND DISPOSAL**

Without ensuring the proper disposal of installed and removable digital storage, information security risks can be created by reassigning, surplus, transferring, trading-in, disposing of computers, or replacing digital storage media and computer software. Therefore, once digital CHRI media devices are determined to no longer be needed by the agency, devices shall be sanitized and disposed of according to the most current FBI CJIS Security Policy. Due to the presence of temporary files (data remanence), devices where digital media was once stored, processed, and/or used for dissemination (fax, scanners, computers, laptops, etc.) shall be sanitized in a manner that gives assurance that the information cannot be recovered prior to disposal of or upon the reassigning or recycling of such devices. An "erase" feature (e.g., putting a document in a "trash can" icon) or deleting a file is not sufficient for sensitive information, because the information may still be recoverable. The agency will provide steps for the sanitization and disposal of devices where CHRI media was once stored, processed, and/or used. Michigan Virtual Charter Academy will consult with K12's information technology professionals to sanitize the device, and clear (wipe) the data. This process will be witnessed by the authorized user, or the LASO.

Michigan Virtual Charter Academy will take the following steps for digital sanitization:

- a. MVCA will seek the expertise of K12's Information Technology professionals to sanitize the devices, or other Information Technology professional designated by the MVCA Board of Directors.
- b. Sanitization of digital media devices will be conducted or witnessed by an authorized user.
- c. MVCA may use any of the following methods of sanitization:
  1. When clearing data (wiping) use three passes with a disk wiping utility using the DoD 5220.22-M (E) method.
    - i. Writes zero bytes (0x00)

- ii. Writes high bytes (0xFF)
  - iii. Writes pseudo-random bytes
2. When purging the data, use a National Security Agency/Central Security Service (NSA/CSS) approved degausser except for optical media such as CDs/DVDs where it must be physically destroyed.
3. Physical destruction includes shredding, disintegrating, cutting, drilling, or grinding.
4. Any other reasonable method.

## **DISPOSAL OF PHYSICAL MEDIA**

Once physical CHRI media (paper copies) is determined no longer needed by the agency, media shall be destroyed and disposed of according to the FBI CJIS Security Policy. Formal procedures for the secure disposal or destruction of physical media:

Michigan Virtual Charter Academy will take the following steps to dispose of physical media:

- a. The LASO shall immediately shred the CHRI on the premises.
- b. CHRI results will not be placed in a shredding bin or recycling bin for shredding or disposal by another individual or organization.
- c. Michigan Virtual Charter Academy will follow Michigan Public School CHRI record Retention policies. CHRI will be maintained for the duration of employment plus ten (10) years.

## **PHYSICAL PROTECTION**

Michigan Virtual Charter Academy, through its Educational Products and Services Provider, K12, shall document and implement a physical protection policy and procedures to ensure CHRI and information system hardware, software, and media are physically protected through access control measures.

## **PHYSICALLY SECURE LOCATION**

Michigan Virtual Charter Academy will ensure both sufficient physical and personnel security controls exist for the protection of CHRI and associated information systems. A physically secure location is a facility, an area, a room, or a group of rooms within a facility. Michigan Virtual Charter Academy will:

- a. Prominently post the perimeter of the physically secured location and keep separate from non-secure locations by physical controls.
- b. Keep a current list of K12 personnel with authorized access to the physically secure location or use a method of credentials to keep track of authorized personnel.
- c. Ensure all physical areas where CHRI or information systems are stored and/or used for processing shall be controlled. Individuals requiring access to such locations will be verified before granting access. Physical access to information system distribution and transmission lines within the physically secure location will be controlled and safeguarded.
- d. Position information system devices that display CHRI in such a way as to prevent unauthorized individuals from accessing and viewing CHRI.



- e. Ensure methods are in place to monitor, detect, and respond to information system incidents for individuals attaining physical access to secured areas.
- f. Validate all visitors before admittance to the physically secure locations, and visitors will be escorted and monitored at all times.
- g. Authorize and control information system-related items entering and exiting the physically secure location.

## **CONTROLLED AREA**

If the Academy cannot meet all of the controls required for establishing a physically secure location but has an operational need to access or store CHRI, the Academy shall designate an area, a room, or a storage container, as a controlled area for the purpose of day-to-day CHRI access or storage. At a minimum:

- a. Access must be limited to the controlled area during CHRI processing times and to authorized personnel only, approved by the Academy's Educational Products and Services Provider, K12, to access or view CHRI.
- b. CHRI will be locked and secured to prevent unauthorized access when unattended.
- c. Information system devices and documents containing CHRI will be positioned in such a way as to prevent an unauthorized individual from access or view.
- d. Encryption requirements will be implemented for digital storage (i.e. data "at rest") of CHRI.

## **INCIDENT RESPONSE**

Michigan Virtual Charter Academy, through its Educational Products and Services Provider, K12, shall establish operational incident handling procedures for instances of an information security breach. Information security incidents are major incidents that significantly endanger the security or integrity of CHRI. The Academy, through K12 will identify responsibilities for information security incidents and include how and who to report such incidents to. The Academy, through K12, shall ensure that appropriate security incident capabilities exist, and incorporate the lessons learned from ongoing incident handling activities. The Academy, through K12, will ensure that procedures exist and are implemented for a follow-up action of a security breach and for the collection of evidence in cases of legal action. All individuals with direct or indirect access to CHRI shall be trained on how to handle an information security incident, and such training is to be included within the Academy's Security Awareness Training as provided by K12. (See section on Security Awareness Training at the end of this document.) Procedures shall be in place to track and document information security incidents, whether physical or digital, on an ongoing basis. When an incident has been determined to be a breach involving CHRI, the Academy, through k12, will report the security breach to the MSP ISO by use of the "Information Security Officer (ISO) Computer Security Incident Response Capability Reporting" form (CJIS-016).

Michigan Virtual Charter Academy's incident response steps are as follows:

- a. The LASO is the only individual with access to CHRI.
  - i. Should the LASO suspect a breach, the LASO shall notify the MVCA Head of School within 24 hours. The HOS shall notify the Academy Board President immediately.

- ii. Should the MVCA Head of School suspect a breach, the MVCA Head of School shall notify the Academy Board President within 24 hours.
  - iii. Should a K12 manager suspect a breach, the K12 manager shall notify his/her director, the MVCA Head of School, and the Academy Board President within 24 hours.
  - iv. Should an employee of the Educational Products and Services Provider, K12, or a contractor suspect a breach, the individual shall notify a K12 manager, the MVCA Head of School and the Academy Board President within 24 hours.
- b. If any person suspects that a CHRI information security breach has occurred, that person must confer with the Academy Board of Directors and the MVCA Head of School regarding the suspected incident. The MVCA Head of School may confer with various Academy (K12) departments such as Operations, Special Programs, Administrative Assistants, or Counseling to discover whether any individual accessed or received CHRI information. The MVCA Head of School will report results to the LASO. The MVCA Head of School may counsel, or remind individuals that the LASO is the only person permitted to receive CHRI documentation. This counseling may occur even when there is no or limited evidence to support the suspected breach.
- c. Michigan Virtual Charter Academy shall utilize the following digital and physical safeguard procedures:
1. Michigan Virtual Charter Academy shall follow its Information Security Policy to maintain software and / or hardware to prevent unauthorized access or the intrusion of agency information systems (firewalls, virus detection, malware/spyware detection). Further, MVCA maintains locked doors and/or cabinets to prevent unauthorized physical access to CHRI media.
  2. Michigan Virtual Charter Academy uses information security protocols to monitor and detect unauthorized access to electronic media. Michigan Virtual Charter Academy maintains CHRI media in a locked filing cabinet, and provides access to only the LASO. The building is monitored by alarms and access can only be granted with electronic access and office keys.
  3. Analysis-If a suspected incident occurs, authorized representatives such as the LASO, the Academy Board of Directors, or the MVCA Head of School shall conduct an investigation to identify whether an incident occurred, how the suspected incident occurred and what systems or data were compromised and affected.
  4. Containment-The LASO, Academy Board of Directors, or MVCA Head of School may take action to stop the spread of suspected intrusion, prevent further disclosure, or contain the suspected breach.
  5. Eradication-When necessary, the LASO, Academy Board of Directors, or MVCA Head of School may create a removal plan of the intrusion before the system is restored and steps are taken to prevent reoccurrence.
  6. Recovery-The LASO will take steps to recover the missing, or disclosed CHRI files or documents and then store them according to Michigan Virtual Charter Academy's CHRI storage protocols.
  7. Reporting-Michigan Virtual Charter Academy shall promptly report digital and physical incidents that significantly endanger the security or integrity of Criminal Justice Information (CJI) to the Michigan State Police "Information Security Officer" (ISO) on CJIS-016 FORM in compliance with the Federal Bureau of

Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy. The CJIS-016 FORM can be located at the SAS website: [www.michigan.gov/cjicats](http://www.michigan.gov/cjicats) (Forms).

- d. Should Michigan Virtual Charter Academy choose to take legal action, whether criminal or civil, the LASO, Academy Board of Directors, or MVCA Head of School may contact law enforcement to make a report or contact K12 and MVCA's legal counsel.
- e. The Operations Manager will retain any completed CJIS-016 Form(s) in the same locked filing cabinet that stores MVCA CHRI results at Michigan Virtual Charter Academy.

## **MOBILE DEVICE INCIDENT RESPONSE**

In order to reduce the risk of unauthorized access to stored or viewed CHRI on a mobile device (including smartphones and tablets), Michigan Virtual Charter Academy shall, *in addition to the above reporting requirements for incident response*, establish and implement additional or enhanced incident reporting and handling procedures for mobile devices.

MVCA will document and indicate, for a lost or compromised device, how long the device has been lost. Special reporting of such instances shall apply for the following situations:

- a. For a lost device, the Academy will report if the owner:
  - 1. Believed the device was locked.
  - 2. Believed the device was unlocked.
  - 3. Could not validate the device locked state.
- b. For a total loss of a device (unrecoverable), the Academy will report if:
  - 1. CHRI was stored on the device.
  - 2. The device was locked or unlocked.
  - 3. The Academy was capable of remote tracking or wiping of the device.
- c. The Academy will report any compromise of a device when the intrusion occurs while still in the owner's possession
- d. The Academy will report any compromise of a device when the intrusion occurs while still in the owner's possession outside of the United States.

Michigan Virtual Charter Academy shall establish and implement the following incident handling procedures:

- a. If at any time the LASO loses a device or believes there to be a breach of security, he/she shall report to the MVCA Head of School and report via the CJIS-016 Form.
- b. Since the CJIS-016 Form is the required method used for the reporting of security incidents, including mobile devices, the Academy shall use and retain completed forms on an ongoing basis in order to meet the Policy requirements for tracking.

## **SECONDARY DISSEMINATION**

When permitted by law, and Michigan Virtual Charter Academy releases a CHRI response to another authorized recipient pursuant to authorized sharing provisions, a log of such release(s) shall be established, implemented, and kept current. The log will be maintained indefinitely and be made available upon request to a MSP representative for audit purposes. Fields required for the log are:

- The date the record was shared.
- Record disseminated.
- Requesting agency.
- Requestor's name.
- Method of sharing; either by U.S. Mail, landline fax, or within the Criminal History Record Internet Subscription Service (CHRISS). (No emailing unless encrypted).
- Agency personnel that shared the CHRI.

## **SECURITY AWARENESS TRAINING**

Michigan Virtual Charter Academy, through its Educational Products and Services Provider, K12, will establish, implement, and administer basic Security Awareness Training (SAT) that meets the minimum standards provided within the most current version of the FBI CJIS Security Policy. The LASO will, every two (2) years and starting from the date of the Academy adopting the SAT, review the FBI CJIS Security Policy to ensure that the Academy implemented SAT meets the most current requirement(s). All individuals having access to CHRI, whether digital or physical, shall complete SAT provided by the Academy, through its Educational Products and Services Provider, K12, within six (6) months of assignment and every two (2) years thereafter. The Academy will also include any or all Information Technology (IT) personnel having access to digital systems used to process CHRI. The Academy, through its Educational Products and Services Provider, K12, shall document and keep current completed SAT records current.