



Louisiana Noncriminal Justice
Agency VECHS Onboarding Packet

Contents

Acronym Glossary	4
Introduction	5
Overview & History	5
Criminal History Record Information Databases	5
FBI Criminal Justice Information Services (CJIS) Security Policy	6
Overview & History of VECHS	6
NCPA/VCA & VECHS	7
Qualified Organizations	7
What is Criminal History Record Information (CHRI)?	7
Access to Criminal History Record Information (CHRI)	8
ORIs/Account Numbers	8
User Fees	8
Louisiana Applicant Processing System (LAPS)	8
Civil Agency User Agreement	9
Security Awareness Training and Authorized Personnel	11
Applicant Notification and Record Challenge	11
Applicant Rights and Privacy Statements	11
State and Federal Record Challenge	11
Right to Review - State Record Challenge	12
FBI Identity History Summary checks - Federal Record Challenge	12
Security of Criminal History Record Information (CHRI)	12
Acceptable Use Policy	12
Storage of Criminal History Record Information (CHRI) Policies	13
Physical Protection Policy	13
Controlled Areas	13
Physical Security includes:	14
Media Protection Policy	14
Electronic Security includes:	14
IT personnel's responsibility to:	14
Criminal History Record Information (CHRI) Retention Policy	14
Criminal History Record Information (CHRI) Destruction Policies	15
Physical Destruction Policy	15
Media Sanitation and Disposal Policy	15
Disciplinary and Misuse of Criminal History Record Information (CHRI) Policy	15
Incident Response Policy	16
OTS Information Security Policy – Incident Management	16

Outsourcing	17
Audit	17
Appendices	18
Appendix A FBI CJIS Security Policy	18
Appendix B Outsourcing Security Incident Reporting form	18
Appendix C Agency Privacy Requirements for Non-criminal Justice Applicants	18
Appendix D Non-criminal Justice Applicant's Privacy Rights	18
Appendix E Privacy Act Statement	18
Appendix F OTS Information Security Policy	18
Appendix G Statement of Misuse	18
Appendix H Sample Policies	18
Appendix I Background Check Authorization Form	18
Appendix J LAPS Authorization Form	18
Appendix K Right to Review Authorization Form	18
Appendix L Right to Review Disclosure Form	18
Acknowledgement of Requirements	19

Acronym Glossary

Acronym	Term
CHRI	Criminal History Record Information
CJI	Criminal Justice Information
CJIS	Criminal Justice Information Services
CJISSECPOL	CJIS Security Policy
CSA	CJIS System Agency
FBI	Federal Bureau of Investigation
III	Interstate Identification Index
ISO	Information Security Officer
ARSO	Authorized Recipient Security Officer
LSP	Louisiana State Police
LSP Bureau	Louisiana State Police Bureau of Criminal Identification & Information
NAC	Non-Criminal Agency Coordinator
NCJA	Non-Criminal Justice Agency
NGI	Next Generation Identification
ORI	Originating Agency Identifier
OTS	Louisiana Division of Administration's Office of Technology Services
OTS ISP	Office of Technology Services Information Security Policy
SID	State Identification Number

Introduction

This guide was created to assist non-criminal justice agencies (NCJAs) that submit fingerprints and receive criminal history record information (CHRI) for non-criminal justice purposes pursuant to authorizations allowed by state and federal law. Included in this guide are forms and documents that must be completed to be onboarded as an NCJA as well as information regarding the responsibilities of accessing and maintaining CHRI data.

The Volunteer & Employee Criminal History System (VECHS) in Louisiana was implemented in June of 2019 and is authorized by the National Child Protection Act, as amended (NCPA/VCA), and Louisiana Revised Statute 15:587.7. The overall purpose of this program is to provide state and national CHRI on applicants, employees, and volunteers to qualified organizations.

This guide was created to assist non-criminal justice agencies (NCJAs) that qualify under VECHS to submit fingerprints and receive CHRI for non-criminal justice purposes. Specifically, qualified organizations can use the information received to make eligibility determinations surrounding current and prospective volunteers and employees who should be disqualified from working with or around children, the elderly, or the disabled.

Overview & History

Federal Public Law 92-544, passed by Congress in October 1972, provided for funds to be allocated for the exchange of criminal history identification records for non-criminal justice purposes, pursuant to approved statutes. In 1998, the National Crime Prevention and Privacy Compact Act was passed allowing signatory states to exchange criminal history records for non-criminal justice purposes according to a uniform standard. The 1998 act also established the National Crime Prevention and Privacy Compact Council to regulate and assist in maintaining a method of exchange of criminal history record information which protects both public safety and individual privacy rights. The FBI Criminal Justice Information Services (CJIS) Division houses the largest repository of fingerprint-based criminal history records and is charged with the responsibility and authority to oversee the exchange of such records. Federal laws, regulations, and policies have been formed both to govern the release of information exchanges through the FBI and to require states to regulate access, use, quality, and dissemination of state-held records.

Criminal History Record Information Databases

The FBI maintains an automated database, Next Generation Identification (NGI), that integrates criminal history records submitted by federal, state, local, and tribal agencies. Each state has a criminal records repository responsible for the collection and maintenance of criminal history records submitted by law enforcement agencies in its state. The Louisiana State Police Bureau of Criminal Identification and Information (LSP BCII) is the state's designated repository that stores criminal history record information (CHRI) in the Louisiana Computerized Criminal History (LACCH) database.

CHRI is defined by Title 28 Code of Federal Regulations (CFR) §20.3 as 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. 28 CFR §20.21 further states information is considered CHRI if it confirms the existence or nonexistence of CHRI. CHRI is also described in the FBI CJIS Security Policy (CJISSECPOL), Section 4.1.1, as a subset of Criminal Justice Information (CJI) and is sometimes referred to as "restricted data". Information is considered CHRI if it is transferred or reproduced

directly from CHRI received as a result of a national FBI check and associated with the subject of the record. This includes information such as conviction/disposition data as well as identifiers used to index records regardless of format.

The FBI's NGI database stores the world's largest and most efficient electronic repository of biometric and criminal history information. However, the FBI's NGI database may not contain some records stored in the LSP Bureau's repository. For example, a civil agency authorized by state law to receive records expunged in Louisiana's criminal history database will not receive the expunged record if only a federal background check is conducted in a manner that bypasses the LSP Bureau. Civil agencies must submit fingerprints to the FBI via the LSP Bureau as required by Public Law 92-544 in order to receive the most complete and comprehensive response.

FBI Criminal Justice Information Services (CJIS) Security Policy

The FBI's Criminal Justice Information Services Security Policy (CJISSECPOL) provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of Criminal Justice Information (CJI). This policy applies to every individual-contractor, private entity, non-criminal justice agency representative, or member of a criminal justice entity with access to, or who operate in support of, criminal justice services and information.

The CJISSECPOL integrates presidential directives, federal laws, FBI directives, and the criminal justice community's Advisory Policy Board's decisions, along with nationally recognized guidance from the National Institute of Standards and Technology. As use of criminal history record information (CHRI) for non-criminal justice purposes continues to expand, the CJISSECPOL becomes increasingly important in the secure exchange of criminal justice records. The CJISSECPOL provides a secure framework of laws, standards, and elements of published and vetted policies for accomplishing the mission across the broad spectrum of the criminal justice and non-criminal justice communities. A copy of the CJISSECPOL can be found in Appendix A.

A non-criminal justice agency (NCJA) needs to be aware of the CJISSECPOL as the criminal history record information (CHRI) that results from a fingerprint-based background check is considered criminal justice information. Therefore, the CJISSECPOL provides the requirements and standards for ensuring the security and confidentiality of this information.

I have read and acknowledged the above information. _____

Initials

Overview & History of VECHS

The National Child Protection Act/Volunteers for Children Act (NCPA/VCA) was established in 1993 to create a national criminal history background check system to which a designated agency in each state is required to report child abuse crime information for the purposes of background checks of child care providers. The NCPA/VCA allows governmental and non-governmental agencies to conduct background checks of employees or volunteers who provide services to children, the elderly, or the disabled.

NCPA/VCA & VECHS

The creation of a Volunteer & Employee Criminal History System (VECHS) allows for the dissemination of CHRI to go directly to a governmental or non-governmental entity in states where VECHS programs have been established. This dissemination to a non-governmental entity is granted through the signing of a VECHS waiver by the applicant. This waiver allows the criminal history information to be disseminated directly to a private entity. Private entities who fall under VECHS have the ability to request state and national background checks.

I have read and acknowledged the above information. _____

Initials

Qualified Organizations

Governmental and non-governmental organizations (public or private) who provide care or care placement services, as defined by the NCPA/VCA, to children, the elderly, or the disabled, are considered qualified organizations and are permitted to obtain criminal history record information (CHRI) under the VECHS program. **A physical business office of the applicant must be located in the State of Louisiana in order to be qualified.** Agencies outside of a state's geographical boundaries/jurisdiction cannot be designated as qualified agencies. The Louisiana State Police has the authority to determine whether to conduct particular types of noncriminal justice background checks, and is responsible for establishing the mechanisms and procedures for those checks within its jurisdiction. In addition, the Louisiana State Police possesses limited authority to meet obligations for maintaining appropriate controls, such as user agreements and audits, outside of its jurisdiction, especially with respect to another state's governmental agencies. Examples of unauthorized dissemination include:

1. One state governmental agency shares FBI CHRI with another state's governmental agency for adoption purposes when the child and prospective parents reside in different states, even if both states have approved Pub. L. 92-544 state statutes.
2. Criminal history sharing initiatives involving participation in national interstate compacts, associations, or databases such as those for child placement or employment/licensing in the health care industry.

I have read and acknowledged the above information. _____

Initials

What is Criminal History Record Information (CHRI)?

When an agency submits fingerprints to the LSP Bureau for a background check, the result of that check is criminal history record information (CHRI). A non-criminal justice agency receiving CHRI is responsible for ensuring the security and confidentiality of the record itself and all references to the contents therein.

CHRI, received from the LSP Bureau, does not include driver history records or arrests in which the offender was issued a summons.

I have read and acknowledged the above information. _____

Initials

Access to Criminal History Record Information (CHRI)

A non-criminal justice agency (NCJA) can only receive CHRI if there is a statute in place providing the authority to do so. The statutory authority will either specify that the NCJA can receive state and federal results (from LACCH and NGI, respectively) from fingerprint-based background checks, or receive state-only results. An NCJA cannot receive the results of background checks without a statutory authority. Each authority within the state of Louisiana has been assigned an Applicant Type Code by the LSP Bureau. The LSP Bureau will confirm or provide the statutory authority and correlated Applicant Type Code if unknown to the NCJA.

ORIs/Account Numbers

Once the statutory authority is established, the LSP Bureau will assign an NCJA a nine-character account number called an ORI. The LSP Bureau will notify the NCJA of their ORI upon execution of the Civil Agency User Agreement. The ORI is a critical component of tracking the dissemination of CHRI between the LSP Bureau and the NCJA. **The ORI format for Healthcare Providers is LAHCP####.**

The NCJA is required to include the ORI and Applicant Type Code with every fingerprint submission. These are included in the Background Check Authorization Form (Appendix I), provided to an NCJA by the LSP Bureau. This form is to be used in conjunction with the appropriate Disclosure Form when requesting background checks with fingerprint cards. The LAPS Authorization Form (Appendix J) is for agencies that use the LAPS program.

User Fees

Louisiana Revised Statute 15:587 B(1) enables the Bureau to charge a processing fee for access to criminal history record information (CHRI) for non-criminal justice purposes.

28 C.F.R. § 20.31 allows the FBI to collect fees for non-criminal justice fingerprint-based background checks. The Director of the FBI shall review the amount of the fee periodically, but not less than every four years, to determine the current cost of processing fingerprint identification records for non-criminal justice purposes. The Bureau collects this fee on behalf of the FBI and forwards the money to them monthly.

Louisiana Applicant Processing System (LAPS)

The Louisiana Applicant Processing System (LAPS) is a new program implemented by the Louisiana State Police (LSP) in 2023 to provide fast and efficient criminal history background check results to non-criminal justice agencies. The LAPS program is a digital fingerprint capture system utilizing Idemia's Identogo network of enrollment centers located around the state of Louisiana. The Identogo network allows applicants to submit fingerprints in their local area of domicile, eliminating the need to travel long distances to be fingerprinted or the need to submit fingerprint cards to the Louisiana State Police's Bureau of Identification and Information (LSP

BCII) to obtain a criminal history report. Applicants can schedule their own appointments at a time and place convenient for them. Requesting agencies then log into a web portal to obtain the criminal history background check results for their applicants. Criminal History Record Information (CHRI) remains securely stored in the LAPS web-based results portal in compliance with the CJIS Security Policy, eliminating the need for individual agencies to have to store CHRI locally. Background check results are now available to non-criminal justice agencies in a matter of hours after a fingerprint submission rather than days or weeks. Your agency must work with the LSP BCII directly to receive a LAPS account.

I have read and acknowledged the above information. _____

Initials

Civil Agency User Agreement

Pursuant to the CJISSECPOL, section CA-3 Information Exchange, each agency authorized to receive criminal history record information (CHRI) must sign a User Agreement. A User Agreement is a contractual agreement between the authorized receiving agency, the non-criminal justice agency (NCJA) requesting the results of the background check, and the LSP Bureau. This agreement authorizes the LSP Bureau to share CHRI with the NCJA. Without a User Agreement in place, the LSP Bureau does not have the authority to disseminate CHRI.

A Civil Agency User Agreement shall be in place prior to non-criminal justice agencies receiving CHRI. **If an NCJA does not have a User Agreement, or if the signatory roles have changed since the agreement was executed, the agency must contact the LSP Bureau at LAHCP@la.gov to execute a new agreement.**

The User Agreement contains Terms and Conditions which include the following:

Authority and Purpose: The User Agreement identifies the requesting Agency, the purpose for which criminal history record information is requested, and the specific statutory authority granting access to the information. **Non-criminal justice agencies are prohibited from using criminal history record information for any purpose other than that for which it was requested.**

Sanctions/Penalties: The User Agreement is subject to cancellation by either party with 14 days written notice. The LSP Bureau reserves the right to immediately suspend service for investigation of apparent/alleged violations of the User Agreement or requirements for access. State and federal civil and/or criminal penalties may apply for misuse of CHRI. **CHRI must be used solely for the purpose requested and cannot be disseminated outside of the receiving Agency.**

Misuse of CHRI: The exchange of CHRI is subject to immediate cancellation if dissemination is made outside of the receiving departments or related agencies and if CHRI is used for any other reason that is not stated in Louisiana law. Furthermore, depending upon the nature of the offense and the identity of the offender, federal or state crimes may be charged for the willful, unauthorized disclosure of CHRI. Misuse of CHRI can be a misdemeanor or felony depending on the circumstances.

The User Agreement will be signed and maintained by the following individuals:

Non-criminal Agency Coordinator (NAC): The agency head of each non-criminal justice agency will designate a NAC to act as the primary contact person for that agency. The NAC shall complete LSP Bureau training requirements and shall serve as the point of contact and liaison between the agency and the LSP Bureau. The NAC will ensure all employees with access or potential access to CHRI successfully complete the appropriate level of CJIS Security Awareness Training and will maintain that certification as long as the employee may have access to CHRI. This requirement includes janitorial staff and personnel that work for contractors and vendors. The NAC will also assist LSP Bureau personnel with scheduled audits or any other LSP Bureau requests for information.

Duties of the NAC also include, but are not limited to:

1. **Authorized Personnel List:** The NAC is responsible for maintaining an updated Authorized Personnel List. The Authorized Personnel List contains those individuals whom the agency has identified as authorized to access, handle, and/or destroy CHRI, including agency, contractor, and/or vendor personnel. The authorizations are based solely on the agency's determination, but should be limited to the minimum number of personnel necessary. All personnel who view, handle, use, disseminate, or dispose of CHRI must appear on the list. Anyone included on this list must undergo the appropriate level of CJIS Security Awareness Training.
2. **Agency File Information:** The NAC should inform the LSP Bureau of changes in the agency head or any relevant business information (agency name changes, mailing/physical address changes, etc.). Changes must be made as they occur.
3. **Authorization and Purpose:** A change in an agency's authorization may invalidate the entire User Agreement. If the NAC becomes aware of a change in the authorization for access (e.g., new state statute, etc.), he/she shall contact the LSP Bureau immediately to update the User Agreement and, if necessary, submit the new authorization to the LSP Bureau.

Authorized Recipient Security Officer (ARSO): Pursuant to the CJISSECPOL, the non-criminal justice agency is required to appoint an ARSO to act as liaison with the LSP Bureau and the Division of Administration's Office of Technology Services (OTS) to ensure the agency is in compliance with security procedures. This role was previously known as the LASO. This individual must be knowledgeable in CHRI policies and mandated rules and regulations as well as have knowledge of IT security procedures. ARSOs are designated as the point of contact on security-related issues for their respective agencies and are responsible for instituting the LSP Bureau's incident response reporting procedures at their agency as needed (Appendix B). It is the ARSO's responsibility to ensure the day to day security of the CHRI and ensure the agency's CHRI policies and procedures are enforced, maintain information security documentation, assist the NAC with audits, and keep LSP informed as to any information security needs and problems. It is not uncommon for the NAC and ARSO to be the same person within an agency. See the section titled "Incident Response" for more information related to the duties of the ARSO.

I have read and acknowledged the above information. _____

Initials

Security Awareness Training and Authorized Personnel

Only authorized personnel within a non-criminal justice agency can view, access, or interact with the criminal history record information (CHRI). To be considered authorized personnel, the individuals that require access to the CHRI must complete CJIS Security Awareness Training.

The LSP Bureau provides CJIS Security Awareness Training to all non-criminal justice agencies. This training is completed through an online training and certification resource known as CJIS Online, and includes a course and certification. The NAC for each agency will be given an account by the LSP Bureau and it is the NAC's responsibility to manage users and ensure the training is complete and current for all individuals at their agency who require access to CHRI. The NAC is responsible for ensuring agency personnel with access to CHRI complete this training as part of initial training prior to accessing CJI and annually thereafter.

For the NAC to access the Security Awareness Training, follow the below link and credentials.

Link to the training: cjisonline.com

Username: NAC email address provided to the LSP Bureau on the User Agreement

Password: The NAC will be required to change the password upon the initial login

All personnel who are required to complete Security Awareness Training must sign an Acknowledgement Statement of Misuse acknowledging the notification of the penalties for misuse of CHRI (Appendix G).

The requirement for Security Awareness Training is found in the CJISSECPOL, Awareness and Training (AT) section.

I have read and acknowledged the above information. _____

Initials

Applicant Notification and Record Challenge

Applicant Rights and Privacy Statements

The National Crime Prevention and Privacy Compact Council outlines rights provided to applicants who are the subject of a national fingerprint-based criminal history record check for a non-criminal justice purpose. These rights are detailed in the Agency Privacy Requirements for Non-criminal Justice Applicant's document (Appendix C). A non-criminal justice agency must notify applicants of their privacy rights by providing applicants with a copy of the Non-criminal Justice Applicant's Privacy Rights document (Appendix D) prior to sending an applicant to be fingerprinted. Information is also available in the Privacy Act Statement (Appendix E).

State and Federal Record Challenge

If an NCJA receives CHRI results that contain disqualifying charges without a final court disposition, or that the applicant determines are inaccurate, the NCJA must provide a reasonable time for the applicant to correct or complete their record. Currently, neither the FBI nor the LSP Bureau have defined what qualifies as a

“reasonable time”, therefore it is the responsibility of the NCJA to determine a reasonable time for this process and ensure it is documented in their agency policies. If an applicant elects to correct or complete their record, the NCJA cannot make an eligibility determination until the conclusion of the reasonable time.

NCJAs are required to advise the applicant of the procedures for obtaining changes, corrections, or updates to their criminal record. Information on the processes for challenging a state and federal record are below.

Right to Review - State Record Challenge

Pursuant to LA Revised Statute 15:588, an individual can obtain a certified copy of their personal criminal history record as maintained by the LSP Bureau. Individuals must submit a Right to Review Authorization Form (Appendix K) and a Right to Review Disclosure Form (Appendix L) along with fingerprints and the appropriate fees to the LSP Bureau. Individuals can use this record to identify, if applicable, the date of an arrest, the identity of an arresting agency, and disposition information. This criminal history record may only be given to the individual, an authorized representative, or an attorney.

State website for information about record review and challenge:

<https://lsp.org/about/leadershipsections/support/bcii/fingerprints-and-background-checks/>

FBI Identity History Summary checks - Federal Record Challenge

The U.S. Department of Justice Order 556-73, also known as Departmental Order, establishes rules and regulations for individuals to obtain a copy of their Identity History Summary for review or proof that one does not exist. The individual may submit fingerprints, an Applicant Information Form, and payment directly to the FBI according to the procedures in Title 28 Code of Federal Regulations 16.34.

FBI website for information about record review and challenge and forms:

<https://www.fbi.gov/services/cjis/identity-history-summary-checks>

I have read and acknowledged the above information. _____

Initials

Security of Criminal History Record Information (CHRI)

Non-criminal justice agencies (NCJA) must have written policies and procedures regarding and specific to the access, use, dissemination, and disposal of CHRI. These policies and procedures must be made available to LSP Bureau personnel or the Louisiana CJIS Information Security Officer (ISO) upon request. The following subsections outline the required policies that must be in place along with guidance on protecting the security and confidentiality of the CHRI. **Sample policies are found in Appendix H.**

Acceptable Use Policy

A non-criminal justice agency (NCJA) shall have a written policy identifying the use of CHRI and stating that the records shall only be used for official purposes and will not be disseminated outside of the agency to unauthorized entities. This policy should also reference the specific reason the agency is requesting CHRI (for example, for the purpose of employment or licensing) and include the agency’s statutory authority or applicant

type. The statutory authority and applicant type will be provided by the LSP Bureau prior to the non-criminal justice agency receiving CHRI.

The requirement for an acceptable use policy is found in Public Law 92-544 and Title 28, C.F.R. 20.33, and 50.12(b).

Storage of Criminal History Record Information (CHRI) Policies

Non-criminal justice agencies (NCJA) have the option to store CHRI either physically, in hard copies, or electronically, on a computer or in an electronic system. The LSP Bureau strongly recommends storing CHRI in the secure LAPS web-based results portal to ease the burden of the non-criminal justice agency in protecting the security and confidentiality of the records. CHRI stored within LAPS does not purge and will be retained indefinitely. Storage of CHRI within local systems, removable storage devices, or within the cloud are discouraged due to the resource investment necessary to satisfy all federally-mandated security requirements. When an NCJA stores the CHRI physically, a physical protection policy is required. When an NCJA stores the CHRI electronically, both a physical protection policy and a media protection policy are required. Details of each policy are described in the subsections below.

CHRI includes the actual results received from fingerprint-based background checks along with any documentation identifying the existence or non-existence of CHRI. Maintaining an external tracking system identifying such an existence is considered to be CHRI and will need to meet the appropriate storage requirements.

Physical Protection Policy

Agencies are required to establish appropriate administrative and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity. Agencies must have these procedures written, and specific to CHRI, in their agency policy. This includes maintaining the criminal history record information in a secure location that is not readily accessible to individuals not authorized to see it. An example of this type of secure storage would be maintaining the CHRI records in a locked file cabinet, in a locked room, only accessible to authorized personnel.

Controlled Areas

If an agency cannot meet all of the controls required for establishing a physically secure location (description available in CJISSECPOL Physical and Environmental Protection (PE), PE-17 Alternate Work Site), but has an operational need to access or store CHRI, the non-criminal justice agency 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. To be considered a controlled area, the NCJA shall:

- Limit access to the controlled area during CHRI processing times to only those authorized personnel trained to access or view CHRI.
- Lock the area, room, or storage container when unattended.
- Position information system devices (computers used to retrieve and view CHRI) and documents containing CHRI in such a way as to prevent unauthorized individuals from access and view.

An NCJA must specify in their CHRI physical protection policy that the records are stored in a controlled area.

Physical Security includes:

- Protection of the criminal history record information as confidential.
- Limitation of visitor access to controlled areas.
- Positioning of computer and system devices (laptops, cellular phones, I-pads, or any kind of handheld devices used to access, process, or store CHRI media) in such a way that prevents unauthorized personnel from gaining physical or visual access.
- Locking of rooms, areas, or storage containers where CHRI media is accessed, processed and/or stored.
- CHRI shall NOT be stored in an individual's personnel file if the personnel file could be accessible to individuals who are unauthorized to view or access the CHRI.

The requirements for a physical protection policy are found in the CJISSECPOL, Physical and Environmental Protection (PE) section.

Media Protection Policy

Media protection policy and procedures shall be documented and implemented to ensure that access to digital and physical media in all forms is restricted to authorized individuals. The NCJA must have procedures written, and specific to CHRI, in their agency policy for securely handling, transporting, and storing electronic CHRI.

Electronic Security includes:

- Restricting access to the digital/electronic CHRI and the systems/computers the records are on to authorized individuals.
- Password use and management.
- Protection from viruses, worms, Trojan horses, and other malicious code.
- Appropriate use and management of e-mail, spam, and attachments.
- Use of encryption for transmission and storage of sensitive/confidential information through electronic means.

IT personnel's responsibility to:

- Install protection from viruses, worms, Trojan horses, and other malicious code through scheduled electronic scanning and definition updates.
- Provide scheduled data backup and storage.
- Provide timely application of system patches as part of configuration management (i.e. Windows updates should be performed monthly).
- Provide physical and electronic access control measures.
- Provide protection measures for agency network infrastructure (i.e. Perimeter firewalls, intrusion prevention, web content filtering, email spam, and virus filtering).

The requirements for a media protection policy and electronic storage/access to CHRI are found in the CJISSECPOL, listed in this document as Appendix A.

Criminal History Record Information (CHRI) Retention Policy

A non-criminal justice agency (NCJA) may store criminal history record information in hard copy (physical) format or electronic format. The CHRI needs to be accessed only for the length of time it is needed to make eligibility determinations and allow adequate time for an applicant to complete or challenge the accuracy of the information in the record. **An NCJA must have a written policy stating the duration of time the CHRI is maintained within the agency.** If a retention timeframe is mandated per the NCJA's statutory authority to

receive CHRI, or by a governing entity's record retention guidelines, this would also need to be stated in the agency's policy with the specific timeframe. CHRI stored within the LAPS web-based results portal is retained indefinitely and does not purge.

Criminal History Record Information (CHRI) Destruction Policies

At the end of the NCJA's retention timeframe, CHRI shall be destroyed. There are specific requirements for the destruction of CHRI that must be followed and included in the NCJA's CHRI destruction policy. **When an NCJA stores the CHRI physically, the agency is required to have a Physical Destruction Policy. When an NCJA stores the CHRI electronically or digitally, the agency is required to have a Media Sanitation and Disposal Policy.**

Physical Destruction Policy

To compliantly destroy physical CHRI, an NCJA has two options. The NCJA must choose one of these options to destroy the CHRI and ensure it is properly documented in the agency's policies.

Option 1: Physical CHRI will be shredded by cross shredding and witnessed or performed by authorized personnel within the agency.

Option 2: Physical CHRI will be incinerated and witnessed or performed by authorized personnel within the agency.

Media Sanitation and Disposal Policy

To compliantly destroy and sanitize electronic CHRI, an NCJA has three options. The NCJA must choose one of these options to destroy the electronic CHRI and ensure it is properly documented in the agency's policies.

Option 1: 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.

Option 2: The NCJA will degauss the electronic CHRI prior to disposing of or reusing the computer/device/system the electronic CHRI was stored on. Degaussing the CHRI data must be completed or witnessed by authorized personnel within the agency. (Degaussing is neutralizing a magnetic field to erase information from a magnetic disk or other storage device).

Option 3: If the computer/device that the CHRI data is stored on is no longer operational, the NCJA must physically destroy the device. Destruction of the device containing electronic CHRI must be completed or witnessed by authorized personnel within the agency.

Disciplinary and Misuse of Criminal History Record Information (CHRI) Policy

A non-criminal justice agency (NCJA) must have a written policy outlining the steps they will take if it is identified that there has been a misuse of CHRI. This policy must minimally include the following:

- 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.

The requirements for a Disciplinary Policy are found in the CJISSECPOL, Personnel Security (PS) section.

Incident Response Policy

The non-criminal justice agency's (NCJA) ARSO is responsible for all security-related issues and instituting the LSP Bureau's incident response reporting procedures at their agency, as needed. **To fulfill this responsibility, the NCJA must have a written Incident Response Policy.**

The CHRI Incident Response Policy must:

- Establish operational incident handling procedures that include adequate preparation, detection, analysis, containment, recovery, and user response activities.
- Track, document, and report incidents to appropriate agency officials and/or authorities, including the LSP CJIS ISO.

The requirements for an Incident Response Policy are found in the CJISSECPOL, Incident Response (IR) section.

OTS Information Security Policy – Incident Management

The Louisiana Division of Administration (DOA) Office of Technology Services (OTS) Information Security Policy (OTS ISP) outlines the Incident Management Program (pgs. 39-44). This program clearly establishes the phases, actions, responsibilities, and documentation requirements for handling all incidents. This section of the Information Security Policy applies to any and all efforts related to the detection, action, documentation, and communication of an incident (Appendix F).

I have read and acknowledged the above information. _____

Initials

Outsourcing

In accordance with the National Crime Prevention and Privacy Compact Council, if a non-criminal justice agency (NCJA) shares or disseminates the criminal history record information (CHRI) the agency receives with a third party entity (e.g. separate department, governmental agency, non-governmental entity, county IT, or vendor/service provider) for any purpose, including but not limited to storage, disposal, or eligibility determinations, the NCJA must first complete the Outsourcing Approval Process. An NCJA cannot distribute CHRI to a third party or store the CHRI in a software solution without first obtaining approval from the LSP Bureau.

The Louisiana State Police is not approving outsourcing requests at this time. Should the LSP reopen the outsourcing approval process, your agency will be notified by the state.

I have read and acknowledged the above information. _____

Initials

Audit

Non-criminal Justice Agencies (NCJA) that are authorized to receive CHRI for non-criminal justice purposes are subject to an audit to ensure compliance with state and federal rules regarding fingerprint submissions and CHRI use. The NCJA will be audited once in every three year audit cycle in order to assess compliance with state and federal policies and regulations. The NCJA may also be audited by the FBI during the FBI audit of the Louisiana State Police.

The LSP Bureau's Non-Criminal Justice Agency Audit Program is conducted through an online system called CJIS Audit. The NCJA will be notified of their login credentials and access to the audit 30 days prior to audit assignment. The audit questionnaire will assess an NCJA's level of compliance with the state and federal requirements around accessing, storing, and maintaining CHRI as described, but not limited to the information, in this packet. Below is a timeline of the audit process:

- ☐ 30 days prior to the NCJA audit being issued, the LSP Bureau or representatives will email the NCJA to validate contact information
- ☐ The NCJA confirms contact information
- ☐ 30 days after the initial audit notification email is sent, the NCJA Audit will be issued
- ☐ The NCJA must complete and submit the NCJA Audit questionnaire within 15 days
- ☐ The LSP Bureau or representatives will review the audit and develop a report including the initially identified areas of non-compliance
- ☐ The NCJA must respond to each item on the report with further information, corrective action plans, and/or estimated dates of correction within 15 days
- ☐ The LSP Bureau or representatives will conduct a final review of the audit and monitor non-compliant findings through correction

I have read and acknowledged the above information. _____

Initials

Appendices

Appendix A	<u>FBI CJIS Security Policy</u>
Appendix B	<u>Outsourcing Security Incident Reporting form</u>
Appendix C	<u>Agency Privacy Requirements for Non-criminal Justice Applicants</u>
Appendix D	<u>Non-criminal Justice Applicant's Privacy Rights</u>
Appendix E	<u>Privacy Act Statement</u>
Appendix F	<u>OTS Information Security Policy</u>
Appendix G	<u>Statement of Misuse</u>
Appendix H	<u>Sample Policies</u>
Appendix I	<u>Background Check Authorization Form</u>
Appendix J	<u>LAPS Authorization Form</u>
Appendix K	<u>Right to Review Authorization Form</u>
Appendix L	<u>Right to Review Disclosure Form</u>

Acknowledgement of Requirements

Please email a signed copy of this entire document to LAHCP@la.gov and keep a copy for your records.

Signature of Agency Head

Title and Printed Name

Date

Signature of Agency NAC

Title and Printed Name

Date

Signature of Agency ARSO

Title and Printed Name

Date

Volunteer & Employee Criminal History System (VECHS) Application for Qualified Entities



Louisiana State Police Bureau of Criminal Identification & Information (LSP BCII) VECHS Program

The VECHS Program in Louisiana was implemented in 2019 and is authorized by the National Child Protection Act (NCPA/VCA) of 1993, as amended, and Louisiana Revised Statute 15:587.7.

In order to be considered a qualified entity for the VECHS program, one must be a governmental or non-governmental organization who provides care or care placement services to children, the elderly, or the disabled.

The VECHS program does not allow agencies who fit the above criteria, but are required to conduct background checks under other state statutes to participate. If you are unsure as to whether your entity qualifies for the VECHS program, the Louisiana Noncriminal Justice Agency VECHS Onboarding Packet, made available on our website, may provide guidance and further clarification.

Please use the attached VECHS Application for Qualified Entities to provide the LSP BCII with the necessary information to determine whether your entity falls within the guidelines and parameters set forth by the NCPA/VCA, as amended, the FBI, and Louisiana Revised Statute 15:587.7. Once the LSP BCII has made a determination on your eligibility, you will be contacted with further instructions on how the entity's user agreement between the LSP BCII and the qualified entity will be executed.

VECHS Application for Qualified Entities

Louisiana State Police

Bureau of Criminal Identification & Information



Entity Information

Entity Name:				
ORI:				
Mailing Address:				
	Street Address			Unit #
	City	State	Zip	Parish
Physical Operating Address (the physical business office of the applicant must be located in the State of Louisiana for audit purposes):				
	Street Address			Unit #
☐ Check here if Physical Address is same as Mailing Address	City	State	Zip	Parish

Contact Information

Contact Person Name:			
Phone:		Ext:	
Email Address:		Fax:	
Agency Head: (Please Print)		Email Address:	

VECHS Application for Qualified Entities

Louisiana State Police

Bureau of Criminal Identification & Information



Summary of Services

Please check all appropriate areas below that apply to the service(s) provided by your entity to children, the elderly, and/or the disabled. NOTE: A "child" includes any unmarried person less than 18 years of age that has not been emancipated by order of a court. An "elderly person" means any person 60 years of age or older. A "disabled person" includes any person with a mental or physical impairment who requires assistance to perform one or more daily tasks.

Type of Person(s)	Care or Treatment	Education, Training, or Instruction	Supervision	Recreation	Care Placement
Child	☐	☐	☐	☐	☐
Elderly	☐	☐	☐	☐	☐
Disabled	☐	☐	☐	☐	☐

Please describe, in detail, the services your entity provides that would qualify your entity to receive state and national criminal history record checks under this program.

VECHS Application for Qualified Entities

Louisiana State Police

Bureau of Criminal Identification & Information



Please provide a list of each position that you would request a state and national criminal history record check on through the VECHS Program. Please include the job description for each as they relate to the services provided.

Title/Position	Job Duties/Description

Will you conduct background checks on employees, volunteers, or both?

☐
☐
☐

Employees Only
Volunteers Only
Both

VECHS Application for Qualified Entities

Louisiana State Police

Bureau of Criminal Identification & Information



Submission of Application

It is your responsibility to determine whether your agency is otherwise statutorily required to complete criminal history record checks on current or prospective employees and volunteers. Please verify your statutory requirements for record checks with the Louisiana Bureau of Criminal Identification & Information (LAHCP@la.gov) before submitting your VECHS application.

Please submit your completed application using the information below. For further information, please contact us at the email listed.

Louisiana State Police
Bureau of Criminal Identification & Information - LCJIS
LAHCP@la.gov

Printed Name of Agency Head	
Signature of Agency Head:	
Date:	

For LSP Use Only	
☐	Approved
☐	Denied - Reason for Denial _____
Signature of LSP Compact Officer or Designee: _____	

AUTHORITY: Louisiana Revised Statute 15:579

COMPLIANCE: Voluntary; however, failure to complete this Agreement will result in denial of request.

CIVIL AGENCY USER AGREEMENT

between the

LOUISIANA STATE POLICE (LSP)

Bureau of Criminal Identification and Information (Bureau)

hereinafter shall be known as "LSP Bureau" and

I. Agency Information

Agency Authorized Recipient (Agency Name)

Government Agency

☐ Yes

☒ No

Applicant Type

HCPE and HCPV

Physical Address

Originating Agency Identifier (ORI)

LAHCP _ _ _ _

City

State

ZIP Code

Outsourcing

Is your agency outsourcing any functions that may allow contractor access to Criminal History Record Information (CHRI)? Examples of outsourcing include, but are not limited to, performing information technology (IT) services, storage and/or destruction of criminal history record results, making fitness recommendations for employment or Licensing and obtaining missing dispositions. ☐ Yes ☐ No
If yes, provide contractor name, phone and email address below:

Noncriminal Agency Coordinator- (NAC) Authorized Personnel's Full Name and Title (Individual authorized to request and receive Criminal History Record Information (CHRI) on behalf of the agency).

Phone Number

FAX Number

NAC's Email Address

Authorized Recipient Security Officer (ARSO)- (Formally known as LASO) Authorized Personnel's Full Name and Title (This individual is the primary Information Security contact between the Agency, the Bureau and Office of Technology Services (OTS))

Phone Number

FAX Number

ARSO's Email Address

A request for

ACCESS AND RECEIPT OF CRIMINAL HISTORY RECORD INFORMATION

The Agency listed on page 1 shall be hereinafter referred to as the "Agency."

II. Purpose

This Agreement is established to provide Criminal History Record Information (CHRI) to the Agency requesting fingerprint/name-based criminal background checks for the purpose of employment, licensing and/or volunteer placement.

Pursuant to Title 34 USC 40316 access and receipt of fingerprint-based criminal history background checks must be explicitly authorized by federal law or a state statute approved by the U.S. Attorney General; and only individuals identified to be fingerprint background checked in such law or the authorizing statute may be fingerprinted. Name-based background checks must be authorized by Louisiana law.

The Agency is seeking background checks for the following purpose(s):

III. Background Check Information

What is the purpose of the background check? Provide details: (i.e. job(s), responsibilities and customers/clients served).

Provide the federal or state law(s) authorizing the criminal background check purpose(s).

NCPA / VCA

IV. The Parties Agree As Follows

The LSP BOI will:

1. Provide the Agency with CHRI in response to fingerprint-based or name-based background checks for civil purposes as allowed by state statute and federal law.
2. Provide the Agency with assistance in interpreting CHRI; however, the LSP Bureau will not provide advice or opinions on an individual's eligibility based on the CHRI.
3. Strive to ensure the completeness and accuracy of the CHRI.
4. Conduct audits of the agency to ensure compliance with this Agreement.
5. Restrict access and receipt of CHRI by the Agency if the LSP Bureau determines the Agency or its directors, officers, agents, or employees have violated the terms of this Agreement.

The Agency will:

1. Comply with state and federal laws, rules, regulations, procedures, and policies, including, but not limited to, the most current version of the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy and the Louisiana Noncriminal Justice Agency Guide regarding the access, use, and dissemination of CHRI.
2. Only use CHRI for the purpose requested as stated in the Louisiana Noncriminal Justice Agency Guide.
3. Obtain and retain any required documents mandated by state or federal law for the purpose of submitting and processing a fingerprint-based CHRI background check for each individual request.
4. Establish the necessary security and management controls for the security and confidentiality of CHRI received in accordance with the most current version of the FBI CJIS Security Policy and Louisiana Noncriminal Justice Agency Guide. This includes, but is not limited to,:
 - a. Designating a Noncriminal Agency Coordinator (NAC) who will act as liaison between the Agency and LSP Bureau. The NAC will receive audit information from the LSP Bureau and serve as the on-site contact person during audits.
 - b. Designating a Authorized Recipient Security Officer (ARSO) who is responsible for ensuring compliance with the terms of this Agreement and state and federal laws, rules, regulations, procedures, and policies regarding access, use, and dissemination of CHRI.
 - c. Ensuring its officers, employees, agents, and any other persons associated with the Agency who have access to CHRI, have received security awareness training.
 - d. Ensuring its officers, employees, agents, and any other persons associated with the Agency, abide by all state and federal laws, rules, regulations, procedures, and policies regarding access, use, and dissemination of CHRI; including, but not limited to, any LSP Bureau system(s) approved for use by the Agency for the access, receipt, and retention of CHRI. Additionally, the Agency acknowledges and understands that the use of this system provides for tracking and monitoring of computer access and location-specific variables, as authorized by federal and state laws, rules, regulations, procedures, and policies, including, but not limited to, the most current version of the FBI CJIS Security Policy and Louisiana Noncriminal Justice Agency Guide as it pertains to CHRI. Tracking and monitoring is to ensure the use, storage, dissemination, and processing of CHRI is completed in an appropriate environment and limited to authorized personnel.

- e. Establishing and implementing minimum screening requirements as required by CJIS Security Policy for its officers, employees, agents, and any other persons associated with the Agency who have access to CHRI. No individual may be granted access by the Agency when a felony conviction of any kind exists, unless explicitly approved by the LSP Bureau or CJIS System Officer (CSO).
 - f. Restricting access to physical or electronic CHRI to authorized personnel. Physical copies shall be maintained in a controlled, secure environment, such as in a locked cabinet in a room not accessible to all staff and visitors. When a physically secured location cannot be met, electronic media shall be protected with encryption that meets the most current FBI CJIS Security Policy.
 - g. Disseminating CHRI only when authorized by state or federal law approved by the U.S. Attorney General.
 - h. Ensuring the Agency establishes incident response policy and procedures, including an operational incident handling capability for agency information systems, whether physical or electronic. The Agency shall track, document, and promptly report a security incident of physical or electronic CHRI to the LSP Bureau Information Security Officer (ISO) who shall report the incident to the Louisiana CJIS ISO, Local Agency Security Officer, appropriate Agency officials, and/or local authorities.
 - i. Establishing and implementing policy and procedures for CHRI media protection, including, but not limited to, storage and access, media transport, electronic CHRI sanitization, and physical disposal.
- 5. Notify individuals of their right to update, challenge, or correct any discrepancies within his or her CHRI, and the Agency providing direction on how to do so.
 - 6. Retain supporting documentation for a minimum of three years from the time CHRI results are returned for audit purposes. Documentation, including but not limited to, Authorization Forms that support the Agency's purpose for requesting the individual to complete a background check coincides with an authorized purpose in state or federal law. The LSP Bureau recognizes the Agency may have a document retention policy that requires a time period greater than three years.
 - 7. Allow the LSP Bureau to conduct on-site audits to ensure compliance with the terms of this Agreement.
 - 8. Immediately notify the LSP Bureau of any changes to sections I and III provided in this Agreement. If access is no longer needed nor authorized by applicable state or federal law, rule, regulation, procedure or policy, the Agency must immediately notify the LSP Bureau to terminate access.
 - 9. Maintain and keep current a list of all Agency employees with digital or physical access to CHRI and their purpose for access.
 - 10. The Agency agrees to pay all applicable State and Federal fees on all transactions processed by the LSP Bureau or the FBI from any civil scan device within said Agency.

V. Criminal History Record Information Limitations

The Agency understands CHRI results have the following limitations:

1. The LSP Bureau retains identification records for the State of Louisiana only. Criminal record background checks completed through the FBI are forwarded by request through the LSP Bureau on behalf of the Agency.
2. CHRI is compiled from information submitted to the LSP Bureau from agencies tasked with criminal justice functions. Although the LSP Bureau makes reasonable efforts to ensure all information is submitted as required by law, the LSP Bureau is not responsible for incorrect or missing CHRI.
3. CHRI is constantly being updated as new CHRI is submitted to the LSP Bureau. CHRI is only valid as of the date and time the record check was completed.
4. The LSP Bureau encourages the reporting of all felonies, misdemeanors and arrests under local ordinances that substantially correspond to a violation of state law.
5. The LSP Bureau Repository contains only arrest events resulting from a fingerprint submission at time of arrest. Arrests for which a summons was issued will not appear in the Repository.

VI. Entire Agreement

This Agreement is the complete and exclusive statement of the agreement between the Parties with respect to the subject matter thereof, and supercedes all prior negotiations, representations, proposals and other communications between the Parties either oral or written. The Agreement may only be amended by a written document signed by the Parties, by and through their duly authorized representatives.

VII. Term and Termination

This Agreement is effective when signed by the Parties, by and through their duly authorized representatives, and shall remain in effect until terminated as hereinafter set forth. Either Party may terminate this Agreement for any reason; provided that at least 14 days advance written notice of termination is given to the non-terminating Party by the terminating Party. Either Party may immediately terminate this Agreement without advance written notice if either party, including any of its officers, employees, agents and any other persons associated with either Party, violates any applicable state or federal law, rule, regulation, procedure or policy. If access is no longer needed nor authorized by applicable state or federal law, rule, regulation, procedure or policy, the Agency must immediately notify the LSP Bureau to terminate access. The LSP Bureau may immediately terminate Agency access when an applicable state or federal law, rule, regulation, procedure or policy no longer allows for Agency access.

VIII. Indemnity & Hold Harmless

The Agency agrees to indemnify and hold harmless the LSP Bureau, its Secretary and employees from and against any and all claims, demands, actions, suits and proceedings by others; against all liability to others, including but not limited to any liability for damages by reason or any cause of actions whatsoever, or against any loss, cost, expense, damage resulting there from, arising out of or involving any negligence on the part of the Agency in the exercise or enjoyment of this Agreement. The Agency realizes that the LSP Bureau does not warrant the accuracy of the computerized information.

IX. Agency Approval

The "Agency Representative" must have the authority to commit the Agency to the above security and audit requirements, typically the head of the organization or the relevant unit, rather than the contact (listed on page one) who will have access to CHRI results.

Agency Name	
Printed or Typed Authorized Agency Representative Name	Title
Signature of Authorized Agency Representative	Date
X. LSP Bureau Approval	
Signature of LSP Bureau Chief Administrator	Date
Captain Saleem El-Amin	
Submit completed Agreement via email to: LAHCP@la.gov	
Mail: Louisiana State Police Bureau of Criminal Identification and Information Attn: Security and Access Section 7919 Independence Blvd. A-6 Baton Rouge, LA 70806	