



CITY OF NEW BRAUNFELS POLICIES AND PROCEDURES

PROCEDURE(S): CRIMINAL HISTORY RECORD INFORMATION (CHRI) PROPER ACCESS, USE, AND DISSEMINATION PROCEDURES

EFFECTIVE DATE: MAY 7, 2025

REVISION DATE(S):

A. Purpose

The intent of the following policies is to ensure the protection of the Criminal History Record Information (CHRI) until such time as the information is purged or destroyed in accordance with applicable record retention rules.

The following policies were developed using the FBI's Criminal Justice Information Services (CJIS) Security Policy. The City of New Braunfels may complement this policy with a local policy; however, the CJIS Security Policy shall always be the minimum standard. The local policy may augment, or increase the standards, but shall not detract from the CJIS Security Policy standards.

Scope

The scope of this policy applies to any electronic or physical media containing Texas DPS CHRI while being stored, accessed, or physically moved from a secure location from the City of New Braunfels. In addition, this policy applies to any authorized person who accesses, stores, and/or transports electronic or physical media. Pursuant to Texas Government Code 411.129, the authorized agency is granted the authority to access criminal history records within the DPS Secure Site for background searches for specific non-criminal justice purposes.

Criminal History Record Information (CHRI)

CHRI, is a subset of CJI and for the purposes of this document is considered interchangeable. Due to its comparatively sensitive nature, additional controls are required for the access, use and dissemination of CHRI. In addition to the dissemination restrictions outlined below the Texas Government Code 411.084 defines CHRI as "(a-1) The term "criminal history record" information under Subsection (a) does not refer to any specific document produced to comply



CITY OF NEW BRAUNFELS POLICIES AND PROCEDURES

PROCEDURE(S): CRIMINAL HISTORY RECORD INFORMATION (CHRI) PROPER ACCESS, USE, AND DISSEMINATION PROCEDURES

EFFECTIVE DATE: MAY 7, 2025

REVISION DATE(S):

with this subchapter but to the information contained, wholly or partly, in a document 's original form or any subsequent form or use."

Proper Access, Use, and Dissemination of CHRI

Information obtained from the Interstate Identification Index (III) is considered CHRI. Rules governing the access, use, and dissemination of CHRI are found in Title 28, Part 20, CFR. The III shall be accessed only for an authorized purpose. Further, CHRI shall only be used for an authorized purpose consistent with the purpose for which III was accessed.

The staff authorized to obtain Criminal History Record Information (CHRI) will use the guidelines in the Texas DPS [Secure Website Training Reference Manual](#) for the steps in performing the search of the CHRI along with their authorized legislative authority for purpose of search.

Personnel Security Screening

Access to CHRI is restricted to authorized personnel. Authorized personnel is defined as an individual, or group of individuals, who have been appropriately vetted through a name-based record check and have been granted access to CHRI data. Agencies located within states having passed legislation authorizing or requiring civil fingerprint-based background checks for personnel with access to CHRI for the purposes of licensing or employment shall submit name-based record check prior to giving personnel direct access to CHRI, those who have direct responsibility to configure and maintain computer systems and networks with direct access to CHRI, and any persons with access to physically secure locations or controlled areas containing CHRI to provide a service. Agencies without this legislative authorization or requirement are exempted from the name-based background check requirement until such time as appropriate legislation has been written into law.

[Texas DPS Secure Site](#) access will be determined based on the least privilege principle (need-to-know basis) to mitigate risks.



CITY OF NEW BRAUNFELS POLICIES AND PROCEDURES

PROCEDURE(S): CRIMINAL HISTORY RECORD INFORMATION (CHRI) PROPER ACCESS, USE, AND DISSEMINATION PROCEDURES

EFFECTIVE DATE: MAY 7, 2025

REVISION DATE(S):

Physical Security

While the City of New Braunfels typically does not store physical documents, any copies that are maintained will be kept in a physically secure area within the Human Resources office. A physically secure location refers to a designated area within a facility that is equipped with both physical and personnel security controls, sufficient to safeguard TX DPS CHRI and related information systems.

The City will designate authorized personnel with access to any CHRI copies, and in the rare instance a physical document is stored, it will be secured in a locked office or desk area assigned to the appropriate team member. Only authorized individuals will have access to these areas. Additionally, the City will maintain an up-to-date list of authorized personnel, regularly verifying access levels and contact information at least once a year. In the event that an authorized user no longer requires access, the City will promptly contact DPS to deactivate their access and ensure proper mitigation of any risks.

Physical security measures will be implemented to protect all transmission and storage mediums of CHRI, including physical access controls, encryption, and password protection.

Media Protection

Controls shall be in place to protect electronic and physical media containing CHRI while at rest, stored, or actively being accessed. “Electronic media” includes memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, backup medium, optical disk, flash drives, external hard drives, or digital memory card. “Physical media” includes printed documents and imagery that contain CHRI.



CITY OF NEW BRAUNFELS POLICIES AND PROCEDURES

PROCEDURE(S): CRIMINAL HISTORY RECORD INFORMATION (CHRI) PROPER ACCESS, USE, AND DISSEMINATION PROCEDURES

EFFECTIVE DATE: MAY 7, 2025

REVISION DATE(S):

The agency shall securely store electronic and physical media within physically secure locations or controlled areas. The agency shall restrict access to electronic and physical media to authorized individuals. If physical and personnel restrictions are not feasible then the data shall be encrypted per [Section 5.10.1.2](#). CHRI will not be transmitted via any unsecure or unencrypted electronic messaging tools. CHRI will not be stored on any unsecured electronic device, or unsecured cloud storage.

Electronic systems will be password protected, encrypted, and/or protected from unauthorized use with firewalls, virus or spyware protection or other similar software. The system will initiate a system lock for inactivity set to 10 minutes at all times.

If CHRI is printed, users will only print CHRI on a secure, not networked printer (personal printer), or on a printer with a secure password protected print feature (pass code feature). When retention of CHRI is no longer necessary or is not permitted by law, the criminal history record information shall be disposed of properly. A secure manner of disposal must be used to destroy thoroughly all elements of the records and preclude unauthorized viewing, access, or use.

Media Transport

Controls will be implemented to protect electronic and physical media containing CHRI to prevent inadvertent or inappropriate disclosure. While the City of New Braunfels does not typically transport CHRI, in the rare event that such a need arises, electronic and physical media will be securely controlled during transport outside of designated areas. Only authorized personnel will be permitted to handle or transport such media.

Media Sanitization and Disposal

When no longer usable, hard drives, diskettes, tape cartridges, CDs, ribbons, hard copies, printouts, and other similar items used to process, store and/or transmit FBI CJI shall be



CITY OF NEW BRAUNFELS POLICIES AND PROCEDURES

PROCEDURE(S): CRIMINAL HISTORY RECORD INFORMATION (CHRI) PROPER ACCESS, USE, AND DISSEMINATION PROCEDURES

EFFECTIVE DATE: MAY 7, 2025

REVISION DATE(S):

properly disposed of in accordance with measures established by City of New Braunfels. Disposal procedures will include a method sufficient to preclude recognition or reconstruction of information. Physical media (printouts and other physical media) shall be disposed of by shredding using City of New Braunfels shredders or placed in locked shredding bins for safe shredding offsite.

IT systems that have been used to process, store, or transmit TX DPS CHRI and/or sensitive and classified information shall not be released from City of New Braunfels' control until the equipment has been sanitized and all stored information has been cleared using one of the above methods.

Account Management

The agency shall manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The agency shall validate information system accounts at least annually and shall document the validation process.

All accounts shall be reviewed at least annually by the designated point of contact (POC) or his/her designee to ensure that access and account privileges commensurate with job functions, need-to-know, and employment status on systems that contain Criminal History Record Information. The POC may also conduct periodic reviews.

The facility/agency/organization shall maintain CCH verification forms or the appropriate CCH verification log for audit purposes. The facility/agency/organization shall also maintain proof of purpose in the form of job and volunteer applications from audit to audit.

Remote Access

The City of New Braunfels shall authorize, monitor, and control all methods of remote access to the information systems that can access, process, transmit, and/or store Texas DPS CHRI. Remote access is any temporary access to an agency's information system by a user (or an



CITY OF NEW BRAUNFELS POLICIES AND PROCEDURES

PROCEDURE(S): CRIMINAL HISTORY RECORD INFORMATION (CHRI) PROPER ACCESS, USE, AND DISSEMINATION PROCEDURES

EFFECTIVE DATE: MAY 7, 2025

REVISION DATE(S):

information system) communicating temporarily through an external, non-agency-controlled network (e.g., the Internet).

The City of New Braunfels shall employ automated mechanisms to facilitate the monitoring and control of remote access methods. The City of New Braunfels shall control all remote accesses through managed access control points. The City of New Braunfels may permit remote access for privileged functions only for compelling operational needs but shall document the rationale for such access in the security plan for the information system. Or The City of New Braunfels shall prohibit remote access under any circumstance.

Utilizing publicly accessible computers to access, process, store or transmit CHRI is prohibited. Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.

Personally Owned Information Systems

A personally owned information system shall not be authorized to access, process, store or transmit CHRI unless the agency has established and documented the specific terms and conditions for personally owned information system usage. A personal device includes any portable technology like camera, USB flash drives, USB thumb drives, DVDs, CDs, air cards and mobile wireless devices, laptops, or any personal desktop computer.

Reporting Information Security Events

The agency shall promptly report incident information to appropriate authorities to the Texas Department of public safety. Information security events and weaknesses associated with information systems shall be communicated in a manner allowing timely corrective action to be taken. Some examples of Security events include, cyber-attacks, ransomware, successful phishing attacks, inappropriate dissemination, sharing credentials or any other event that might have an impact on the security of an agency assets. Formal event reporting and escalation



CITY OF NEW BRAUNFELS POLICIES AND PROCEDURES

PROCEDURE(S): CRIMINAL HISTORY RECORD INFORMATION (CHRI) PROPER ACCESS, USE, AND DISSEMINATION PROCEDURES

EFFECTIVE DATE: MAY 7, 2025

REVISION DATE(S):

procedures shall be in place. If a security breach is detected the agency shall complete and submit Facility/Agency [Incident Reporting Form](#) and send to:

Audit & Training Supervisor
Crime Records Division
Compliance & Training Bureau
Texas Department of Public Safety
Email: cjis.audit@dps.texas.gov
Fax: 512-424-2909

Wherever feasible, the agency shall employ automated mechanisms to assist in the reporting of security incidents. All employees, contractors and third-party users shall be made aware of the procedures for reporting the different types of events and weakness that might have an impact on the security of agency assets and are required to report any information security events and weaknesses as quickly as possible to the designated point of contact.

Policy Violation/Misuse Notification

Violation of any of the requirements contained in the Access and Dissemination Policy, User and Entity Agreements, CJIS Security Policy or Title 28, Part 20, CFR, by any authorized personnel will result in suitable disciplinary action, up to and including loss of access privileges, civil and criminal prosecution and/or termination. If the confidentiality of CHRI is violated, the facility will follow its Employee Disciplinary/Corrective Action Policy and report the violation to DPS via the [Incident Reporting Form](#).

Likewise, violation of any of the requirements contained in the Access and Dissemination Policy, User and Entity Agreements, CJIS Security Policy or Title 28, Part 20, CFR, by any visitor can result in similar disciplinary action against the sponsoring employee and can also result in termination of services with any associated consulting organization or prosecution in the case of criminal activity.



CITY OF NEW BRAUNFELS POLICIES AND PROCEDURES

PROCEDURE(S): CRIMINAL HISTORY RECORD INFORMATION (CHRI) PROPER ACCESS, USE, AND DISSEMINATION PROCEDURES

EFFECTIVE DATE: MAY 7, 2025

REVISION DATE(S):

Links:

- Texas DPS Secure Site: <https://securesite.dps.texas.gov/DpsWebsite/Login.aspx?returnUrl=/DpsWebsite/Support/index.aspx>
- CJIS Launch Pad: <https://texas.cjisapps.com/noncrim/launchpad/>
- CJIS Security Policy: <https://le.fbi.gov/cjis-division/cjis-security-policy-resource-center>
- Access and Dissemination Policy: <https://securesite.dps.texas.gov/DpsWebsite/CriminalHistory/SecurityPolicy.aspx>
- Support & FAQ's: <https://securesite.dps.texas.gov/DpsWebsite/Support/Index.aspx>
- Secure Website Training Reference Manual: https://securesite.dps.texas.gov/lms/pluginfile.php/233/mod_resource/content/3/Secure%20Site%20Training%20Module%20User%20Guide.pdf

Incident Reporting Form – City of New Braunfels

Agency must promptly notify DPS of any incident, security breach, unauthorized, and or misuse of criminal history record information and system networks with CHRI access.

Section 1: Agency Information

Agency Point of Contact:	
Agency Phone:	Agency Email:

Section 2: Details of Incident

Date of Report:	Date of Incident
Location(s) of Incident:	
Area Affected (Check all that apply)	
<input type="checkbox"/> Misuse <input type="checkbox"/> Dissemination <input type="checkbox"/> Data Intrusion (Ransomware/Hack) <input type="checkbox"/> Physical <input type="checkbox"/> Digital <input type="checkbox"/> Other:	
Method of Detection	
<input type="checkbox"/> DPS Audit <input type="checkbox"/> Internal Audit <input type="checkbox"/> Other	
Description of Incident:	

Section 3: Actions Taken by Agency

--

Copy to:

Attn: Audit & Training Supervisor
TX DPS - Crime Records Division
Compliance & Training Bureau

Email To: CJIS.Audit@dps.texas.gov or Fax: 512-424-2909

Link for [CJIS Launch Pad - CHRI & Audit Resources](#)