TEXAS DEPARTMENT OF PUBLIC SAFETY

SECURITY POLICY FOR NON-CRIMINAL JUSTICE AGENCIES' ACCESS, USE, AND DISSEMINATION OF CRIMINAL HISTORY RECORD INFORMATION

I.ACCESS BY CRIMINAL and NON-CRIMINAL JUSTICE ENTITIES

A. Legislative Authority for Criminal and Non-Criminal Justice Entities' Access

Policy: A criminal or non-criminal justice entity legislatively authorized by Chapter 411, Subchapter F of the Texas Government Code or other state or federal law to receive criminal history record information (CHRI) from the Department of Public Safety (Department) may access the DPS Crime Records Service Secure Site. All criminal or non-criminal justice entities granted access to the DPS CHRI will be subject to all applicable state and federal laws, rules, regulations and policies that relate to the obtaining, use, storage, dissemination and destruction of CHRI.

The Federal Bureau of Investigation (FBI) may authorize certain Texas entities access to FBI criminal history record information based upon approved Texas statutes or federal law.

Commentary: The DPS CRS Secure Site is maintained by the Department and may be accessed pursuant to Chapter 411, Subchapter F of the Texas Government Code, Federal mandates or other Texas laws. A criminal or non-criminal justice entity granted access to the DPS CRS Secure Site may submit criminal history inquiries through the Computerized Criminal History Search (CCH) or through fingerprint submission. Results will be provided on-line through CCH or the Fingerprint-based Applicant Clearinghouse of Texas (FACT). The CCH will provide an entity with records originating in Texas only. In those instances where fingerprints are submitted under a statute approved for access to the FBI records, DPS will provide the criminal history record response through the Fingerprint-based Applicant Clearinghouse of Texas (FACT).

B.Agency User Agreements

Policy: A criminal or non-criminal justice entity requesting access to the DPS Crime Records Service Secure Site must provide the Department with a signed written user agreement in which the entity agrees to comply with Department policies regarding the use of the DPS CRS Secure Site or information. The user agreement will include standards and sanctions governing the criminal or non-criminal justice entity's utilization of the DPS CRS Secure Site or information and will incorporate the policies set forth in this document. These policies also apply to access, use, storage, dissemination and destruction of FBI criminal history record information, when appropriate.

Commentary: None.

II. PERSONNEL SECURITY

A. Authorized Users

Policy: A criminal or non-criminal justice entity must provide the Department with the name, sex, race, date of birth and title of each official/employee of the criminal or non-criminal justice entity who will utilize information received from the DPS CRS Secure Site. The Department will perform a name-based background check on each name submitted, and reserves the right to

require a fingerprint-based background check prior to approving access for any official/employee. Only those persons approved by the Department, hereinafter referred to as authorized officials/employees, will be allowed access to DPS CRS Secure Site or information on behalf of the criminal or the non-criminal justice entity. An official/employee who is not approved due to the results on the name-based check may dispute the findings through the submission of fingerprints. Contracted personnel, including IT must undergo additional requirements. Basic security awareness training is required for all personnel who have access to the CHRI within six months of initial assignment, and biennially thereafter. Refer to Section VI, Criminal Justice Information Services (CJIS) Security Policy for more detail.

The Department may limit the number of authorized officials/employees needing access to DPS CRS Secure Site. In addition, DPS shall enforce the most restrictive set of rights, privileges and guidelines governing access to DPS CRS Secure Site.

Commentary: Only authorized users may access the information received from the DPS CRS Secure Site. The number of authorized users shall be limited to the number reasonably necessary to perform criminal history checks for the purposes permitted by law. The security awareness training may be taken through CJIS Online.

B. User Identifier

Policy: A Department issued user entity identifier shall be used in each transaction in the DPS CRS Secure Site for retrieval of CHRI.

Commentary: The Department will assign a user identifier to each criminal or non-criminal justice entity authorized by the Department to access the DPS CRS Secure Site for CHRI. This user identifier serves to identify the criminal or non-criminal justice entity accessing the DPS CRS Secure Site and ensures the proper level of access for the criminal or non-criminal justice entity.

C. Personnel Sactions

Policy: A criminal or non-criminal entity with access to the DPS CRS Secure Site shall employ a formal sanctions process for personnel failing to comply with established information security policies and procedures.

Commentary: A criminal or non-criminal justice agency shall develop a written policy.

III. FACILITY AND INFORMATION SECURITY

A. Facility Security Standards

Policy: The location of all CHRI received from the DPS CRS Secure Site must have adequate physical security to protect against any unauthorized viewing or access to displayed, stored or printed criminal history record information at all times. Refer to Section VI, Criminal Justice Information Service (CJIS) Security Policy for more detail.

Commentary: File cabinets or file systems used to maintain physical CHRI must be protected from unauthorized viewing or access. Computer monitors used to display and view CHRI should be strategically placed so unauthorized viewing is not possible. For example, either locking of the file cabinet or locking access to the room the files are housed is one component of complying with this policy.

B. Physical Protection

Policy: A physical protection policy and procedures shall be documented and implemented to ensure the CHRI and information system hardware, software, and media are physically protected through access control.

Commentary: The agency shall develop a written policy.

C. Information Security Standards

Policy: Criminal history record information obtained from the DPS or FBI is sensitive information and must be maintained in a secure records environment to prevent the unauthorized viewing or use of the criminal history record information. Electronically stored, or transferred electronic media containing CHRI shall have a minimum encryption of 128 bit or be certified to meet FIPS 140-2 standards. The information system shall prevent further access to the system by initiating a session lock after a maximum of 30 minutes of inactivity. Users can directly initiate session lock mechanisms to prevent inadvertent viewing when the device is unattended. A session lock is not a substitute for logging out of the information system.

Commentary: An example of 'encryption' is a cryptographic mechanism like a passphrase; 'session lock' is a screen saver with password.

Policy: The use of publically owned computers to access criminal justice information is strictly prohibited.

Commentary: None

Policy: When retention of criminal history record information is no longer necessary or is not permitted by law, the criminal history record information shall be properly disposed. A secure manner of disposal must be utilized to thoroughly destroy all elements of the records and preclude unauthorized viewing, access or use. Digital Media shall be sanitized, that is, overwritten at least three times or degaussed prior to disposal or release for reuse by unauthorized individuals. Destruction and sanitation must be performed or witnessed by person (s) authorized by DPS as an 'Access and/or Data' user to the system's information.

Commentary: Disposal procedures should include a method sufficient to preclude recognition or reconstruction of information (i.e., cross-cut shredding). Inoperable electronic media must be destroyed (cut-up, shredded, etc.). The method should also provide verification that the disposal procedures were successfully completed by initiating the DPS Audit Verification Form or other forms of documentation.

D. Media Protection

Policy: A 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. Procedures shall be defined for securely handling, transporting, storing, sanitation and destruction of CHRI.

Commentary: The agency shall develop written policies.

IV. CRIMINAL HISTORY RECORD INFORMATION

A. Obtaining, Use and Dissemination of Criminal History Record Information

Policy: A criminal or non-criminal justice entity may retrieve criminal history record information through the DPS CRS Secure Site only for legislatively authorized purposes. Criminal history record information received from the DPS CRS Secure Site shall be used only for legislatively authorized purposes and may not be disseminated to a person not authorized to receive the information. Upon request by the Department, all users must provide an authorized purpose for all criminal history record information inquiries. The ability to retrieve criminal history record information is subject to cancellation if the information is obtained or used in an unauthorized manner or disseminated to a person not authorized to receive the criminal history record information. Criminal sanctions are also in place for the improper obtaining, use and dissemination of criminal history record information.

Commentary: Generally, criminal history record information held by the DPS and the FBI is confidential and may be disseminated only as authorized by state or federal statute. If CHRI is released to another authorized agency, and that agency was not part of the releasing agency's primary information exchange agreement(s), the releasing agency shall log such dissemination. Specific criminal or non-criminal justice entities are legislatively authorized to receive criminal history record information for limited or specified purposes. The criminal or non-criminal justice entity is responsible for complying with all laws governing the criminal or non-criminal justice entity's access to, use of and dissemination of criminal history record information. State law makes it unlawful for a person to obtain confidential criminal history record information in an unauthorized manner, use the information for an unauthorized purpose, or disclose the information to a person not entitled to the information. State law also makes it unlawful for a criminal or non-criminal justice entity to provide a person with a copy of the person's criminal history record information obtained from the Department unless authorized to do so by a specific state statute.

B. Commercial Dissemination

Policy: The commercial dissemination of criminal history record information obtained through the DPS CRS Secure Site is prohibited.

Commentary: The marketing of DPS CRS Secure Site data for profit is not permitted. State law makes it a felony offense to obtain, use, or disclose, or employ another to obtain, use or disclose, criminal history record information for remuneration or for the promise of remuneration.

V. INCIDENT RESPONSE

A. Reporting Security Events

Policy: The agency shall promptly report incident information to appropriate authorities. Security events including identified weaknesses associated with the event shall be communicated in a manner allowing timely corrective action to be taken. Formal event reporting and escalation procedures shall be in place. 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 weaknesses that might have an impact on the security of agency assets and are required to report any security events and weaknesses as quickly as possible to the designated point of contact.

Commentary: The agency shall develop an incident response plan. The plan shall include or enhance the reporting and handling of mobile device scenarios. All incidences shall be reported to the Department of Public Safety with the Incident Reporting form.

VI. CRIMINAL JUSTICE INFORMATION SERVICES (CJIS) SECURITY POLICY

A. CSP Version 5.8 (last updated 06/01/2019)

Policy: The CJIS Security Policy outlines the requirements for all criminal and non-criminal justice entities that access CJI and the DPS CRS Secure Site.

Commentary: The CJIS Security Policy may be found at the link below, with Appendix J for the non-criminal justice agency supplemental guidance.
https://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center

B. Security Audits

Policy: A security audit will be performed on a triennial basis by the Department for the purpose of measuring the criminal or non-criminal justice entity's compliance with the laws, rules, regulations and policies relating to the DPS CRS Secure Site and the criminal history record information obtained there from. Audits may be conducted on a more frequent basis if the audit reveals that an agency has not complied with applicable statutes, regulations and policies. The Department has the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.

Commentary: The agency will continue to retain audit records for longer than one (1) year until it is determined they are no longer needed for the administrative, legal, audit, or other operational purposes.

For assistance: Access and Dissemination Bureau at 512-424-7364 or CJIS.Audit@dps.texas.gov