OFFICE OF THE DIRECTOR OF POLICE
THE UNIVERSITY OF TEXAS SYSTEM
POLICY AND PROCEDURE MANUAL

Subject			Policy Number
Criminal History Record Information (CHRI): Proper Access, Use and Dissemination Procedures			**501**
Effective Date June 12, 2020	Revision Date	Reevaluation Date Annually	Number of Pages
Reference Standards Title 28, Part 20, Code of Federal Regulations (CFR) Texas Government Code 411.081-411.085 CALEA: 81.2.8			

I. PURPOSE

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

The scope of this policy applies to any electronic or physical media containing FBI CJI while being stored, accessed or physically moved from a secure location from within a University of Texas System Police facility. In addition, this policy applies to any authorized person who accesses, stores, and/or transports electronic or physical media.

The following policy was developed based on the FBI's Criminal Justice Information Services (CJIS) Security Policy. The standards included within this policy shall be considered the minimum required for information protection purposes.

II. DEFINITIONS

A. Texas Commission on Law Enforcement (TCOLE)- Regulatory state agency that issues, maintains, regulates all licensed Texas telecommunicators, jailers, police cadets, and police officers.

B. Criminal Justice Information (CJI)- CJI is the term used to refer to all of the FBI CJIS provided data necessary for law enforcement and civil-service agencies to perform their missions including, but not limited to biometric, identity history, biographic, property, and case/incident history data.

C. Criminal History Record Information (CHRI)- CHRI, is a subset of CJI and for the purposes of this document is considered interchangeable/synonymous. 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, Title 28, Part 20, Code of Federal Regulations (CFR), defines CHRI and provides the regulatory guidance for dissemination of CHRI.

D. Texas DPS Secure Site FACT Clearinghouse- A secure site maintained by the Texas Department of Public Safety that requires secure log-in to access a database of secure fingerprint based criminal history records.

III. POLICY

A. 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 criminal justice authorized purposes only. An authorized purpose includes but is not limited to the following: driver's license returns, criminal history returns, and equivalent inquiries. Further, CHRI shall only be used for an authorized purpose consistent with the purpose for which III was accessed. Dissemination to another agency is authorized if (a) the other agency is an Authorized Recipient of such information and is being serviced by the accessing agency, or (b) the other agency is performing noncriminal justice administrative functions on behalf of the authorized recipient and the outsourcing of said functions has been approved by appropriate CJIS Systems Agency (CSA) or State Identification Bureau (SIB) officials with applicable agreements in place.

B. Personnel Security Screening and Account Management
Access to CJI and/or CHRI is restricted to authorized personnel. Authorized personnel are defined as an individual, or group of individuals, who have been appropriately vetted through a national fingerprint-based record check and have been granted access to CJI data. The State of Texas and TCOLE require fingerprint-based background checks be completed for all personnel with access to CHRI. This includes personnel who will have direct access to CJI, those who have direct responsibility to configure and maintain computer systems and networks with direct access to CJI, and any persons with access to physically secure locations or controlled areas containing CJI.

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. The Office of Director of Police (ODOP) will require that each institution police department review active subscriptions each year in December. This will be a compliance check item for the biennial inspection of institution police departments conducted by ODOP.

All accounts shall be reviewed at least annually by the designated CJIS 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 Justice Information. The POC may also conduct periodic reviews.

C. Hiring licensed TCOLE Positions

1. A fingerprint-based background check will be conducted on all applicants who receive a conditional offer of employment using the Texas DPS Secure Site FACT Clearinghouse.
2. It shall be the policy of The University of Texas System Police to protect the integrity of the CHRI database and all data and information obtained through use of department computers by strictly following the procedures outlined in this order. Failure to comply with this policy can result in disciplinary action or termination.
3. Upon resignation or termination applicant names should be removed from the system within 72 hours.
4. The system should be validated annually for accuracy.

D. DPS Secure Site

1. Access to the Texas DPS Secure Site is limited to sworn peace officers who are assigned to the recruiting unit at each Institution. Users who are no longer part of the recruiting unit will have their access removed immediately. Authorized users are validated on an annual basis to ensure accuracy.
2. Authorized users of the Texas DPS Secure Site must complete the appropriate DPS training.
3. All employees with access to Criminal Justice Information must be fingerprinted and pass a fingerprint-based background check.
4. All employees with access are also required to complete Security Awareness Training within 6 months of being hired, and every 2 years thereafter.
5. No personal hardware (PC, laptop, etc) should be used for accessing the Texas DPS Secure Site.
6. A personally owned information system shall not be authorized to access, process, store or transmit CJI 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 including but not limited to camera, USB flash drives, USB thumb drives, DVDs, CDs, air cards and mobile wireless devices such as Androids, Blackberry OS, Apple iOS, Windows Mobile, Symbian, tablets, laptops or any personal desktop computer. When bring your own devices (BYOD) are authorized, the devices shall be controlled in accordance with the requirements in Section 5.13 of the CJIS Security Policy.
7. The University of Texas System Police shall authorize, monitor, and control all methods of remote access to the information systems that can access, process, transmit, and/or store FBI CJI. Remote access is any temporary access to an agency's information system by a user (or an information system) communicating temporarily through an external, non-agency controlled network (e.g., the Internet).

8. The University of Texas System Police shall employ automated mechanisms to facilitate the monitoring and control of remote access methods. The University of Texas System Police shall control all remote accesses through managed access control points. The University of Texas System Police 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.
9. Utilizing publicly accessible computers to access, process, store or transmit CJI 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.

E. Physical Building, Computer Access, Servers, and Equipment

A physically secure location is a facility or an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect the FBI CJI and associated information systems. The perimeter of the physically secure location shall be prominently posted and separated from non-secure locations by physical controls.

1. Only authorized personnel will have access to physically secure non-public locations. The University of Texas System Police (Office of Director of Police) and each institution police department will maintain and keep current a list of authorized personnel, respectively.
2. All physical access points into the agency's secure areas will be authorized before granting access. The agency will implement access controls and monitoring of physically secure areas for protecting all transmission and display mediums of CJI. Authorized personnel will take necessary steps to prevent and protect the agency from physical, logical and electronic breaches.
3. Individual computers must have a "time-out" where the computer locks independently within 30 minutes of inactivity.
4. Individual offices are locked when not in use.
5. The local network equipment shall be in a physically secure location.
6. All computers used for processing CHRI data shall have anti-virus software installed in addition to having the most recent updates for the operating system and a firewall enabled.
7. All storage media containing or used for CHRI data that is no longer used shall be secure-formatted using methodology that over-writes all data in three iterations or degaussed prior to disposal or release for reuse by unauthorized personnel; if no longer needed media will be destroyed. Inoperable electronic media shall be physically destroyed. Sanitation or destruction will be carried out by authorized personnel only.

F. CHRI Data

1. CHRI data shall be accessed ONLY from secure locations. A secure location is defined as the areas of The University of Texas System Police that are not open to the public and are accessible only by authorized personnel.

2. All CHRI printouts shall be promptly filed with the corresponding application packet. Packets should be kept in a secure file drawer when not in use. CHRI printouts that are no longer needed should be immediately shredded or incinerated. Disposal or destruction will be carried out by authorized personnel only.

G. Media Protection

1. Controls shall be in place to protect electronic and physical media containing CJI 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 CJI.
2. 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.

H. Media Transport

1. Controls shall be in place to protect electronic and physical media containing CJI while in transport (physically moved from one location to another) to prevent inadvertent or inappropriate disclosure and use. The agency shall protect and control electronic and physical media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel.

I. Media Sanitization and Disposal

1. When no longer usable, hard drives, diskettes, tape cartridges, CDs, ribbons, hard copies, print-outs, and other similar items used to process, store and/or transmit FBI CJI shall be properly disposed of in accordance with measures established by the University of Texas System Police.
2. Physical media (print-outs and other physical media) shall be disposed of by authorized personnel by shredding using University of Texas System Police issued shredders.
3. Electronic media (hard-drives, tape cartridge, CDs, printer ribbons, flash drives, printer and copier, etc.) shall be disposed of by one of the University of Texas System Police methods:
   a) Overwriting (at least 3 times)- an effective method of clearing data from magnetic media. As the name implies, overwriting uses a program to write (1s, 0s, or a combination of both) onto the location of the media where the file to be sanitized is located.
   b) Degaussing- a method to magnetically erase data from magnetic media. Two types of degaussing exist: strong magnets and electric degausses. Note that common magnets (e.g., those used to hang a picture on a wall) are fairly weak and cannot effectively degauss magnetic media.

c) Destruction- a method of destroying magnetic media. As the name implies, destruction of magnetic media is to physically dismantle by methods of crushing, disassembling, etc., ensuring that the platters have been physically destroyed so that no data can be pulled.

4. IT systems that have been used to process, store, or transmit FBI CJI and/or sensitive and classified information shall not be released from University of Texas System Police's control until the equipment has been sanitized and all stored information has been cleared using one of the above methods.

J. Data Breach, Unauthorized Use, or Policy Violations

1. If the agency discovers that they had a data breach, unauthorized use or policy violation, the agency shall promptly report the incident to the CJIS State Agency, The Department of Public Safety.
2. It shall be the responsibility of each authorized user to report any violations of this security policy up the chain-of-command and complete the Agency Incident Reporting Form. Attached is the Agency Incident Reporting form.
3. Information security events and weaknesses associated with information systems 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 event 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.
4. Violation of any of the requirements contained in the 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.
5. Likewise, violation of any of the requirements contained in the 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.

Michael J. Heidingsfield
Director of Police