Overview

The National Crime Prevention and Privacy Compact (Compact) establishes standards and processes for exchanging criminal history records among states and between states and the Federal Bureau of Investigation (FBI) for non-criminal justice purposes such as licensing or employment. Article VI of the Compact provides for a Compact Council with the authority to establish rules and procedures that control use of the Interstate Identification Index (III) system for non-criminal justice purposes. The III is the system of federal and state criminal history records maintained by the FBI.

The provisions of the Security and Management Control Outsourcing Standard (Outsourcing Standard) are established by the Compact Council pursuant to Title 28 Code of Federal Regulations 906 and are subject to the scope of that rule. They apply to all personnel, systems, networks, and facilities supporting and/or acting on behalf of the non-criminal justice agency to perform non-criminal justice administrative functions related to the processing of criminal history record information (CHRI), to include but not limited to:

a. Making fitness determinations/recommendations
b. Obtaining missing dispositions
c. Disseminating CHRI as authorized by Federal statute, Federal Executive Order, or State statute approved by the United States Attorney General
d. Other authorized activities relating to the general handling, use and storage of CHRI

The intent of the Outsourcing Standard is to provide non-criminal justice agencies with information on the required procedures, responsibilities and controls to maintain adequate security and integrity of CHRI while under the control or management of an outsourced, third party contractor (Contractor). The Outsourcing Standard requires the Contractor to maintain a security program consistent with federal and state laws, regulations, and standards, to include the FBI Criminal Justice Information Services (CJIS) Security Policy, as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.

Requirements *

Texas governmental and non-governmental agencies authorized by federal statute, federal executive order, or approved Public Law 92-544 statute, hereafter referred to as Authorized Recipient (AR), may utilize the Outsourcing Standard.

Prior to engaging in outsourcing of any non-criminal justice administrative function, the AR shall request and receive written permission from the Texas Department of Public Safety (TX DPS). All requests must be mailed to:

Attention: ADB Manager
DPS Crime Records
Austin, Texas
P.O. Box 4143
Austin, TX 78765-4143

The request must include the specific authority for the outsourced work, criminal history record check requirements, and/or a copy of relevant portion of the contract as requested. The contract shall, at a minimum, incorporate by reference the Outsourcing Standard. The contract must specify the terms and condition of access to CHRI; limit the use of such information to the purpose for which it is provided; limit retention to a period of time not to exceed that period of time the AR is permitted to retain such

information; prohibit dissemination except as specifically authorized; ensure the security and confidentiality of the information; provide for audits and sanctions; provide conditions for termination of the contract; and ensure Contractor personnel comply with the Outsourcing Standard.

The Authorized Recipient shall:

1. Execute a contract or agreement prior to providing a Contractor access to CHRI.
2. Conduct national fingerprint-based background checks of Contractor personnel having access to CHRI, if such checks are required of the AR's personnel.
3. Maintain updated records of Contractor personnel with access to CHRI (update within 24 hrs. of changes to access).
4. Maintain a list of Contractor personnel that completed the aforementioned background check.
5. Ensure the Contractor maintains site security per CJIS Security Policy guidelines.
6. Notify the Contractor within 60 calendar days of changes or updates to the Outsourcing Standard and/or the CJIS Security Policy.
7. Ensure the current version of the Outsourcing Standard and the CJIS Security Policy are incorporated by reference at the time of contract, contract renewal, or within the 60 calendar notification period.
8. Make available the relevant portions of the current and approved contract relating to CHRI to TX DPS and FBI Compact Officer, upon request.
9. Approve the contractor network topology if related to outsource functions, and any future modifications to the network configuration.
10. Monitor the actions of the Contractor for compliance with the Outsourcing Standard and CJIS Security Policy.
11. Conduct an audit within 90 days of the date the Contractor first receives CHRI and certify to TX DPS that the audit was conducted. The Authorized Recipient shall certify to the State Compact Officer that the audit was conducted.
12. Provide written notice to TX DPS if any early voluntary termination of the contract.
13. Appoint an Information Security Officer who shall document technical compliance with this Outsourcing Standard.
14. Establish a security incident response policy and reporting procedure for the security of CHRI.
15. Immediately (within one hour) notify TXDPS of any PII breach.
16. Provide a written report, including corrective action of any PII breach within five calendar days to TXDPS.
17. Approve the Contractor Security Program and provide written approval to TX DPS.
18. Ensure Contractor personnel receive Security Awareness Training prior to their appointment/assignment and provide annual refresher training annually, not later than the anniversary date of the contract.
19. Ensure the Contractor site(s) is a physically secure location.
20. Within four hours, notify TX DPS and the FBI Compact Officer of any security violation or termination of the contract.
21. Within five calendar days of receipt of the written report from the Contractor, provide a written report to TX DPS to include any corrective actions taken.

The Contractor shall:

1. Comply with the Outsourcing Standard, CJIS Security Policy and all federal and state laws regarding access to CHRI.
2. Develop and document a Security Program (physical, personnel, and information technology) to comply with the Outsourcing Standard and the CJIS Security Policy.
3. Ensure that the Security Program includes the description of the implementation of the security requirements described in the Outsourcing Standard and the CJIS Security Policy; Security Training; a written security violation plan; a process for reporting security violations.
4. Develop and maintain a written policy for discipline of personnel that violate the security provision of the contract.

5. Responsible to set, maintain, and enforce the standards for the selection, supervision, and separation of personnel with access to CHRI.
6. Make facilities available for announced and unannounced audits performed by the AR, TX DPS, or the FBI on behalf of the Compact Council.
7. Security Program is subject to review by the AR, TX DPS, and the FBI CJIS Division.
8. Maintain CHRI only for the period of time necessary to fulfill its contractual obligations but not to exceed the period of time that the AR is authorized to maintain and does maintain CHRI.
9. Maintain a log of any dissemination of CHRI for a minimum of 365 days.
10. Protect CHRI stored in an electronic format against unauthorized access.
11. Ensure personnel performing work under the contract are aware of the Outsourcing Standard requirements and the laws governing the security and integrity of CHRI.
12. Confirm in writing that personnel has certified in writing, prior to CHRI access, that he/she understands the Outsourcing Standard and laws that apply to his/her responsibilities.
13. Maintain certification in a file that is subject to review during audits.
14. Maintain records of personnel with access to CHRI and update records within 24 hours of changes.
15. Maintain a list of Contractor personnel that completed the aforementioned background check, if required.
16. Notify the AR within 24 hours when additions or deletions occur to the personnel list.
17. Ensure the security system complies with the CJIS Security Policy.
18. Provide secure storage and disposal of all hard copy and media associated with the system to prevent access by unauthorized personnel.
19. Assign a unique identifying number to personnel with access to CHRI to detect unauthorized access.
20. Suspend any personnel that commits a security violation upon detection or awareness, pending investigation.
21. Within one hour of discovery, notify the AR of any security violation or termination of the contract.
22. Within five calendar days, provide the AR a written report documenting the violation, corrective action, date, time, and summary of the prior notification.
23. Protect all PII in the possession and control when handling, using or storing CHRI.
24. Notify authorized individuals of their right to report PII breaches directly to the FBI.
25. Immediately (within one hour of discovery) notify the AR and TXDPS of any PII breach or potential PII breach.
26. Within five calendar days provide the AR and TXDPS a written report of such violations and corrections taken.

Exemption from Above Provisions

An Information Technology (IT) contract example

If the following exist:

1. Access to CHRI by the IT contractor is limited solely for the development and /or maintenance of the AR's computer system.
2. Access to CHRI is incidental, but necessary, to the duties being performed by the IT contractor.
3. The computer system is located within the AR's facility.
4. The AR's personnel supervise or work directly with the IT contractor.
5. The AR maintains complete control of the IT contractor's access to the computer system and CHRI contained within.
6. AR retains all duties/responsibilities for the performance of authorized noncriminal justice administrative functions, unless a separate contract is executed to perform noncriminal justice administrative functions within the Outsourcing Standards.

The following sections must be included in the contract:

The Authorized Recipient shall:

1. Request and receive written permission from TX DPS to include the specific authority for outsourced work.
2. Execute a contract with Contractor before access to CHRI is granted to perform required outsource duties and at a minimum, incorporate by reference and have appended thereto this Outsourcing Standard.
3. Conduct national fingerprint-based background checks of Contractor personnel having access to CHRI, if such checks are required of the AR's personnel and /or a copy of the relevant portion of the contract as requested.
4. Maintain updated records of Contractor personnel with access to CHRI (update within 24 hrs. of changes to access).
5. Maintain a list of Contractor personnel that completed the aforementioned background check.
6. Ensure the Contractor maintains site security per CJIS Security Policy guidelines.
7. Notify the Contractor within 60 calendar days of changes or updates to the Outsourcing Standard and/or the CJIS Security Policy.
8. Ensure the current version of the Outsourcing Standard and the CJIS Security Policy are incorporated by reference at the time of contract, contract renewal, or within the 60 calendar notification period.
9. Develop and maintain a written policy for discipline of contractor employees who violate the security provisions of the contract which includes this Outsourcing Standard by reference.
10. Develop and maintain a written incident reporting plan for security events, to include violations and incidents.
11. Within four hours, notify TX DPS and the FBI Compact Officer of any security violation or termination of the contract.
12. Within five calendar days of receipt of the written report from the Contractor, provide a written report to TX DPS to include any corrective actions taken.
13. Written notice to TXDPS shall include the following:
    a. Termination of contract for security violations.
    b. Security violations involving the unauthorized access to CHRI.
    c. The contractor name and the unique identification number, the nature of the security violation. Intentional or unintentional and number of times violation occurred.

The Contractor shall:

1. Comply with the Outsourcing Standard, CJIS Security Policy and all federal and state laws regarding access to CHRI.
2. Ensure personnel performing work under the contract are aware of the Outsourcing Standard requirements and the laws governing the security and integrity of CHRI.
3. Confirm in writing that personnel has certified in writing, prior to CHRI access, that he/she understands the Outsourcing Standard and laws that apply to his/her responsibilities.
4. Maintain certification in a file that is subject to review during audits.
5. Maintain records of personnel with access to CHRI and update records within 24 hours of changes.
6. Maintain a list of Contractor personnel that completed the aforementioned background check, if required.
7. Notify the AR within 24 hours when additions or deletions occur to the personnel list.
8. Immediately (within one hour of discovery) notify the AR and TXDPS of any security violations to include unauthorized access to CHRI.
9. Within five calendar days provide the AR and TXDPS a written report.
10. Written notice to TXDPS shall include the following:
    a. Termination of contract for security violations.
    b. Security violations involving the unauthorized access to CHRI.
    c. The contractor name and the unique identification number, the nature of the security violation. Intentional or unintentional and number of times violation occurred.
11. Protect all PII when handling, using or storing CHRI.
12. Notify authorized individuals of their rights to report PII breaches directly to the FBI, should they believe their information has been mishandled or compromised.
13. Immediately (within one hour of discovery) notify the AR and TXDPS of any PII breach or potential breach.
14. Within five calendar days provide the AR and TXDPS a written report documenting such violation and corrective action taken to resolve such violation including time, date and a summary.

*The terms presented in this document provides a minimum basis for the security of the system and CHRI access. This Outsourcing Standard only grants or authorizes rights to the Contractor, the AR, and the FBI. In addition, only the Compact Council can modify the Outsourcing Standards. The CJIS Security Policy is integrated by reference and made part of the Outsourcing Standard.

Refer to the Security and Management Control Outsourcing Standard for Non-Channelers for additional information.

https://www.fbi.gov/file-repository/compact-council-security-and-management-control-outsourcing-standard-for-non-channelers.pdf/view

For any questions or additional information please contact:
Texas Department of Public Safety
Access and Dissemination Bureau
Audit and Training Unit
512-424-7364 or
CJIS.Audit@dps.texas.gov