CJIS Vendor Agreement

1. Purpose:

The intent of this agreement and the policies and procedures herein is to facilitate compliance in Colorado with FBI-CJIS policy. The Colorado Bureau of Investigation (CBI), as the CJIS Systems Agency (CSA) for the state of Colorado, agrees to provide supporting services to private and public entities contracted by any Colorado Contracting Government Agency (CGA). To ensure vendor personnel undergo a fingerprint-based background check and to ensure audits of CJIS systems are accurate and consistent, the CBI will provide the policies and systems to allow background check results for a vendor employee to be accessible to CGA's and to allow audit findings from Shared CJIS Systems to be accessible to CGA's.

2. Policy:

As CSA, the CBI maintains and operates the CCIC computer system under shared management pursuant to the CCIC and NCIC User Agreements. As part of these agreements, the CBI establishes and enforces policies ensuring compliance with the FBI CJIS Security Policy. Section 5 of the CJIS Security Policy mandates background checks and audits are performed within each state under the authority of the CSA. The services defined in this document are intended to improve statewide compliance with the CJIS security policy.

Definitions:

Access (to Criminal Justice Information) — The physical or logical (electronic) ability, right, or privilege to view, modify, or make use of CJI.

Board of Executive Directors (BED) – The Executive Board within the CCIC Advisory Board consisting of Chiefs, Sheriffs, and other selected CJA Chief Executives.

CJIS Security Policy — The FBI CJIS Security Policy document as published by the FBI CJIS ISO.

CJIS Systems Agency Information Security Officer (CSA ISO) — The appointed FBI CJIS Division personnel responsible to coordinate information security efforts at all CJIS interface agencies.

CJIS Systems Agency (CSA) — A duly authorized state, federal, international, tribal, or territorial criminal justice agency on the CJIS network providing statewide (or equivalent) service to its criminal justice users with respect to the CJI from various systems managed by the FBI CJIS Division.

Contracting Government Agency (CGA) — The government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private vendor.

Criminal Justice Information (CJI) — Criminal Justice Information is the abstract term used to refer to all of the FBI CJIS provided data necessary for law enforcement agencies to perform their mission and enforce the laws, including but not limited to: biometric, identity history, person, organization, property (when accompanied by any personally identifiable information), and case/incident history data. In addition, CJI refers to the FBI CJIS-provided data necessary for civil agencies to perform their mission; including, but not limited to data used to make hiring decisions. The following type of data are exempt from the protection levels required for CJI: transaction control type numbers (e.g. ORI, NIC, FNU, etc.) when not accompanied by information that reveals CJI or PII.

Criminal Justice Information Services Division (FBI CJIS or CJIS) — The FBI division responsible for the collection, warehousing, and timely dissemination of relevant CJI to the FBI and to qualified law enforcement, criminal justice, civilian, academic, employment, and licensing agencies.

Direct Access — Defined in the CJIS security policy as: (1) Having the authority to access systems managed by the FBI CJIS Division, whether by manual or automated methods, not requiring the assistance of, or intervention by, any other party or agency. (2) Having the authority to query or update national databases maintained by the FBI CJIS Division including national queries and updates automatically or manually generated by the CSA.

Indirect Access – Defined in the CJIS security policy as: Having the authority to access systems containing CJI without providing the user the ability to conduct transactional activities (the capability to query or update) on state and national systems (e.g. CJIS Systems Agency (CSA), State Identification Bureau (SIB), or national repositories).

Personally Identifiable Information (PII) – PII is information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name.

Shared CJIS System – An outsourced, individual computer system which contains CJI, and which provides access/service to multiple CGA's. Examples include cloud storage systems and regionalized Computer-Aided Dispatch (CAD) systems.

Subcontractor – a business or person that carries functions in support of or proximity to CJIS data, that is contracted by a vendor (see below).

Vendor – A private contractor, with a current and active contract to provide services to a criminal justice agency which require, or in performance of work provide, access to CJI.

Vendor Administrator — The person designated at the vendor organization who is the CBI's primary point of contact for employee approvals, denials, and subsequent arrests, as well as vendor audits.

3. CBI CJIS Systems Agency (CSA) Responsibility:

The CBI serves as the Colorado CJIS Systems Agency (CSA). As such, the CBI will provide connectivity to CCIC, NCIC, and Nlets and provide operational support. Additionally, CJIS Vendors will be provided with services to reduce the cost and burden of CJIS compliance to the vendor and CGA's alike. These consolidated services will allow CJIS Vendors to undergo these processes once for the state, instead of once for each CGA within the state and include:

3.1. Fingerprint-Based Background Check

The CBI shall ensure fingerprints submitted for background checks mandated by the CJIS Security Policy, section 5.12.1.2, are processed and results are available to CGA's. This will ensure each vendor employee may submit one set of fingerprints to one CGA and support all of the vendor's CGA's.

3.1.1. CGA Background Checks

The CGA may elect to perform their own background check on a vendor employee, even where the vendor has completed a fingerprint based background check elsewhere within Colorado.

3.2. Audit

Every three years, the CBI will conduct audits of each criminal justice agency. As part of those audits, the CBI reviews services and systems provided by vendors to CGA's. Many CGA's use shared CJIS systems in order to improve information sharing or to reduce support costs. The CBI reserves the authority to determine whether shared CJIS systems are audited separately for each CGA, or once for all CGA consumers of the service. Consolidated findings of policy violations by the vendor shall be reflected in the audits of the CJIS Vendor's supported CGA's. Additionally, the FBI audit staff will conduct audits at least once every three years. This audit shall include a sample of state and local criminal justice agencies.

3.2.1. External Audits – In Lieu of CBI Audit

The CBI may accept audits provided by external entities in lieu of performing a separate audit.

3.2.2. Sanctions for Violations

The CBI may sanction CGA's and vendors for failure to meet the standards of the policies referenced in this document. Sanctioned agencies shall work collaboratively with their respective vendors to develop and report mitigation plans and timelines to achieve compliance. The CBI will implement sanctions under advisement of the BED and reserves the right revoke vendor and CGA access for failure to accomplish CJIS compliance.

3.2.3. Confidentiality

The CBI will share vendor audit findings with CGA's. Requests for detailed information which may comprise trade secrets, security vulnerabilities, or other types of information determined to be sensitive by the CBI discovered or revealed through CJIS security processes will not be shared with the CGA. The CGA will be referred directly to the CJIS Vendor for access to any information not provided by the CBI.

4. Vendor Responsibility:

The CJIS Vendor shall comply with all applicable standards of the CJIS security policy. These standards may apply differently to different CJIS Vendors depending on the services provided. The Vendor shall work proactively with their CGA(s) to ensure responsibility of contract parties related to CJIS compliance are appropriately assigned and maintained.

Each Vendor shall appoint a Vendor Administrator. The Vendor Administrator oversees compliance with CJIS systems, CCIC, and Nlets policies. See section 5 of this agreement for the full scope of Vendor Administrator responsibilities.

4.1. Incorporated Standards

Vendors with direct access or indirect access to CJI shall handle all CJI following the requirements of the laws and policies listed below and incorporated into this agreement:

- CJIS Security Policy
- Title 28, Code of Federal Regulations, Part 20 (relevant standards)

Vendors supporting systems which provide direct access to CJI shall also follow the regulations listed in the laws, polices, and manuals incorporated into this agreement:

- NCIC Operating Manual
- CCIC Training Manual
- Interstate Identification Index / National Fingerprint File Operational and Technical Manual
- Title 28, Code of Federal Regulations, Part 23

4.2. Enrollment

To apply for participation in the CBI CJIS Vendor Management Program, the vendor shall submit a Vendor Onboarding Packet to the CBI, to include:

- The signature page of this agreement, signed and completed by the Vendor CEO (or designee) and Vendor Administrator;
- Fingerprint Account Application Form;
- W-9 Request for Taxpayer Identification Number and Certification form (if requesting an account that is invoiced monthly; see Account Application Form for details);
- Current contract with a Colorado criminal justice agency.
    i. Pursuant to the CJIS Security Policy, private contractors (vendors) designated to perform criminal justice functions for a CJA shall be eligible for access to CJI; however, in order to submit fingerprints and to receive CJI, there must be a contract between the vendor company and a criminal justice agency. For participation in the CBI CJIS Vendor Management Program, a contract must exist between the vendor and at least one Colorado criminal justice agency. A

minimum of one contract must be submitted with the Vendor Onboarding Packet before the vendor is approved for the program.

ii. Subcontractors shall submit two contracts: one between the vendor and the subcontractor, and one between the vendor and the CGA(s).

4.3. Fingerprinting

The Vendor shall ensure fingerprints are submitted for background checks of each Vendor employee working with CJI, to include the Vendor Administrator. The Vendor is responsible for all fees associated with fingerprint processing and CJIS rap-back services where available.

4.4. Audit Responsibilities

Audit information requested by CBI or FBI auditing purposes is to be provided in a complete and timely manner. Audits may be conducted onsite, over the phone, or via online questionnaire at the CBI's discretion.

4.5. Access to CJIS Information – Security Awareness Training

Vendor staff members shall be trained in information security awareness pursuant to the CJIS security policy within six months of assignment and shall recertify biennially thereafter.

4.6. Other Agreements

Each CJIS Vendor may have one or more contracts with CGAs. Pursuant to the CJIS Security Policy, the CJIS security addendum shall be incorporated in all such contracts. Due to the diverse nature of CJIS Vendor businesses, the CBI may elect to sign a secondary agreement to supplement this agreement. Any secondary agreement shall be available for CGA and FBI review.

5. Vendor Administrator Responsibility:

The Vendor Administrator unifies responsibility for individual user discipline and serves as the primary CBI point of contact for handling all matters concerning the use and misuse of CJIS systems. The Vendor Administrator is the primary point of contact during CBI audits. Individual duties of the Vendor Administrator may be delegated to a designee where the designee has specialized authority or knowledge.

The Vendor Administrator will receive all communication from the CBI regarding the authorization status of vendor personnel, for example, whether the applicant has a criminal history. Because confirmation of a criminal history's existence is considered criminal justice information, the Vendor Administrator must also submit fingerprints for a background check and complete routine Security Awareness training. Fingerprints must be submitted, processed, and approved before the Vendor Administrator can receive any details regarding the authorization status of vendor personnel.

If the vendor chooses to deliver required Security Awareness training through CJIS Online (www.cjisonline.com), it is the responsibility of the Vendor Administrator to create user profiles for each participating vendor employee, and monitor these employees' certification status within CJIS Online. A comprehensive guide to employee management within CJIS Online will be provided to the Vendor Administrator during onboarding to the Vendor Management Program. If the vendor chooses not to use

CJIS Online for delivery and tracking of Security Awareness training, an alternative program may be used with curriculum and reporting that meets CJIS standards and has been approved by the CBI.

Pursuant to section 5.12.2 of the CJIS Security Policy, the Vendor Administrator shall notify the CBI immediately at cdps.cbi.cjisvendors@state.co.us if a participating employee has left the company or has been reassigned to a position where CJI will not be accessed.

When a new Vendor Administrator is designated, the vendor will notify the CBI Crime Information Management Unit in writing of that appointment within ten days of the appointment. The notification must include a revised CJIS Vendor Agreement and Account Application Form to reflect the new Vendor Administrator's information.

5.1. Contracting Government Agency

This agreement remains separate of all contracts between the CJIS Vendor and CGAs. Issues which may arise between the vendor and the CGA shall be resolved between the contract parties.

Pursuant to their CCIC User agreements, CGAs are responsible for determining how they can use the vendor's services in a manner compliant with the CJIS Policy. CGAs' compliance with the CJIS Policy will be dependent, in part, upon CGAs' individual use of contracted services.

End of Agreement

CBI CJIS SYSTEMS VENDOR AGREEMENT ACKNOWLEDGMENT

As a CJIS Vendor supporting CJIS systems within the state of Colorado, we hereby acknowledge the responsibilities as set out in this document as well as those documents incorporated by reference. The Vendor also agrees to comply with all state and federal statutes and regulations as may apply, and to use the information received over CJIS systems for criminal justice purposes only.

We acknowledge these responsibilities have been developed and approved by the CBI and/or the FBI in order to ensure the security, reliability, confidentiality, completeness, and accuracy of all records contained in or obtained by means of CJIS systems.

We acknowledge a failure to comply with these responsibilities will subject the CBI, CGA and this Vendor to various sanctions as recommended by the NCIC Advisory Policy Board, the BED, and/or the respective Directors of the CBI and/or the FBI.

To preserve the integrity of CCIC, the CBI reserves the right to suspend service to the CGA, Vendor, connected system, or an individual system user when the security or dissemination requirements are violated. The CBI may reinstate service upon receipt of satisfactory assurance that violation(s) have been corrected. Either the CBI or the vendor may discontinue service upon thirty days' advance written notice.

This agreement remains separate from all contracts between the CJIS Vendor and CGAs. Issues which may arise between the Vendor and the CGA shall be resolved between the contract parties.

IN WITNESS WHEREOF, the parties hereto caused this agreement to be executed by the proper officers and officials. This agreement will become effective upon the date signed.

Business Name	
Address:	

Vendor CEO or Designee	Title and Printed Name	Date
Vendor Administrator	Title and Printed Name	Date
CBI Director/Designee	Title and Printed Name	Date

Once signed, return this page to:

MAIL
CBI CJIS Vendor Management Program
690 Kipling Street, Suite 4000
Denver, CO 80215

FAX
(303) 239-5858

EMAIL
cdps.cbi.cjisvendors@state.co.us