Louisiana State Police CJIS Vendor Agreement

1. Purpose

This agreement intends to facilitate compliance with the Criminal Justice Information Services (CJIS) Security Policy (CJISSECPOL) and the requirements established by the Louisiana State Police (LSP) for vendors providing services to Criminal Justice Agencies (CJAs) in Louisiana. The Louisiana State Police is designated as the CJIS Systems Agency (CSA) for Louisiana, and as such is responsible for ensuring all entities, public or private, protect Criminal Justice Information (CJI) accordingly. By executing this agreement with the LSP, the vendor is electing to participate in the LSP's Centralized Vendor Vetting Program (CVVP) and comply with the requirements set by the CJISSECPOL and the state of Louisiana. The CVVP will assess the technical compliance of the vendor's proposed product and/or service. Additionally, all vendor personnel supporting the contract will be screened for suitability in accordance with the CJIS Security Policy.

CVVP Approved Vendors will be required to maintain compliance with technical and personnel requirements established in this agreement. The LSP will review approved vendor's offerings and personnel annually and reassess on a triennial basis.

This agreement is independent from all contracts between the vendor and client CJAs. Execution of this agreement does not constitute purchase, or intent of purchase, of any vendor offering by the state of Louisiana or the Louisiana State Police.

2. Policy

As CSA, the Louisiana State Police administers, operates, and maintains the Louisiana Law Enforcement Telecommunication System (LLETS) pursuant to both Louisiana Statutes and the LLETS and National Crime Information Center (NCIC) User Agreements. Additionally, the LSP enforces the requirements of the CJISSECPOL to ensure compliance from protecting CJI, including, but not limited to, personnel security and formal audits. Formal audits may include but are not limited to, examination and verification of policies, procedures, protocols, processes, rules, forms, records, physical environment, storage, and systems associated with CJI.

2.1 Definitions:

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

CJIS Security Policy (CJISSECPOL) — The CJISSECPOL contains information security requirements, guidelines, and agreements reflecting the will of law enforcement and criminal justice agencies for protecting the sources, transmission, storage, and generation of Criminal Justice Information (CJI). The CJISSECPOL integrates presidential directives, federal laws, FBI directives and the criminal justice community's APB decisions along with nationally recognized guidance from the National Institute of Standards and Technology.

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. the LSP is the CSA for Louisiana

Criminal Justice Agency (CJA) — The courts, a governmental agency, or any subunit of a governmental agency which performs the administration of criminal justice pursuant to a statute or executive order and which allocates a substantial part of its annual budget to the administration of criminal justice. State and Federal Inspectors General Offices are included.

Criminal Justice Information (CJI) — Criminal Justice Information is the abstract term used to refer to all of the FBI and the LSP CJIS provided data necessary for criminal justice 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.

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 — (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.

Escorted Access – When a vendor employee must be accompanied by a CJA employee while in secured areas where CJI may be reasonably or physically present.

Indirect Access – 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).

Security Incident - Any event that compromises or could compromise the confidentiality, integrity, or availability of an organization's information or information systems.

Shared CJIS System – An outsourced, individual computer system which contains CJI, and which provides access/service to multiple CJAs. 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 CJI, that is contracted by a vendor (see below).

Unescorted Access – When a vendor employee is allowed access to secured areas where CJI may be reasonably or physically present without being accompanied by a CJA employee.

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

Vendor Administrator — The person designated at the vendor organization who is the vendor's primary point of contact to the LSP. The Vendor Administrator is; responsible for ensuring vendor employee screening information is provided to the LSP in a timely manner; is the vendor contact for vendor employee matters (e.g. approvals, denials, subsequent arrest notifications); is responsible for security matters; and is responsible for any required vendor audits.

2.2 Incorporated Standards

The following documents and regulations are hereby incorporated into this Agreement for all Vendors with access to CJI:

- CJISSECPOL, including the requirements specified under the CJIS Security Addendum
- Title 28, Code of Federal Regulations, Part 20 (relevant standards).

The Vendor shall comply with these regulations and policy requirements, including all changes and updates, throughout the lifetime of the contract for the applications and services provided to Louisiana CJAs.

Additionally, the following documents are hereby incorporated into this Agreement for vendors with direct access to CJI:

- NCIC Operating Manual
- LLETS Operating Manual
- Interstate Identification Index / National Fingerprint File Operational and Technical Manual

Vendors with direct access to CJI shall comply with the requirements of this Agreement and all incorporated requirements of these documents related to applications and services provided to Louisiana CJAs.

Vendors providing services identified as Criminal Intelligence applications shall comply with Title 28, Code of Federal Regulations, Part 23.

3. Louisiana State Police Responsibilities

As the CSA for Louisiana, the LSP provides connectivity to state and national CJIS systems, and operational support for CJIS access. The LSP is responsible for ensuring CJIS compliance within Louisiana for public and private entities that perform and support the administration of criminal justice, including vendors. The LSP established and maintains the Centralized Vendor Vetting Program (CVVP) as a single source for Louisiana CJAs to fulfill initial vendor compliance requirements identified within the CJISSECPOL. The LSP allows 60-90 days for the vetting process.

The LSP provides access to CJIS Online to allow vendors and CJAs to track vendor employee security requirements. The LSP shall assign a CVVP account number to the vendor for vendor tracking throughout the approval and maintenance process. The LSP shall provide an executed copy of the LSP-CJIS Vendor Agreement Acknowledgment to the Vendor. Execution of this agreement is independent from receiving CVVP approval. Upon initial approval by the Vendor Review Committee, the LSP shall notify the Vendor Administrator and provide instructions for fingerprint submission.

3.1 Fingerprint-based Background Check

As required by the CJIS Security Policy, all employees with responsibilities for configuring systems and networks with direct access to CJI, as well as employees with physical and/or logical access to CJI, must undergo fingerprint-based background checks. This may include support personnel, such as, human resources staff, janitorial staff, and facility maintenance personnel.

The LSP shall receive, process, and adjudicate, vendor personnel fingerprints submitted in accordance with this agreement. CJA's shall have access to view the CVVP cleared and denied vendor personnel through CJIS Online. As per the CJISSECPOL, the LSP is the final approval authority for access to criminal justice information in Louisiana.

LSP will provide personnel approval letters to the Vendor Administrator for vendor employees that have successfully completed all aspects of the CVVP personnel vetting. Successful completion includes passing the fingerprint-based background check, completion of CJIS Security Awareness and Cyber-Security training, and execution of the CJIS Security Addendum. All personnel are subjected to a fingerprint-based background check every five years to remain in compliance.

3.1.1 Additional Fingerprint-Based Background Checks

Louisiana CJAs may elect to perform a separate fingerprint-based check on vendor personnel, in addition to, or in place of the review completed by the LSP under this agreement. The CJA may review additional records beyond fingerprint check results.

3.2 Audits

The LSP shall conduct an online technical audit-questionnaire of the vendor's CJIS related applications and/or services prior to granting Vendor Approval. As the delivery of services by the vendor may vary by client, the LSP

reserves the authority to determine whether shared vendor CJI systems are audited overall, inclusive of the vendor and all of its contracted CJAs, or separately, auditing the vendor and each CJA individually. The LSP shall provide the vendor with a list of non-compliant issues and suggested corrective actions based on the findings of the initial audit. Upon satisfaction of the Louisiana CJIS Information Security Officer (ISO), the LSP shall notify the Vendor Administrator of technical approval.

The LSP shall conduct an annual compliance check-in to determine if the approved technical configuration or the vendor's personnel list have changed. If the technical configuration of the vendor's offering has changed, the LSP shall initiate a full online technical audit-questionnaire. The LSP shall conduct an online technical audit-questionnaire of the vendor's offering on a triennial basis. The triennial vendor audit will be scheduled based on the most recent full vendor technical audit.

3.2.1 External Audits - Lieu of an LSP Audit

As provided by the CJIS Security Policy, the LSP may accept CJIS audits conducted by a CSA from another state in lieu of performing an audit as required in section 3.2.

3.2.2 Sanctions for Noncompliance

Non-compliant vendors, as identified in the CVVP, and CJAs shall work collaboratively to develop and report to the LSP, mitigation plans and timelines to achieve compliance, prior to sanctions being issued. The LSP may sanction vendors and CJAs for failure to comply with the policies referenced in this document. The LSP reserves the right to revoke vendor and CJA access to criminal justice information for failure to comply with CJISSECPOL requirements and LLETS policies.

If an approved vendor is found to be non-compliant following an additional online audit-questionnaire, the vendor will be required to complete a Plan of Action and Milestones (POAM) form outline corrective action plans and dates of completion to correct findings. The LSP shall review the proposed POAM and determine timeframe approval. Upon POAM approval, the LSP shall follow up with the vendor administrator every six (6) months or based on the timeframes approved. During the vendor's next audit questionnaire, the LSP shall provide a letter to the vendor administrator identifying previous non-compliant findings. If the vendor is found to be non-compliant during their next audit-questionnaire, the vendor will be removed from the approval list and access to criminal justice information will be revoked.

3.2.3 Security Incidents

As provided by the CJIS Security Policy, the LSP reserves the right to revoke vendor and CJA access to criminal justice information for failure to comply with CJISSECPOL requirements and LLETS policies. In the case of any security incident, vendors with CJI access are required to notify the CVVP team immediately, but not to exceed 72 hours after discovery of the incident to the CJIS Systems Officer (CSO), CJIS Information Security Officer (ISO), and other entities as required by the CJISSECPOL IR-6. Upon notification, the vendor's access to CJI may be terminated and/or the vendor may be

removed from the CVVP approval list upon an internal investigation. The vendor shall be notified what requirements must be met to reinstate access and/or receive approval.

3.2.4 Removals

Vendors who request to be on a hold for any reason will receive a three month due date to resume the process. If this timeframe is not met, the LSP reserves the right to remove the vendor from the process and will provide formal notification to the vendor administrator and sponsoring agency. If a Vendor removes themselves from the CVVP, the Vendor Administrator must notify the LSP and provide the reasoning for removal.

Should the vendor wish to restart the process, submission of a new vendor agreement and sponsorship form will be required. In addition, all components of the audit process will need to be completed regardless of previous submissions.

3.2.5 Onsite Security Review

As provided by the CJIS Security Policy, the LSP reserves the right to conduct an on-site physical security review of the vendor's facilities housing CJI. In the case where an on-site physical review is required, LSP shall coordinate the scope, scheduling, and availability with the vendor administrator in advance. LSP will also communicate any requests for audit artifacts and supporting documentation prior to the on-site audit to the vendor administrator. If any non-compliant findings are found as a result of the onsite audit, LSP will coordinate with the vendor administrator for issue resolution.

4. CJIS Vendor Responsibilities

Completion of the Louisiana State Police Centralized Vendor Vetting Program (CVVP) is only available to vendors with clients in Louisiana.

CJIS vendors are those that offer applications or services in support of the administration of criminal justice as defined in 28 CFR part 20.3 (b). The vendor shall comply with all applicable statutes, policies, rules, and regulations governing access to criminal justice information (CJI). The vendor shall appoint a Vendor Administrator to act as a single point of contact with the LSP regarding the CVVP including, all matters relating to the establishment and maintenance of compliance with CJIS policies and this Agreement.

4.1 Enrollment

For the purposes of enrollment in the CVVP, the Vendor shall submit the following:

- The Louisiana State Police Vendor Sponsorship Form, signed by the Sponsoring CJA and the Vendor Administrator.
- This Agreement, completed and signed by the Vendor CEO (or designee) and the Vendor Administrator.

The Vendor Administrator shall identify all subcontractors included in or supporting the vendor's offering. If the identified subcontractor's work enables access to CJIS data, the subcontractor shall be required to enroll in the CVVP. The subcontractor's access to CJI shall be determined by the Louisiana CJIS ISO.

The LSP shall notify the Vendor Administrator upon receipt and acceptance of the enrollment documents and next steps in the CVVP.

4.2 Technical Approval

The vendor shall provide audit information and artifacts requested by the LSP in a complete and timely manner. The vendor may be asked to provide additional documentation or clarification on the initial audit responses. If non-compliant issues are identified, the vendor shall provide corrective action plans and dates of correction. A vendor will not be permitted to progress in the CVVP until all compliance issues have been corrected. Audits may be conducted onsite, remotely, or electronically at the LSP's discretion.

If the vendor identifies a subcontractor(s) to their offering, the vendor shall not proceed in the CVVP process until the identified subcontractor(s) have received approval for their technical audits.

4.3 Personnel Approval

Upon the completion and approval of the online technical audit-questionnaire, the LSP will provide the vendor administrator with instruction for completion of the CVVP personnel screening requirements. Each vendor employee with responsibilities for configuring systems and networks with direct access to CJI, as well as employees with physical and/or logical access to CJI, must complete personnel screening. CVVP Personnel Screening includes fingerprint-based background checks, completion of CJIS Security Awareness Training, completion of Louisiana Cyber-Security Training, and execution of the CJIS Security Addendum. The Vendor Administrator shall provide the LSP a list of vendor employees that will be required to complete the personnel screening process.

4.3.1 Fingerprint -Based Background Checks

The Vendor Administrator shall submit two sets of fingerprint cards for each vendor employee with access to CJI. The vendor is responsible for all applicable fingerprint processing fees. Detailed instructions for completing the fingerprint-based background check will be provided by the LSP at the appropriate time in the process. All personnel are subjected to a fingerprint-based background check every five years to remain in compliance.

4.3.2 CJIS Security Awareness Training

The Vendor Administrator shall ensure all vendor employees with access to CJI complete required CJIS security awareness training using CJIS Online, within six months of assignment. Vendor employee training certifications shall remain current for the duration of the employee's access to CJI while employed by the vendor.

4.3.3 Louisiana Cyber Security Training

The Vendor Administrator shall ensure all vendor employees with access to CJI complete Louisiana Cyber Security Training. The Louisiana Cyber Security Training covers topics such as cyber threats, vulnerabilities, risk management, incident response, and recovery. Access and instructions for completion will be provided by the LSP at the appropriate time in the CVVP process. Vendor employees shall be required to renew Cyber Security Training annually on the anniversary of CVVP vendor approval during the Annual Compliance Check In.

4.3.4 CJIS Security Addendum

Each contract between the vendor and a criminal justice agency for CJIS related services and applications shall incorporate the CJIS Security Addendum. The LSP reserves the right to require additional agreements to supplement the addendum. Any additional agreement shall be available for CJA and FBI review.

4.4 Vendor Administrator Responsibilities

The Vendor Administrator shall serve as the vendor's primary point of contact for CJIS compliance issues to the LSP. Vendor Administrator duties may be delegated to subject matter experts or designees within the vendor company.

4.4.1 The Vendor Administrator shall:

1. Ensure the required documentation is submitted to the LSP for enrollment
2. Ensure all Vendor employees with access to CJI are:
    a. Enrolled in CJIS Online
    b. Properly screened, i.e., fingerprints are submitted to the LSP
    c. Complete the CJIS Security Awareness Training
    d. Ensure all Vendor employees with access to CJI complete the Louisiana Cyber-Security Awareness Training
    e. Notified of CJIS security and confidentiality requirements, i.e., sign the CJIS Security Addendum Certification page
3. Upload Vendor Employee Security Addendum certification pages into CJIS Online
4. Notify the LSP immediately regarding any changes to Vendor employee status, including but not limited to
    a. personnel additions,
    b. separation from Vendor employment,
    c. reassignment to other non-CJIS related duties, or
    d. any arrests or convictions occurring after an initial employee approval by the LSP.
5. Notify the LSP immediately via a Security Incident Reporting Form if any breaches or security incidents occur.

5. Non-CJIS Vendor Responsibilities

Certain vendors may provide services that do not perform the administration of criminal justice as identified in 28 CFR part 20.3 (b), (e.g., custodians, HVAC maintenance), but their employees have unescorted access into CJIS Security Policy defined physically secure locations to perform their duties. These vendors (Non-CJIS Vendors) shall complete an abbreviated version of the CVVP requirements. The abbreviated version of the CVVP will include sections 4.1, 4.3 - 4.3.3, and 4.4 of this agreement in their entirety. The LSP shall be the determining authority for Non-CJIS vendors.

6. Criminal Justice Agency Vendor Screening

The CVVP is designed to assist criminal justice agencies (CJA) with completing the CJIS Security Policy technical and personnel requirements for utilizing vendors in the administration of criminal justice. As such, CJAs may use CVVP Approved Vendors without performing additional technical and personnel screening.

Louisiana criminal justice agencies may elect to conduct separate screening processes for vendors cleared by the CVVP. In such cases, the criminal justice agency shall be responsible for vendor compliance related to the vendor's technical offering and personnel security requirements. Additionally, the criminal justice agency shall be audited by the LSP for compliance regarding its vendor vetting and maintenance processes.

7. Confidentiality

Information provided by the vendor as part of the CVVP, including but not limited to audit reports and personally identifiable information (PII) submitted for background checks of vendor personnel, shall be confidential, kept secure from unauthorized access, and exempt from public disclosure. The vendor’s proprietary business operations, artifacts submitted for review in the CVVP, and employee PII shall be kept secure and confidential.

The vendor’s approval status for the online technical audit-questionnaire and personnel vetting may be shared with Louisiana Criminal Justice Agencies as necessary for audit purposes. The vendor’s product and or service name, which has been approved by the CVVP shall be made publicly available on the Louisiana State Police website.

LSP-CJIS VENDOR AGREEMENT ACKNOWLEDGMENT

The Vendor, supporting CJIS systems within the state of Louisiana, hereby acknowledges 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 access Criminal Justice Information for criminal justice purposes only.

The Vendor acknowledges these responsibilities have been developed and approved by the LSP 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. The Vendor acknowledges a failure to comply with these responsibilities could subject the LSP, CJA and this Vendor to various sanctions as recommended by the FBI CJIS Advisory Policy Board (APB) and/or the respective Directors of the LSP and/or the FBI.

To preserve the integrity of LLETS, the LSP reserves the right to suspend service to the CJA, Vendor, connected system, or an individual system user when the security or dissemination requirements are violated. The LSP may terminate services immediately if a violation is discovered. The LSP may reinstate service upon receipt of satisfactory assurance that violation(s) have been corrected.

This agreement remains separate from all contracts between the Vendor and CJAs. Issues which may arise between the Vendor and the CJA 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 shall become effective upon the date signed.

Business Name	
Address	

Provide the name and a description of each Product and/or Service with access to CJI that will be implemented in Louisiana and vetted through the CVVP
each product and/or service with access to CJI may be vetted and approved separately

Has the company ever completed a Louisiana State Police or federally issued CJIS audit? If so, has the company ever been denied the ability to do business in any state or for a federal entity due to the findings of that audit? If so, please explain.

List all subcontractors used in the company's CJI related offering, including any cloud service or data center providers.

_____

Vendor CEO or Designee Date

_____

Vendor Administrator Date

_____

LSP CSO or Designee Date

Once signed, return this document to LSP.VendorVetting@la.gov.