AUTHORIZED RECIPIENT USER AGREEMENT CONDITIONS FOR RELEASE OF CRIMINAL OFFENDER RECORD INFORMATION

This User Agreement, entered into by the California Department of Justice (hereinafter referred to as "CA DOJ") and the Authorized Recipient (hereinafter referred to as the "Authorized Applicant Agency") is intended to set forth the terms and conditions under which criminal offender record information (CORI) will be provided to the Authorized Applicant Agency as an employer, licensing agency, or other agency authorized by state and/or federal statute. The CA DOJ and the Authorized Applicant Agency are subject to and shall comply with all applicable state and federal laws, rules, and regulations relating to the receipt, use, and dissemination of CORI derived from the systems of the CA DOJ and Federal Bureau of Investigation (FBI).

In response to fingerprint-based criminal history record checks, the CA DOJ will provide state CORI available to the Authorized Applicant Agency in accordance with state statute. In the event access to federal CORI is authorized for the Authorized Applicant Agency, the CA DOJ will facilitate the dissemination of federal CORI between the agency and the FBI.

The records and data compiled by criminal justice agencies for purposes of identifying criminal offenders is referred to as CORI. It may also include: a summary of arrests, pretrial proceedings, the nature and disposition of criminal charges; information pertaining to sentencing, incarceration, rehabilitation, and release; or information depicting employment, licensing, and certification history. Criminal justice agencies throughout the state provide this information to the CA DOJ, and it is maintained in a statewide repository. This confidential information is disseminated to applicant agencies, authorized by California statute for the purposes of adoption, employment, certification, licensing, and permitting determinations. The following information describes each Authorized Applicant Agency's responsibility for accessing, storing, handling, disseminating, and destroying CORI.

By signing these Terms and Conditions, the Authorized Applicant Agency acknowledges that:

1. The Authorized Applicant Agency must notify applicants subject to a criminal record check that their fingerprints will be retained by the CA DOJ and searched against other fingerprints on file, including latent fingerprints.

2. The Authorized Applicant Agency must notify applicants of their right to obtain a copy of their criminal history record, if any. An applicant has the right to challenge the accuracy and completeness of their criminal history record, and to obtain a determination as to the validity of their record before the agency makes a final determination concerning their eligibility for adoption, employment, certification, licensing, or permitting.

3. For each applicant subject to a criminal history record check, the Authorized Applicant Agency shall retain the documentation that substantiates their authorizing relationship with the applicant (i.e., a copy of the applicant's completed and signed Request for Live Scan Service form (BCIA 8016) and employment or license application).

4. The Authorized Applicant Agency understands it is required to designate at least one Custodian of Records (COR) representative for their agency, pursuant to California Penal Code section 11102.2. The COR serves as the primary point of contact and actively represents their agency in all matters pertaining to accessing, storing, handling, disseminating, and destroying CORI.

AUTHORIZED RECIPIENT USER AGREEMENT CONDITIONS FOR RELEASE OF CRIMINAL OFFENDER RECORD INFORMATION

5. The Authorized Applicant Agency understands the confidential information received by the CA DOJ shall only be directly accessed by the confirmed COR(s) for the agency.

6. The Authorized Applicant Agency shall ensure state and federal fingerprint-based background checks are conducted on all personnel who have unescorted access to unencrypted CORI or unescorted access to physically secure locations or controlled areas (during times of CORI processing).

    a. If personnel have a criminal record, their access to CORI shall not be granted until the CA DOJ reviews the matter to determine if access is appropriate.

    b. If personnel with access to CORI are subsequently arrested or convicted, their access to CORI shall be suspended until the CA DOJ reviews the matter to determine if continued access is appropriate.

7. The Authorized Applicant Agency must uphold a standard of security for all personnel, who access *or* view CORI. It is required for the Employee Statement form to be filled out, signed, and kept on file by the COR representative(s). Personnel required to sign the form may include administrative staff that view CORI but do not have direct access to it. The form covers the responsibility of viewing confidential information and the consequences for any misuse.

    a. The Authorized Applicant Agency shall employ a formal sanctions process for personnel failing to comply with established information security policies and procedures.

8. Basic security awareness training shall be completed within six (6) months of initial assignment, and biennially thereafter, for all personnel who have access to *or* view CORI. The CA DOJ utilizes an online testing system called “CJIS Online” to help facilitate and track this training requirement.

9. The Authorized Applicant Agency understands that all responses or subsequent notifications containing CORI are sent electronically and received in the Applicant Agency Justice Connection (AAJC). The confidential information received shall only be used for the sole purpose for which it was requested.

10. The Authorized Applicant Agency and the COR(s) must ensure that all information associated with their agency profile and user account(s) in AAJC are kept up-to-date. All requests to make changes to the agency profile or user account(s) should be done through AAJC. This information must be updated in a timely manner.

11. The Authorized Applicant Agency must establish procedures for handling, processing, storing, and communicating to protect the CORI received from unauthorized disclosure, alteration, or misuse.

AUTHORIZED RECIPIENT USER AGREEMENT CONDITIONS FOR RELEASE OF CRIMINAL OFFENDER RECORD INFORMATION

12. The Authorized Applicant Agency must document and implement media protection policy and procedures required to ensure that access to electronic and physical media in all forms is restricted to authorized individuals for securely handling, transporting, and storing media.

    a. The Authorized Applicant Agency assumes ultimate responsibility for managing the security of CORI received. The Authorized Applicant Agency shall restrict access to physical or electronic copies of CORI to its COR(s); assisting administrative personnel may only view CORI under the supervision of a COR.

    b. All physical copies of CORI must be properly stored in a confidential location and destroyed when no longer needed. The information received needs to be stored separately from employee personnel files.

13. The Authorized Applicant Agency must document and implement physical protection policy and procedures required to ensure CORI and information system hardware, software, and media are physically protected through access control measures.

14. The Authorized Applicant Agency shall ensure the protection of CORI by establishing operational incident handling procedures. The agency shall track, document, and report incidents to appropriate agency officials and/or authorities.

15. CORI may only be shared for secondary dissemination to an employment or licensing agency only when explicitly allowed by law. It is required to log any sharing of CORI, either sending or receiving. Logs shall include, at a minimum, the date, the sending and receiving agencies, the record(s) shared, the statutory authority to share CORI, the means of transmission, and the person who disseminated the CORI. CORI is exempt from disclosure under the California Public Records Act.

16. The Authorized Applicant Agency shall immediately notify the CA DOJ when an authorized relationship no longer exists with an applicant (e.g., when the applicant is not hired, when the employment of the applicant is terminated, when the applicant's license or certificate is revoked, or when the applicant may no longer renew or reinstate the license or certificate), pursuant to Penal Code section 11105.2(d).

    a. A notification must be submitted within five days via a No Longer Interested (NLI) request in the Applicant Agency Justice Connection (AAJC) portal to NLI the applicant.

17. The Authorized Applicant Agency must periodically reconcile their list of active applicants to ensure it is accurate and up-to-date.

18. The Authorized Applicant Agency shall retain all records necessary to facilitate a security audit by the CA DOJ by retaining audit records for at least one (1) year. Once the minimum retention period has passed, the agency shall continue to retain audit records until they are no longer needed for administrative, legal, audit, or other operational purposes.

AUTHORIZED RECIPIENT USER AGREEMENT CONDITIONS FOR RELEASE OF CRIMINAL OFFENDER RECORD INFORMATION

19. The Authorized Applicant Agency shall not outsource any noncriminal justice ancillary functions to contractors without seeking and obtaining written approval from the CA DOJ. Noncriminal justice ancillary functions include, but are not limited to, accessing, storing, handling, disseminating, and destroying CORI.

20. The Authorized Applicant Agency shall not permit the use of personally owned information systems to access, process, store, or transmit CORI unless it establishes and documents the specific terms and conditions for personally owned information system usage.

    a. Publicly accessible computers (e.g., hotel business center computers, convention center computers, public library computers, public kiosk computers) shall not be used to access, process, store, or transmit CORI.

21. The Authorized Applicant Agency shall: (a) establish usage restrictions and implementation guidance for mobile devices accessing, processing, storing, or transmitting CORI; and (b) authorize, monitor, and control wireless access to information systems that access, process, store, or transmit CORI in accordance with section 5.13 of the Criminal Justice Information Services (CJIS) Security Policy.

22. The Authorized Applicant Agency shall maintain documentation that demonstrates the agency is compliant with the requirements of section 5.10 of the CJIS Security Policy, to include but not limited to:

    a. Boundary Protection
    b. Encryption
    c. Intrusion Detection Tools and Techniques
    d. Voice Over Internet Protocol
    e. System and Information Integrity Policy and Procedures

23. If the Authorized Applicant Agency intends to receive CORI via Secure File Transfer Protocol (SFTP) or record any information (e.g., date of arrest and conviction, nature of charges, conviction status) received from the CA DOJ into a database or cloud environment, it shall submit documentation to the CA DOJ that demonstrates the agency is compliant with or is ready to implement all requirements of the CJIS Security Policy, including but not limited to the requirements specified in sections 5.4, 5.5, 5.6, 5.7, and 5.10 of the CJIS Security Policy.

24. It is the Authorized Applicant Agency's responsibility to understand how they are authorized to conduct background checks, and to notify the CA DOJ if the agency's statutory authority to access CORI changes or no longer exists.

25. The Authorized Applicant Agency must notify the CA DOJ when authorization to receive CORI should be terminated (i.e. there is no longer a need to conduct background checks or the agency closes).

AUTHORIZED RECIPIENT USER AGREEMENT CONDITIONS FOR RELEASE OF CRIMINAL OFFENDER RECORD INFORMATION

Once every three (3) years, as a minimum, the CA DOJ and the FBI are authorized to conduct audits to assess agency compliance with this agreement and with applicable statutes, regulations, and policies. Audits may be conducted on-site or remotely. I have read and understand the preceding Terms and Conditions in the Authorized Recipient User Agreement. As the agency head or person in charge, I understand that failure to comply with these conditions may result in the suspension or termination of access to CORI. Furthermore, I acknowledge the DOJ reserves the right to revise these conditions or impose additional conditions, at any time it deems necessary to protect the confidentiality and security of information maintained by the Department.

Signature: _____ Date: _____

Printed Name: _____

Contributing Agency/Organization Name: _____

Contributing Agency/Organization E-mail Address: _____

Contributing Agency/Organization Mailing Address: _____

Contributing Agency/Organization City, State, Zip Code: _____