CALIFORNIA DEPARTMENT OF JUSTICE
BUREAU OF CRIMINAL IDENTIFICATION AND INFORMATION

APPLICANT COMMUNICATION NETWORK

TERMS AND CONDITIONS FOR PRIVATE SERVICE PROVIDERS IN CALIFORNIA

Private service providers in California, approved by the Department of Justice (DOJ) to establish and maintain a connection to the DOJ Applicant Communication Network for purposes of transmitting non-criminal justice requests for criminal offender record information to DOJ, shall be required to comply with all requirements set forth in this document.

1. Definitions

For purposes of this document, terms are defined as follows:

1.01 Applicant - Any person who, as a condition of obtaining a license, certificate, permit, or employment, is required to submit his/her fingerprints to DOJ for a criminal background check.

1.02 Applicant Information - Personal and confidential information, regarding an Applicant, including fingerprint images, Social Security Number, California Driver's License, or any other personal identification numbers provided by or collected from an Applicant, which is relevant and necessary to accomplish an electronic fingerprint transaction for transmission to DOJ.

1.03 Live Scan - A computer-based device that allows for the capture of digitized fingerprint images and Applicant data, and the electronic transmission of fingerprint images and data to centralized computers at DOJ.

1.04 Network - The electronic communication system, established by DOJ pursuant to section 11077.2 of the California Penal Code, to facilitate the transmission of requests for criminal offender record information from private service providers in California.

1.05 Operator - Any person who operates a Live Scan device and/or provides Applicant fingerprinting services on behalf of a DOJ-approved Provider.

1.06 Provider - A private fingerprint service provider in California, approved by DOJ to establish a connection to the DOJ Applicant Communication Network for purposes of transmitting electronic Applicant transactions for criminal offender record information to DOJ for employment, licensing, certification, or custodial child placement purposes.

1.07 Provider Representative - The person duly authorized to represent the Provider and act on its behalf, with defined authority for implementing and ensuring ongoing compliance with all requirements set forth in these Terms and Conditions. The Provider Representative must be a California resident and is

subject to the Certification requirements set forth in section 3.02 of this document. For the purposes of the duties and responsibilities set forth in this document, the Provider Representative and the Provider shall be considered to be one and the same.

2. Scope

2.01 This document establishes the minimum internal controls deemed necessary by DOJ to adequately protect the security and stability of the Network, and the privacy rights of individual Applicants. The Provider may impose any additional, more stringent controls it deems necessary and/or appropriate.

2.02 The Terms and Conditions apply to all personnel, equipment, software, systems, networks, communication links, and facilities supporting and/or acting on behalf of the Provider.

2.03 Approval to establish and maintain connectivity to the Network, either directly or indirectly, shall be contingent upon full compliance at all times with all requirements set forth in this document. Failure or refusal to fully comply with all requirements herein may result in the temporary or permanent termination of the Provider's direct connection to the Network, ability to transmit electronic fingerprints to DOJ through an indirect Network connection, or ability to forward electronic fingerprints to DOJ on behalf of other DOJ-approved Provider(s).

3. Personnel Security

3.01 The Provider shall be responsible for the actions of any person or entity acting on its behalf and/or providing services in support of it.

3.02 Unless exempted under the provisions of section 11102.1(a) of the California Penal Code, the Provider, and every Operator providing services on a Provider's behalf, shall possess and maintain a valid Fingerprint Roller Certificate issued by DOJ. The Provider shall not allow any Operator to provide fingerprint services on its behalf unless he/she possesses a valid Fingerprint Roller Certificate.

3.03 The Provider shall maintain a current list of all Operators providing fingerprint services on its behalf. A copy of the list shall be provided to DOJ upon request.

4. Site Security

4.01 All hardware and software associated with the capture and/or transmission of Applicant fingerprints to DOJ shall be adequately secured at all times to reasonably protect against theft, damage, and/or unauthorized access or use by any person.

5. Information Security

5.01 Applicant information is confidential and the use of this information for any purpose other than the purpose for which it was expressly provided by the Applicant is strictly prohibited. Violation of an Applicant's absolute right to privacy may subject the Provider and/or its Operator(s) to criminal and/or civil liability, and may result in termination of the Provider's connectivity to the Network.

5.02 Except as expressly authorized by DOJ, Applicant information shall not be replicated, sold, shared, modified, archived, stored, or used to supplement any existing data base, file, record or report, or create any new data base, file, record or report.

5.03 A Provider forwarding electronic fingerprint records to DOJ on behalf of another DOJ-approved Provider is strictly prohibited from stripping or extracting any data from the records it forwards, except as expressly authorized in writing by DOJ.

5.04 Applicant information, as defined in Section 1.02, shall not be collected or transmitted outside of the State of California.

5.05 Applicant information, as defined in Section 1.02, shall be collected and verified by the Live Scan Operator conducting the transaction.

5.06 The Live Scan Operator shall reasonably verify the identity of each Applicant by comparison to a valid (unexpired) photo identification, presented at the time of fingerprinting, to the appearance of the Applicant, and to the information contained on the Request for Live Scan Services form. Fingerprint services shall not be provided to any Applicant who does not present proper and valid photo identification, and whose identity cannot be reasonably verified through this comparison.

5.07 Once a transaction has been transmitted, the Provider is strictly prohibited from using a previously captured fingerprint image for any purpose other than resubmitting a record that was rejected by DOJ due to faulty data.

5.08 Applicant fingerprint transaction records may be temporarily retained in an electronic storage medium, within the Live Scan device, pending successful transmission of the record to DOJ. In no event, however, may any Applicant fingerprint image or record be retained, in either electronic or hard copy form, for longer than 30 calendar days from the date of the initial transmission of the fingerprint record to DOJ.

5.09 Every person who, in the course of their normal duties, collects, processes, facilitates, or supports the transmission of Applicant fingerprints to DOJ, or who manages, administers, accesses, develops, or maintains the systems supporting the Provider, shall be required to sign a DOJ Security and Disclosure Certification form, appended hereto, acknowledging that they understand their responsibilities

for protecting confidential Applicant information, the restrictions concerning the use of such information, and the penalties for misuse. Signed copies of the Certification forms shall be retained by the Provider and shall be made available to DOJ upon request.

6. System Security

6.01 A dedicated system shall be utilized for transmitting electronic Applicant fingerprints to DOJ. The Provider shall not use the system to run any other business application(s), unless expressly authorized by DOJ in advance.

6.02 The Provider shall obtain DOJ approval prior to establishing any network linkage to another DOJ-approved Provider (peer to peer), for the purpose of accomplishing an indirect connection to the Network.

6.03 Any network linkage authorized by DOJ pursuant to section 6.02, which allows electronic Applicant fingerprints to be transmitted from the Live Scan Provider, and forwarded to DOJ through another Provider's direct connection to the Network (peer to peer relationship) via WAN, LAN, or Internet, shall be secured by a firewall to provide a point of defense, and a controlled and audited access to servers, from both inside and outside of the network.

6.04 The DOJ-approved transmission path, which enables connectivity to the Network, originating from the Live Scan Provider, and transversing through any inter-connected systems, and ultimately terminating at DOJ, shall not be modified in any way without advance notice to, and express written approval from DOJ.

6.05 All equipment used for transmitting and/or forwarding electronic Applicant fingerprints to DOJ shall be segregated and screened against unauthorized use. Data integrity must be maintained in order to detect the unauthorized creation, alteration, or deletion of Applicant data or images.

6.06 All unused user or system accounts shall be removed or disabled.

7. Security Violations

7.01 All security violations, or suspected security violations shall be immediately reported to DOJ. Reports of security violations shall include the date of the incident(s), the parties involved (if known), the nature and scope of the incident, and any action(s) taken, including steps to protect against future violations.

7.02 DOJ reserves the right to investigate all reported or suspected security violations and to take any action it deems appropriate and/or necessary to protect the security and stability of the Network and the privacy rights of individual applicants, including termination of the Provider's connection to the Network.

8. Quality Controls

8.01 Remedial training may be required if, at any time, DOJ determines that the rate of

record rejects due to poor image quality, or data errors, exceeds acceptable levels. Failure to obtain appropriate training and resolve unacceptable fingerprint record reject levels in a timely manner may result in termination of the Provider's connectivity to the Network.

8.02 The Provider shall only utilize hardware and software that is currently certified and approved by DOJ for the Applicant software type, the National Institute of Standards and Technology, and the Federal Bureau of Investigation (FBI).

8.03 All equipment associated with the capture and transmission of electronic Applicant fingerprint records shall be maintained in good working condition at all times.

8.04 All manufacturer software upgrades, including the installation of any patches deemed necessary by the manufacturer, shall be applied in a timely fashion and shall remain current.

8.05 All DOJ customization software upgrades and DOJ validation table updates shall be applied in a timely fashion and shall remain current.

8.06 All Applicant fingerprint records shall be transmitted to DOJ within 24-hours from the time the fingerprints were obtained from the Applicant.

8.07 The Provider shall maintain a log of all Applicant fingerprint transactions. The log shall clearly identify the name of the Operator who performed each transaction, the name of the Applicant fingerprinted, the date the Applicant was fingerprinted, the type of photo identification presented, and the Applicant Tracking Identifier (ATI) number associated with the transaction. The Provider shall maintain the log for a minimum of one year from the date of the oldest transaction, and shall make the log available to DOJ upon request. Access to the log shall be controlled by the Provider.

8.08 The Provider shall retain a copy of the "Request for Live Scan Service" form associated with each Applicant fingerprint transaction for a period of 12 months, for purposes of security audit review. The copies shall be stored in a locked storage medium to reasonably protect against theft, damage, or access by any unauthorized person. The copies shall be destroyed by cross-cut shredding after the 12-month retention period has elapsed.

9. <u>Fees</u>

9.01 The Provider shall establish a billing account with DOJ for purposes of collecting and remitting DOJ and FBI processing fees.

9.02 DOJ and FBI processing fees that are not billable to the requesting entity shall be collected by the Provider at the time fingerprint services are rendered to the Applicant. All processing fees shall be remitted to DOJ in a timely manner by the Provider. Failure to remit payment in a timely manner may result in termination

of the Provider's Network connection.

9.03 The Provider may charge the Applicant a separate fingerprint rolling fee as compensation for its services. The amount of the fee, and acceptable method(s) of payment shall be determined by the Provider.

9.04 Any Applicant who returns to the Provider to be reprinted because his/her initial fingerprint submission was rejected due to poor fingerprint image quality, shall not be charged an additional rolling fee by the Provider. The Applicant may, however, be charged a rolling fee if the original fingerprint transaction was performed by a different service Provider.

10. Audits

10.01 The Provider shall be subject to periodic, unannounced, on-site visits by DOJ to audit for compliance with the provisions of the Terms and Conditions, and any applicable laws, regulations, policies, practices, or other requirements deemed necessary by DOJ. The audits shall be reasonable in both scope and length, and shall occur during the Provider's normal business hours. Audits will be conducted in a manner that is least disruptive to the Provider's business operations.

10.02 Failure to cooperate, and/or refusal to provide documents, logs, lists, files, records or any other information requested by DOJ, may result in the temporary or permanent termination of the Provider's connection to the Network.

11. Miscellaneous Provisions

11.01 These Terms and Conditions do not confer, grant, or authorize any rights or privileges to any entity or person other than the Provider and the Provider's authorized representative.

11.02 All reports, notices, requests, and/or correspondence shall be forwarded by First Class Mail to:

Bureau Chief
Bureau of Criminal Identification and Information
Department of Justice
P.O. Box 903417
Sacramento, CA 94203-4170

CALIFORNIA DEPARTMENT OF JUSTICE
APPLICANT COMMUNICATION NETWORK

AGREEMENT TO TERMS AND CONDITIONS FOR PRIVATE SERVICE PROVIDERS IN CALIFORNIA

Provider: _____

Provider Representative: _____

Mailing Address: _____

Telephone Number: _____ Facsimile Number: _____

Email Address: _____

The Provider's connection to the Department of Justice (DOJ) Applicant Communication Network is contingent upon implementation of, and adherence at all times, to all requirements set forth in the Terms and Conditions, including any changes thereto.

DOJ reserves the right to amend or modify the Terms and Conditions, and/or impose additional requirements and/or restrictions, at any time it deems necessary to protect the stability and security of the Network.

DOJ reserves the right to terminate the Provider's connection to the Network at any time, without prior notice, if it has reason to believe that the security or stability of the Network has been, or will be, compromised in any way.

This Agreement is not effective unless, and until, approved by DOJ, and signed by both parties.

In signing this Agreement, I certify that I have read and understand the foregoing Terms and Conditions for establishing and maintaining a connection to the DOJ Applicant Communication Network, and agree to and accept responsibility for compliance with all requirements therein.

_____ _____
Signature of Provider Representative Date

Approved:

_____ _____
DOJ Representative (Printed Name) Title

_____ _____
Signature of DOJ Representative Date

Live Scan Service Providers
Security and Disclosure Certification

Individuals providing Live Scan fingerprinting services collect and have access to personal Applicant information, including fingerprint images, which is considered to be confidential under California law. The California Department of Justice (DOJ) is committed to protecting the privacy rights of individuals, and protecting personal information from unauthorized access, use, or disclosure. As an individual providing Live Scan fingerprinting services on behalf of _____, you are responsible for understanding and complying with the
(Name of Provider) following duties and responsibilities related to the protection, use and handling of confidential Applicant information.

1) You may request and collect only that information which is necessary to perform an Applicant Live Scan transaction.

2) You may not deliberately enter false or incomplete data or images, or omit or modify existing valid data in an attempt to affect the outcome of an Applicant's criminal history background check.

3) You are strictly prohibited from using any personal Applicant information for any purpose other than the purpose for which the information was expressly provided by the Applicant. You may not share, replicate, compile, remove, delete, alter, or disclose information collected from or regarding Applicants.

4) You may not remove materials from the area approved for the placement and use of a Live Scan device and accompanying secured storage areas without specific authorization from the DOJ. The only exception to this is during the use of a portable Live Scan device, when materials are transported to and from the site where the Live Scan device is used.

5) You must take reasonable precautions to protect Applicant information from unauthorized access. These reasonable precautions include, but are not limited to: ensuring that any Live Scan device is unaccessible when unattended; ensuring that unauthorized persons are not allowed to view the screen of a Live Scan device; storing materials containing confidential information in a secure place; and immediately reporting unauthorized or suspicious individuals or activities to the Live Scan Provider or to the DOJ.

I have read and understand the duties, responsibilities, and restrictions stated above, and have received a copy. I understand that failure to comply with these policies may result in administrative action up to and including criminal and/or civil prosecution in accordance with applicable statutes.

_____	_____
Printed Name of Employee	**Job Title**
_____	_____
Signature of Employee	**Date**

BCII LS SD 01 (4-2004)