Florida Department of Law Enforcement
Criminal Justice Information Services Division

Registered Livescan Submitter User Agreement

for Private Entities and Private Vendors
Submitting Electronic Fingerprints to the
Florida Department of Law Enforcement
Under Section 943.053(13), Florida Statutes

REGISTERED LIVESCAN SUBMITTER NAME:_____

I. This Agreement, entered into between the Florida Department of Law Enforcement, User Services Bureau (hereinafter referred to as FDLE), an agency of the state of Florida with headquarters in Tallahassee, Florida, and

Registered Livescan Submitter Business Name:
_____,
(hereinafter referred to as RLS), located at:

Address: _____
Address 2: _____
City: _____ State: _____ Zip Code: _____

II. Purpose

A. Electronic fingerprint submissions are required by the Federal Bureau of Investigation for conducting criminal history record checks on a variety of professions, occupations, positions, and licenses, and must precede the release of national criminal history record information to the non-criminal justice licensing, employing or regulatory agency authorized to receive such information.

B. FDLE, as the central repository of criminal history record information within the state of Florida and the state point of contact for the FBI, receives and processes electronic fingerprint submissions through FDLE's Civil Workflow Control System (CWCS).

C. Section 943.053(13)(a), F.S., requires private electronic fingerprint submitters agree to comply with certain standards and practices, as set forth in the terms and conditions of this User Agreement.

D. As used in this Agreement, a Registered Livescan Submitter (RLS) is a private vendor engaged in the business of providing electronic fingerprint submission services on behalf of entities or agencies authorized to request criminal history background checks for official purposes, and/or is a private entity submitting the electronic fingerprints of its own employees, volunteers, contractors and associates for permitted criminal history record checks. The RLS is a private contractor, and is not acting as the agent or servant, or on behalf, of FDLE or any government agency, except for the limited purpose of acting as a "third-party agent" for FDLE within the intent of Section 501.171(6), Florida Statutes.

III. Standards

To meet statutory requirements for the acceptance and processing of electronic fingerprint submissions, the RLS agrees to adhere to the standards listed below. The RLS must have documented processes in place to ensure all employees are meeting the appropriate standards.

A. Identification

1. All persons responsible for collecting personal identifying information from individuals being fingerprinted must meet current written state and federal guidelines as outlined in the "Identity Verification Program Guide," and incorporated here by reference, available on FDLE's website. At a minimum, identification of individuals must be verified by requiring them to provide a valid government-issued form of identification that includes the individual's photograph.

B. Quality Standards

1. Persons responsible for capturing electronic fingerprints will be familiar with the proper procedures for capturing fingerprints as outlined in "Recording Legible Fingerprints," and incorporated here by reference, available on FDLE's public website.

2. No person may take his or her own fingerprints for submission to FDLE under any circumstances. The RLS will not allow a person to roll his or her own fingerprints on any livescan device operated by the RLS. The RLS may not scan hard copy fingerprint cards for submission to FDLE that are, or should reasonably be known to have been, taken by the person.

3. Fingerprint images submitted electronically must adhere to FDLE and the FBI quality standards. Fingerprint images submitted must be of sufficiently high quality to avoid rejection or an inability to conduct fingerprint comparisons. Fingerprint images of insufficient quality may be rejected or not processed.

4. FDLE has established as an acceptable FBI Integrated Automated Fingerprint Identification System (IAFIS) rejection rate of less than 5% of the total electronic fingerprint submissions by the RLS. If the RLS rejection rate is equal to or higher than 5% over a twelve month period, the RLS will be notified of the rejection rate in excess of the established standard.

    a. Upon notice, the RLS shall take immediate corrective action to ensure electronic fingerprint submissions are within the acceptable rejection rate.

    b. The RLS will have electronic submissions monitored and evaluated for a subsequent three month period. If after this period, the rejection rate remains equal to or higher than 5%, the RLS must demonstrate to FDLE the measures implemented to address the rejection issue. FDLE will determine if the measures taken by the RLS are sufficient for future electronic fingerprint submissions.

    c. FDLE reserves the right to revoke approval for an RLS to submit electronic fingerprint transactions, if an RLS fails to meet the acceptable rejection rate or address such issues satisfactorily.

IV. Payment of Fees

A. The RLS is solely responsible for payment of fees required by state and federal law to FDLE. All fees are subject to change.

1. The RLS will provide FDLE a valid credit card number to meet payment requirements. The RLS acknowledges providing a credit card number, will authorize FDLE to apply this method of payment to satisfy any and all amounts due.

2. The RLS acknowledges and agrees to maintain current valid credit card information with FDLE. The RLS also agrees to notify FDLE immediately of any change in credit card information which would affect payment, such as a change in card number or expiration date.

3. The RLS may collect the fees for a state and national criminal history check, and any applicable fingerprint retention fees, from the individual or entity on whose behalf the fingerprints are submitted.

4. Failure to pay the amount due may result in the refusal by the FDLE to accept future fingerprint submissions until all amounts due are paid in full.

V. Personally Identifiable Information (PII)

A. The RLS assumes full legal responsibility for the security of PII obtained from the individual being fingerprinted.

B. Section 501.17, F.S., requires a "covered entity," as defined, which would include an RLS, to "give notice to each individual in this state whose personal information was, or the covered entity reasonably believes to have been, accessed as a result of [a] breach, "defined as "unauthorized access of data in electronic form containing personal information".

1. "PII" means an individual's first name, or first initial and last name, in combination with any one or more of the following data elements for that individual:

a. Social security number;

b. A driver license or Identification Card number, passport number, military identification number, or other similar number issued on a government document used to verify identity;

c. A financial account number or credit or debit card number, In combination with any required security code, access code, or password that is necessary to permit access to an individual's financial account;

d. Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or

e. An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual.

2. A user name or e-mail address, in combination with a password or security question and answer that would permit access to an online account for the purposes of this agreement.

C. In addition to other duties required by Section 501.171, F.S. the RLS will provide notification of breach to the affected individual(s) no later than 30 days following the determination of the breach, unless otherwise authorized by law.

D. The RLS will notify FDLE immediately, either by written or electronic notice, if PII is compromised.

E. The RLS agrees the PII collected from the individuals is used for the sole purpose of submitting a fingerprint-based criminal history record check to FDLE.

F. The RLS will promptly delete and destroy any PII that no longer has value for the purposes of performing a criminal history record check as authorized by state and federal law.

VI. Audit

A. FDLE will conduct inquiries with regard to any allegations or potential security violations, as well as perform routine audits.

B. The RLS will facilitate a security audit by FDLE, and cooperate fully in any such audit as FDLE or other authorities may deem necessary. Examples of records subject to audit are electronic logging or electronic correspondence associated with identity verification of applicants; internal policies and procedures outlining the steps taken to assure physical and technical security of information; and a current, signed User Agreement with FDLE.

VII. General

A. This User Agreement is exclusive to the parties of the agreement listed in Section I. The agreement cannot be transferred or assigned to other parties. If the RLS changes ownership, a new User Agreement must be executed between the new ownership and FDLE.

B. If FDLE amends or modifies the terms of this User Agreement, a new agreement will be executed by the parties.

IN WITNESS HEREOF, the parties hereto have caused this agreement to be executed by the proper officers and officials.

NAME OF REGISTERED LIVESCAN SUBMITTER _____

AGENCY HEAD _____ **TITLE** _____
(PLEASE PRINT) (PLEASE PRINT)

AGENCY HEAD _____
(SIGNATURE)

DATE _____

WITNESS _____ **TITLE** _____

DATE _____

FLORIDA DEPARTMENT OF LAW ENFORCEMENT

BY _____ **TITLE** **CJIS SYSTEMS OFFICER**

WITNESS _____ **TITLE** _____

DATE _____