Andy Frain Services, Inc. Biometric Data Protection Policy

LAST UPDATED: 3/14/19	**VERSION 2.0**

I. Introduction

A. Purpose and Application

This Biometric Data Protection Policy, as amended and restated effective March 14, 2019 (the "Policy") sets forth the data protection policies and procedures applicable to treatment of Andy Frain Services, Inc.'s (the "Company") customer and employee Biometric Data. Company from time to time may need to facilitate, collect and/or use certain biometric information about individuals in order to obtain security licenses, and/or badges or access credentials to a secured area. These can include customers, suppliers, business contacts, employees and other people the organization has a relationship with or may need to contact. This policy describes how this Biometric Data must be collected, handled and stored to meet the company's data protection standards — and to comply with the law. The loss of Biometric Data can result in substantial harm to individuals, including embarrassment, inconvenience, and fraudulent use of the information. Protecting the confidentiality and integrity of Biometric Data is a critical responsibility that must be taken seriously at all times. Compliance with this Policy is mandatory.

This purpose of this Policy is ensure that Company:

- Complies with biometric data protection laws and follows general principles for protection of Biometric Data;
- Protects the rights of staff, customers and partners;
- Is open about how it stores and processes individuals' data;
- Protects itself from the risks of a data breach

Modifications to data regulations are expected from time to time, some of which may require amendment of this Policy. If any provision of this Policy is inconsistent with the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, the Texas Biometric Privacy Act or any other applicable state or national biometric privacy laws (to the extent applicable to Company), this Policy will be interpreted to comply with any such applicable law.

B. Scope

This Policy applies to all Company employees, agents, and representatives ("Representatives" or "you"), including any contractor or consultant or third-party provider of services to the Company ("Third-Party Service Provider") who have access to Biometric Data the Company has collected or otherwise has in its possession. This Policy applies to all Biometric Data collected, maintained, transmitted, stored, retained, or otherwise used by the Company regardless of the media on which that information is stored and whether relating to employees, customers, or any other person. Questions about this Policy should be directed to the Company's Privacy Officer.

C. Maintenance and Amendment

This Policy will be maintained by the designated Privacy Officer. The Privacy Officer may update this Policy as he or she deems necessary or appropriate to ensure continued compliance with applicable data protection laws.

D. Other Company Policies

This Policy should be read in conjunction with and incorporates by reference the Company's Information Security Policy, the Andy Frain Services, Inc. Personal Information Protection Policy and other administrative policies that may affect the use and disclosure of personal data and remedial action to be taken in the event of policy violations. The Privacy Officer is responsible for resolving any conflicts between the terms of this Policy and any other Company policy as they apply to Biometric Data.

E. Policy Effective Date

This Policy has been amended and restated effective March 14, 2019, except where otherwise provided herein.

II. Definitions

A. "Biometric Data" means data the Company has collected or otherwise maintains or has in its possession, regardless of how it is captured, converted, stored, or shared, based on an individual's "Biometric Identifier" used to identify an individual. Biometric Data does not include information derived from items or procedures excluded under the definition of biometric identifiers.

B. "Biometric Identifier" means information that identifies or can be used to identify or authenticate an individual, directly or indirectly, using a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. Biometric identifiers do not include writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color. Biometric identifiers do not include donated organs, tissues, or parts as defined in the Illinois Anatomical Gift Act or blood or serum stored on behalf of recipients or potential recipients of living or cadaveric transplants and obtained or stored by a federally designated organ procurement agency. Biometric identifiers do not include biological materials regulated under the Genetic Information Privacy Act. Biometric identifiers do not include information captured from a patient in a health care setting or information collected, used, or stored for health care treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act of 1996. Biometric identifiers do not include an X-ray, roentgen process, computed tomography, MRI, PET scan, mammography, or other image or film of the human anatomy used to diagnose, prognose, or treat an illness or other medical condition or to further validate scientific testing or screening.

C. **"Data Subject"** means the person about whom Biometric Data is collected.

D. **"Data Breach"** means any accidental or unlawful act or omission that compromises or breaches the security, confidentiality, or integrity of Biometric Data or the physical, technical, administrative, or organizational safeguards the Company or a Third-Party Service Provider has put in place to protect Biometric Data. The accidental or unlawful destruction, loss or alteration of or unauthorized access to, disclosure, access to, or acquisition of Biometric Data is a Data Breach.

III. Collecting, Using, Handling, and Retaining Biometric Data

A. **Notice and Collection.** It is Company policy that whenever Company collects Biometric Data for any purpose, including for securing a sensitive or protected area, human resources, security officer licensing or employment purposes, the Company must first inform the Data Subject of the collection and purpose of the collection of the Biometric Data and obtain a written consent and release before Biometric Data is collected. The Company must also inform the Data Subject how the Company will use, process, store, disclose, protect, and for how long the Company will retain that Biometric Data by presenting the Data Subject with a privacy notice, consent and release. In any event, Company must obtain from each Data Subject at the time of the collection of or prior to collection of Biometric Data an executed written consent and release. Biometric Data captured for purposes of the operation of Livescan or other fingerprinting equipment shall utilize a notice substantially in the form attached to this Policy. Company may only collect Biometric Data in compliance with applicable Company policies, notices, and Data Subject consent, and the Biometric Data collected must be limited to that which is reasonably necessary to accomplish the Company's legitimate business purposes or as necessary to comply with law.

B. **Disclosure**. It is the Company's policy that Company shall not sell, lease, trade, or otherwise profit from a person's or a customer's Biometric Data. It also the policy of the Company that Company shall not disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless (1) the subject of the biometric identifier or biometric information or the subject's legally authorized representative consents to the disclosure or redisclosure; (2) the disclosure or redisclosure completes a financial transaction requested or authorized by the subject of the biometric identifier or the biometric information or the subject's legally authorized representative; (3) the disclosure or redisclosure is required by State or federal law or municipal ordinance; or (4) the disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

C. **Storage of Data**. These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT manager or data controller. When data is stored on paper**,** it should be kept in a secure place where unauthorized people cannot see it. These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.

- Employees should make sure paper and printouts are not left where unauthorized people could see them, like on a printer.

- Data printouts should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorized access, accidental deletion and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared between employees.

- If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.

- If data is stored on equipment or hard drive (like digital fingerprint scanning equipment), this equipment or hard drives should be kept locked away securely when not being used.

- Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing services.

- Servers containing personal data should be sited in a secure location, away from general office space.

- Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.

- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.

- All servers and computers containing data should be protected by approved security software and a firewall.

D. <u>Access, Use and Sharing of Biometric Data</u>. Company may only access Biometric Data when the information relates to and is necessary to perform job duties. You may not access Biometric Data for any reason unrelated to your job duties. You may not use Biometric Data in a way that is incompatible with the notice given to the Data Subject at the time the information was collected. If you are unsure about whether a specific use or disclosure is appropriate, you should consult with your supervisor. You may only share Biometric Data with another Company employee, agent, or representative if the recipient has a job-related need to know the information. Biometric Data may only be shared with a Third-Party Service Provider if it has a need to know the information for the purpose of providing the contracted services and if sharing the Biometric Data complies with the privacy notice provided to the Data Subject. You may not share Biometric Data with a Third-Party Service Provider without prior written supervisor approval and a fully executed written contract.

Biometric Data is of no value to Company unless the business can make use of it. However, it is when Biometric Data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with Biometric Data, employees should ensure the screens of their computers are always locked when left unattended.
- Biometric Data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure.
- Biometric Data must be encrypted before being transferred electronically. The IT manager can explain how to send data to authorized external contacts.

D. **Accuracy.** You must collect, maintain, and use Biometric Data that is accurate, complete, and relevant to the purposes for which it was collected. The more important it is that the Biometric is accurate, the greater the effort Company should put into ensuring its accuracy. It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Company will make it easy for data subjects to update the information Company holds about them. For instance, via the company website.

E. **Security.** You are responsible for protecting Biometric Data. The Company has implemented an Information Security Program (ISP) that sets forth technical, administrative, and physical safeguards for the protection of Biometric Data. You must follow the security procedures set out in the ISP at all times.

1. General Rule

A Representative is permitted to use and/or disclose Biometric Data for the purposes set forth in this Policy. When using and disclosing Biometric Data, however, the Company and its Representative must take reasonable steps to safeguard the Biometric Data and keep it confidential, and to ensure that it is not intentionally or unintentionally used or disclosed for a purpose or in a manner inconsistent with this Policy. Any violation of this Policy must be reported to the Privacy Officer, who will (1) act as necessary to maintain the security of any Biometric Data, (2) take such action as he or she deems appropriate to prevent any similar violation in the future, (3) take steps necessary to mitigate any damages caused by the violation, and (4) impose appropriate sanctions against the Representative accountable for the violation. If the Privacy Officer determines that sanctions are warranted against a Representative causing such violation, he or she will issue sanctions, up to and including termination.

The Privacy Officer will document all sanctions issued for a violation of this Policy and any applicable sanctions and actions taken to prevent similar violations.

2. Physical Security

Biometric Data in physical form (*e.g.*, printed material and notes) is maintained and stored at the Company offices is a secured employee personnel file. Company employees must have registered badge access to enter the building and each floor. All visitors must register with the building and must be accompanies by an employee at all times. Biometric Data is generally in digital form. Responsible Employees are discouraged from maintaining Biometric Data in physical form and are responsible for securing any such Biometric Data or destroying it after use. If a Representative needs to retain the Biometric Data other than in its designated location for a limited period, he or she must take reasonable steps to ensure that only he or she, or another Representative with a legitimate reason to use or disclose the Biometric Data, has access.

When materials containing Biometric Data are in use, the Representative must take reasonable steps to ensure that such materials are viewable only by the Representative. For example, if a Representative has Biometric Data in printed material on his or her desk, he or she must destroy the material or lock his or her office before leaving his or her immediate work area for any significant amount of time. If another person enters a Representative's immediate work area while the Representative is viewing Biometric Data, the Representative must remove the Biometric Data from the view of the other person (unless the other person is a Representative whose duties include the matters to which the Biometric Data relates).

3. Electronic Security

Biometric Data in electronic form (*e.g.*, e-mail, databases, and computer files containing Biometric Data) must be maintained and stored in a secure manner by the Company. Electronic Transmissions containing Biometric Data must, to the extent reasonably possible, be protected to prevent interception by parties other than the intended recipient, or access by unauthorized users. Biometric Data maintained, stored, or transmitted by the Company is also subject to the Company's Information Security Policy.

F. <u>Data Subject's Rights</u>. Individuals have rights when it comes to how their Biometric Data is handled. These rights may vary depending on the applicable jurisdiction, but may include for example:

- the right to know what Biometric Data the Company has collected and maintains about the individual and/or with whom the Company has shared the Biometric Data;
- the right to access the Biometric Data; or
- a right to deletion or restriction of the Biometric Data.

You must comply with applicable laws regarding the rights of Data Subjects. If you are unsure of the applicable legal requirements, or if you receive a request or complaint from a Data Subject regarding the handling of his or her Biometric Data, please contact the Privacy Officer.

G. Retention and Disposal. You should keep Biometric Data only for the amount of time it is needed to fulfill the legitimate business purpose for which it was collected or to satisfy a legal requirement. In any event, Biometric Data shall be destroyed on or before the earlier of the date the initial purpose for collecting Biometric Data has been satisfied or within three (3) years of the last interaction with the individual from whom Biometric Data was collected by Company. In Texas or other jurisdiction with more stringent rules relating to dates of destruction, such more stringent guidelines shall apply.

Biometric Data shall be destroyed consistent with Company's information destruction policy. In any event, Biometric Data shall be permanently purged from equipment and devices such as fingerprint machines. Data printouts shall be shredded and disposed of securely and permanently, subject only to a log record reflecting destruction of the data.

H. Lawfulness. Company shall not sell, lease, trade, or otherwise profit from a person's or a customer's Biometric Data. Company may only disclose Biometric Data consistent with lawful basis including based upon consent, to comply with a subpoena or as otherwise required by State or federal law or municipal ordinance. Company has a legitimate purpose to collect Biometric Data: to conduct or facilitate on behalf of employees legally required background screenings to obtain a security license or permit and/or badge or access credential to a secured area.

IV. Training Employees and Supervising Contractors

All Company personnel who have access to Biometric Data must be educated and trained on this Policy and the treatment of Biometric Data. In addition, Biometric Data is entrusted to a Third-Party Service Provider, proper management and supervision over the outside party's handling of that Biometric Data must be ensured through appropriate contracts. Personnel with responsibility for supervising employees or managing Third-Party Service Provider relationships must be trained on supervision over those employees and Third-Party Service Providers.

V. Reporting a Data Breach

If you know or suspect that a Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the legal department and follow the Security Incident Response Plan. You should preserve all evidence relating to the potential Data Breach.

VI. Monitoring Compliance and Enforcement

Everyone who works for or with Company has some responsibility for ensuring data is collected, stored and handled appropriately. Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, the following people have key areas of responsibility:

- The **Privacy Officer, <u>James Stephenson</u>,** is responsible for:

  - Keeping the board updated about data protection responsibilities, risks and issues.
  - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
  - Arranging data protection training and advice for the people covered by this policy.
  - Handling data protection questions from staff and anyone else covered by this policy.
  - Dealing with requests from individuals to see the data Company holds about them (also called 'subject access requests').
  - Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

- The **IT Manager, <u>Jeff McClain</u>,** is responsible for:

  - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
  - Performing regular checks and scans to ensure security hardware and software is functioning properly.
  - Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.

The Privacy Officer is responsible for administering and overseeing implementation of this Policy and, as applicable, developing related operating procedures, processes, policies, notices, and guidelines. If you are concerned that any provision of this Policy, or any related policy, operating procedure, process, or guideline designed to protect Biometric Data, has been or is being violated, please contact the Privacy Officer. The Company will conduct periodic reviews and audits to assess compliance with this Policy. Employees who violate this Policy and any related guidelines, operating procedures, or processes designed to protect Biometric Data and implement this Policy may be subject to discipline.

VII. <u>Related Policies</u>

Other Company policies also apply to the collection, use, storage, protection, and handling of Biometric Data and may be relevant to implementing this Policy. You should familiarize yourself with these policies, including:

- Information Security Policy.
- Document Retention Policy.
- Personal Information Protection Policy
- HIPAA Privacy and Security Policies

VIII. Amendment and Revision

This Policy may be revised from time to time. This Policy was last revised on March 14, 2019.

ANDY FRAIN
est. 1924
SERVICES®

Livescan Consent to Release of Biometric Data (Livescan Fingerprints)

I, _____ (employee), acknowledge and consent that I have been informed that Andy Frain Services, Inc. intends to collect or obtain my fingerprints for the purpose of submitting on my behalf a background investigation required to obtain my security officer's license or access badge to a secured area and that my fingerprints will be retained by Andy Frain Services, Inc. for a sufficient amount of time to allow the applicable licensing or badging agency to verify my criminal history record information files of the Illinois State Police (ISP) and/or the Federal Bureau of Investigation (FBI).

I understand and consent to my fingerprints being transmitted electronically through the Livescan or similar fingerprinting equipment to the ISP and/or the FBI for purposes of completing the background screening required by law. I understand that my fingerprints will be retained by Andy Frain Services, Inc. for the purposes set forth in this Privacy Notice and will subsequently be destroyed by Andy Frain Services, Inc. once the purpose of their collection has been satisfied, but in any event no later than three (3) years from the date of collection. I hereby authorize the release of my fingerprints and biometric information and further authorize the release of any criminal history record information that may be collected or obtained regarding me from any agency, organization, institution, or entity having such information on file. In addition, I authorize my photo to be taken, submitted to the ISP and/or FBI; photographic images may be shared for licensing and employment purposes only.) I further understand that I have the right to challenge any state or federal criminal history record information disseminated from these criminal justice agencies regarding me that may be inaccurate or incomplete.

Office Location of Activity: _____

Agency ORI Number: **__IL920020Z_____**

Purpose Code: **___SEC_____**

APPLICANT NAME: _____
Last First Initail Please print.

ADDRESS: _____

SSN: _____

DOB: _____

TELEPHONE NUMBER: _____

DRIVER'S LICENSE OR STATE ID#: _____

Date/Time/Location of Activity: _____

Applicant Signature: _____

Technician: _E. Millard_____

LiveScan TCN#: _LS_____

Photo ID Provided: YES _____ NO _____

LiveScan Agency License: 262.000032
Andy Frain Services
761 Shoreline Drive
Aurora, Il 60504
630-820-3820

Additional Information Required:

Are you a US Citizen _____ If No, what country are you a citizen of _____

What US state or Country were you born in _____

Sex _____

Race _____

Hair Color _____

Eye Color _____

Height _____

Weight _____

_____
Name: _____
Dated: _____

ANDY FRAIN
est. 1924
SERVICES®

BIOMETRIC INFORMATION CONSENT AND RELEASE

Andy Frain Services, Inc. ("Company") now offers Livescan fingerprint submission for employees wishing to electronically submit their fingerprints for purposes of obtaining a security license. Employee hereby acknowledges he or she has received Company's Privacy Notice regarding biometric information, has been informed of Company's practices concerning biometric information and consents to such collection, storage and use as follows:

1. Employee acknowledges that state licensing law and regulations require or permit Company to conduct a criminal background investigation on employees seeking to be licensed by state law to provide security services.

2. Employee further acknowledges that state licensing law and regulations require or permit Employee to submit his or her fingerprints electronically for purposes of allowing the state to conduct its own criminal background investigation as a condition precedent to issuing a security license.

3. Employee further acknowledges that some states permit the Company to assist Employee with the collection and submission to the applicable state agency of Employee's fingerprints.

4. Employee acknowledges that the Company intends to or may collect or obtain Employee's fingerprints and Employee consents to such collection and storage for the purpose of submitting on Employee's behalf a request to the state or other agency to conduct a criminal background investigation required in order to obtain either a security officer's license or an access badge to a secured area. Employee acknowledges and consents that Employee's fingerprints will be retained by Company on the Livescan machine for a sufficient amount of time to allow the applicable licensing or badging agency to verify Employee's criminal history record information files maintained by the state agency and/or the Federal Bureau of Investigation (FBI).

5. Employee consents to, specifically requests Company to transmit on Employee's behalf and releases Company to transmit Employee's fingerprints electronically through the Livescan machine or similar fingerprinting equipment and technology to the applicable state agency and/or the FBI for purposes of completing the criminal background screening required by law. Employee understands that his or her fingerprints will be retained by the Company for the purposes above and will subsequently be destroyed by the Company once the purpose of their collection has been satisfied, but in any event no later than three (3) years from the date of collection in the State of Illinois and no later than one (1) year from the date of collection in the State of Texas.

6. Employee hereby authorizes the release of his or her fingerprints and further authorizes the

release of any criminal history record information that may be collected or obtained from any agency, organization, institution, or entity having such information on file.

7. In addition, Employee authorizes his or her photo to be taken and submitted to the applicable agency and/or FBI; photographic images may be shared for licensing and employment purposes only. Employee further understands that he or she will have the right to challenge any state or federal criminal history record information disseminated from these criminal justice agencies that may be inaccurate or incomplete.

8. Employee's biometric data will not be disclosed by the Company without Employee's consent unless disclosure is permitted by applicable law. Employee's biometric data will be permanently deleted from the Livescan machine within a reasonable time after the return of Employee's credentials.

9. Employee acknowledges he or she has received, reviewed and understands Andy Frain Services' Privacy Notice – Biometric Data.

10. By signing this form, Employee consents to the collection, storage and use of biometric information as set forth in Andy Frain's Privacy Notice and in this Consent and Release, and Employee agrees that Company may use and hereby releases Employee's biometric information to be used solely for purposes of submitting Employee's criminal background investigation and applying for a security license or access credential.

11. Employee understand that he or she may revoke this consent in writing prior to Employee's submission of fingerprints. Thereafter, Employee may still revoke this consent, provided, however, Employee acknowledges that his or her fingerprints will already have been submitted to the state and/or FBI.

_____

EMPLOYEE NAME - PRINTED

_____ _____

SIGNATURE **DATE**