

Biometric Information Privacy Policy

A-Karrasel (“Company”) has instituted the following biometric information privacy policy. This Policy replaces and supersedes all previous policies related to biometric information. The Company reserves the right to amend this Policy at any time, without notice. The Company may expand its use of biometric data in the future. In the event the Company begins collecting biometric data for any additional purpose, the Company will update this Policy.

A copy of this document will be made available to the public at <https://www.akarrasel.com/employee-resources/>.

Biometric Data Defined

As used in this policy, biometric data includes “biometric identifiers” and “biometric information” as defined in the Illinois Biometric Information Privacy Act, 740 ILCS § 14/1, et seq.

- “Biometric identifier” means 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 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 information” means any information, regardless of how it is captured, converted, stored, or shared, based on an individual’s biometric identifier used to identify an individual. Biometric information does not include information derived from items or procedures excluded under the definition of biometric identifier.

Purpose for Collection of Biometric Data

The Company, through its vendor/licensor (Procare Software) utilizes the 8inch Procare Touch System to collect, store, and use biometric data solely for timekeeping and attendance purposes..

The Company will not sell, lease, trade, or otherwise profit from employees’ biometric data.

The Company’s policy is to protect and store biometric data in accordance with applicable standards and laws including, but not limited to, the Illinois Biometric Information Privacy Act.

Collection of Biometric Data Procedures

Prior to collecting an employee’s biometric data, the Company will obtain the consent of the employee. The Company will inform the employee of the reason his or her biometric information is being collected and the length of time the data will be stored.

Biometric timeclocks are computer-based systems that scan an employee’s finger for purposes of identification. The computer system extracts unique data points and creates a unique mathematical representation used to verify the employee’s identity, for example, when the employee arrives at or

departs from the workplace. The biometric data itself is not recorded or stored, and cannot be regenerated from the digital data.

Disclosure

The Company uses the 8inch Procure Touch System through Procure Software in order to capture an employee's time and attendance. Any biometric data contained in the 8inch Procure Touch System will not be disclosed or disseminated without/unless:

- a. First obtaining written employee consent to such disclosure or dissemination;
- b. The disclosed data completes a financial transaction requested or authorized by the employee;
- c. Disclosure is required by state or federal law or municipal ordinance; or
- d. Disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

Retention Schedule

The Company shall retain employee biometric data only until and shall request that its vendors and the licensor of the Company's time and attendance software permanently destroy such data when, the first of the following occurs:

- The initial purpose for collecting or obtaining such biometric data has been satisfied, such as the termination of the employee's employment with the Company, or
- Within 3 years of the employee's last interaction with the Company.

Data Storage

The Company shall use a reasonable standard of care to store, transmit and protect from disclosure any paper or electronic biometric data collected. Such storage, transmission, and protection from disclosure shall be performed in a manner that is the same as or more protective than the manner in which the Company stores, transmits and protects from disclosure other confidential and sensitive information, including personal information that can be used to uniquely identify an individual or an individual's account or property, such as genetic markers, genetic testing information, account numbers, PINs, driver's license numbers and social security numbers.

Biometric Information Privacy Policy Acknowledgement and Consent

The employee named below has been advised and understands that A- Karrasel (“Company”), through its time and attendance software will collect, retain, and use biometric data for the purpose of identifying employees and recording time entries when utilizing the Company’s biometric timeclocks or timeclock attachments.

I have read the Company’s Biometric Information Privacy Policy and understand that my fingerprint data will not be disclosed by the Company without my consent unless the disclosure is required by law or by valid legal subpoena.

Your fingerprint data will be permanently deleted from the Company’s systems within a reasonable period after your termination of employment pursuant to the Company’s Biometric Information Privacy Policy. A copy of the Company’s Biometric Information Privacy Policy is available upon request and is posted at: <https://www.akarrasel.com/employee-resources/>.

The employee understands that he or she is free to decline to provide biometric identifiers and biometric information to the Company for use of the Company’s time and attendance software without any adverse employment action. The employee may revoke this consent at any time by notifying the Company in writing.

The undersigned employee acknowledges that he/she has received the attached Biometric Information Privacy Policy, and that he/she voluntarily consents to the Company’s software’s collection, storage, and use of biometric data through a biometric timeclock for time and attendance purposes, including to the extent that it utilizes the employee’s biometric identifiers or biometric information as defined in the Illinois Biometric Information Privacy Act.

Employee Signature Date

Employee Name (print)