BIOMETRIC INFORMATION PRIVACY POLICY

In select locations, **[Proman Staffing LLC]**, including its subsidiaries, parent companies, and affiliated entities (the "Company"), has used a timekeeping system by which certain non-exempt employees/workers used their fingers, hands, and/or faces to clock in and out of work or otherwise record their hours worked. This policy outlines the collection, use and storage of the data and information utilized by the timekeeping system to the extent that the timekeeping system is regulated by the Illinois Biometric Information Privacy Act, 740 ILCS 14/1 *et seq*. ("BIPA"), the Texas Capture or Use of Biometric Identifier Act ("CUBIA"), Tex. Bus. & Com. Code Ann. § 503.001 *et seq*., the Washington House Bill 1493, Wash. Rev. Code Ann. § 5031.010 *et seq*., the California Consumer Privacy Act ("CCPA"), Cal. Civ. Code § 1798.100 *et seq.*, or any other state or federal law that regulates the use and collection of biometrics, whether that law is enacted at the time this Policy is implemented or whether the law is enacted after this Policy is implemented.

Biometric Identifiers and Information Defined ("Biometric Data")

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 set*. "Biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. "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 BIPA's definition of biometric identifiers.

Biometric Data also includes "biometric identifier" as defined in Washington House Bill 1493, Wash. Rev. Code Ann. § 5031.010 *et seq.* as "data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify specific individuals" regardless of how it is captured or stored. Biometric Data does not include information or data excluded from te definition of "biometric identifier" under Wash. Rev. Code Ann. § 5031.010 *et seq.*

Biometric Data also includes "biometric identifier" as defined in the CUBIA, Tex. Bus. & Com. Code Ann. § 503.001 *et seq*. as "a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry" collected for a "commercial purpose."

Biometric Data also includes "biometric information" as defined in the CCPA, Cal. Civ. Code § 1798.140 *et seq.* as "an individual's physiological, biological, or behavioral characteristics, including an individual's deoxyribonucleic acid ("DNA"), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health or exercise data that contain identifying information."

Biometric Data also includes any definition of "biometric identifier," "biometric information," or definition of "biometric(s)" under any other state or federal law.

Purpose for Collection of Biometric Data

To the extent the timekeeping system is regulated by BIPA, CUBIA, Washington House Bill 1493, CCPA, or any other state or federal law that regulates biometrics, the Company, its vendors, and/or the licensor of the Company's time and attendance software collect, store, and use Biometric Data for employee/worker identification, timekeeping, payroll, fraud prevention, and pre-employment hiring purposes.

Informed Consent and Authorization

To the extent that the Company, its vendors, and/or the licensor of the Company's time and attendance software collect, capture, store or otherwise obtain Biometric Data relating to an employee/worker, the Company is:

a. Informing the employee/worker in writing that the Company, its vendors, and/or the licensor of the Company's time and attendance software may be collecting, capturing, storing or otherwise obtaining the employee/worker's Biometric Data, and that same may be provided to its vendors and the licensor of the company's time and attendance software for the purposes stated in this policy;

b. Informing the employee/worker in writing of the specific purpose and length of time for which the employee/worker's Biometric Data is being collected, stored, and used; and

c. Requesting and obtaining a written release signed by the employee/worker (or his or her legally authorized representative) authorizing the Company, its vendors, and/or the licensor of the Company's time and attendance software to collect, store, and use the employee/worker's Biometric Data for the specific purposes disclosed by the Company, and for the Company to provide such Biometric Data to its vendors and the licensor of the company's time and attendance software.

The Company, its vendors, and/or the licensor of the Company's time and attendance software will not sell, lease, trade, or otherwise profit from Biometric Data that may be collected, stored, or obtained other than to the extent that the Company's vendors and the licensor of the Company's time and attendance software are paid for products or services used by the Company in the ordinary course of business.

Disclosure

Other than as set forth in this Policy, the Company will not disclose or disseminate any Biometric Data to anyone other than its vendors and the licensor of the Company's time and attendance software providing products and services without first obtaining written employee/worker consent to such disclosure or dissemination unless:

a. The disclosed data completes a financial transaction requested or authorized by the employee/worker;

b. Disclosure is required by state or federal law or municipal ordinance; or

c. Disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

Retention Schedule

The Company shall retain any Biometric Data obtained from an employee/worker only until the first of the following occurs:

- The initial purpose for collecting or obtaining any Biometric Data has been satisfied, such as the termination of the employee/worker's employment with the Company; or
- Within 3 years of the employee/worker's last interaction with the Company; or
- Within the first anniversary of the date the purpose for collecting the Biometric Data expires;

The Company also shall request that its vendors and the licensor of the Company's time and attendance software permanently destroy such data on the same Retention Schedule.

Protection from Disclosure

The Company shall use a reasonable standard of care in the industry to store, transmit and protect from disclosure any Biometric Data. 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.

A copy of this Policy is publicly available upon request from Human Resources hr@promanstaffing.com and is also available at https://www.promanstaffing.com/privacy-policy/.