PACESETTER'S BIOMETRIC INFORMATION PRIVACY POLICY

Pacesetter Steel Service, Inc. (the "Company") has instituted the following policy related to any and all biometric data that the Company collects, stores, uses, and/or transmits in connection with the Company's operations.

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 identifiers.

Purpose for Collection of Biometric Data

The Company and/or its vendors (including the licensor of Company's time, attendance, and payroll software) collect, store, use, and/or transmit biometric data in connection with the Company's operations, including for the purposes of pre-employment hiring matters, identifying employees, recording employee time and attendance, identity verification, workplace security, and fraud prevention.

Authorization

To the extent that the Company and/or its vendors collect, capture, use, or otherwise obtain biometric data relating to an employee, the Company will first:

- Inform the employee in writing that the Company and/or its vendors are collecting, capturing, or otherwise obtaining the employee's biometric data, and that the Company may provide such biometric data to its vendors;
- Inform the employee in writing of the specific purpose and length of time for which the employee's biometric data is being collected, stored, and used; and
- Receive a written release signed by the employee (or his or her legally authorized representative) authorizing the Company and/or its vendors to collect, store, and/or use the employee's biometric data for the specific purposes disclosed by the Company, and for the Company to provide such biometric data to its vendors.

The Company and/or its vendors will not sell, lease, trade, or otherwise profit from employees' biometric data; provided, however, that the Company may pay its vendors for products and services used by the Company that utilize such biometric information.

Disclosure

The Company will not disclose or disseminate any biometric data to anyone other than its vendors without/unless:

- The subject of the biometric data or the subject's legally authorized representative consents to the disclosure or dissemination;
- The disclosure or dissemination completes a financial transaction requested or authorized by the subject of the biometric data or the subject's legally authorized representative;
- The disclosure or dissemination is required by State or federal law or municipal ordinance; or
- The disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

Retention Schedule

The Company will retain employee biometric data only until, and will request that its vendors 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 the employee moves to a role within the Company for which the biometric data is not used; or
- Within 3 years of the employee's last interaction with the Company.

Data Storage

The Company will store, transmit, and protect biometric data using a reasonable standard of care. Such storage, transmission, and protection from disclosure will 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 of the Company and its employees, 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 confirmation, account numbers, PINs, driver's license numbers, and social security numbers.