Biometric Information Privacy Policy

Chicago Magnesium Casting Company (the "Company") has instituted the following biometric information privacy policy:

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 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.

"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, its vendors, and/or the licensor of the Company's time and attendance software may collect, store, and use biometric data solely for employee identification, fraud prevention, and pre-employment hiring purposes.

Disclosure and Authorization

To the extent that the Company, its vendors, and/or the licensor of the Company's time and attendance software collect, capture, or otherwise obtain biometric data relating to an employee, the Company must first:

a. Inform the employee in writing that the Company, its vendors, and/or the licensor of the Company's time and attendance software are collecting, capturing, or otherwise obtaining the employee's biometric data, and that the Company may provide such biometric data to its vendors and the licensor of the Company's time and attendance software;

b. 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

c. Receive a written release signed by the employee (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'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 employees' biometric data; provided, however, that the Company's vendors and the licensor of the Company's time and attendance software may be paid for products or services used by the Company that utilize such biometric data.

Disclosure

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 using biometric data 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 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.

Notwithstanding the foregoing, the Company shall retain employee biometric data beyond the foregoing time period where required to do so by a valid warrant or subpoena issued by a court of competent jurisdiction.

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.