The Timken Company
Biometric Data Privacy Policy

Policy Authority: The Global Data Privacy Office has authority and is responsible for any and all amendments or changes to this Policy. Final interpretation of this Policy will be by the General Counsel or his/her appointee.

Purpose: The purpose of this policy is to define the policy and procedures for the collection, use, safeguarding, storage, retention, and destruction of Biometric Data in compliance with all applicable laws, including, but not limited to, the Illinois Biometric Information Privacy Act (BIPA)

Scope: This policy applies to all employees and contractors of the Company and its subsidiaries.

Policy Statement: It is the policy of The Timken Company (the "Company) to protect, use and store Biometric Data in accordance with applicable laws including, but not limited to, the Illinois Biometric Information Privacy Act. This policy outlines the procedures for the collection, use, safeguarding, storage, retention, and destruction of Biometric Data gathered by or associated with the system(s) utilized by Company.

Procedure: The Company, directly or indirectly, through vendors or licensees may use or utilize Biometric Data for the purposes of access to premises, areas, or computer systems, participation in events or programs and other similar purposes. The Company, its vendors or licensees may disclose Biometric Data to vendors who provide software or services supporting this purpose. The Company will not otherwise disclose Biometric Data unless a) specific consent is obtained, b) disclosure is required by law, or c) disclosure is required by a valid warrant or subpoena. The Company will not sell lease, trade, or otherwise profit from an employee's Biometric Data. The Company will destroy any employee Biometric Data within a reasonable time, not to exceed three years, from the effective date of a employee's resignation, retirement, or termination from the Company. The Company and its vendors protect the Biometric Data gathered in compliance with applicable laws and will protect it in the same manner that it stores, transmits, and protects its own confidential and sensitive information.

The Company will obtain written consent when and where such consent is required under applicable law, including existing employees and new employees.

Exceptions: Jurisdiction-Specific or Local Law Requirements: This Policy is subject to applicable local law restrictions, which may vary from the provisions contained herein. Please refer to any jurisdiction-specific / local law addendums attached to this Policy that modify the application of this Policy in your local jurisdiction. Contact your local legal representative for questions about applicability in your local jurisdiction.

Violations: Violations of this Policy may result in disciplinary action, up to and including discharge, for employees. For non-employees, violations can result in contract termination and other remedies

Defined Terms and Acronyms:

> **Biometric Identifiers:** 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 scientific testing or screening, demographic data, tattoo

descriptions, or physical descriptions. 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 ("HIPAA").

Biometric Information: Any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identity used to identify an individual. Biometric information does not include information derived from items or procedures excluded under the definition of Biometric Identifiers.

Biometric Data: Includes both Biometric Identifiers and Biometric Information.