



Policy Information Security Policy/Employee Handbook, Section 5-23

DATE November 18, 2021

Updated September 1, 2024

Part 4 Written Notice Regarding the Collection and Use of Biometric Data

1. **Introduction.** Southshore Enterprises, Inc., Southshore Distribution, LLC, and United Container Co. (hereinafter referred to as “the Company”) has instituted the following policy related to any biometric data that the Company processes during the ordinary course of business operations.
2. **Purpose.**
 - 2.1. To ensure that all biometric data that is collected, stored, used, or transmitted by the Company is protected, stored, used, and deleted in accordance with all applicable laws and regulations, including, but not limited to, the Illinois Biometric Privacy Act, 740 ILCS § 14/1, et seq.
3. **Scope.**
 - 3.1. This Policy applies to all Company employees, temporary workers, and independent contractors. Additionally, this Policy applies to all persons who enter onto Company premises and to anyone who has access to biometric data on behalf of the Company.
 - 3.2. The policy applies to all biometric data collected, maintained, transmitted, stored, retained, or otherwise used by the Company, regardless of the form of media on which the information is stored.
 - 3.3. Because protecting the confidentiality and integrity of biometric data is a critical responsibility that must be taken seriously at all times, compliance with this policy is mandatory.
4. **Policy.**
 - 4.1. 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.

- a. “Biometric identifier” means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry.
- b. “Biometric information” means any information, regardless of how it is captured, converted, stored, or transmitted, based on an individual’s biometric identifier used to identify an individual.
- c. “Biometric data” also includes any similar state or local law definitions related to any biological characteristics of a person, or information based upon such a characteristic, including but not limited to, “biometric identifier” as defined under Tex. Bus. & Com. Code §503.001, “biometric identifier” as used in Wash. Rev. Code Ann. §19.375.020, “biometric information” as used in the California Consumer Privacy Act, “biometric information” as used in the New York Stop Hacks and Improve Electronic Data Security Act, and “biometric data” as used in Arkansas Code §4-110-103.

- 4.2. Purpose for Collection of Biometric Data. The Company and its service providers (for example, its security camera provider, payroll provider, connected-operations platform provider, or temporary staffing agency) may collect, store, use, and transmit biometric data during the ordinary course of Company business. Prior to the collection, storage, use, or sharing of any such data, the Company will obtain written consent from each person whose data is to be collected, used, stored, or transmitted.

The Company and its service providers will collect, store, use, and transmit biometric data strictly for the purposes of identity verification, workplace security, fraud prevention, and safety enhancement. Neither the Company nor its service providers will sell, lease, or trade any biometric data collected.

- 4.3. The Use of Two-Way Dash Cam Technology. The Company employs two-way dash cam technology to collect video recordings for the purposes of ensuring the safety of our drivers, enhancing the security of cargo, and preventing fraudulent activities. The recordings obtained through the use of this technology are a type of biometric data. As such, they are collected, stored, used, and transmitted in strict accordance with the requirements of this policy.

To ensure compliance with the highest standards for collection, storage, use, transmission, and deletion of the data collected through dual dash cam technologies, the Company has partnered with Samsara, a third-party vendor. Samsara is recognized as a best-in-class provider of fleet-management support services with a proven track record of adherence to the industry’s highest standards for protection of biometric data. Specifically, Samsara ensures that biometric data is protected by limiting the amount of data it collects, encrypting that data prior to transmission, and storing the encrypted data on a secure cloud storage service. To read Samsara’s full data security policy, visit: <https://www.samsara.com/legal/security>.

- 4.4. Retention Schedule. The Company will only retain biometric data until either the initial purpose for collecting or obtaining the data has been satisfied or three (3) years have passed since the Company's last interaction with the individual whose biometric data has been retained, whichever comes first.
- 4.5. Data Storage. The Company will use a reasonable standard of care to store, transmit, and protect from disclosure any biometric data collected. 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, including personal information that can be used to uniquely identify an individual or an individual's account or property, such as account numbers, PINs, driver's license numbers, and social security numbers. Additionally, the Company will limit the number of persons who have access to any biometric data to only those persons who have a legitimate need to access such data, and it will instruct those persons on the importance of proper storage, transmission, and protection of biometric data.
- 4.6. Destruction of Data. Upon the conclusion of the retention period, or at the request of the individual whose biometric data has been collected, all biometric data will be permanently deleted using methods that ensure the data cannot be recovered or reconstructed.

5. Procedure.

- 5.1. Authorization. To the extent that the Company or its service providers collect, capture, or otherwise obtain biometric data relating to any person, the Company will first:
 - a. Inform the person in writing that the Company or its service providers are collecting, capturing, or otherwise obtaining the person's biometric data;
 - b. Inform the person in writing of the specific purpose and length of time for which the biometric data is being collected, stored, and used; and
 - c. Receive a written release signed by the person (or his or her legally authorized representative) authorizing the Company and its service providers to collect, store, and use the person's biometric data for the specific purposes disclosed by the Company and for the Company to provide such biometric data to its service providers.
 - d. Inform the person consenting to the collection, storage, use, and sharing of biometric data that he or she may withdraw consent to such collection, storage, use, and sharing at any time.

The Company and its service providers will not sell, lease, trade, or otherwise profit from employees' biometric data.

5.2. Disclosure. The Company will not disclose or disseminate any biometric data to anyone other than its authorized service providers unless:

- a. the subject of the biometric data or the subject's legally authorized representative consents to the disclosure or dissemination;
- b. 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;
- c. the disclosure or dissemination is required by state or federal law or municipal ordinance; or
- d. the disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

6. **Effective Date.** This Policy is effective as of November 18, 2021.

6.1. Revision History: November 18, 2021

6.2. Revision History: September 1, 2024

Biometric Information Privacy Employee Consent Form

By signing below, you acknowledge and agree to the following:

Southshore Enterprises, Inc., Southshore Distribution, LLC, and United Container Co. (hereinafter referred to as “the Company”) and its service providers will collect, capture, receive, or acquire one or more of the following biometric identifiers about you (collectively referred to as “your Biometric Data”): a retina or iris scan, a fingerprint, a voiceprint, a scan of hand or face geometry, or any other unique information regarding a biological pattern or characteristic that can be used to identify a specific individual.

The Company may collect, store, use, and transmit your Biometric Data for the purpose of identity verification, workplace security, fraud prevention, and safety enhancement (collectively, “Permitted Purposes”). As way of example, some of the Permitted Purposes include the following. The Company has an internal CCTV system that may capture your face geometry that is provided and monitored by the Company’s service providers. Moreover, the Company and its service providers collect, retain, and use biometric data for the purpose of recording time entries when utilizing the Company’s biometric timeclocks or timeclock attachments. Biometric timeclocks are computer-based systems that scan an employee’s finger for purposes of identification. Finally, the Company uses two-way dash cam technology for the purposes of ensuring driver safety, enhancing the security of cargo, and preventing fraudulent activities.

The Company may retain your Biometric Data for as long as is necessary for the Permitted Purposes, but in no case for longer than three years after your last interaction with the Company.

You have received and read the following three documents: the *Written Notice Regarding the Collection and Use of Biometric Data*, the *Dash Cam Policy and Procedures*, and the *Data Privacy and Security Policies Consent Acknowledgment*. You understand that you are voluntarily consenting to the collection, storage, use, and transmission of your Biometric Data.

You understand that you are free to decline to provide your Biometric Data to the Company. You also understand that you may revoke this consent at any time by notifying the Company in writing.

Employee/Individual Signature

Printed Name

Date