Sample Biometric Policy

*This document should be reviewed and approved by your legal council.

Biometric Information Privacy Policy

(Company) has adopted the following biometric information privacy policy:

Definitions

"Biometric Data", including biometric identifiers and biometric information, means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry, regardless of how it is captured, converted, stored, or shared, which is used to identify an individual.

Purpose for Collection of Biometric Data

(Company) and the vendor of (Company)'s time and attendance software collect, store, and use biometric data solely for employee identification and fraud prevention purposes.

Disclosure and Authorization

To the extent that (Company) and the vendor of (Company)'s time and attendance software collect, capture, or otherwise obtain biometric data relating to an employee, (Company) must first:

a. Inform the employee in writing that (Company) and the vendor of (Company)'s time and attendance software are collecting, capturing, or otherwise obtaining the employee's biometric data, and that (Company) is providing such biometric data to the vendor of (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 (Company) and the vendor of (Company)'s time and attendance software to collect, store, and use the employee's biometric data for the specific purposes disclosed by (Company), and for (Company) to provide such biometric data to the vendorsand the licensor of (Company)'s time and attendance software

(Company) and the vendors of (Company)'s time and attendance software will not sell, lease, trade, or otherwise profit from employees' biometric data; provided, however, that (Company)'s vendor of (Company)'s time and attendance software may be paid for products or services used by (Company) that utilize such biometric data.

Disclosure

(Company) will not disclose or disseminate any biometric data to anyone other than the vendor of (Company)'s time and attendance software 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

(Company) shall retain employee biometric data only until, and shall request that the vendor of (Company)'s time and attendance software permanently destroy such data when, the first of the following occurs:

a. The initial purpose for collecting or obtaining such biometric data has been satisfied, such as the termination of the employee's employment with (Company), or the employee moves to a role within (Company) for which the biometric data is not used; or

b. Within 1 year of the employee's last interaction with (Company).

Data Storage

(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 (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.

Acknowledgement

(Company) will not disclose or disseminate any biometric data to anyone other than the vendor of (Company)'s time The employee named below has been advised and understands that (Company) and the vendor of (Company)'s time and attendance software collect, retain, and use biometric data for the purpose of identifying employees and recording time entries when utilizing (Company)'s biometric timeclocks or timeclock attachments. Biometric timeclocks are computer-based systems that scan an employee's finger for purposes of identification. The computer system extracts unique data points and creates a unique mathematical representation used to verify the employee's identity, for example, when the employee arrives at or departs from the workplace.

Both State and Federal statutes regulate the collection, storage, use, and retention of "biometric identifiers" and "biometric information." "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.

The employee understands that he or she is free to decline to provide biometric identifiers and biometric information to (Company) and the vendor of (Company)'s time and attendance software without any adverse employment action. The employee may revoke this consent at any time by notifying (Company) in writing.

The undersigned employee acknowledges that he or she has received this Biometric Information Privacy Policy, and that he or she voluntarily consents to (Company)'s and the vendor of (Company)'s time and attendance software to collect, store, and use his or her biometric data through a biometric timeclock, including to the extent that it utilizes the employee's biometric identifiers or biometric information as defined in applicable biometric privacy regulations, and voluntarily consents to (Company) providing such biometric data to the vendor of (Company)'s time and attendance software.

Employee Signature Date

Employee Name (Print)