

## **BIOMETRIC INFORMATION PRIVACY POLICY**

Sound Seal, Inc. (the “Company”) has instituted this biometric information privacy policy to govern the collection, use, storage and retention of biometric data. It is the Company’s policy to collect, use, store and retain biometric data in accordance with applicable laws, including but not limited to, the Illinois Biometric Information Privacy Act. The Company reserves the right to amend this policy at any time.

### **Biometric Data Defined**

As used in this policy, biometric data includes “biometric identifiers” and “biometric information.”

“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, its vendors, and/or the licensors of the Company’s time and attendance software collect, store, and use biometric data for the purpose of identifying employees and recording time entries through biometric time clocks or time clock attachments.

### **Disclosure and Authorization**

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

- a. will 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 is providing such biometric data to its vendors and the licensors of the Company’s time and attendance software;
- b. will 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;

- c. will receive a written release signed by the employee (or his or her legally authorized representative) authorizing the Company, its vendors, and/or the licensors 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 licensors of the Company's time and attendance software; and
- d. will not disclose or otherwise disseminate any biometric data to anyone other than its vendors and the licensors of the Company's time and attendance software providing products and services using biometric data unless:
  - i. the employee (or his or her legally authorized representative) consents to such disclosure;
  - ii. the disclosure completes a financial transaction requested or authorized by the employee (or his or her legally authorized representative);
  - iii. the disclosure is required by state or federal law or municipal ordinance; or
  - iv. the disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

The Company, its vendors, and/or the licensors 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.

### **Retention Schedule**

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

### **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 of the Company and its employees.

\* \* \* \*

## BIOMETRIC INFORMATION PRIVACY CONSENT FORM

The employee named below has been advised and understands that Sound Seal, Inc. (the “Company”), its vendors, and/or the licensors of the Company’s time and attendance software collect, use, store, and retain biometric data for the purpose of identifying employees and recording time entries through biometric time clocks or time clock attachments. Biometric time clocks 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.

The Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.* (“BIPA”), regulates the collection, use, storage 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 the Company, its vendors, and/or the licensors of the Company’s time and attendance software but that agreeing to provide such biometric identifiers and information is a condition of employment. The employee may revoke this consent at any time by notifying the Company in writing, but doing so will preclude employment by the Company.

The undersigned employee acknowledges that he/she has received the attached *Biometric Information Privacy Policy*, and that he/she voluntarily consents to the Company’s, its vendors’, and/or the licensors of the Company’s time and attendance software’s collection, use, storage, and retention of biometric data in connection with the use of biometric time clocks in accordance with the attached *Biometric Information Privacy Policy*, including to the extent that it utilizes the employee’s biometric identifiers or biometric information as defined in BIPA, and voluntarily consents to the Company providing such biometric data to its vendors, and/or the licensors of the Company’s time and attendance software.

---

Name of Employee

---

Signature of Employee

---

Date