Biometric Information and Security Policy

Policy Statement and Purpose

This Biometric Information and Security Policy ("Policy") summarizes Sunbelt Rentals, Inc.'s ("Sunbelt") policy and procedures for the collection, use, safeguarding, storage, retention, and destruction of Biometric Information and Data ("Biometric Data") collected by Sunbelt and/or its vendors in accordance with Illinois Biometric Privacy Act, 740 ILCS § 14/1, *et seq*., and other laws and regulations. Sunbelt recognizes the sensitivity of Biometric Data and takes seriously its obligations to maintain the confidentiality and security of such data.

Sunbelt uses a Biometric Identifier, specifically a fingerprint, for team member timekeeping. Sunbelt and/or its vendor(s) collects, stores, and uses team member Biometric Information and Data for the purposes of granting team members access to Sunbelt's timekeeping systems and to document team members' clock in/out time(s).

Definitions

As used in this policy, Biometric Data includes but is not limited to "biometric identifiers" and "biometric information" as defined in the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq*.

- **Biometric Identifier.** A fingerprint, voiceprint, retina or iris scan, hand or face geometry scan. 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 Information or Biometric Data.** 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.

Collection of Biometric Data

Sunbelt, in some instances, may collect, store and use Biometric Data for purposes of identifying team members for payroll, security, access, or other purposes. The biometric equipment measure and collect unique data points and create unique mathematical representations to verify a team member's identity. Sunbelt collects, stores, and uses this data solely for team member identification, security, and fraud prevention.

Currently, Sunbelt uses biometric equipment and software ("biometric equipment") provided by a third-party vendor, Dormakaba (Kaba). It is important to know that the method used by Kaba does not store any fingerprint image, but only an anonymous, mathematical reference template. The personal features of the fingertip are vectorized and converted into a complex numerical code. The relevant personnel number is allocated to this value. A fingerprint image cannot be reproduced under any circumstances. The mathematical reference template is stored locally on the clock-in/clock-out device and on Sunbelt's server. The information is not stored by any third party and is not accessible by any third-party.

Disclosure and Authorization

To the extent that Sunbelt, or any other vendors and/or the licensors of the biometric equipment Sunbelt uses, or may decide to use in the future, to collect, capture or otherwise obtain biometric data regarding its team members, Sunbelt:

- Will inform the team member about the collection, storage, and use of such biometric data;
- Will inform the team member of the specific purpose and length of time for which the biometric data is being collected, stored and used;
- Will secure a written authorization/consent from the team member (or the team member's legally authorized representative) allowing Sunbelt or any other vendors and/or the licensors of the biometric equipment Sunbelt uses, or may decide to use in the future, to collect, store and use team member's biometric data for the specific purposes disclosed by Sunbelt. This authorization will allow Sunbelt to provide such information to vendors and/or the licensor of the devices used as needed to comply with all legal requirements;
- Will not disclose, re-disclose, or otherwise disseminate an team member's biometric data unless:
- The team member or the team member's legally authorized representative consents to such disclosure or re-disclosure;
- The disclosure or re-disclosure completes a financial transaction requested or authorized by the team member or the team member's legally authorized representative;
- The disclosure or re-disclosure is required by state or federal law or municipal ordinance; or
- The disclosure is required pursuant to a valid warrant or subpoena issued by a court or agency of competent jurisdiction.

Retention Schedule

Sunbelt shall retain team member Biometric Data only until, and shall request that its vendors and the licensor of Sunbelt's biometric equipment 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 team member's employment with Sunbelt, or the team member moves to a role within Sunbelt for which the Biometric Data is not used; or
- Within 3 years of the team member's last interaction with Sunbelt as a team member in a classification where such Biometric Data is required.

Data Storage, Transmission, and Protection

Sunbelt shall use a reasonable standard of care to store, transmit, and protect Biometric Data. 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 Sunbelt stores, transmits, and protects from disclosure other confidential and sensitive personal information that can be used to uniquely identify an individual.

In circumstances where Sunbelt retains Biometric Data, Sunbelt will permanently destroy an individual's Biometric Data within six (6) months of when the initial purpose for collecting or obtaining such Biometric Data has been satisfied, such as:

- The team member's employment is terminated;
- The team member transfers to a position for which the Biometric Data is not used; or
- Sunbelt no longer uses the Biometric Information Data.

If any of Sunbelt's vendors and/or licensors require access to Biometric Information and Data in order to fulfill the purpose of collecting such information, Sunbelt will request that they follow the above destruction schedule.

Policy Enforcement

All team members are required to abide by this Policy as a condition of employment. Refusal to comply and provide the required consent to use biometric information will result in termination. Sunbelt's Human Resources Department is responsible for the enforcement and administration of this Policy. If you have any questions about the Policy, please contact Human Resources.