AAI BIPA POLICY AND CONSENT

Purpose

This Biometric Information and Security Policy ("Policy") defines AAI's policy and procedures for collection, use, safeguarding, storage, retention, and destruction of biometric data collected by AAI and/or its vendors.

AAI uses biometric identification systems for employee timekeeping with regard to payroll. AAI and/or its vendor(s) collects, stores, and uses employee biometric data for the purpose of granting employees access to AAI's timekeeping systems and to document employees' (i) clock in/out time(s); (ii) clock in/out location(s); and (iii) attempts/failures/errors in biometric data scans.

Policy

AAI's policy is to protect and store biometric data in accordance with applicable standards and laws, including, but not limited to, the Illinois Biometric Information Privacy Act.

An individual's biometric data will not be collected or otherwise obtained by AAI without prior written consent of the individual. AAI will inform the employee of the reason his or her biometric information is being collected and the length of time the data will be stored.

Definition

Biometric data means personal information stored by AAI and/or its vendor(s) about an individual's physical characteristics that can be used to identify that person. Biometric data can include fingerprints, voiceprints, a retina scan, scans of hand or face geometry, or other data.

Procedure

AAI and/or its vendor(s) collects, stores, and uses biometric data for the purposes of giving employees access to AAI's timekeeping systems and for maintaining accurate records of employee time.

Prior to collecting biometric data, AAI will obtain the consent of the employee. A sample consent form is included with this policy statement.

AAI will not sell, lease, trade, or otherwise profit from an individual's biometric data. AAI will not disclose biometric data unless (a) consent is obtained, (b) disclosure is required by law, or (c) disclosure is required by a subpoena.

AAI will store, transmit, and protect biometric data using a reasonable standard of care and in a manner that is the same as or exceeds the standards followed in maintaining other confidential and sensitive information.

AAI will permanently destroy an employee's biometric data from AAI's systems, or the systems of AAI's vendor(s), within a reasonable time following the employee's termination from AAI.

In the event AAI begins collecting biometric data for any additional purpose, AAI will update this procedure.

A copy of this policy will be made publicly available at http://www.aainvh.com/.

Consent to Collection of Biometric Data

Your hand geometry or other biometric data will be collected and stored by AAI and/or its vendor(s) for the purpose of verifying your identity for access to the AAI timekeeping system. Your biometric data will not be disclosed by AAI without your consent unless the disclosure is required by law or by valid legal subpoena. Your biometric data will be permanently deleted from AAI's systems within a reasonable time after your employment with the company ends, not to exceed 3 years from that date. A copy of AAI's Biometric Information and Security Policy is available upon request, is included in the AAI employee handbook, and is posted at http://www.aainvh.com/.

By signing below, you consent to AAI's collection, use, and storage of your hand geometry or other biometric data for the above defined purpose.

_____

Team Member Signature Date