



## **AZZ Inc. Biometric Information Security Policy**

### **I. Purpose**

The purpose of this Biometric Information Security Policy (“Policy”) is to define and explain AZZ Inc.’s (“AZZ”) policies and procedures for the collection, use, safeguarding, storage, retention, and destruction of an employee’s Biometric Data (as defined below) collected by AZZ.

AZZ collects, stores, and uses Biometric Data in connection with, and during, an employee’s employment with AZZ, including but not limited to timekeeping systems, payroll, building or site access, security, verification, safety, and compliance. AZZ may use certain third party services and/or equipment to collect, store, or use Biometric Data, but such third party collection, storage, and use will be strictly limited to AZZ’s administrative purposes and will not be disclosed to a third party for any other purpose.

### **II. Policy Statement**

This Policy replaces and supersedes all previous policies related to biometric information. AZZ reserves the right to amend this Policy at any time, without notice. AZZ may expand its use of Biometric Data in the future. In the event AZZ begins collecting Biometric Data for any additional purpose, AZZ will update this Policy.

A copy of this Policy will be made available upon request. A copy of this Policy is also available to the public at: [www.azz.com](http://www.azz.com).

### **III. Definition of Biometric Data**

For purposes of this Policy, “Biometric Data” means personal information stored by AZZ about an employee’s physical characteristics that can be used to identify that person. Biometric Data can include fingerprints, voiceprints, facial shape, retinal or iris scans, or a scan of hand or face geometry.

### **IV. Policy**

- AZZ’s policy is to protect and store Biometric Data in accordance with applicable standards and laws.
- An employee's Biometric Data will not be collected or otherwise obtained by AZZ without the prior written consent of the employee. AZZ 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. A consent statement is included in this Policy.
- AZZ will not sell, lease, trade, or otherwise profit from an employee's Biometric Data.
- Biometric Data will not be disclosed by AZZ unless (a) consent is obtained from the employee, (b) disclosure is necessary to complete a financial transaction requested or authorized by the employee, (c) disclosure is required by State or federal law or regulation, or municipal ordinance, or (d) disclosure is required by subpoena.
- Biometric Data will be stored using a reasonable standard of care for AZZ’s industry and in a manner that is the same or exceeds the standards used to protect other confidential and sensitive information held by AZZ.



- AZZ will destroy Biometric Data in accordance with its information Retention Policy, as outlined below.

**V. Procedures**

- Prior to collecting an employee’s Biometric Data, AZZ will obtain the written consent of the employee.
- Employees will have their Biometric Data registered on a third party’s virtual database. This database is a cloud based application which is hosted on a server at data centers utilized by the third party. Any third party holding AZZ employee Biometric Data shall hold such Biometric Data as if such third party were AZZ under this Policy. In the case of certain timekeeping services utilized by AZZ, a “hand template” method is recorded, and not a “fingerprint.” Hand templates are stored in a table within a database maintained by the third party. AZZ has a segregated database to ensure that AZZ employee hand templates are never co-mingled or inappropriately accessed.
- Only a limited group of AZZ administrators have authority to add/remove hand templates; however, this authority does not give such AZZ administrators access to visually review, export, or modify the hand template in any way.
- No AZZ employee will have direct access to Biometric Data.
- AZZ will permanently destroy and delete Biometric Data from its systems, and require the same of any third party possessing Biometric Data, in compliance with AZZ’s information and data Retention Policy, but at no time later than two (2) years after an employee’s separation from AZZ.

**VI. Consent To Collection of Biometric Data**

I understand that my Biometric Data may be collected, stored, and used by AZZ Inc. in connection with my employment with AZZ, including but not limited to timekeeping systems, payroll, building or site access, security, verification, safety, and compliance. I understand that my Biometric Data will not be disclosed by AZZ without my consent unless the disclosure is required by law or by valid legal subpoena, and except to certain third party services for the purposes stated above. I understand that AZZ will permanently destroy and delete Biometric Data from its systems, and require the same of any third party possessing Biometric Data, in compliance with AZZ’s information and data Retention Policy, but at no time later than two (2) years after my separation from AZZ. A copy of AZZ’s Biometric Information Security Policy is available upon request, and is posted at: [www.azz.com](http://www.azz.com).

I hereby acknowledge and agree that I have been provided with a copy of AZZ’s Biometric Information Security Policy, I have read such Policy, and I understand all the terms of the Policy. By signing below, I expressly and voluntarily consent to AZZ’s collection, storage, and use of my Biometric Data for the above-defined purpose as of the first day of my employment with AZZ.

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

Employee Name (printed): \_\_\_\_\_

—