# Sample

Red text denotes a field that needs to be changed by the user.

# Biometric Data Privacy Policy

[Company] has established the following Biometric Privacy Policy:

**Biometric Data Defined**

As used in this policy, the following terms are defined as:

1. "Biometric Identifier" means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual. "Biometric identifier" does not include a physical or digital photograph, video or audio recording or data generated therefrom, or information collected, used, or stored for health care treatment, payment, or operations under the federal health insurance portability and accountability act of 1996.
2. “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 of Biometric Data Collection**

[Company], its vendors, and/or the provider of [Company]’s time, attendance, and workforce management solutions collect biometric identifiers to facilitate an accurate and efficient timekeeping system, indentify employees, and/or for fraud prevention.

The biometric information [Company] collects will not be used for any other purpose and will not be shared with any third party unless required by law or subpoena. **[Company] will not sell, rent, or trade your Biometric Information.**

**Disclosure**

[Company], its vendors, and/or the licensor of [Company]’s time, attendance, and workforce management solutions will collect, capture, and use employee biometric data, after doing the following:

1. Inform the employee that [Company], vendors, and/or licensor will collect, capture, or otherwise obtain biometric data from the employee;
2. Provide the employee the specific purpose and length of time for which their biometric data will be collected, used, and retained;
3. Obtain a signed written release by the employee (or their legally authorized representative) authorizing [Company], vendors, and/or the [Company]’s licensor of time, attendance, and workforce management solutions to collect, store, and use employee’s biometric information for the specific purposes outlined and discloused by [Company]

[Company], their vendors, and/or the [Company]’s licensor of time, attendance, and workforce management solutions will not sell, disclose, or trade the employee’s biometric information

**Retention Policy**

[Company], its vendors, and licensor shall retain biometric data for a maximum of one year from the last data of interaction with the employee. You may directly request the deletion of your biometric information by submitting a written request to [Company].

**Data Storage**

[Company] shall use a reasonable standard of care when collecting, storing, and transmitting biometric information. Biometric Information will be destroyed within [a reasonable period of time with a maximum of one year from the last employee interaction] after employment with [Company] ends.

**Legal Disclaimer:** This document is intended for informational purposes only and does not constitute legal information or advice. Transmission of documents or information does not create an attorney-client relationship. This document must be reviewed and approved by client and client’s legal advisors.