Azimuth, LLC's Information Collection Policy

740 ILCS 14/1 et seq. is known as the Biometric Information Privacy Act ("BIPA") in its entirety.

Pursuant to BIPA "Biometric Information" is defined as 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.

Pursuant to BIPA "Biometric Identifier" is defined as 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 donated organs, tissues, or parts as defined in the Illinois Anatomical Gift Act or blood or serum stored on behalf of recipients or potential recipients of living or cadaveric transplants and obtained or stored by a federally designated organ procurement agency. Biometric identifiers do not include biological materials regulated under the Illinois Genetic Information Privacy Act. 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 identifiers do not include an X-ray, roentgen process, computed tomography, MRI, PET scan, mammography, or other image or film of the human anatomy used to diagnose, prognose, or treat an illness or other medical condition or to further validate scientific testing or screening.

Azimuth, LLC ("Company"), prior to obtaining possession of any individual Biometric Information, shall:

1. Have a written policy freely available to the all employees ("Written Policy");
2. The Written Policy shall establish a retention schedule and guideline for permanently destroying Biometric Identifiers and/or Biometric Information when the initial purpose for collecting or obtaining such Biometric Identifiers or information has been satisfied or within 3 years of the individual's last interaction with the Company, whichever occurs first;
3. That the Company that is in possession of Biometric Identifiers or Biometric Information must comply with its established retention schedule and destruction guidelines unless a court of competent jurisdiction has issued a valid warrant or subpoena for the Biometric Identifiers or Biometric Information.

Company shall not collect, capture, purchase, receive through trade, or otherwise obtain a person's or customer's Biometric Identifier or Biometric Information unless Company first:

1. Informs the subject or the subject's legally authorized representative in writing that a Biometric Identifier or Biometric Information is being collected or stored;
2. Informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a Biometric Identifier or Biometric Information is being collected, stored, and used; and
3. Receives a written release executed by the subject of the Biometric Identifier or Biometric Information or the subject's legally authorized representative and Company.

Company acknowledges that it shall not sell, lease, trade, or otherwise profit from a person's or a customer's Biometric Identifier or Biometric Information. Company further acknowledges that it shall not disclose, even if previously disclosed, or otherwise disseminate a person's Biometric Identifier or Biometric Information unless:

1. The subject of the Biometric Identifier or Biometric Information or the subject's legally authorized representative consents to the disclosure or redisclosure;
2. The disclosure or redisclosure completes a financial transaction requested or authorized by the subject of the Biometric Identifier or the Biometric Information or the subject's legally authorized representative;
3. The disclosure or redisclosure is required by State or federal law or municipal ordinance; or
4. The disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

Company acknowledges that if it is in possession of a Biometric Identifier or Biometric Information it shall:

1. Store, transmit, protect from disclosure all Biometric Identifiers and Biometric Information using the reasonable standard of care within the CC's industry; and
2. Store, transmit, and protect from disclosure all Biometric Identifiers and Biometric Information in a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information.

Biometric Time Clock Policy Acknowledgement of Consent

The Illinois Biometric Information Privacy Act, 740 ILCS 14/1, et seq. ("BIPA") regulates the collection, storage, use, and retention of "biometric identifiers" and "biometric information." Biometric identifier means a retina or iris scan, finger print, 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 named below understands that Azimuth, LLC ("AZI"), its vendors, clients, and/or the licensor of AZI's time and attendance software collect, retain, and use biometric data for the purpose of identifying employees and recording time entries when utilizing biometric time clocks or time attachments. Biometric time clocks are computer – based systems that scan an employees' finger (retina, face or other biometric identifier) for purposes of identification. The computer system extracts data points and creates a unique mathematical representation used to verify the employee's identity, for example when the employee arrives at or departs from the workplace.

The employee understands that Biometric Information will be stored and used for lawful time keeping purposes during the time of the assignment utilizing the biometric clock, and for an additional period of time thereafter in accordance with the law. The biometric information will be permanently destroyed no later than six (6) months following the date of separation from any assignment utilizing biometric information.

The employee understands that he/she/they is free to decline to provide biometric identifiers ad biometric information to AZI, its clients, and/or the licensor of the time and attendance software without any adverse employment action. The employee may revoke this consent at any time by notifying AZI in writing.

The undersigned employee acknowledges that he/she/they has received the attached Biometric Information Privacy Policy and that he/she/they voluntarily consents AZI, its clients, vendors, and/or the licensor of the time and attendance software's collection, storage, and use if biometric identifiers or biometric information as defined in BIPA, and voluntarily consents to the use of the biometric clock.

_____

Employee signature Date

_____

Employee Printed Name