CITADEL TIME & ATTENDANCE SYSTEM

BIOMETRIC DATA DISCLOSURE AND AUTHORIZATION AGREEMENT

IMPORTANT: READ THIS BIOMETRIC DATA DISCLOSURE AND AUTHORIZATION AGREEMENT ("AGREEMENT") CAREFULLY BEFORE CONTINUING BIOMETRIC REGISTRATION. BY SELECTING "I HAVE READ AND ACCEPT THE TERMS OF THIS AGREEMENT" YOU SIGNIFY THAT YOU HAVE READ, UNDERSTOOD AND AGREE TO FOLLOW THE TERMS AND CONDITIONS OF THIS AGREEMENT, INCLUDING, WITHOUT LIMITATION, THE TERMS AND CONDITIONS OF DOCUMENTS WHICH ARE INCORPORATED BY REFERENCE HEREIN. IF YOU DO NOT AGREE TO ALL THE TERMS AND CONDITIONS IN THIS AGREEMENT, YOU MUST SELECT "I DECLINE" AND MAY NOT REGISTER EMPLOYEE BIOMETRIC DATA.

A. Definitions.

"Workwell Technologies" refers to "Workwell Technologies, Inc."

"Citadel" refers to the Citadel Time & Attendance System and associated software as a service platform provided by Workwell Technologies as well as any other related media form, media channel, mobile website or mobile application.

"You" or "Your" refer to any individual or entity ordering or using Citadel.

"Your Data" refers to any data or images that you input, scan or import into Citadel or is derived from Citadel, including, but not limited to, information regarding employees, time cards, hours worked, users, departments, or other data.

As used in this policy, biometric data includes "biometric identifiers" and "biometric information" as defined in the Illinois Biometric Information Privacy Act, 740 ILCS § 14/1, et seq. or such other statutes or regulations that apply in your state. "Biometric identifier" means 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 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 information" refers to 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.

"Biometric data" refers to personal information stored by Workwell Technologies 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.

B. Biometric Data Disclosure and Authorization

To the extent that you, your vendors, and/or the licensor of your time and attendance software collect, capture, or otherwise obtain biometric data relating to an employee, you must first:

a. Inform your employee in writing that you, your vendors, and/or the licensor of your time and attendance software are collecting, capturing, or otherwise obtaining the employee's biometric data, and that you are providing such biometric data to your vendors and the licensor of your time and attendance software;
b. Inform the employee in writing of the specific purpose and length of time for which the employee's biometric data is being collected, stored, and used; and
c. Receive a written release signed by the employee (or his or her legally authorized representative) authorizing you, your vendors, and/or the licensor of your time and attendance software to collect, store, and use the employee's biometric data for the specific purposes disclosed by you, and for you to provide such biometric data to its vendors and the licensor of your time and attendance software.

You, your vendors, and/or the licensor of your time and attendance software will not sell, lease, trade, or otherwise profit from employees' biometric data; provided, however, that your vendors and the licensor of your time and attendance software may be paid for products or services used by you that utilize such biometric data.

Disclosure

You will not disclose or disseminate any biometric data to anyone other than your vendors and the licensor of your time and attendance software providing products and services using biometric data without/unless:

a. First obtaining written employee consent to such disclosure or dissemination;
b. The disclosed data completes a financial transaction requested or authorized by the employee;
c. Disclosure is required by state or federal law or municipal ordinance; or

Disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

C. Retention Schedule

Workwell will permanently destroy an employee's biometric data from Workwell's systems, or the systems of Workwell vendor(s) within one (1) year, 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 employee's employment with the Company, or the employee moves to a role within the Company for which the biometric data is not used; or
- You request to discontinue your Citadel services.

You may delete biometric data IDs and templates for employees upon your discretion directly through the cloud portal and on devices.

Workwell will permanently destroy all your other data from Workwell's systems, or the systems of Workwell vendor(s), within one (1) year of your request to discontinue your Citadel services.

D. Data Storage

You shall use a reasonable standard of care to store, transmit and protect from disclosure any paper or electronic biometric data collected. Such storage, transmission, and protection from disclosure shall be performed in a manner that is the same as or more protective than the manner in which you store, transmit and protect from disclosure other confidential and sensitive information, including personal information that can be used to uniquely identify an individual or an individual's account or property, such as genetic markers,

genetic testing information, account numbers, PINs, driver’s license numbers and social security numbers.