



TIME & ATTENDANCE SERVICES TERMS AND CONDITIONS

Last updated – September 29, 2026

This Time & Attendance Services Addendum (the “**Addendum**”) forms part of the Agreement (as defined in Viventium’s Master Terms and Conditions) between Viventium and User that governs User’s use of Viventium’s products and services.

Capitalized terms not defined herein have the meanings set forth in the Agreement.

1) Scope of Addendum

- a) **Services Covered.** This Addendum governs Viventium’s time and attendance and related reporting services (the “**T&A Services**”).

2) Definitions

- a) **“Biometric Data”** means any biometric identifier, biometric information, biometric data, or similar data regulated under applicable Biometric Information Laws, including data generated by the technological processing, measurement, or analysis of an individual’s biological, physical, physiological, or behavioral characteristics that is used or intended to be used, alone or with other data, to identify, verify, or authenticate an individual. Biometric Data may include fingerprints, voiceprints, scans or records of hand or face geometry, facial maps or templates, and iris or retina scans, but excludes information expressly excluded from the definition of biometric identifiers, biometric information, or biometric data under applicable Biometric Information Laws.
- b) **“Biometric Information Laws”** means all applicable federal, state, and local laws, rules, and regulations governing the collection, capture, enrollment, use, disclosure, security, storage, retention, destruction, or other processing of Biometric Data, including the Illinois Biometric Information Privacy Act, 740 ILCS 14/1 *et seq.*; the Washington biometric-identifiers law, Wash. Rev. Code ch. 19.375; the Texas Capture or Use of Biometric Identifier Act, Tex. Bus. & Com. Code § 503.001; the Colorado Privacy Act, Colo. Rev. Stat. §§ 6-1-1301 *et seq.*, including § 6-1-1314; and any amendments, implementing regulations, or successor laws.
- c) **“Hardware”** means any physical device purchased from or approved by Viventium for use in connection with the T&A Services.
- d) **“Punch Data”** means data reflecting clock-in, clock-out, breaks, schedules, or other timekeeping records of User’s personnel.
- e) **“Location Data”** means geographic-location information associated with User’s personnel or their devices, including latitude and longitude coordinates, derived street addresses, geofencing results, and map-display information collected or generated in connection with the T&A Services.

3) Provision of T&A Services

- a) **Generally.** User acknowledges and agrees that the T&A Services are “Services” under the Agreement. Viventium is only required to provide the T&A Services when the T&A Services are operated by User according to the Documentation or other applicable terms of use and in an environment that meets the minimum requirements.

4) User Responsibilities

- a) **Configuration, Review, and Compliance.** User is solely responsible for configuring and maintaining all pay codes, schedules, overtime rules, rounding rules, meal and rest-break rules, time-entry restrictions, approval workflows, and other settings within the T&A Services. User is also solely responsible for determining what constitutes compensable time and for interpreting and complying with applicable wage-and-hour laws, collective-bargaining agreements, employment policies, and other requirements applicable to its personnel. User will timely review, audit, correct, and approve Punch Data and other timekeeping

records before using such information to process payroll or make employment decisions. User will establish reasonable backup timekeeping procedures for periods when the T&A Services, Hardware, network connectivity, or other systems are unavailable and will timely enter or reconcile any resulting records. The T&A Services do not independently determine whether User's configurations, policies, or timekeeping practices comply with applicable law.

- b) **Compliance With Biometric Information Laws.** User is solely responsible for determining whether and how to use any biometric functionality and for complying with the obligations applicable to User as an employer, controller, or other collector or user of Biometric Data. Before enabling biometric functionality for any individual, User will: (i) provide all notices and disclosures required by Biometric Information Laws, including the purpose and duration of collection, use, storage, and disclosure; (ii) obtain a valid written consent or release authorizing the collection, use, storage, and disclosure of Biometric Data by User, Viventium, and Viventium's service providers for purposes of providing the T&A Services; (iii) adopt and make available any required retention and destruction policy; and (iv) provide any required alternative method of time entry. User will retain evidence of each notice, consent, and release for the period required by applicable law and will provide such evidence to Viventium upon reasonable request. User will not submit or permit Viventium to process Biometric Data for any individual for whom the required notice, consent, or release has not been provided or obtained.
- c) **Withdrawal and Other Requests.** User will maintain procedures through which individuals may withdraw consent or exercise other rights concerning their Biometric Data. User will promptly notify Viventium at support@viventium.com of any withdrawal or other request requiring action by Viventium and will immediately discontinue the individual's use of biometric functionality. Viventium may suspend or disable biometric functionality if Viventium reasonably believes that User has failed to comply with this Section or applicable Biometric Information Laws. Viventium may provide reasonable compliance assistance but does not provide legal advice or warrant that such assistance will satisfy User's obligations.
- d) **Location Data Compliance.** User is solely responsible for determining whether and how to enable location-based functionality and for complying with all laws applicable to User's collection, use, monitoring, and disclosure of Location Data. Before enabling such functionality, User will provide all required notices, obtain all required consents or authorizations, establish any required workplace policies, and provide an alternative time-entry method where required by applicable law. User will not use the T&A Services or Location Data for unlawful employee monitoring, discrimination, retaliation, or any purpose inconsistent with the notices provided to its personnel.
- e) **Hardware Environment.** User will install, operate, and maintain Hardware in accordance with the Documentation and will provide network connectivity, electrical service, and an operating environment meeting Viventium's specifications. User will use Hardware only at User's legitimate business locations and will not relocate Hardware without complying with Viventium's applicable instructions.

5) Hardware

- a) **Hardware Sold Separately.** If User purchases or uses Hardware in connection with the T&A Services, the Hardware must be purchased from Viventium or a vendor approved by Viventium. Hardware purchased from Viventium is subject to Viventium's Time & Attendance Hardware Terms and Conditions, which are incorporated into the Agreement. Except as expressly provided in those terms, any claim or issue relating to Hardware will not relieve User of its obligation to pay Fees when due. User will not modify the Hardware, install unapproved software, or connect unapproved devices or peripherals to the Hardware.

6) Data Security & Privacy

- a) **Punch Data Access and Export.** During the Term, User may access and export Punch Data using the functionality generally made available through the T&A Services. Upon User's reasonable written request, Viventium will provide Punch Data in Viventium's then-standard export format, subject to applicable security-verification procedures. Viventium is not required to create a custom export, develop or provide an API, or provide Punch Data in a format not then generally supported, and may charge its then-current rates for any agreed custom services. Following termination or expiration, User's access to the T&A Services and Punch Data may cease. If User requests an export within thirty (30) days after termination or

expiration, Viventium will use commercially reasonable efforts to provide Punch Data that remains available under Viventium's applicable data-retention practices and may charge a reasonable fee. User acknowledges that Viventium is not User's official recordkeeper and that User is solely responsible for reviewing, correcting, approving, exporting, and retaining all timekeeping records required by applicable law.

- b) **Service Providers and Subprocessors.** Viventium may engage affiliates, service providers, and subprocessors to assist in providing the T&A Services, including providers of hosting, data storage, biometric technology, device management, mapping, and geocoding services. Viventium will require such parties to protect User Data in accordance with Viventium's applicable contractual and legal obligations. Viventium's use of such parties will not relieve Viventium of its obligations under the Agreement, but Viventium's responsibility remains subject to all limitations, exclusions, defenses, and remedies set forth in the Agreement.
- c) **Biometric Data.** As between the Parties, User determines whether to enable biometric functionality and the business purposes for which Biometric Data is processed through the T&A Services. User instructs and authorizes Viventium to process Biometric Data as reasonably necessary to provide, maintain, secure, and support the T&A Services; prevent fraud or unauthorized access; comply with applicable law; and carry out User's lawful instructions. Viventium will not sell, lease, trade, or otherwise profit from Biometric Data. Viventium will disclose Biometric Data only: (i) to User; (ii) to service providers and subprocessors as reasonably necessary to provide the T&A Services; (iii) as authorized by the individual's valid consent or release and permitted by applicable law; or (iv) as permitted or required by applicable law or valid legal process. Viventium will protect, retain, and destroy Biometric Data in accordance with the obligations directly applicable to Viventium under Biometric Information Laws and Viventium's applicable retention and destruction practices. Upon receiving notice from User that an individual has withdrawn consent, that the original purpose for processing has been satisfied, or that deletion is otherwise required, Viventium will process the request in accordance with applicable law and Viventium's documented procedures. User acknowledges that Viventium's ability to act on such circumstances depends upon User providing complete and timely notice.
- d) **Location Data.** The T&A Services may collect and process Location Data when User's personnel use location-enabled functionality, including in connection with recording a timekeeping event. Viventium may disclose Location Data to mapping, geocoding, hosting, and other service providers as reasonably necessary to provide the T&A Services. Viventium may also process Location Data for information security, fraud prevention, legal compliance, and as otherwise instructed by User. Unless otherwise identified in the Documentation or an Ordering Document, the T&A Services are not designed to continuously monitor the location of User's personnel.

7) Warranties & Disclaimers

- a) **Disclaimer.** Except as expressly stated in the Agreement, the T&A Services are provided **"as is"** and Viventium disclaims all other warranties or guaranties, including any warranties of merchantability, fitness for a particular purpose, title and non-infringement.

8) Miscellaneous

- a) **Modification.** Viventium may modify this Addendum in accordance with the modification provisions set forth in the Master Terms and Conditions.