AGENDA PLACEMENT FORM
(Submission Deadline – Monday, 5:00 PM before Regular Court Meetings)

Date: 07/18/2025

Meeting Date: 07/28/2025

Submitted By: Steve Watson

Department: County Auditor

Signature of Elected Official/Department Head:

Jennifer Lyn 1st Asst Auditor

Court Decision:
This section to be completed by County Judge's Office

APPROVED
Johnson County Commissioners Court

7-28-25

Description:

Consideration to approve agreement for time keeping software as a service for Timeclock Plus, LLC Quote # Q047231 with a term length of 60 months, a year 1 cost of $82,451.34 and an annual recurring cost of $39,554.07 plus overages based on actual usage, Timeclock Plus, LLC Service Terms and Conditions, Exhibit A - TCP Services Agreement, Exhibit B - Johnson County Contract Terms Addendum, Exhibit C - TCP Service Level Agreement, Exhibit D - TCP Global Data Privacy Policy, and Exhibit E - TCP Hardware Support and Maintenance Agreement - Addendum with authorization for the County Judge to sign.

(May attach additional sheets if necessary)

Person to Present: Steve Watson

(Presenter must be present for the item unless the item is on the Consent Agenda)

Supporting Documentation: (check one)   ☑ PUBLIC   ☐ CONFIDENTIAL

(PUBLIC documentation may be made available to the public prior to the Meeting)

Estimated Length of Presentation: _____ minutes

Session Requested: (check one)

☐ Action Item ☐ Consent ☐ Workshop ☐ Executive ☐ Other _____

Check All Departments That Have Been Notified:

☑ County Attorney   ☑ IT   ☐ Purchasing   ☑ Auditor

☑ Personnel   ☐ Public Works   ☐ Facilities Management

Other Department/Official (list) _____

Please List All External Persons Who Need a Copy of Signed Documents
In Your Submission Email

Approved in CC on 9/11/2023

CLIENT INFORMATION

Shipping Method: UPS Ground

Purchased for: Johnson County
Bill To: Johnson County

Billing Address: 2 North Main Street
Cleburne, Texas 76033
United States

Billing Contact Name: Mark Graham

Billing Contact Email: mgraham@johnsoncountytx.org

Billing Contact Phone: (817) 556-6350

Contract Contact Name: Mark Graham

Contract Contact Email:
mgraham@johnsoncountytx.org

BILLING TERMS

INITIAL TERM	RENEWAL TERM	PAYMENT TERM	PAYMENT METHOD
60 MONTHS	60 MONTHS	NET 30	CHECK

ITEM DESCRIPTION	PRICE PER UNIT	QUANTITY	CHARGE TYPE	ORDER TOTAL
ESTIMATED IMPLEMENTATION SERVICES (TIME & MATERIALS)	$192.50	160	ONE-TIME	$30,800.00
ENTERPRISE LICENSE ANNUAL CHARGE	$38.40	970	RECURRING	$37,248.00
OVERAGE ENTERPRISE LICENSE ANNUAL CHARGE	$38.40		USAGE	$0.00
HARDWARE SUPPORT & MAINTENANCE	$2,306.07	1	RECURRING	$2,306.07
*RDT	$1,315.30	2	ONE-TIME	$2,630.60
*RDT + MAG	$1,483.30	4	ONE-TIME	$5,933.20
*BATTERY BACKUP	$201.60	6	ONE-TIME	$1,209.60
*POWER OVER ETHERNET (POE) 802.3AF	$266.70	6	ONE-TIME	$1,600.20
*WIFI 802.11 A/C ADAPTER	$97.30	6	ONE-TIME	$583.80
HARDWARE S&H	$139.87	1	ONE-TIME	$139.87

SUBTOTAL	**$82,451.34**

TAXES	$0.00
GRAND TOTAL	$82,451.34
CURRENCY	USD

SPECIAL TERMS: OMNIA CONTRACT 14-10

SERVICE TERMS & CONDITIONS

TimeClock Plus, LLC ("TCP"), a Delaware limited liability company, will provide Client and its authorized Employees and Users access to the Services during the Initial Service Term in accordance with the complete terms and conditions (collectively the "Licensing Agreement")attached hereto.

This Order Form is entered into as of the Date approved by the Commissioenrs Court of Johnson County and signed by the County Judge (the "Effective Date") by and between TimeClock Plus, LLC and the entity named in the Bill To section herein (the "Client"), and is subject to the Licensing Agreement. In the event of any conflict between the Order Form and the Terms and Conditions (as applicable), the terms of the Order Form shall control, subject however, to the terms and conditions set forth in the Johnson County Contract Terms Addendum.

Client shall pay all fees or charges in accordance with those outlined on the Order Form. Except for cases of TCP breach, all fees are committed and non-cancelable during the term of the agreement, subject to the terms and conditions of the Johnson County Contract Terms Addendum.
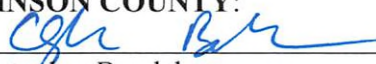
The individuals executing this Agreement on behalf of each Party represent and warrant to the other Party that they are fully authorized and legally capable of executing this Agreement on behalf of such Party and that such execution is binding upon such Party.

This Agreement incorporates the following documents which are attached hereto and are incorporated herein:

Exhibit A - TCP Services Agreement
Exhibit B – Johnson County Contract Terms Addendum
Exhibit C - TCP Service Level Agreement (SLA)
Exhibit D – Global Data Privacy Policy updated September 25th, 2024
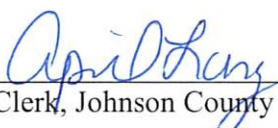Exhibit E – TCP Hardware Support & Maintenance Agreement - Addendum

APPROVED AS TO FORM AND CONTENT:

JOHNSON COUNTY:

Christopher Boedeker
As Johnson County Judge

7-28-25
Date

Attest:

County Clerk, Johnson County

7-28-25
Date

TIMECLOCK PLUS:

Authorized Representative of TIMECLOCK PLUS

7/24/2025
Date

Printed Name: Derek McIntyre

Title: COO

EXHIBIT A

TCP Services Agreement

THIS TCP SERVICES AGREEMENT (the "Agreement") is entered into as of _____ ("Effective Date"), by and between **TimeClock Plus, LLC**, a Delaware limited liability company with its principal office located at 1 Time Clock Drive, San Angelo, TX 76904 ("TCP"), JOHNSON COUNTY, a political subdivision of the State of Texas, with its principal office located at   2 North Main Street, Cleburne, Texas 76033 ("Client").

WHEREAS TCP and Client (the "Parties") desire to enter into this Agreement for the provision of hosted services by TCP to Client, as provided herein.

NOW, THEREFORE, in reliance on the mutual covenants, promises, representations, and agreements set forth herein, the Parties agree as follows:

1.   **Definitions**.

1.1   "Active License" means an Employee or Designated User that has not been marked as either terminated or suspended within TCP Services for whom Client is required to pay a fee under this Agreement.

1.2   "Affiliate" means any parent or subsidiary corporation, and any corporation or other business entity controlling, controlled by, or under common control with a Party.

1.3   "Biometric Data" means any information based on an individual's retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry, which is used to identify an individual, regardless of how it is captured, converted, stored, or shared.

1.4   "Client Data" means all of Client's data processed or stored by or transmitted to TCP in connection with the TCP Services, including, without limitation, all Personal Data contained therein.

1.5   "Designated User" means an individual Employee who is authorized by Client to access the administrative features of the TCP Services, and whose Personal Data may be processed or stored by or transmitted to TCP in connection with the TCP Services.

1.6   "Employee" means Client's individual employee, manager, administrator, worker, consultant, substitute, or contractor.

1.7   "Hardware Support and Maintenance Agreement" means any agreement that extends services to current TimeClock Plus terminals, clocks, and biometric devices, and maintenance releases for related products purchased or licensed by the Client from TCP or a registered reseller, as applicable.

1.8 "Initial Term" has the meaning set forth in Section 10.

1.9 "Monthly License Fee" means TCP's then current fees applicable for each of Client's Active Licenses based on the aggregated Permissions to access and use the TCP Services measured over the course of each calendar month, as outlined on an invoice or Order Form. This fee may be prorated during the first month of the Initial Term and prorated for the last month of the Initial Term.

1.10 "Order Form" means a written document, including, but not limited to, a TCP issued invoice, a TCP issued order form, or a Client issued purchase order, which has been mutually agreed upon and executed by the Parties for ordering products and/or services, and which expressly incorporates the terms of this Agreement.

1.11 "Permissions" means the permission(s) granted to Client's Employees to access features within TCP Services, as outlined on an invoice or Order Form. Permissions are applied within the TCP Services by Client's Designated Users.

1.12 "Personal Data" means any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular Employee or Designated User.

1.13 "Privacy Policy" means TCP's Global Data Privacy Policy attached hereto as EXHIBIT D.

1.14 "Service Level Agreement" means the Service Level Agreement that serves as an addendum to this Agreement. The Service Level Agreement is attached hereto as EXHIBIT C.

1.15 "Subprocessor" means any third-party entity that processes Personal Data on behalf of TCP and to which TCP discloses Personal Data for a business purpose pursuant to a written contract, provided that the contract prohibits such entity from retaining, using, or disclosing the Personal Data for any purpose other than for the specific purpose of performing the services identified in such contract.

1.16 "Supported Hardware" means any hardware purchased or leased from TCP that is coverable under a Hardware Support and Maintenance Agreement attached hereto as Exhibit E.

1.17 "TCP Services" means the TCP software application(s) hosted by TCP in accordance with TCP's then-current hosting environment, any associated documentation, and any ancillary services described in this Agreement or an Order Form.

1.18 "TCP Technology" means the computer hardware, software, and other tangible equipment and intangible computer code contained therein used by TCP in the provision of the TCP Services.

1.19 "Term" has the meaning set forth in Section 10.

1.20   "Use Fees" means the fees set forth on the applicable invoice or Order Form, including, but not limited to, Monthly License Fees and Hardware Support and Maintenance Agreement Fees.

2.   Delivery of Services.

2.1   TCP Services. Subject to the terms and conditions of this Agreement and the Privacy Policy, TCP grants to Client, its Affiliates and their Designated Users a limited, non-transferable (except in compliance with Section 22), nonexclusive right and subscription license to access and use the TCP Services during the Term only for the internal business purposes of processing, storing, and maintaining Client Data. TCP shall provide to Client the TCP Services during the Term in accordance with the terms and conditions of this Agreement, the Privacy Policy, the Service Level Agreement, the Hardware Support and Maintenance Agreement (if applicable), and any additional terms outlined in an Order Form.

2.2   Client Responsibilities. Client's use of the TCP Services is subject to the terms of this Agreement, the Privacy Policy, the Service Level Agreement, the Hardware Support and Maintenance Agreement (if applicable), and any additional terms outlined in an Order Form. The aforementioned documents are attached hereto as described above.

2.2.1   Access. Client is responsible for maintaining the confidentiality of Client's account and password and for restricting access to its computer systems, and Client agrees to accept responsibility for all activities that occur under Client's account or password, including but not limited to any acts or omissions by Designated Users. Client shall inform each Designated User of the terms and conditions governing such Designated User's use of the TCP Services as set forth herein and shall cause each Designated User to comply with such terms and conditions.

2.2.2   Restrictions on Use. Client acknowledges and agrees that Client will not use the TCP Services for the benefit of any third party. Client agrees not to attempt to, nor allow any third party to: (i) use the TCP Services in any manner that could damage, disable, overburden, or impair TCP's servers or networks or interfere with any other party's use and enjoyment of the TCP Services; (ii) attempt to gain unauthorized access to any services, user accounts, computer systems, or networks through hacking, password mining, or any other means; (iii) copy, distribute, rent, lease, lend, sublicense, transfer the TCP Services, make the TCP Services available to any third party, or use the TCP Services on a service bureau or time sharing basis, (iv) decompile, reverse engineer, or disassemble the TCP Services or otherwise attempt to reconstruct or discover any source code, underlying ideas, algorithms, file formats, or programming interfaces of the TCP Services, (v) create derivative works based on the TCP Services; (vi) modify, remove, or obscure any copyright, trademark, patent, or other notices or legends that appear on the TCP Services or during the use and operation thereof; (vii) publicly disseminate performance information or analysis (including benchmarks) relating to the TCP Services; or (viii) use the TCP Services in a manner which violates or infringes any laws, rules, regulations, third party intellectual property rights, or third party privacy rights. Client may not use any automated means, including agents, robots, scripts, or spiders to

access or manage the TCP Services, except solely to the extent as may be specifically enabled and authorized by TCP in writing. TCP may take any legal and technical measures to prevent the violation of this provision and to enforce this Agreement.

2.3   Third Party Services.

2.3.1   Client may require the TCP Services to interoperate with platforms or other online services operated by third parties ("Third-Party Platforms") pursuant to an agreement between TCP and the operators of such Third-Party Platforms, an agreement between Client and the operators of such Third-Party Platforms, or through application programming interfaces ("APIs") or other means of interoperability which are generally made available by such operators.

2.3.2   As applicable, Client hereby grants TCP the limited right to access such Third-Party Platforms with Client's credentials and on behalf of the Client in connection with the performance of the TCP Services. Client acknowledges and agrees that TCP's agreements with the operators of such Third-Party Platforms and the terms governing the use of APIs may be modified, suspended, or terminated at any time, and TCP shall have no liability with respect to any such modification, suspension, or termination. Client is responsible for ensuring that its use of the TCP Services in connection with any Third-Party Platform, and TCP's access to such Third-Party Platforms on Client's behalf, complies with all agreements and terms applicable to such Third-Party Platform.

2.4   Client Data.

2.4.1   General. Client hereby grants TCP a worldwide, royalty-free, non-exclusive, limited license to use, host, copy, transmit, display, modify, and create derivative works of Client Data for the express purpose of providing the TCP Services. Client acknowledges and agrees that it will determine the means and purposes of processing Client Data and that TCP acts solely as a service provider that processes Client Data on behalf of and at the direction of Client for the sole purpose of performing the TCP Services under this Agreement. Client is responsible for ensuring that all Designated Users who provide instructions to TCP on Client's behalf are authorized. Client shall have sole responsibility for the accuracy, quality, content, legality, and use of Client Data and the means by which any Personal Data is obtained from Designated Users and Employees and transferred to TCP, and Client is solely responsible for any transfer of Personal Data to any third-party data controller or data processor (*e.g.*, human resources or payroll application), and TCP shall have no liability in connection therewith. Client agrees to implement data protection-related procedures that will not be less protective than those imposed on TCP by this Agreement and the Privacy Policy.

2.4.2   Restrictions on TCP's Processing of Client Data. TCP is expressly prohibited from processing any Client Data for any purpose other than for the specific purpose of performing the TCP Services unless requested by Client or required by applicable law. TCP is prohibited from selling Personal Data under any circumstances and for any purpose. No other collection, use, disclosure, or transfer (except to

Subprocessors in accordance with <u>Section 22</u>) of Client Data is permitted without Client's express prior written instruction. TCP acknowledges and agrees that it understands and will comply with each of the restrictions and obligations set forth in this <u>Section 2.4.2</u>.

2.4.3   <u>Subprocessors</u>. TCP has appointed Subprocessors for the purpose of providing data hosting and security services. Client acknowledges and agrees that Subprocessors may process Client Data in accordance with the terms of this Agreement, the Privacy Policy and any Order Form. TCP's agreements with its Subprocessors impose data protection-related processing terms on such Subprocessors that are no less protective than the terms imposed on TCP in this Agreement and the Privacy Policy. The Privacy Policy contains an overview of the categories of Subprocessors involved in the performance of the relevant TCP Services. The appointment of a Subprocessor to perform part or all the TCP Services hereunder shall not relieve TCP of any liability under this Agreement.

3.   Data Security.

3.1   <u>Security Standards</u>.

3.1.1   TCP shall implement reasonable security procedures consistent with industry standards to protect Client Data from unauthorized access, including without limitation (i) industry-standard encryption of data at rest within TCP's data centers; (ii) web application firewalls; (iii) virus detection and anti-virus software; (iv) authentication techniques, such as user names and passwords, or authorization formats, which limit access to particular TCP personnel; and (v) additional security controls consistent with SOC 2 Type II reporting standards.

3.1.2   The Parties shall implement administrative, technical and physical security procedures consistent with industry standards and applicable data protection laws to protect Client Data from unauthorized access, including by adopting access policies that prevent the internal sharing or inadvertent communication of login credentials.

3.1.3   Client is responsible for reviewing the information made available by TCP relating to data security and making an independent determination as to whether the TCP Services meet Client's requirements and obligations under applicable data protection laws. Client acknowledges that data security measures taken by TCP are subject to technical progress and development and TCP may update or modify such security measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the TCP Services.

3.2   <u>Security Breach Notifications</u>. TCP will promptly report to Client any unauthorized access to Client Data within TCP's or its Subprocessors' systems upon discovery and in accordance with applicable data breach notification laws. TCP will use diligent efforts to promptly remedy any breach of security that permitted such unauthorized access. TCP's notification of or response to any security incident under this

Section 3.2 shall not be construed as an acknowledgment by TCP of any fault or liability with respect to such security incident.

      3.3   Data Backup and Retention. TCP shall undertake commercially reasonable efforts to backup Client Data with a restore point objective of twenty-four (24) hours. Client Data shall be backed up and retained in accordance with TCP's retention policy as set forth in the Privacy Policy.

4.   Data Privacy. TCP will process Employee Personal Data in accordance with the terms of this Agreement, the Privacy Policy and all applicable data protection laws. Client must maintain its own data collection, disclosure, retention, and storage policies in compliance with applicable law.

      4.1   Biometric Data. To the extent that Client collects, captures, stores, or otherwise uses Biometric Data relating to an individual, Client must (i) first inform the individual from whom Biometric Data will be collected, in writing and prior to collecting his or her Biometric Data, that Biometric Data is being collected, stored, and/or used; (ii) indicate, in writing, the specific purpose(s) (which may not be other than employment-related purposes) and length of time for which Biometric Data is being collected, stored, and/or used; and (iii) receive a written release from the individual (or his or her legally authorized representative) authorizing the Client, TCP, TCP's third-party service providers (who are subject to restrictions no less restrictive than those imposed on TCP herein) to collect, store, and/or use the Biometric Data and authorizing the Client to disclose such Biometric Data to TCP and TCP's third-party service providers

      4.2   Requests. Client agrees to adopt a commercially reasonable policy for managing data requests from Designated Users and Employees, which policy shall safeguard the rights of such data subjects and respect the original purpose of such data collection. Client, as the Party which determines the means and purposes for processing Client Data, shall be responsible for receiving, investigating, documenting, and responding to all Designated User and Employee requests for inspection or erasure of Personal Data.

      4.3   Assistance. If Client receives a request from a Designated User or Employee to exercise such individual's rights under applicable data protection laws, and Client requires TCP's assistance to respond to such request in accordance with applicable data protection laws, TCP shall assist the Client by providing any necessary information and documentation that is under TCP's control. TCP shall be given reasonable time to assist the Client with such requests in accordance with applicable law.

      4.4   Client's Privacy Policy. Where required by law, Client agrees to adopt a privacy policy in alignment with this Agreement and all applicable laws governing the collection, use, transfer and retention of Personal Data. Client agrees to provide TCP, upon reasonable request, Client's adopted privacy policy.

5. Confidential Information.

5.1   Each Party (the "Receiving Party") acknowledges that it will have access to certain confidential information of the other Party (the "Disclosing Party") concerning the Disclosing Party's business, plans, customers, software, technology and products, other information held in confidence by the Disclosing Party, and Personal Data. In addition, a Disclosing Party's confidential information will include (i) all information in tangible or intangible form that is marked or designated as confidential or that, under the circumstances of its disclosure, should be considered confidential, and (ii) the TCP Technology and related algorithms, logic, design, specifications, and coding methodology, and to the extent permitted by law, the terms and conditions of this Agreement, but not its existence (all of the foregoing being referred to as "Confidential Information").

5.2   The Receiving Party agrees that it will not use in any way, for its own account or the account of any third party, except as expressly permitted by, or required to achieve the purposes of, this Agreement, nor disclose to any third party (except as required by law or to that party's attorneys, accountants and other advisors as reasonably necessary), any of the Disclosing Party's Confidential Information, and will take reasonable precautions to protect the confidentiality of such Confidential Information in at least the same manner as is necessary to protect its own Confidential Information and in accordance with applicable data protection laws. To the extent that the Receiving Party is permitted to retransmit any Confidential Information it receives from the Disclosing Party, the mode of retransmission must be at least as secure as the mode by which the Disclosing Party transmitted the Confidential Information to the Receiving Party.

5.3   Information will not be deemed Confidential Information hereunder if such information: (i) is known to the Receiving Party prior to receipt from the Disclosing Party, whether directly or indirectly, from a source other than one having an obligation of confidentiality to the Disclosing Party; (ii) becomes known (independently of disclosure by the Disclosing Party) to the Receiving Party, whether directly or indirectly, from a source other than one having an obligation of confidentiality to the Disclosing Party; (iii) becomes publicly known or otherwise ceases to be secret or confidential, except through a breach of this Agreement by the Receiving Party; or (iv) is independently developed by the Receiving Party without use of or reference to the Confidential Information.

6.   Cooperation With Authorities. If either Party is requested to disclose all or any part of any Confidential Information under a subpoena or inquiry issued by a court of competent jurisdiction or by a judicial or administrative agency or legislative body or committee, the Receiving Party shall (i) immediately notify the Disclosing Party of the existence, terms and circumstances surrounding such request; (ii) consult with the Disclosing Party on the advisability of taking legally available steps to resist or narrow such request and cooperate with the Disclosing Party on any such steps it considers advisable; and (iii) if disclosure of the Confidential Information is required or deemed advisable, exercise its best efforts to obtain an order, stipulation or other reasonably acceptable assurance that the Confidential Information or part thereof required to be disclosed shall retain its confidentiality and remain otherwise subject to this Agreement.

Although TCP will not systematically monitor the Client Data, TCP reserves the right, upon prior written notice to Client, to remove access to Client Data to comply with applicable law, provided, however, that access to such Client Data will be restored upon a mutual determination of the Parties that such Client Data is in compliance with, or has been modified to be in compliance with, applicable law.

7.   Supplemental Services; Master Agreement.

7.1   TCP may provide to Client supplemental services in accordance with a Statement of Work or a separate services agreement.

7.2   Client may elect to purchase additional products and services via Order Forms from time to time. The Parties agree that this Agreement is a master agreement such that additional transactions, excluding leased hardware, will be governed by the terms and conditions hereof. Pricing for additional transactions shall be in accordance with TCP's then-current pricing schedule. Client agrees that absent TCP's express written acceptance thereof indicated by execution by an officer of TCP, the terms and conditions contained in any purchase order or other document issued by Client to TCP for the purchase of additional services, shall not be binding on TCP to the extent that such terms and conditions are additional to or inconsistent with those contained in this Agreement.

7.3   Hardware purchased from TCP and incorporated into TCP Services requires the purchase of a Hardware Support and Maintenance Agreement, which shall be renewed for the term of this Agreement.

8.   Use Fees.

8.1   In consideration for the performance of the TCP Services, Client shall pay TCP the Use Fees. During the Term, Client will be billed in advance an amount equal to charges as indicated in the applicable invoice or Order Form. All other charges for TCP Services received and expenses incurred during a month will be billed at the end of the month in which the TCP Services were provided. Payment by Client for all Use Fees is due upon receipt of each TCP invoice, and in no event shall such payment be received by TCP later than thirty (30) days after the invoice, except in cases where a Net Terms Agreement has been authorized by TCP. All payments will be made to TCP in U.S. dollars.

8.2   TCP Services charges will be equal to the number of total Active Licenses multiplied by the Monthly License Fee which is based on the aggregated Permissions for each Active License. Client is responsible for Monthly License Fees for the maximum number of Active Licenses during any calendar month. Client may add additional Employees, Designated Users and Permissions as desired each month by paying the Monthly License Fees on the next billing cycle. Client agrees to promptly update the status in the TCP Services for any Active License which has been terminated or suspended.

8.3   Employees and Designated Users added at any time during a calendar month will be charged in full for that billing period. Because Client is billed in advance for TCP Services, if Client increases its Active License count or increases Permissions during a calendar month, Client will receive an invoice reflecting the increased Active License count with overage charges incurred from the previous month and prorated over the number of months remaining in the Term.

8.4   Hardware Support and Maintenance charges will be equal to the percentage set forth in the applicable Hardware Support and Maintenance Agreement multiplied by the total purchase price of the Supported Hardware.

8.5   Except as set forth in Section 8.6 of this Agreement, after the first anniversary of this Agreement, TCP may increase the Use Fees at any time effective thirty (30) days after providing notice to Client; provided, however, that any such increase will not occur more than once in a consecutive twelve (12) month period.

8.6   Client may prepay greater than one (1) year with TCP Services and, in doing so, suspend any increase in Use Fees until expiration of the Initial Term. After the Initial Term, TCP may increase the Use Fees by no more than 10% at any time effective thirty (30) days after providing notice to Client; provided, however, that any such increase will not occur more than once in a consecutive twelve (12) month period.

9.   Taxes. As applicable, Client shall, in addition to the other amounts payable under this Agreement, pay all sales, use, value added or other taxes, whether federal, state or local, however named, arising out of the transactions contemplated by this Agreement, except that Client shall not be liable for taxes based on TCP's aggregate income.

10.   Term; Guaranteed Payment. This Agreement commences on the Effective Date and, unless terminated earlier in accordance with Section 11, will remain in effect for the term specified in the applicable Order Form ("Initial Term") and then shall automatically renew for subsequent **one (1) year terms**   thereafter, unless either Party gives written notice of non-renewal at least thirty (30) days prior to the end of the then current term (the Initial Term and subsequent renewal terms being referred to as the "Term").   For avoidance of doubt, except as otherwise set forth in the terms and conditions of this Agreement and the Johnson County Contract Terms Addendum, all fees mutually agreed to in an Order Form are committed and non-cancelable.

11.   Termination for Cause. A Party may terminate this Agreement for cause if (i) the other Party breaches any material term or condition of this Agreement and fails to cure such breach within thirty (30) days after receipt of written notice of the same, or in the case of failure to pay Use Fees, thirty (30) days; (ii) the other Party becomes the subject of a voluntary petition in bankruptcy or any voluntary proceeding relating to insolvency, receivership, liquidation or composition for the benefit of creditors; or (iii) the other Party becomes the subject of an involuntary petition in bankruptcy or any involuntary proceeding relating to insolvency, receivership, liquidation or composition for the benefit of creditors, and such petition or proceeding is not dismissed within sixty (60) days of

filing. Notwithstanding the foregoing, if a material breach by Client, by its nature, cannot be cured, TCP may terminate this Agreement immediately.

12.   Effect of Termination. Without prejudice to any right or remedy of a Party with respect to the other Party's breach hereunder, upon the effective date of any termination of this Agreement:

12.1   TCP's obligation to provide the TCP Services shall immediately terminate;

12.2   after such termination and upon Client's reasonable request, no later than thirty (30) days from termination, TCP shall provide Client Data to Client in a SQL database file format; and

12.3   within thirty (30) days of such termination, each Party will destroy or return all additional Confidential Information of the other Party in its possession and will not make or retain any copies of such Confidential Information except as required to comply with any applicable legal or accounting record keeping requirement.

13.   Intellectual Property Ownership. Subject to the limited rights expressly granted hereunder, TCP reserves all right, title, and interests in and to the TCP Services and TCP Technology, including all intellectual property rights embodied therein, which shall remain the sole and exclusive property of TCP or its licensors. No rights are granted to Client hereunder other than as expressly set forth herein. This Agreement does not transfer from TCP to Client any ownership interest in the TCP Services or TCP Technology and does not transfer from Client to TCP any ownership interest in Client Data.

14.   Client Representations and Warranties.

14.1   Client represents and warrants that (i) it has the legal right to enter into this Agreement and perform its obligations hereunder, and (ii) the performance of Client's obligations and use of the TCP Services by Client, its Designated Users and Employees will not violate any applicable laws, including all applicable domestic and international data protection laws, or cause a breach of duty to any third party, including Employees.

14.2   Client represents and warrants that all Personal Data included in the Client Data has been collected from all Employees and Designated Users and will be transferred to TCP in accordance with all applicable data protection laws, including, but not limited to, the EU General Data Protection Regulation 2016/679 and the Illinois Biometric Information Privacy Act, to the extent applicable. Client acknowledges and agrees that (i) TCP is a service provider and processes Client Data solely on behalf of and at the direction of Client, and exercises no control whatsoever over the content of the Client Data passing through the TCP Services or that is otherwise transferred by Client to TCP, and (ii) it is the sole responsibility of Client to ensure that the Client Data passing through the TCP Services or that is otherwise transferred by Client to TCP complies with all applicable laws and regulations, whether now in existence or hereafter enacted and in force.

14.3   Client represents and warrants that its Affiliates' use of the TCP Services, if any, shall not relieve Client of any liability under this Agreement, and Client shall be responsible and liable for the acts and omissions of its Affiliates hereunder as if performed or omitted by Client.

14.4   In the event of any breach of any of the foregoing representations or warranties in this Section 14, in addition to any other remedies available at law or in equity, TCP will have the right to suspend immediately any TCP Services if deemed reasonably necessary by TCP to prevent any harm to TCP and its business. TCP will provide notice to Client and an opportunity to cure, if practicable, depending on the nature of the breach. Once cured, TCP will promptly restore the TCP Services.

15.   **TCP Representations and Warranties**. TCP represents and warrants that (i) it has the legal right to enter into this Agreement and perform its obligations hereunder, and (ii) the performance of its obligations and delivery of the TCP Services to Client will not violate any applicable laws or regulations of the United States or cause a breach of any agreements between TCP and any third parties.

16.   **Mutual Representations and Warranties.** Each Party represents and warrants that it has implemented a comprehensive written information security program that includes appropriate administrative, technical and physical safeguards to: (i) ensure the safety and confidentiality of Personal Data; (ii) protect against unauthorized access to and use of Personal Data; (iii) protect against anticipated threats or hazards to the security or integrity of Personal Data, and (iv) comply with applicable data protection laws.

17.   **Limited Warranty**. TCP represents and warrants that the TCP Services and related products, as described with this Agreement, will perform in accordance with all TCP published documentation, contract documents, contractor marketing literature, and any other communications attached to or referenced in this Agreement and that the TCP Services will be free of errors and defects that materially affect the performance of the TCP Services ("Limited Warranty"). Client's sole and exclusive remedy for breach of the Limited Warranty shall be the prompt correction of non-conforming TCP Services at TCP's expense.

18.   **Warranty Disclaimer**. EXCEPT FOR THE EXPRESS LIMITED WARRANTY SET FORTH IN SECTION 170 (LIMITED WARRANTY), THE TCP SERVICES ARE PROVIDED BY TCP ON AN "AS IS" BASIS, AND CLIENT'S USE OF THE TCP SERVICES IS AT CLIENT'S OWN RISK. TCP AND ITS SUPPLIERS DO NOT MAKE, AND HEREBY DISCLAIM, ANY AND ALL OTHER EXPRESS AND/OR IMPLIED WARRANTIES, INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AGAINST HIDDEN DEFECTS, AND ANY WARRANTIES ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE. TCP DOES NOT WARRANT THAT THE TCP SERVICES WILL BE UNINTERRUPTED OR ERROR-FREE. NOTHING STATED OR IMPLIED BY TCP WHETHER THROUGH THE TCP SERVICES OR OTHERWISE SHOULD BE CONSIDERED LEGAL COUNSEL. TCP HAS NO RESPONSIBILITY TO NOTIFY CLIENT OF ANY CHANGES IN THE LAW THAT MAY AFFECT USE OF THE TCP SERVICES. ANY ORAL STATEMENT OR

IMPLICATION BY ANY PERSON CONTRADICTING THE FOREGOING IS UNAUTHORIZED AND SHALL NOT BE BINDING ON TCP. CLIENT ACKNOWLEDGES THAT IN ENTERING INTO THIS AGREEMENT, CLIENT HAS RELIED UPON CLIENT'S OWN EXPERIENCE, SKILL AND JUDGMENT TO EVALUATE THE TCP SERVICES AND THAT CLIENT HAS SATISFIED ITSELF AS TO THE SUITABILITY OF SUCH SERVICES TO MEET CLIENT'S BUSINESS AND LEGAL REQUIREMENTS.

19.   Indemnification.

19.1   Client hereby acknowledges and agrees that TCP may not be aware of all rights available to Client's Designated Users or Employees under all data protection regimes. Client, to the extent permitted by Texas law, and subject to the limitations and provisions of Article 11, Section 7 of the Texas Constitution shall indemnify, defend and hold harmless TCP, its Affiliates, Subprocessors, officers, managers, directors, employees, agents, advisors and other representatives (the "TCP Indemnitees") from and against any lawsuit, liability, loss, cost or expense (including reasonable attorneys' fees) actually incurred or suffered by TCP Indemnitees of every kind and nature to the extent caused by or resulting from (i) any breach of a representation or warranty made by Client under this Agreement; or (ii) a third-party claim made against a TCP Indemnitee arising from or related to Client's failure to comply with any applicable domestic or foreign data protection laws or regulations. Client shall have the right to control any defense provided pursuant to this Section 19.1, provided, however, that Client shall not, without TCP's prior written consent, (A) enter into any settlement or compromise or consent to the entry of any judgment that does not include the delivery by the claimant or plaintiff to the applicable TCP Indemnitee of a written release from all liability in respect of such third party claim, or (B) enter into any settlement or compromise with respect to any third party claim that may adversely affect the applicable TCP Indemnitee other than as a result of money damages or other monetary payments that are indemnified hereunder.

19.2   TCP will indemnify, defend and hold harmless Client and its Affiliates (the "Client Indemnitees") from and against any lawsuit, liability, loss, cost or expense actually incurred or suffered by a Client Indemnitee of every kind and nature to the extent caused by or resulting from a third-party claim made against a Client Indemnitee that the TCP Technology infringes on any U.S. intellectual property right of a third party; provided, however, that TCP is notified in writing of such claim promptly after such claim is made upon Client. TCP shall have the right to control any defense provided pursuant to this Section 19.2. In no event shall Client settle any such claim without TCP's prior written approval. If such a claim is made or if the TCP Technology, in TCP's opinion, is likely to become subject to such a claim, TCP may, at its option and expense, either (i) procure the right to continue using the TCP Technology or portion thereof, or (ii) replace or modify the TCP Technology or portion thereof so that it becomes non-infringing. If TCP determines that neither alternative is reasonably practicable, TCP may terminate this Agreement with respect to the portion of the TCP Technology infringing or alleged to infringe. TCP shall have no liability or obligation under this Section 19.2 if the claim arises from (i) any alteration or modification to the TCP Technology other than by TCP, (ii) any combination of the TCP Technology with other programs or data not furnished by TCP,

or (iii) any use of the TCP Technology prohibited by this Agreement or otherwise outside the scope of use for which the TCP Technology is intended.

20.   Liability Limitation.   Except for claims arising out of <u>Section 19.2</u> (TCP's Intellectual Property Indemnity) and <u>Section 5</u> (Confidential Information), in no event shall TCP's aggregate liability, if any, including liability arising out of contract, negligence, strict liability in tort or warranty, or otherwise, exceed the sum of amounts paid by Client to TCP during the twelve (12) months immediately prior to the date of the claim.

21.   Notices.   Any notice or communication required or permitted to be given hereunder may be delivered by hand, deposited with an overnight courier, sent by email (provided delivery is confirmed), or U.S. Mail (registered or certified only), return receipt requested, to the address set forth on the initial page hereof.

22.   Assignment.   This Agreement shall not be assigned by either Party without the prior written consent of the other Party, which shall not be unreasonably withheld; provided, however, that either Party may, without the prior consent of the other, assign all of its rights under this Agreement to (i) such Party's parent company or a subsidiary of such Party, (ii) a purchaser of all or substantially all of such Party's assets related to this Agreement, or (iii) a third party participating in a merger, acquisition, sale of assets or other corporate reorganization in which such Party is participating. This Agreement shall bind and inure to the benefit of the Parties and their respective successors and permitted assigns.

23.   Continuing Obligations.   Those clauses the survival of which is necessary for the interpretation or enforcement of this Agreement shall continue in full force and effect in accordance with their terms notwithstanding the expiration or termination hereof, such clauses to include the following: (i) any and all warranty disclaimers, limitations on or limitations of liability and indemnities granted by either Party herein; (ii) any terms relating to the ownership or protection of intellectual property rights or Confidential Information of either Party, or any remedy for breach thereof; and (iii) the payment of taxes, duties, or any money to either Party hereunder.

24.   Marketing.   During the Term hereof, Client agrees that TCP may publicly refer to Client, orally and in writing, as a customer of TCP. Any other reference to Client by TCP requires the written consent of Client.

25.   Force Majeure.   Except for the obligation to make payments, neither Party will be liable for any failure or delay in its performance under this Agreement due to any cause beyond its reasonable control, including acts of war, terrorism, acts of God, epidemic, earthquake, flood, embargo, riot, sabotage, labor shortage or dispute, governmental act or complete or partial failure of the Internet (not resulting from the actions or inactions of TCP), provided that the delayed Party: (i) gives the other Party prompt notice of such cause, and (ii) uses its reasonable commercial efforts to promptly correct such failure or delay in performance.

26.   Dispute Resolution. For any dispute, controversy or claims arising out of or relating to this Agreement or the breach, termination, interpretation or invalidity thereof or any Invoice, or Order Form, the Parties shall endeavor for a period of two (2) weeks to resolve the Dispute by negotiation. This period may be extended by mutual agreement of the Parties. In the event the Dispute is not successfully resolved, the Parties agree to submit the Dispute to litigation in the State District Courts of Johnson County, Texas or the Federal District Courts of the Northern District of Texas, Dallas Division.

27.   Class Action Waiver. THE PARTIES WAIVE ANY RIGHT TO ASSERT ANY CLAIMS AGAINST THE OTHER PARTY AS A REPRESENTATIVE OR MEMBER IN ANY CLASS OR REPRESENTATIVE ACTION, EXCEPT WHERE SUCH WAIVER IS PROHIBITED BY LAW OR DEEMED BY A COURT OF LAW TO BE AGAINST PUBLIC POLICY. TO THE EXTENT EITHER PARTY IS PERMITTED BY LAW OR COURT OF LAW TO PROCEED WITH A CLASS OR REPRESENTATIVE ACTION AGAINST THE OTHER, THE PARTIES AGREE THAT: (I) THE PREVAILING PARTY SHALL NOT BE ENTITLED TO RECOVER ATTORNEYS' FEES OR COSTS ASSOCIATED WITH PURSUING THE CLASS OR REPRESENTATIVE ACTION (NOT WITHSTANDING ANY OTHER PROVISION IN THIS AGREEMENT); AND (II) THE PARTY WHO INITIATES OR PARTICIPATES AS A MEMBER OF THE CLASS WILL NOT SUBMIT A CLAIM OR OTHERWISE PARTICIPATE IN ANY RECOVERY SECURED THROUGH THE CLASS OR REPRESENTATIVE ACTION.

28.   Applicable Law; Jurisdiction; Limitations Period. This Agreement shall be construed under the laws of the State of Texas, without regard to its principles of conflicts of law.

29.   Counterparts; Facsimile Signatures. This Agreement may be executed in multiple counterparts, each of which, when executed and delivered, shall be deemed an original, but all of which shall constitute one and the same instrument. Any signature page of any such counterpart, or any email transmission thereof, may be attached or appended to any other counterpart to complete a fully executed counterpart of this Agreement, and any email transmission of any signature of a Party shall be deemed an original and shall bind such Party.

30.   Miscellaneous. This Agreement along with the JOHNSON COUNTY CONTRACT TERMS ADDENDUM, constitutes the entire understanding of the Parties with respect to the subject matter of this Agreement and merges all prior communications, understandings, and agreements. This Agreement may be modified only by a written agreement signed by the Parties. In the case of any conflict between this Agreement and the Privacy Policy, the Privacy Policy shall control. The failure of either Party to enforce any of the provisions hereof at any time shall not be a waiver of such provision, any other provision, or of the right of such Party thereafter to enforce any provision hereof. If any provision of this Agreement is declared invalid or unenforceable, such provision shall be deemed modified to the extent necessary and possible to render it valid and enforceable. In any event, the unenforceability or invalidity of any provision shall not affect any other provision of this Agreement, and this Agreement shall continue in full force and effect and

be construed and enforced as if such provision had not been included or had been modified as above provided.

[Signature Page Follows]

Accepted by:

Client   **TimeClock Plus, LLC**

By: _____   By: _____

Name: Christopher Boedeker   Name: Derek McIntyre

Title: County Judge   Title: COO

Exhibit B

_____

JOHNSON COUNTY CONTRACT TERMS
ADDENDUM TO TIMECLOCK PLUS, LLC AGREEMENT
(TCP Timeclock)

_____

The Johnson County Commissioners Court Finds, and the Parties Agree, as Follows:

1.1

This **Addendum** is part of an Agreement between **JOHNSON COUNTY, TEXAS,** a political subdivision of the State of Texas, (hereinafter referred to as "**COUNTY**" or **"JOHNSON COUNTY"** and **TIMECLOCK PLUS, LLC TIMECLOCK PLUS, LLC** may be referred to herein as **"TIMECLOCK PLUS"** or **"COMPANY"**.

1.2

JOHNSON COUNTY and TIMECLOCK PLUS as applicable, may be collectively identified as the **"Parties"** or each individually a **"Party"**. **This Addendum is part of the Agreement with TIMECLOCK PLUS and is intended to modify (as set forth in this Addendum) all documents, including any Quotes or Proposals put forth by TIMECLOCK PLUS. This Addendum modifies (as set forth in this Addendum)** any other document proffered to **COUNTY by TIMECLOCK PLUS** or their agents and other documents defining the Agreement between **JOHNSON COUNTY, TEXAS and TIMECLOCK PLUS.**

1.3

NOT APPLICBLE (Co-op Reference)

1.4

This Addendum, combined with the terms of the attached Proposal from TIMECLOCK PLUS, LLC, upon execution by both parties, constitutes a contractual Agreement between JOHNSON COUNTY, TEXAS and TIMECLOCK PLUS, LLC

2.1

This Agreement will be governed by and construed according to the laws of the <u>State of Texas</u>. Venue for any action or claim arising out of the Agreement must be in the state district courts in Johnson County, Texas or the federal district courts in Dallas County, Texas.

2.2

Any provision stating that County agrees to waive any right to trial by jury is hereby

deleted.

2.3

Limitations for the right to bring an action, regardless of form, shall be governed by the laws of the State of Texas, Texas Civil Practice and Remedies Code §16.070, as amended, and any provision to the contrary is hereby deleted.

2.4

Under Texas law, a contract with a governmental entity that contains a claim against future revenues is void; therefore, any term which provides for such a claim is hereby deleted. JOHNSON COUNTY will, upon request of a party to the contract, certify the funds available to fulfill the terms of this Agreement.

3.1

The Parties agree that under the Constitution and laws of the State of Texas, JOHNSON COUNTY **CANNOT enter into an agreement whereby JOHNSON COUNTY agrees to indemnify or hold harmless any other party**; therefore, all references of any kind to JOHNSON COUNTY indemnifying and holding harmless any individuals or entities for any reason whatsoever are hereby deleted.

3.2

Article XI, Section 7(a) of the Texas constitution provides in relevant part:

> **… But no debt for any purpose shall ever be incurred in any manner by any city or county unless provision is made, at the time of creating the same, for levying and collecting a sufficient tax to pay the interest thereon and provide at least two per cent (2%) as a sinking fund, except as provided by Subsection (b) …**

This provision is interpreted with respect to contractual obligations of Texas county and city government entities to prohibit such government entities from entering into an indemnity agreement and to nullify such agreement provisions.

4.1

The Parties agree and understand that COUNTY is a political subdivision of the State of Texas, and therefore has certain governmental immunity, sovereign immunity and limitations on liability, and that COUNTY'S general liability and vehicle insurance coverage is with the Texas Association of Counties Risk Pool and said "insurance coverage" is limited to the statutory maximum limits of the Texas Tort Claims Act; therefore, any provisions to the contrary are hereby deleted. The Parties agree and understand that COUNTY does not waive any of its common law, statutory or constitutional defenses to which it may be entitled.

4.2

The Parties agree and understand that COUNTY will not agree to waive any rights and remedies available to COUNTY under the Uniform Commercial Code ("UCC"); therefore, any provision to the contrary is hereby deleted.

4.3

The Parties agree and understand that COUNTY will not agree to be responsible for any sales tax, use tax, or any other taxes, fees, fines or penalties that may be imposed, levied or assessed by any federal, state or local government or agency which relates to the Agreement, the equipment or its use; therefore, any provision to the contrary is hereby deleted.

4.4

The Parties agree and understand that COUNTY will provide statutory workers compensation for its employees; however, COUNTY does not agree to include a waiver of subrogation, and therefore any provisions to the contrary are hereby deleted.

5.1

Pursuant to Texas Government Code Section 2251.021 and this Agreement, a payment by a governmental entity under a contract is overdue on the 31st day after the later of:
   a.   the date the governmental entity receives the goods under the contract;
   b.   the date the performance of the service under the contract is completed; or
   c.   the date the governmental entity receives an invoice for the goods or service.

Pursuant to Texas Government Code Section 2251.025 and this Agreement, a payment begins to accrue interest on the date the payment becomes overdue. The rate of interest that accrues on an overdue payment is the rate in effect on September 1 of the fiscal year in which the payment becomes overdue. The rate in effect on September 1 is equal to the sum of: (1) one percent; and (2) the prime rate as published in the Wall Street Journal on the first day of July of the preceding fiscal year that does not fall on a Saturday or Sunday. Interest on an overdue payment stops accruing on the date the governmental entity or vendor mailed or electronically transmits the payment. Therefore, all provisions to the contrary are hereby deleted.

5.2

Texas Local Government Code Section 113.064. Approval of Claims by County Auditor, provides:

> **"(a) In a county that has the office of county auditor, each claim, bill, and account against the county must be filed in sufficient time for the auditor to examine and approve it before the meeting of the commissioners court. A claim, bill, or account may not be allowed or paid until it has been examined and approved by the auditor…."**

Texas law requires that all disbursements of County funds be approved by the County Auditor and the Commissioners Court prior to such disbursement. JOHNSON COUNTY can and will make due disbursements following the approval of the disbursement by Commissioners Court (following the COUNTY'S receipt and review of a proper invoice through the proper COUNTY department

responsible for the purchase of the goods or services). JOHNSON COUNTY cannot and does not authorize any entity to directly access County funds. TIMECLOCK PLUS understands that the JOHNSON COUNTY Commissioners Court normally meets on the second and fourth Monday of each month or the day following such Monday if the Monday is a County holiday. TIMECLOCK PLUS further understands that invoices must be received by the COUNTY **not less than fourteen (14) days prior** to the Commissioners Court meeting in order for a payment to be reviewed by the necessary departments and offices and placed on the "bill run" for the Commissioners Court.

5.3

JOHNSON COUNTY does not authorize TIMECLOCK PLUS or any entity to initiate debit entries to JOHNSON COUNTY'S account at any financial institution. Any provision in any document authorizing an entity to access COUNTY funds or financial accounts electronically or otherwise and to make withdrawals or transfers of such funds is hereby deleted and is of no effect and the Agreement shall be deemed modified to comport with payment procedure prescribed by Texas law for Texas counties.

6.1

No officer, member, or employee of COUNTY, and no member of its governing body and no other public officials of the governing body of the locality or localities in which the project or purchase is situated or being carried out who exercises any functions or responsibilities in the review or approval of the undertaking or carrying out of this project or purchase shall participate in any decision relating to this Agreement which affects his/her personal interest, have any personal or pecuniary interest, direct or indirect, in this Agreement or the proceeds thereof.

6.2

To the extent, if any, that any provision in this Agreement is in conflict with Texas Government Code §552.001 *et seq.,* as amended (the "Public Information Act"), the same shall be of no force and effect. Furthermore, it is expressly understood and agreed that JOHNSON COUNTY, its officers and employees may request advice, decisions and opinions of the Attorney General of the State of Texas in regard to the application of the Public Information Act. In the event of a request for documents or materials pursuant to the Texas Public Information Act (Texas Government Code Chapter 552) or similar law pertaining to documents or information COUNTY reasonably believes that **TIMECLOCK PLUS** might lawfully seek to claim as confidential, then COUNTY will forward the request to **TIMECLOCK PLUS.** It shall be the obligation of **TIMECLOCK PLUS** to prepare and submit to the Texas Attorney General's Office any claim and supporting brief or materials necessary to assert a claim that the documents or materials may be withheld pursuant to Texas Government Code Chapter 552 or other applicable law. County will cooperate with **TIMECLOCK PLUS** in making such submission to the Texas Attorney General's Office. **TIMECLOCK PLUS acknowledges and understands that contracts, agreements, payment and revenue of a political subdivision of the State of Texas are public information and are not confidential.**

6.3

Services and products provided under the Agreement shall be provided in accordance with all applicable state and federal laws.

6.4

Under the Constitution and laws of the State of Texas, public property is exempt from forced sales and liens may not attach thereto.

6.5

It is understood and agreed that JOHNSON COUNTY will not be subject to arbitration; therefore, any paragraph or provision requiring arbitration, is hereby deleted.

6.6

JOHNSON COUNTY shall be responsible for the acts or failure to act of its employees, agents or servants, provided; however, its responsibility shall be subject to the terms, provisions and limitations of the Constitution and laws of the State of Texas, particularly the Texas Tort Claims Act.

7.1

TIMECLOCK PLUS certifies that pursuant to Section 231.006 of the Texas Family Code (regarding unpaid child support) that the individual or business entity named in this contract is not ineligible to receive the specified payment(s) and acknowledges that this contract may be terminated and payment may be withheld if this certification is inaccurate. **TIMECLOCK PLUS** hereby certifies that it is not ineligible to receive State or Federal funds due to child support arrearages

7.2

TIMECLOCK PLUS verifies that it does not boycott Israel and will not boycott Israel during the term of this contract. The term "boycott Israel" is as defined by Texas Government Code Section 808.001, effective September 1, 2017. **TIMECLOCK PLUS** verifies that it is not engaged in business with Iran, Sudan, or any foreign terrorist organization. The term "foreign terrorist organization" means an organization designated as foreign terrorist organization by the United States Secretary of State as authorized by 8 U.S.C. Section 1189.

7.3

TIMECLOCK PLUS verifies that it complies with Texas Government Code Chapter 2274 and further verifies that it does not have a practice, policy, guidance, or directive that discriminates against a firearm entity or firearm trade association; and, will not discriminate during the term of the contract against a firearm entity or firearm trade association.

7.4

TIMECLOCK PLUS verifies that it complies with Texas Government Code Chapter

2274 and further verifies that it:

(1) does not boycott energy companies; and

(2) will not boycott energy companies during the term of the contract.

In this provision:

(1) "Boycott energy company" has the meaning assigned by Section 809.001.

(2) "Company" has the meaning assigned by Section 809.001, except that the term does not include a sole proprietorship.

(3) "Governmental entity" has the meaning assigned by Section 2251.001.

7.5 RESERVED

7.6

TIMECLOCK PLUS certifies by signature of its authorized representative on this document that it does and will so long as this Agreement is in effect comply fully with Section 889 of the National Defense Authorization Act for Fiscal Year 2019 (NDAA FY19) and Section 5949 of the National Defense Authorization Act for Fiscal Year 2023 (NDAA FY23) and with any additional existing and future "China Tech Prohibitions" promulgated or enacted by the Unites States Government.

7.7

TIMECLOCK PLUS certifies by signature of its authorized representative on this document that it complies with the China Tech Prohibitions and any products used during the professional services will also comply with the "China Tech Prohibitions".

7.8

Further, **TIMECLOCK PLUS** certifies by signature of its authorized representative on this document that it will not use any products or equipment on this project that does not comply with the "China Tech Prohibitions".

8.1

Notwithstanding any other provisions contained in the contract documents, any amendment to the terms of the contract must be specifically approved by the Commissioners Court

of JOHNSON COUNTY and signed by the Johnson County Judge or the COUNTY employee or official to whom authority has been explicitly delegated by the Commissioners Court.

8.2

Notwithstanding any other provision in this Addendum or the associated documents, to the extent **TIMECLOCK PLUS** is being contracted to provide information technology and services or to maintain and make available information for use by JOHNSON COUNTY and the public, including documents, data, content and records then said documents, data, content and records are and shall be the exclusive property of JOHNSON COUNTY, TEXAS or the State of Texas or a political subdivision thereof.

8.3

To the extent TIMECLOCK PLUS is being contracted to provide construction management services, construction services or engineering services and to accumulate data and information then TIMECLOCK PLUS shall make any accumulated data, records or information available for use by Johnson County. Accumulated data, records and information are and shall be the property of Johnson County, Texas or the State of Texas.

8.4

At the termination of this Agreement, to the extent TIMECLOCK PLUS possesses or controls access to JOHNSON COUNTY data, upon request by COUNTY, TIMECLOCK PLUS must copy the data to a storage medium in common use at the time or as agreed to by the Information Technology Department of JOHNSON COUNTY and deliver such medium and data to JOHNSON COUNTY INFORMATION TECHNOLOGY DEPARTMENT. TIMECLOCK PLUS recognizes such data is data of the State of Texas or a political subdivision thereof and must be maintained according to the laws of the State of Texas governing the retention and storage of such data. Destruction of such data contrary to law and contrary to the rules promulgated by the Texas State Library and Archives Commission may be subject to criminal prosecution and civil liability.

8.5

All provisions of the agreement are modified such that in no event would JOHNSON COUNTY have less than 120 days from notice of termination of the Agreement to secure any data or records in a useable and readable format. JOHNSON COUNTY'S securing of such data or records is intended to be done and will be allowed to be accomplished in a common and economically efficient method extant at the time of extracting, copying and securing such data and records.

8.6

The parties agree Johnson County is NOT bound and shall not be bound to or liable for any condition, duty, obligation or requirement that is set forth only by reference to additional Documents that are not part of the physical document approved by the

Commissioners Court and made part of the minutes of the Johnson County Commissioners Court. Provisions which COMPANY seeks to make terms of the contract or agreement by references to links or websites for contract terms are rejected by JOHNSON COUNTY and CANNOT and WILL NOT be enforced against JOHNSON COUNTY.

8.7

JOHNSON COUNTY is not subject to any provision that may be changed without notice or that may be changed without specific overt consideration and approval by the Commissioners Court of Johnson County acting on that change, modification or amendment to the contact or its terms occurring after the date of the execution of this Addendum.

8.8

Notwithstanding any provision set forth in the Master Services and Purchasing Agreement for Agency or any other document put forth by TIMECLOCK PLUS, JOHNSON COUNTY does not waive any rights or remedies available to a Texas political subdivision pursuant to Texas law. This provision supersedes any contrary provision.

8.9

TIMECLOCK PLUS will not factor its receivables (from JOHNSON COUNTY) to any company or bank without the permission of the Johnson County Commissioners Court.

9.1

In the event of any conflict between the terms and provisions of this Addendum and the terms and provisions of those contractual provisions tendered to JOHNSON COUNTY in the Agreement, this Addendum shall control and amend the contractual provisions of the Agreement and any provision to the contrary is hereby deleted. *THE TERMS OF THIS JOHNSON COUNTY CONTRACT TERMS ADDENDUM SHALL BE FULLY OPERATIVE AND HAVE PRIORITY OVER ALL OTHER DOCUMENTS AND TERMS AND ANY TERM TO THE CONTRARY IN OTHER DOCUMENT(S) PUT FORTH BY TIMECLOCK PLUS IS HEREBY DELETED.*

APPROVED AS TO FORM AND CONTENT:

JOHNSON COUNTY:

Christopher Boedeker
As Johnson County Judge

Date 7-28-25

Attest: _____
County Clerk, Johnson County

Date 7-28-25

TIMECLOCK PLUS:

[signature]

Signature of Authorized Person

7/24/2025

Date

Derek McIntyre

Printed Name of Authorized Person

COO

Position of TIMECLOCK PLUS Authorized Person

Exhibit C
TCP SERVICE LEVEL AGREEMENT (SLA)

This Service Level Agreement is an addendum to the Master Licensing Agreement, hereafter referred to as the "Licensing Agreement", made and entered into by and between TimeClock Plus, LLC ("TCP") and Client. TCP reserves the right to continuously improve the Support and Maintenance and to adapt such services to changes in technology and to TCP's business environment. All Support and Maintenance will be provided in accordance with applicable data protection laws and the Privacy Policy which can be found at www.tcpsoftware.com/legal.

1.   **Definitions**. Capitalized terms herein, but not included in this Section 1, shall have the meaning set forth in the Licensing Agreement and/or attached Addendums.

　　1.1   "24/7 Support" means continuous service is provided for twenty-four hours per day, seven days per week, and throughout the year.

　　1.2   "Downtime" shall mean "unplanned" network unavailability within TCP's United States network for thirty (30) consecutive minutes due to the failure of TCP to provide services for such period. Downtime shall not include any packet loss or network unavailability during TCP's scheduled maintenance of the Internet Data Center(s), network and software services.

　　1.3   "Issue" means a failure of the Software to substantially conform to the functional specifications set forth in TCP published documentation.

　　21.4   "Performance Problem" shall mean a material deterioration in the performance of the Humanity Services excluding any Downtime.

　　1.5   "Response Time" means the time period in which the assigned support resource shall provide Client with an initial technical response as a result of an Issue reported by Client.

　　1.6   "Service Credit" shall mean an amount equal to the pro-rata monthly recurring connectivity charges (i.e., all monthly recurring bandwidth-related charges) for one (1) day of software services.

　　1.7   "Software" means the certain software program(s) purchased by Client. Software includes TCP Services as defined in the Licensing Agreement.

　　1.8   "Standard Support" means the Standard support level of Support and Maintenance as set out in Section 3.

　　1.9   "Standard Support Hours" means the hours between 7:00 am PST and 7:00 pm PST, excluding Saturday, Sunday, and TCP recognized employee holidays.

　　1.10   "Support and Maintenance" means the support and maintenance services to be provided by TCP to the Client. All Support and Maintenance will be provided to Client in accordance with the terms of this Service Level Agreement.

　　1.11   "Term" has the same meaning as defined in the Order Form or Licensing Agreement.

　　1.12   "Updates" means service packs, patches, hot fixes, or workarounds for a particular version of the Software. All Updates are licensed to Customer and subject to the terms and conditions of the License Agreement.

1.13 "Workaround" means a modification or "patch" for a particular version of the Software, which may be of a temporary or interim nature, to help cure or avoid an Issue.

2. **Support and Maintenance Services**. In consideration of the Client's payment of the applicable fees related to the TCP Services, TCP agrees to provide Support and Maintenance for the duration of the Term, and solely for the Software.

3. **Software Support and Maintenance.**

3.1 Software Maintenance. TCP will provide 24/7 Support to Client via both telephone and electronic mail. Client may report an Issue during Standard Support Hours by calling 888-973-6030 or any time by emailing support@tcpsoftware.com. TCP shall use commercially reasonable efforts to maintain the Software so that it operates without Issues. Software maintenance includes the Software features that TCP makes generally available to its Client base during the applicable Term. These Software features, include Updates to the Software.

3.2 Software Support. Support Services include:

3.2.1 Information gathering and analysis of Software to identify Issues;

3.2.2 Chat, email, or telephone consultation regarding the use and operation of the Software that does not rise to the level of training;

3.2.3 Configuration changes for the Software;

3.2.4 Repair or replacement of open source software with functionally equivalent software; and

3.2.5 Issue correction in accordance with the Support Response Time Goals below.

3.3 Severity Classification and Response Time Goals. Issues are classified according to severity of impact on the use of the Software, according to the Support Response Time Goal chart below. All disputes regarding severity classification will be resolved by TCP in its sole discretion.

Support Response Time Goals

Severity	Impact	Response Time Goal
Level 1	Production system is down, impacting all applications and associated business systems. No Workaround exists.	A Level 1 Issue will immediately be assigned to a TCP Support Technician who will contact Client within one (1) business hour with an initial response. The support technician will then work without interruption on the Issue until a resolution is reached, either in the form of a complete fix, or an interim Workaround solution that will cause the level of urgency to drop to Level 2.
Level 2	Production system performance is degraded, but operational; Issue affects essential functions and no Workaround exists; or Issue is blocking critical systems tests or deliverables.	A Level 2 Issue will immediately be assigned to a TCP Support Technician who will contact Client within two (2) business hours with an initial response. The support technician will then work without interruption during standard support hours until a resolution is reached, either in the form of a complete fix, or an interim Workaround solution that will cause the level of urgency to drop to Level 3.
Level 3	General product questions relating to development, feature issues, or Documentation.	A Level 3 Issue will be assigned to a TCP Support Technician who will contact Client within one (1) business day with an initial response. The support technician will work on the issue during Standard Support Hours.

4.   **Performance Problem**. In the event that TCP discovers or is notified by Client that Client is experiencing a Performance Problem, TCP will take all commercially reasonably actions necessary to determine the source of the Performance Problem.

4.1   **Discovery of Source; Notification of Client**. Within four (4) hours of discovering or receiving notice of the Performance Problem, TCP will use commercially reasonable efforts to determine whether the source of the Performance Problem is limited to the Humanity Services or whether the Performance Problem arises from the Client equipment or Client's connection to the Internet. TCP will notify Client of its findings regarding the source of the Performance Problem promptly after the additional four (4) hour period.

4.2   **Correction**. If the source of the Performance Problem is within the sole control of TCP, then TCP will use commercially reasonable efforts to remedy the Performance Problem within four (4) hours of determining the source of the Performance Problem. If the source of and remedy to the Performance Problem reside outside of the sole control of TCP, then TCP will use commercially reasonable efforts to notify the party responsible for the source of the Performance Problem and cooperate with it to resolve such problem as soon as possible.

4.3   **Service Credits for Performance Problems**. In the event that TCP (i) is unable to determine the source of the Performance Problem within the time periods described in Section 5; or (ii) is the sole source of the Performance Problem and is unable to remedy such Performance Problem within the time period described in Section 6, TCP will deliver a Service Credit to Client for each four (4) hour period incurred in excess of the time periods for identification and resolution described above; provided, however, that in no event shall Client be entitled to more than two (2) Service Credits for a given calendar day.

4.4   **Client Must Request Service Credit**. Upon receipt of a written request from Client for a prior calendar month requesting information regarding a specific instance of Downtime or Performance Problem, TCP will provide Client with a related incident report from which Client may determine any Downtime and/or Performance Problems. In order to receive a Service Credit in connection with a particular instance of Downtime or a Performance Problem, Client must notify TCP within thirty (30) days from the time Client becomes eligible to receive a Service Credit. Failure to comply with this requirement will forfeit Client's right to receive a Service Credit for the applicable instance of Downtime or Performance Problem.

4.5   **Maximum Service Credit**. The aggregate maximum number of Service Credits to be issued by TCP to Client for any and all Downtime and Performance Problems that occur in a single calendar month shall not exceed seven (7) Service Credits. Any Service Credits owed shall be issued in the TCP invoice in the month following the Downtime or Performance Problem, unless the Service Credit is due in Client's final month of Service. In such case, a refund for the dollar value of the Service Credit will be mailed to Client.

5.   **Obligations of Client**

5.1   Support Contact. All communications relating to Support and Maintenance will be supervised, coordinated, and undertaken by a primary Client contact unless additional contacts are designated as an approved contact persons by Client's primary contact. Issues related to the security of Clients Data, including but not limited to, password resets, may require approval of Client's primary contact.

5.2   Pre-Call Procedures. Prior to requesting support from TCP, Client shall comply with all published operating and troubleshooting procedures for the Software. If such efforts are unsuccessful in eliminating the Issue, Client shall then promptly notify TCP of the Issue. Client shall confirm that the following conditions are true before contacting Service Provider for support:

5.2.1   If possible, the situation giving rise to the Issue is reproducible in the Software;

5.2.2 The Client contact has the technical knowledge regarding the Software, any other software or hardware systems involved, and in the facts and circumstances surrounding the Issue;

5.2.3 The entire system is available to the Client contact during any communication with the assigned TCP support technician; and

5.2.4 If requested and required, Client must make available to TCP a technical representative during Standard Support Hours for all Issues. TCP reserves the right to suspend all work relating to any Issues during periods for which the Client does not provide access to Client's technical representative or requested data to continue to work on the Issue.

5.3   Remote Connection. If appropriate, Client will cooperate with TCP to allow and enable TCP to perform Support and Maintenance via remote connection using standard, commercially available remote control software.

5.4   Disclaimer. TCP shall not be responsible for providing Support and Maintenance, Updates, or any other support and maintenance to the extent that Issues arise because Client (i) misuses, improperly uses, mis-configures, alters, or damages the Software; (ii) uses the Software with any hardware or software not recommended or sold by TCP; (iii) uses the Software at any unauthorized location; or (iv) otherwise uses the Software in a manner not in accordance with the License Agreement.

6.   **Limitations of Support and Maintenance Services**.

6.1   Non-Compliance Problems. If Client notifies TCP of a problem and TCP correctly determines that the problem is due to Client's incorrect or improper use of the Software or failure to comply with the terms of the License Agreement an attached Addendums, the resolution of such problem is not covered by Support and Maintenance. However, TCP may provide additional services to correct the problem pursuant to a separate Statement of Work.

6.2   Third-Party Products. Support and Maintenance does not cover the operation or use of third-party hardware or software or Software modified by any party other than TCP or used in any manner in violation of the License Agreement or inconsistent with TCP published product documentation.

7.   **Downtime Periods**. In the event Client experiences Downtime, Client shall be eligible to receive a one-time Service Credit for each Downtime period; provided, however, that in no event shall Client be entitled to more than two (2) Service Credits for any given calendar day. For example, if Client experiences one (1) Downtime period, then Client shall be eligible to receive one (1) Service Credit; if Client experiences two (2) Downtime periods, whether from a single event or multiple events, then Client shall be eligible to receive two (2) Service Credits.

7.   **Termination; Effects of Termination**

7.1 TCP will provide Support and Maintenance services for the Term of the Agreement as defined by the applicable Order Form.

7.2 Termination of Support Terms. If TCP or Client terminates the License Agreement in accordance with the terms provided therein, then the Support and Maintenance hereunder will also terminate. Further, TCP may terminate this Agreement upon the following conditions:

7.2.1   if Client fails to make any payments due hereunder within ten (10) days after TCP delivers notice of default to Customer;

7.2.2   by giving prior written notice to Client if Client fails to perform any material obligation required of it hereunder, and such failure is not cured within thirty (30) days from Client's receipt of TCP's notice to cure such non-performance of material obligation; or

7.2.3   if Client files a petition for bankruptcy or insolvency, has an involuntary petition filed against it, commences an action providing for relief under bankruptcy laws, files for the appointment of a receiver, or is adjudicated a bankrupt concern.

7.3   Termination Option for Chronic Problems. Client may terminate this Agreement and without liability or penalty to TCP by notifying TCP within ten (10) days following the occurrence of either of the following: (i) Client experiences more than five (5) Downtime periods in any three (3) consecutive calendar month period; or (ii) Client experiences more than eight (8) consecutive business hours of Downtime due to any single event. Such termination will be effective thirty (30) days after receipt of such notice by TCP.

8.   **Warranty**. TCP warrants all services performed under this Agreement shall be performed in a workmanlike and professional manner. EXCEPT AS OTHERWISE STATED IN THIS AGREEMENT TCP MAKES NO OTHER WARRANTIES, EXPRESS OR IMPLIED INCLUDING EXPRESS OR IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT.

EXHIBIT D

TimeClock Plus, LLC.

Global Data Privacy Policy

Last Updated September 25th, 2024

As a provider of workforce management solutions, TimeClock Plus, LLC ("TCP Software," "we," or "us") respects the privacy of our clients and others who use our website, mobile application, products, and services. In connection with providing our services and operating our business and website, we process certain Personal Data, including from our Clients, prospective clients, and, for certain Clients, end-users of our products. We have adopted this Global Data Privacy Policy so that you can learn how we collect, use, and otherwise process your Personal Data.

This Global Data Privacy Policy covers information collected through the following websites:

1. TCPSoftware.com
2. Humanity.com
3. Aladtec.com
4. ScheduleAnywhere.com
5. WhenToWork.com
6. Timeco.com

This Global Data Privacy Policy, which includes each of the sub-policies identified below, applies to the Personal Data we collect from you, including via your access to and use of the Services and, for Clients, is incorporated into and is subject to the TCP Software Terms of Service, which can be found at: https://www.tcpsoftware.com/legal.

The Global Data Privacy Policy consists of and incorporates each of the following:

- TimeClock Plus, LLC Privacy Policy for All Personal Data Except U.S. Resident Biometric Data
- TimeClock Plus, LLC Privacy Policy for the Processing of Biometric Data from U.S. Residents
- TimeClock Plus, LLC Data Privacy Framework (DPF) Privacy Policy for Data Transferred to the United States from the EU, the UK (including Gibraltar) and/or Switzerland

This Global Data Privacy Policy uses certain defined terms identified in the "Definitions" section at the end of this Global Data Privacy Policy.

TimeClock Plus, LLC Privacy Policy for All Personal Data Except U.S. Resident Biometric Data

With the exception of biometric data collected from U.S. residents, which is addressed separately within the Global Data Privacy Policy, this policy explains how TCP processes, uses and discloses all Personal Data it collects, including from Clients, end-users of our products (e.g., Client staff) for those Clients for whom TCP hosts data, prospective clients, and individuals who visit our website.

In this Privacy Policy, you will find information regarding:

- Collection and Sources of Personal Data
    - Personal Data We Receive Directly From You
    - Personal Data We Host on Behalf of Clients

- o   Personal Data We Receive From Other Sources
- o   Cookies and Tracking Technologies
- Purposes for Processing and Disclosures of Personal Data
  - o   General Purposes for Processing and Disclosures of Any and All Categories of Personal Data
  - o   Other Purposes for Processing and Disclosures of Specific Categories of Personal Data
    - ▪ Personal Data We Receive Directly From You
    - ▪ Personal Data We Host on Behalf of Clients
    - ▪ Personal Data We Receive From Other Sources
- Data Sales
- Data Retention
- Protection of Personal Data
- International Data Transfers
- Your Rights & Choices
- Other Important Information about Our Practices
- Changes to This Privacy Policy
- Contact Us

Collection and Sources of Personal Data.

Personal Data We Receive Directly From You.

TCP may collect the following categories of Personal Data directly from you:

a. *Client Account Data*. We may collect Personal Data in connection with Client management and account set-up and management, finance, dispute resolution, and for consolidated management and reporting. Client Account Data may include contact information, billing and banking information, Client account preferences and settings, and Client communications concerning the implementation and maintenance of the Services.

b. *Communications Data*. We may collect Personal Data that you provide when you express an interest in obtaining additional information about the Services, have questions or concerns about the Services, use our "Contact Us" or similar features, sign up for our emails or attend an event or webinar, or download certain content. Such information may include contact information such as name, job title, company name, phone number, and email address.

c. *Human Resources Data*. We may collect Personal Data from employees and job applicants, including contact information, social security number, background reports, job history, certain health or dietary information, payroll and banking information, and other Personal Data incident to the employment relationship.

d. *Reputation & Creditworthiness Data*. We may collect Personal Data in connection with performing diligence on our Clients, prospective clients, Service Providers or prospective service providers, and business partners or prospects. This data may include contact details, information concerning business practices, creditworthiness, reputation and business history, and job titles or roles.

e. *Transaction and Payment Data.* When you sign up for events or purchase some or all of the Services, we may require that you provide contact information such as name and address, billing information, such as billing name and address, credit card number, or bank account information.

f. *Visitor Data*. We may collect Personal Data from you when you visit our offices, including your name, who you are visiting, company name, and time and date of arrival and departure.

Personal Data We Host on Behalf of Clients.

TCP processes and stores Personal Data concerning Client staff on behalf of those Clients who have engaged us to do so. In particular, we process the following categories of Personal Data for Clients:

   a. *Profile Data.* We may process general demographic data about you that you or your employer enters into the Services. Profile data may include username, password, first name, last name, address, email, phone number, job title, employee ID, taxpayer ID, gender, date or birth, hire date, termination date, language preference, payroll classification, employment classification, pay rates, work schedules, employment contracts, and labor union affiliation.
   b. *Service Data*. We may process Personal Data collected from you in connection with using the Services, including clock-in time, clock-out time, clock-in location, clock-out location, leave requests, including vacation, sick, and other third-party defined leave reasons, leave accruals, FMLA cases, and hours worked.
   c. *EU Resident Special Category Data*. We may collect certain "special categories" of Personal Data, as identified in the GDPR, from EU residents including photographic images, racial, or ethnic data, biometric data, physical or mental health data, and data concerning religious or other beliefs.

Personal Data We Receive From Other Sources.

We may also receive Personal Data about you from other sources, including:
   • Third-party lead providers from whom we have purchased Personal Data. We may combine this information with Personal Data provided by you. This "*Lead Data*" may include business contact data, social media data, and usage data (including web user behavior and IP addresses).
   • Consumer reporting agencies or other background investigation or credit check service providers in connection with our collection of Human Resources Data and Reputation and Creditworthiness Data.

Cookies and Tracking Technologies.

When you use the Services, we collect certain information by automated means, using technologies such as cookies, pixel tags, browser analysis tools, server logs and web beacons. For example, when you visit our website, we may place cookies on your computer.

Cookies are small text files that websites send to your computer or other Internet-connected device to uniquely identify your browser or to store information or settings in your browser. Cookies can contain and/or automatically collect information, such as a user identification code or IP address, which a website will use to track the pages and number of times you have visited, allowing us to recognize you when you return. They also help us provide a customized experience and enable us to detect certain kinds of fraud. The data read from these cookies may be linked to Personal Data. In many cases, you can manage cookie preferences and opt-out of having cookies and other data collection technologies used by adjusting the settings on your browser. All browsers are different, so visit the "help" section of your browser to learn about cookie preferences and other privacy settings that may be available.

Cookies fall into the subcategories below.

   a. *Essential Cookies*. Certain cookies are used for specific purposes that are essential to your secure use and navigation of our website. Without them, TCP may not be able to provide core website functions and features to you, and the website would not operate as well as you or TCP would

like. These cookies collect and use information such as your server preferences, single-session data and corresponding identifier, web beacons and log files (detailed below), and other credential-related information. For EU individuals, essential cookies also help inform TCP whether you require, or have already been served, an affirmative consent request in connection with the GDPR. Essential cookies include analytics cookies, which provide us data that allows TCP to better understand its users and improve the website based on what we have learned from that data.

b. *Preference Cookies*. Other cookies are used to collect and process information about your preferences and similar choices in connection with the website in order to optimize your browsing. Preference cookies include social media cookies, which collect information about your social media usage and other data you may have provided in connection with such usage (if you access the website through a social media website or mobile application, you may have social media cookies). If you wish to modify or change your social media cookies, please visit and review the settings on your applicable social media account(s).

c. *Advertising Cookies*. To help support the Services and further tailor your experience, TCP uses Google Analytics as a third-party vendor. For information on how Google Analytics uses data, please visit "How Google uses data when you use our partners sites or apps", located at http://bit.ly/2jXZ13Y.

We encourage you to consider keeping your cookies enabled because if you choose to disable the receipt of cookies, you may not be able to use or benefit from certain features of the website, particularly the features that are designed to personalize your experience.

Most web browsers automatically accept cookies, but generally allow users to modify their browser settings to display a warning before accepting a cookie, to accept cookies only from certain websites, and/or to refuse all cookies.

Pixel tags and web beacons are tiny graphic images placed on website pages or in our emails that allow us to determine whether you have performed a specific action. When you access these pages or open or click an email, the pixel tags and web beacons generate a notice of that action. These tools allow us to measure response to our communications and improve our web pages and promotions.

In many cases, the information we collect using cookies and other tools is only used in a non-identifiable way, without reference to Personal Data. For example, we use information we collect about website users to optimize our websites and to understand website traffic patterns. In some cases, we do associate the information we collect using cookies and other technology with your Personal Data. This policy applies to the information when we associate it with your Personal Data.

Although our website does not currently have a mechanism to recognize the various web browser "Do Not Track" signals, we do offer individuals choices to manage their preferences, as described above. We do expect our third-party adverting partners to use reasonable efforts to respect browser "Do Not Track" signals by not delivering targeted advertisements to website visitors whose browsers have a "Do Not Track" setting enabled. However, we understand that some companies do not have this capability today. To learn more about browser tracking signals and "Do Not Track," please visit http://www.allaboutdnt.org/.

Purposes for Processing and Disclosures of Personal Data.

General Purposes for Processing and Disclosures of Any and All Categories of Personal Data

In general, TCP may use and disclose *any* Personal Data it maintains about you as follows, pursuant to TCP's legitimate business interests and need to comply with law:

- To manage and mitigate risk, including for insurance functions, to ensure the proper functioning of the Services, to maintain the privacy and security of our data (such as through threat detection, disaster recovery and business continuity activities), and to conduct audits or investigations, in which case we may disclose your Personal Data to Service Providers, insurance providers, tax or financial authorities or consultants, and legal advisors;

- As needed to assess and ensure compliance with applicable laws, legal requirements and company policies, to protect our assets (including to license and protect intellectual property) or to investigate or defend against any claims of illegality or wrongdoing (including to obtain legal advice), or in response to a court order or judicial or other government subpoena or warrant, in which case we may disclose your Personal Data to law enforcement, regulators, governmental authorities or other bodies, courts, tax authorities, insurance providers, legal advisors, and mediators;

- In the event TCP undertakes or is involved in or contemplating (e.g., in connection with due diligence) any merger, acquisition, reorganization, sale of assets, bankruptcy, or insolvency event, in which case we may disclose your Personal Data to buyers or purchasers (or potential buyers or purchasers) and their representatives.

Other Purposes for Processing and Disclosures of Specific Categories of Personal Data

In addition to the general purposes for processing and disclosing any category of your Personal Data, the chart below includes other purposes for which we may process specific categories of your Personal Data and to whom such data is disclosed as well as our legal bases for such processing, consistent with the GDPR.

Personal Data We Receive Directly From You.

Category of Personal Data	Purpose(s) for Processing	Legal Basis for Processing	Categories of Third Parties to Whom Personal Data may be Disclosed
Client Account Data	For account management, to maintain Client relationships and provide the Services, for billing, for quality management and troubleshooting, to develop and expand TCP's products and services, and for research, development, analytics, and business intelligence.	Consent. Performance of a contract.	Service Providers, including those used for website and application development and support, customer relationship management, payment processing and financial services, IT security, support and hosting, and marketing and promotions management.
Communications Data	To initiate or expand a business relationship, to develop or improve upon TCP's products and services, to respond to	Consent.	Service Providers, including those used for website and application development and support, customer relationship

Category of Personal Data	Purpose(s) for Processing	Legal Basis for Processing	Categories of Third Parties to Whom Personal Data may be Disclosed
	inquiries, to market TCP's products and services, and for research, development, analytics, and business intelligence.		management, IT security, support and hosting, and marketing and promotions management.
Human Resources Data	Employment, including recruitment and hiring, interviewing, administering payroll, and managing employees and other staff, and to ensure the safety and security of TCP and its staff.	Pursuit of legitimate business interests. Consent. Performance of a contract. Legal requirement.	Service Providers, including those used for human resources management, financial services, IT security, support and hosting, and legal advice and other professional services. Consumer Reporting Agencies and other background check or identity verification providers.
Reputation & Creditworthiness Data	For quality management and to enforce company standards and policies and for identity verification and risk management and mitigation, including for audit and insurance functions.	Consent. Performance of a contract. Legal requirement.	Service Providers, including those used for customer relationship management, financial services, IT security, support and hosting, and legal advice and other professional services. Consumer Reporting Agencies and other background check or identity verification providers.
Transaction and Payment Data	To process payment required for the Services or events or webinars you have registered to attend, to send transaction-related emails or otherwise communicate with you concerning a transaction, to deliver and provide the Services or conduct events, and to maintain Client relationships.	Consent. Performance of a contract.	Service Providers, including those used for customer relationship management, payment processing and financial services, and IT security, support and hosting.
Visitor Data	To ensure the safety and security of TCP and its staff.	Consent. Vital Interest.	Service Providers, including those used for IT security, support and hosting.

Personal Data We Host on Behalf of Clients.

Categories of Personal Data	Purpose(s) for Processing	Legal Basis for Processing	Categories of Third Parties to Whom Personal Data may be Disclosed
Profile Data	To comply with our contractual obligations and provide the Services to our Clients.	Performance of a contract.	TCP's Clients and other entities when instructed by TCP's Clients, including payroll processors, benefits administration providers, and enterprise resource planning vendors. Service Providers, including those used for application development and support and IT security, support and hosting.
Service Data	To comply with our contractual obligations and provide the Services to our Clients.	Performance of a contract.	TCP's Clients and other entities when instructed by TCP's Clients, including payroll processors, benefits administration providers, and enterprise resource planning vendors. Service Providers, including those used for application development and support and IT security, support and hosting.
EU Resident Special Category Data	*Biometric Data*: Our Clients are contractually obligated to process biometric data only for employment-related purposes. TCP's purpose for processing this data is to comply with our contractual obligations and provide the Services to our Clients.	Consent. Performance of a contract.	TCP's Clients. Service Providers, including those used for IT security, support and hosting.
	Photographic images: Our Clients are contractually obligated to process photographic images data only for employment-related	Consent. Performance of a contract.	TCP's Clients. Service Providers, including those used for IT security, support and hosting.

Categories of Personal Data	Purpose(s) for Processing	Legal Basis for Processing	Categories of Third Parties to Whom Personal Data may be Disclosed
	purposes. TCP's purpose for processing this data is to comply with our contractual obligations and provide the Services to our Clients.		
	Physical or mental health data: Our Clients determine the purpose for which this information is collected. They may wish to process this data to accommodate disabilities and dietary needs and to address emergency health needs. TCP's purpose for processing this data is to comply with our contractual obligations and provide the Services to our Clients.	Performance of a contract.	TCP's Clients.\n\nService Providers, including those used for IT security, support and hosting.
	Racial or ethnic data: Our Clients determine the purpose for which this information is collected. They may wish to process this data to facilitate affirmative action and other inclusion programs. TCP's purpose for processing this data is to comply with our contractual obligations and provide the Services to our Clients.	Performance of a contract.	TCP's Clients.\n\nService Providers, including those used for IT security, support and hosting.
	Religion or beliefs: Our Clients determine the purpose for which this information is collected. They may wish to process this data to meet an individual's specific needs or requests, including dietary requests and to respect religious holidays and other observances. TCP's purpose for processing this data is to comply with our contractual	Performance of a contract.	TCP's Clients.\n\nService Providers, including those used for IT security, support and hosting.

Categories of Personal Data	Purpose(s) for Processing	Legal Basis for Processing	Categories of Third Parties to Whom Personal Data may be Disclosed
	obligations and provide the Services to our Clients.		

Personal Data We Receive From Other Sources.

Categories of Personal Data	Purpose(s) for Processing	Legal Basis for Processing	Categories of Third Parties to Whom Personal Data may be Disclosed
Lead Data	To identify new customers, initiate or expand a business relationship, and create more tailored advertising to provide products and services that may be of interest to you.	Consent. Performance of a contract.	Service Providers, including those used for website and application development and support, customer relationship management, IT support and hosting, data storage, and marketing and promotions management.
Human Resources Data	Employment, including recruitment and hiring, interviewing, administering payroll, and managing employees and other staff, and to ensure the safety and security of TCP and its staff.	Pursuit of legitimate business interests. Consent. Performance of a contract. Legal requirement.	Service Providers, including those used for human resources management, financial services, IT security, support and hosting, and legal advice and other professional services.
Reputation & Creditworthiness Data	For quality management and to enforce company standards and policies and for identity verification and risk management and mitigation, including for audit and insurance functions.	Performance of a contract. Legal requirement.	Service Providers, including those used for human resources management, financial services, IT security, support and hosting, and legal advice and other professional services.

Cookies and Tracking Technologies.

Pursuant to TCP's legitimate business interests and/or your consent, TCP may use information obtained via Cookies and tracking technologies to personalize and optimize your browsing experience and the Services by:

- Providing you tailored content and ads;
- Enabling social media features;
- Safeguarding against spam and malware;
- Analyzing trends, traffic, and user behavior;
- Administering the website;
- Gathering demographic information about our user base as a whole;
- Tracking web and advertising analytics throughout our website and our affiliate websites;
- Remembering your preferences and voluntarily-submitted information;
- Performing location-related functionalities and analytics;
- Participating in market research; and
- to improve the Services.

TCP may disclose this information to Service Providers, including those used for website and application development and support, IT support, security and hosting, and marketing and promotions management.

Data Sales.

TCP does not and will not sell or rent your Personal Data.

Data Retention.

TCP will only retain your Personal Data for as long as necessary to fulfill the purposes for which it is processed, to comply with applicable Data Protection Laws, or as otherwise required for other legitimate legal purposes. TCP has implemented a Data Retention Policy for all types of Personal Data that TCP processes. Personal Data is generally retained in accordance with the retention schedules defined therein. When the retention period has expired, Personal Data will be securely deleted or destroyed.

Protection of Personal Data.

TCP has implemented and maintains commercially reasonable organizational, technical, and physical controls to protect Personal Data from misuse or accidental, unlawful, or unauthorized destruction, loss, alteration, disclosure, acquisition or access. In each case, TCP will strive to provide security that is proportional to the sensitivity of the Personal Data being protected, with the greatest effort being focused on protecting sensitive Personal Data and other Personal Data whose compromise could result in substantial harm or inconvenience.

Please note that you should also take steps to protect your data. For example, when you register for the Services, choose a strong password, and do not share it with anyone else. TCP will never ask you for your password in an unsolicited phone call or email.

In the event TCP learns of a data security breach, TCP (potentially with the help of others such as third-party forensic investigators, legal counsel, and TCP's insurance provider) shall investigate and document the facts relating thereto, its effects and the remedial actions taken and shall notify you within a reasonable period of time to the extent required by and in accordance with applicable Data Protection Laws.

International Data Transfers.

TCP is headquartered in the United States of America. Your Personal Data may be stored and processed by TCP in the United States and TCP may transfer Personal Data pertaining to individuals located outside of the United States to our affiliates and suppliers in the United States, as permitted by applicable Data Protection Laws. Therefore, your Personal Data may be processed outside the European Economic Area ("EEA"), and in countries which are not subject to an adequacy decision by the European Commission and which may not provide for the same level of data protection as the EEA. In this event, we will ensure that such recipient offers an adequate level of protection, for instance by verifying that the recipient is Data Privacy Framework (DPF) certified (TCP is self-certified - see the TimeClock Plus, LLC Data Privacy Framework (DPF) Privacy Policy for Data Transferred to the United States from the EU, the UK (including Gibraltar) and/or Switzerland below), by entering into standard contractual clauses for the transfer of data as approved by the European Commission (Art. 46 GDPR), or by asking for your prior consent to such transfer.

Your Rights & Choices.

Communication Preferences.

TCP will send direct marketing materials if you have provided opt-in consent or if applicable Data Protection Laws otherwise permit. You have the right to opt-out of these communications. To opt-out of commercial emails, simply click the link labeled "unsubscribe" at the bottom of any email we send you. Additionally, you may opt-in or opt-out of communications by calling us at +1 (325) 223-9500. Please note that if you are currently receiving services from TCP and you have decided to opt-out of promotional emails, this will not impact the messages we send to you for purposes of delivering such services.

Review, Correction, Erasure, and Other Individual Rights.

You have the right to request a copy of the Personal Data maintained by or on behalf of TCP unless otherwise prohibited by applicable Data Protection Laws. If the Personal Data is incorrect, incomplete, or not processed in compliance with applicable Data Protection Laws or this Privacy Policy, you have the right to have the Personal Data rectified, restricted, or erased (as appropriate) subject to applicable Data Protection Law.

Additionally, you have the right to object to the processing of your Personal Data on the basis of compelling grounds related to your particular situation or in connection with any direct marketing communications. Restrictions may be lifted if they were temporary, based on certain grounds such as a dispute about data accuracy or the lawfulness of processing or if TCP is in the process of reviewing an objection request, and the basis of the restriction has been resolved. You will be notified about the removal of any such restriction via email or mail. In addition, once a restriction has been implemented, processing can only resume if you grant explicit consent or you request to lift the original restriction and there is no conflict with applicable Data Protection Laws.

You may contact us using the contact information provided in the "Contact Us" section below to request access to your data and to exercise any of the other individual rights afforded to you by applicable Data Protection Laws. TCP will receive, investigate, document, and respond to requests as soon as possible and in accordance with applicable Data Protection Laws. In cases where the request cannot be fulfilled by TCP, we will use best efforts to notify any third-party processing relevant data of the required correction and/or erasure.

In some cases, requests to delete data may be denied in accordance with applicable Data Protection Laws, including, for example, when the data is still needed for processing, where you gave consent and did not

withdraw consent, where there has been a previous processing objection that has been granted, and where the data was processed lawfully or there is a not a legal requirement to delete the data. TCP may also reject the request if it needs access to the data to comply with a law, defend a legal claim or for research/historic/scientific purposes.

Individuals Located in the EEA.

In addition to the rights stated above and below, you also have the right to data portability, as well as the right to be notified of automated decision-making or profiling related to your Personal Data.

Individuals in the EEA, the UK, and Switzerland

Individuals located in the EEA, the UK, and Switzerland may file a complaint if they believe TCP has violated this policy or applicable Data Protection Law. Please see TimeClock Plus, LLC Data Privacy Framework (DPF) Privacy Policy for Data Transferred to the United States from the EU, the UK (including Gibraltar) and/or Switzerland for additional information concerning how you may file such a complaint. TCP's Data Protection Officer will receive, investigate, and document each complaint and respond within a reasonable timeframe in accordance with applicable Data Protection Laws of the outcome of the investigation. of the outcome of the investigation.

VeraSafe has been appointed as TCP's representative in the European Union for data protection matters, pursuant to Article 27 of the GDPR. VeraSafe can be contacted in addition to TCP, only on matters related to the processing of Personal Data. To make such an inquiry, please contact VeraSafe using this contact form: https://www.verasafe.com/privacy-services/contact-article-27-representative

Alternatively, VeraSafe can be contacted at:

VeraSafe Ireland Ltd
Unit 3D North Point House
North Point Business Park
New Mallow Road
Cork T23AT2P
Ireland

California Residents

If you are a California resident, California's "Shine the Light" law, Civil Code sections 1798.80 – 1798.84, includes provisions for securing and disposing of Personal Data, notifying you of a breach of your Personal Data, and for responding to requests by you asking about the businesses' practices related to disclosing Personal Data to third-parties for the third-parties' direct marketing purposes. TCP complies with California Civil Code sections 1798.80 – 1798.84. TCP does not share your Personal Data with third-parties for the third-parties' direct marketing purposes. For more information about your rights under California's Civil Code sections 1798.80 – 1798.84, please visit https://leginfo.legislature.ca.gov.

Effective January 1, 2020, the CCPA provides California residents with additional rights related to data privacy.

Pursuant to the CCPA, upon making a verifiable request, California residents may:

- request (in a format that is portable and, to the extent technically feasible, in a readily useable format that will allow you to transmit it to another entity) access to the specific pieces and

categories of Personal Data that we have collected about you over the past twelve months, the categories of sources of that information, our business or commercial purposes for collecting the information, and the categories of third parties with whom the information was shared;

- submit a request for deletion of Personal Data, subject to certain exceptions, including (without limitation) in the event that we may need to retain Personal Data to complete the transaction for which the Personal Data was collected, detect security incidents or protect against illegal activity, exercise free speech, comply with a legal obligation, or for lawful internal use compatible with the context in which the information was provided by you. If your request is subject to any exception, we may deny your request to delete your data.

Please note that you must verify your identity and request before further action is taken by us. To do so, we may request certain information from you, including a copy of a government-issued ID or other identifier.

To exercise these rights, you may contact us at: DPO@tcpsoftware.com or 1-800-749-8463. You have the right not to be discriminated against for exercising your rights under the CCPA. Consistent with California law, you may designate an authorized agent that is registered with the Secretary of State to make a request on your behalf. In order to designate an authorized agent, please contact us at DPO@tcpsoftware.com. We will require written proof that the person acting as your agent is in fact authorized to act on your behalf.

If you have any questions about this section or whether it applies to you, please contact us at DPO@tcpsoftware.com.

Other Important Information about Our Practices.

Third-Party Content.

This policy only addresses the use and disclosure of information by TCP. Third-party websites, applications, services, goods or advertisements that may be accessible through our website have their own privacy statements and data collection, use and disclosure practices. We encourage you to familiarize yourself with the privacy statements provided by third-parties prior to providing them with information or taking advantage of an offer or promotion. TCP does not control and is not responsible for the content or privacy and data protection practices of third-party websites, applications, services, goods, or advertisements. If you link to or otherwise interact with third-party content, you do so at your own risk. TCP does not endorse, recommend, or make any representations or warranties regarding websites, applications, services, goods, or advertisements that may be linked to or otherwise incorporated into the Services.

Forums, Product Reviews and Other Public Areas.

Our Services, including social media, may provide forums and other public areas where you may communicate with others and publicly post information. Prior to posting in these areas, please read the Third-parties' Terms of Use carefully. The information you post may be accessible to anyone with Internet access, and Personal Data you include in your posting may be read, collected, and used by others. For example, if you post your email address on a forum or in a public area, you may receive unsolicited messages from third parties. Please use caution when posting Personal Data. We do not assert any

ownership over your posts and we are not liable for any statements or representations in posts provided by you. You are solely responsible for your posts.

Children.

TCP's Services, related marketing channels and materials are not directed at children. We do not knowingly collect or sell any Personal Data from children under the age of sixteen (16). If you are a parent or guardian and believe your child has provided TCP with Personal Data without your consent, please contact us by using the information in the "Contact Us" section, below, and we will take necessary steps to remove such Personal Data from our systems.

Changes to this Privacy Policy.

From time to time, we may update this Privacy Policy to reflect new or different privacy practices. Please review our website periodically to check for the latest changes. Under "Last Updated," you can see the date on which this Privacy Policy was last updated. We will notify you about material changes in the way we treat your information by placing a prominent notice on the website so that you can choose whether to continue using the Services.

Contact Us.

Please contact us if you have questions, comments or other concerns about this policy or about TCP's data privacy practices or if you wish to exercise any of your rights under this policy or applicable Data Protection Law at Privacy@tcpsoftware.com. You may also reach us via mail at the address below. If you send us a letter, please provide your name, address, email address, and detailed information about your question, comment, request, or complaint. Letters can be sent to:

TimeClock Plus, LLC
Attn: Legal
1 Time Clock Dr.
San Angelo, TX 76904; USA

TimeClock Plus, LLC Privacy Policy for the Processing of Biometric Data from U.S. Residents

Introduction.

Not all TCP products and services utilize biometric authentication, and not all of TCP's biometric products and services require TCP's participation in the collection, storage or use of biometric data. However, in some cases, TCP may provide hosting services for certain biometric data collected by Clients on such Client's behalf. TCP has instituted the following policy related to any U.S. resident biometric data that is collected, processed and/or stored by TCP and that is subject to the requirements of the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, et seq. ("BIPA"), or any similar law expressly governing the collection, storage, use and/or disclosure of biometric data.

Biometric Information.

The biometric data covered by this policy includes "Biometric Identifiers" as defined by BIPA (i.e., a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry) and "Biometric Information" as defined by BIPA (i.e., any information, regardless of how it is captured, converted, stored, or shared, based on an individual's Biometric Identifier used to identify an individual). With respect to its own employees, TCP may collect, store and /or use biometric data directly for the purpose of authenticating TCP employees, tracking their time and attendance, and for other human resources-related purposes. TCP will inform any such employees, in writing and prior to collection of biometric data, that biometric data is being collected, stored, and/or used and of the specific purpose(s) and length of time for which it is being collected, stored, and/or used and will obtain a written release regarding the same. At the direction and on behalf of its Clients, TCP may also collect, store and/or use biometric data. Clients may utilize TCP's products and services to collect, store and/or use biometric data solely for employment-related purposes, including tracking of time and attendance, in accordance with this policy and applicable law.

Client's Responsibilities.

Clients must maintain their own data collection, disclosure, retention, and storage policies in compliance with applicable law, including BIPA.

TCP Clients agree that any use of TCP's products and services to collect, store and/or use biometric data shall be in compliance with applicable law. With respect to any and all biometric data collected or controlled by Clients, Clients must (unless Client and TCP are expressly exempted under applicable law):

a. Inform the individual from whom biometric data will be collected, in writing and prior to collecting his or her biometric data, that biometric data is being collected, stored, and/or used;
b. Indicate, in writing, the specific purpose(s) (which may not be other than employment-related purposes) and length of time for which biometric data is being collected, stored, and/or used; and
c. Receive a written release from the individual (or his or her legally authorized representative) authorizing the Client, TCP, and TCP's third-party service providers (who are subject to restrictions no less restrictive than those imposed on TCP herein) to collect, store, and/or use the biometric data and authorizing the Client to disclose such biometric data to TCP and TCP's third-party service providers.

Client must ensure that TCP is immediately notified upon termination or other discontinuation of use of TCP's biometric products or services with respect to an employee or other individual.

Disclosure and Sharing of Biometric Information.

TCP will not sell, lease, trade or otherwise profit from any biometric data that it receives from (i) its Client's employees or (ii) TCP's employees. Biometric data will not be used for any purpose other than as described herein.

TCP will not disclose, redisclose or otherwise disseminate any biometric data to any person or entity other than, with respect to biometric data received from its Clients, the Client and TCP's third party service providers and, with respect to biometric data collected from TCP's own employees, TCP's third party service providers, without/unless:

a. First obtaining the written consent of the individual whose biometric data has been collected (or his or her authorized representative) to the disclosure or redisclosure;
b. Disclosure or redisclosure is required by state or federal law or municipal ordinance; or
c. Disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

Retention Schedule.

TCP will retain biometric data until the initial purpose for collecting or obtaining such biometric data has been satisfied, or within three (3) years of an individual's last interaction with the Client and/or TCP, as applicable, whichever occurs first, at which time TCP will permanently delete such biometric data.

Biometric Data Storage.

TCP will use a reasonable standard of care, consistent with the industry in which TCP operates, to store, transmit and protect from disclosure all biometric data, and shall store, transmit, and protect from disclosure all biometric data in a manner that is the same as or more protective than the manner in which TCP stores, transmits, and protects other confidential or sensitive data that can be used to uniquely identify an individual or an individual's account or property.

Your Rights & Choices.

See the "Your Rights & Choices" section of [TCP's Privacy Policy for All Personal Data Except U.S. Resident Biometric Data](#) for information concerning your rights.

TimeClock Plus, LLC Data Privacy Framework (DPF) Privacy Policy for Data Transferred to the United States from the EU, the UK (including Gibraltar) and/or Switzerland

TimeClock Plus, LLC ("TCP") and its affiliate Humanity.com, Inc. complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) as set forth by the U.S. Department of Commerce. TimeClock Plus, LLC ("TCP") and its affiliate Humanity.com, Inc. has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) and the UK Extension to the EU-U.S. DPF with regard to the processing of personal data received from the European Union and the UK (including Gibraltar) in reliance on the EU-U.S. DPF. TimeClock Plus, LLC ("TCP") and its affiliate Humanity.com, Inc. has certified to the U.S. Department of Commerce that it adheres to the Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) with regard to the processing of personal data received from Switzerland in reliance on the Swiss-U.S. DPF. If there is any conflict between the terms in this privacy policy and the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles, the Principles shall govern. To learn more about the Data Privacy Framework (DPF) program, and to view our certification, please visit https://www.dataprivacyframework.gov/.

With respect to personal data received or transferred pursuant to the Data Privacy Framework (DPF), TCP is subject to the regulatory and enforcement powers of the U.S. Federal Trade Commission (FTC).

Pursuant to the Data Privacy Framework (DPF), EU, UK, and Swiss individuals have the right to obtain our confirmation of whether we maintain personal information relating to you in the United States. Upon request, we will provide you with access to the personal information that we hold about you. You may also may correct, amend, or delete the personal information we hold about you. An individual who seeks access, or who seeks to correct, amend, or delete inaccurate data transferred to the United States under Data Privacy Framework (DPF), should direct their query to Privacy@TimeClockPlus.com. If requested to remove data, we will respond within a reasonable timeframe.

We will provide an individual opt-out choice, or opt-in for sensitive data, before we share your data with third parties other than our agents, or before we use it for a purpose other than which it was originally collected or subsequently authorized. To request to limit the use and disclosure of your personal information, please submit a written request to Privacy@TimeClockPlus.com.

In certain situations, we may be required to disclose personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

TCP's accountability for personal data that it receives in the United States under the Data Privacy Framework (DPF) and subsequently transfers to a third party is described in the Data Privacy Framework (DPF). In particular, TCP remains responsible and liable under the Data Privacy Framework (DPF) Principles if third-party agents that it engages to process the personal data on its behalf do so in a manner inconsistent with the Principles, unless TCP proves that it is not responsible for the event giving rise to the damage.

In compliance with the Data Privacy Framework (DPF) Principles, TCP commits to resolve complaints about your privacy and our collection or use of your personal information transferred to the United States pursuant to Data Privacy Framework (DPF). European Union, UK, and Swiss individuals with DPF inquiries or complaints should first contact TCP by email at Privacy@TimeClockPlus.com. TCP's Data

Protection Officer will receive, investigate, and document each complaint and respond to the Individual within a reasonable timeframe of the outcome of the investigation.

By Email:
Data Protection Officer
DPO@tcpsoftware.com

By Mail:
TimeClock Plus, LLC
Attn: Data Protection Officer
1 Time Clock Dr.
San Angelo, TX 76904; USA

TCP has further committed to refer unresolved privacy complaints under the Data Privacy Framework (DPF) Principles to an independent dispute resolution mechanism, DATA PRIVACY FRAMEWORK SERVICES, operated in the United States by BBB National Programs. If you do not receive timely acknowledgment of your complaint, or if your complaint is not satisfactorily addressed, please visit https://bbbprograms.org/programs/all-programs/dpf-consumers/ProcessForConsumers for more information and to file a complaint. This service is provided free of charge to you.

In compliance with the EU-U.S. Data Privacy Framework (DPF), TCP commits to cooperate and comply respectively with the advice of the panel established by the EU data protection authorities (DPAs) with regard to unresolved complaints concerning our handling of human resources data received in reliance on the EU-U.S. DPF in the context of the employment relationship. Complaints related to human resources data should not be addressed to the BBB National Programs Dispute Resolution Process.

Contact details for the EU data protection authorities can be found at https://edpb.europa.eu/about-edpb/about-edpb/members_en

If your Data Privacy Framework (DPF) complaint cannot be resolved through the above channels, under certain conditions, you may invoke binding arbitration for some residual claims not resolved by other redress mechanisms. See Data Privacy Framework (DPF) Annex 1 at https://www.dataprivacyframework.gov/s/article/ANNEX-I-introduction-dpf

Contact Us.

For more information about TCP's Privacy Policies, including the TCP Privacy Policy for Client Data Processing, please contact the Data Protection Officer at Privacy@tcpsoftware.com.

<u>Definitions</u>

The following definitions apply throughout the Global Data Privacy Policy:

- *"CCPA"* means the California Consumer Privacy Act of 2018, codified at Cal. Civ. Code §§ 1798.100-199.
- "*Client*" or "*Clients*" means TCP's business customers, each of which purchases some or all of the Services and enters a service agreement with TCP.
- *"Data Protection Laws"* means all applicable laws and regulations governing the use, disclosure, storage, and transfer of Personal Data, including the GDPR and CCPA.
- "*GDPR*" means the European General Data Protection Regulation (EU 2016/679).
- "*Personal Data*" means "personal data" as defined by the GDPR and "personal information" as defined by the CCPA and includes any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or household. For purposes of this Global Data Privacy Policy, Personal Data does not include data that has been de-identified, whether through aggregation or otherwise, in accordance with applicable Data Protection Laws.
- "*Service Providers*" means any third party entity that processes Personal Data on behalf of TCP and to which TCP discloses Personal Data for a business purpose pursuant to a written contract, provided that the contract prohibits such entity from retaining, using, or disclosing the Personal Data for any purpose other than for the specific purpose of performing the services identified in such contract. For the avoidance of doubt, with respect to individuals in the European Union, "Service Providers" are equivalent to sub-processors pursuant to Article 28(4) of the GDPR. TCP uses Service Providers for various functions, including website and application development and support, customer relationship management, human resources management, payment processing and financial services, IT support, security and hosting, legal advice and other professional services, and marketing and promotions management.
- "*Services*" means the TimeClock Plus website (www.tcpsoftware.com) as well as any product, media form, media channel, mobile website or mobile application related thereto or otherwise provided by TCP, including: (a) software for time and attendance tracking, employee absence management, and workforce scheduling together with any integrations for payroll management, enterprise resource planning, and human capital management; and (b) related support services.

EXHIBIT E

TimeClock Plus
Hardware Support and Maintenance Agreement - Addendum

This Hardware Support and Maintenance Agreement is an addendum to the Master Licensing Agreement or Perpetual Licensing Agreement – EULA, hereafter referred to as the "Licensing Agreement", made and entered into by and between TimeClock Plus, LLC ("TCP") and Client. TCP reserves the right to continuously improve the Hardware Support and Maintenance Services and to adapt such Services to changes in technology and to TCP's business environment. Solely for these purposes, TCP reserves the right to modify, elaborate, remove or add to some or all of the provisions of these Hardware Support and Maintenance Agreement terms at TCP's sole discretion and without further notice, provided that any such improvement or adaptation shall not result in a diminution of the overall level of service. Services shall be provided in accordance with TCP's then current Support Level Agreement ("SLA"), located at https://www.timeclockplus.com/agreements/sla.

1. **Term.** Services provided under this Hardware Support and Maintenance Agreement shall commence on the date of purchase and shall continue for one (1) year from the date of purchase ("Initial Term"), and then shall automatically renew for subsequent one (1) year terms thereafter, unless either Party gives written notice of non-renewal at least ninety (90) days prior to the end of the then current term (the Initial Term and subsequent renewal terms being referred to as the "Term").

2. **Supported Hardware.** All hardware purchased by Client from TCP for which Client has paid a fee for support and maintenance shall be considered Supported Hardware under the terms of this Hardware Support and Maintenance Agreement.

3. **Incident.** An Incident is defined as a single support issue with a TCP hardware product and the reasonable effort needed to resolve it. A single support Incident is a problem that cannot be broken down into subordinate parts. It is possible for one Incident to span multiple telephone calls and multiple emails; it is also possible for one telephone call to include multiple Incidents.

4. **Support Services.** TCP support technicians shall aid in the resolution of hardware support requests in a timely and professional manner. TCP will assist with issues related only to the Supported Hardware. Upon notification of an Incident, an Incident number will be issued, and the Incident number will remain effective and open until satisfactory resolution of the cause of the Incident, or 5 business days without a Client communication, after which the Incident number will be closed.

5.   **Maintenance Services**.   During the term, should a defect in materials or workmanship be identified on supported hardware ("Defective Hardware"), TCP will incur expense to promptly ship Client a comparable hardware device of like kind with the functional equivalent of the Defective Hardware ("Replacement Hardware") to arrive at Client's specified location. Cost to ship replacement hardware outside the United States is the responsibility of Client.

6. **Return of Defective Hardware**.   Upon replacement of Defective Hardware, Client's Defective Hardware shall become the property of TCP and the Replacement Hardware shall become Client's property. Instructions and a return label for return of the Defective Hardware will be included in the packaging of the Replacement Hardware or can be provided upon request. Client shall properly package the shipment when returning the Defective Hardware. The Defective Hardware must be returned to TCP within 14 days of receiving the Replacement Hardware. Should Client fail to return the Defective Hardware, Client agrees to pay TCP the Manufacturer's Suggested Retail Price ("MSRP") of the Defective Hardware. Additionally, Client's ability to request Maintenance Services on any other supported hardware will be suspended until the Defective Hardware is returned to TCP or Client pays TCP the MSRP of the Defective Hardware.

7. **Additional Products**.   If during the Term, Client purchases additional hardware products, this Hardware Support and Maintenance Agreement is amended to include Services for such additional hardware products. The annual fee for such additional hardware products shall be charged at the time of purchase and shall be prorated so that the term of such additional product coverage will expire at the end of the Term.

8. **Limitations**.

8.1. Support Services. Support Services are limited to hardware troubleshooting and hardware configurations as described in the TimeClock Plus product documentation. This Hardware Support and Maintenance Agreement does not cover inquiries on legal time keeping compliance nor does it include in-depth product training. Support Services extend only to platforms and operating environments specified by TCP. TCP is not responsible for integration or configuration with third-party software, hardware, or operating environments except as allowed by the Licensing Agreement and the products purchased from TCP. Client is entitled to an unlimited number of support Incidents during the Term.

8.2. Maintenance Services. Maintenance Services does not cover (a) damage caused by accident, abuse, misuse, liquid contact, fire, earthquake, other external causes, or operating covered hardware outside its intended or permitted use; (b) hardware with a serial number that has been defaced, altered, removed, or modified without written permission from TCP; (c) hardware that has been lost or stolen; (d) cosmetic damage including but not limited to scratches, dents, and broken plastics or ports; (e) consumable parts such as batteries; (f) preventative maintenance; or (g) defects caused by normal wear and tear or otherwise normal aging of product.

9. **Services Requests**. Requests for Services are made by Client to TCP via support portal located at https://timeclockplus.force.com/TCPSupport/s/ . The Client shall provide a reasonable amount of information and assistance related to the Incident for verification and resolution of the Incident. When requesting Replacement Hardware, Client must provide TCP with the serial number of Defective Hardware in question, the problem, the context in which the problem was encountered, a description of the system configuration, the steps necessary to generate or reproduce the problem, and the address TCP will use to ship the Replacement Hardware. Failure to provide reasonable information or assistance may result failure to resolve the Incident.

10. **Miscellaneous**. This Hardware Support and Maintenance Agreement is not transferable. With the exception of the Licensing Agreement, this Hardware Support and Maintenance Agreement supersedes all other written and oral proposals, purchase orders, prior agreements, and other communications between Client and TCP concerning the subject matter of this Hardware Support and Maintenance Agreement, and along with the documents referenced herein constitutes the entire agreement between TCP and Client regarding provision of Support and Maintenance Services. A Hardware Support and Maintenance Agreement does not constitute a certification or warranty, express or implied of any kind. TCP's obligations and responsibilities regarding product warranties are governed solely by the Licensing Agreement under which they are sold or licensed.