TimeClock Plus, LLC and Humanity Time

System and Organization Controls Report (SOC 3)

Independent Report of the Controls to Meet the Trust Services Criteria for the Security, Availability, Confidentiality, and Processing Integrity Categories for the Period of January 1, 2025, through December 31, 2025.

Table of Contents

Assertion of TimeClock Plus, LLC and Humanity Time Management

Assertion of TimeClock Plus, LLC and Humanity Time Management

We are responsible for designing, implementing, operating, and maintaining effective controls within TimeClock Plus, LLC and Humanity Time's software-as-a-service (SaaS) solution system (system) throughout the period January 1, 2025, to December 31, 2025, to provide reasonable assurance that TimeClock Plus, LLC and Humanity Time's service commitments and system requirements relevant to security, availability, confidentiality, and processing integrity were achieved. Our description of the boundaries of the system is presented in section A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period January 1, 2025, to December 31, 2025, to provide reasonable assurance that TimeClock Plus, LLC and Humanity Time's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, and processing integrity (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). TimeClock Plus, LLC and Humanity Time's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in section B.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period January 1, 2025, to December 31, 2025, to provide reasonable assurance that TimeClock Plus, LLC and Humanity Time's service commitments and system requirements were achieved based on the applicable trust services criteria.

Independent Service Auditor's Report

Independent Service Auditor's Report

Daryl Rolley
CEO
TimeClock Plus, LLC
1 Time Clock Dr.
San Angelo, TX 76904

Scope

We have examined TimeClock Plus, LLC and Humanity Time's accompanying assertion titled "Assertion of TimeClock Plus, LLC and Humanity Time Management" (assertion) that the controls within TimeClock Plus, LLC and Humanity Time's software-as-a-service (SaaS) solution system (system) were effective throughout the period January 1, 2025, to December 31, 2025, to provide reasonable assurance that TimeClock Plus, LLC and Humanity Time's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, and processing integrity (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Service Organization's Responsibilities

TimeClock Plus, LLC and Humanity Time is responsible for its service commitment and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that TimeClock Plus, LLC and Humanity Time's service commitments and system requirements were achieved. TimeClock Plus, LLC and Humanity Time has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, TimeClock Plus, LLC and Humanity Time is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements

- Assessing the risks that controls were not effective to achieve TimeClock Plus, LLC and Humanity Time's service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve TimeClock Plus, LLC and Humanity Time's service commitments and system requirements based on the applicable trust services criteria

Our examination also included performing such other procedures as we considered necessary in the circumstances.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

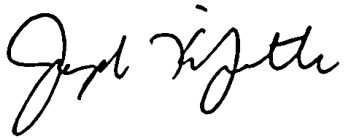
Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within TimeClock Plus, LLC and Humanity Time's software-as-a-service (SaaS) solution system were effective throughout the period January 1, 2025, to December 31, 2025, to provide reasonable assurance that TimeClock Plus, LLC and Humanity Time's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.



Joseph Kirkpatrick
CPA, CISSP, CGEIT, CISA, CRISC, QSA
4235 Hillsboro Pike, Suite 300
Nashville, TN 37215

February 12, 2026

TimeClock Plus, LLC and Humanity Time's Description of Its Humanity Time Software-as-a-Service Solution System

Section A: TimeClock Plus, LLC and Humanity Time's Description of the Boundaries of Its Humanity Time Software-as-a-Service Solution System

Services Provided

TimeClock Plus, LLC and Humanity Time (formerly known as Timeco) partners with Professional Employer Organizations (PEOs) to offer integrated workforce management solutions to new clients. By aligning with PEOs, Humanity Time enhances the PEO's service offerings by providing automated, accurate time tracking, ensuring compliance with labor laws and assisting with payroll processing. This collaboration allows PEOs to present a more comprehensive Human Resources (HR) package to prospective customers. Humanity Time benefits from access to the PEO's extensive client network, accelerating market penetration. Together, they can co-market solutions, customize offerings based on client needs, and deliver seamless onboarding experiences. Marketing to PEOs is handled by the Humanity Time marketing department.

Customer Onboarding

The organization has established formal procedures for onboarding customers. For PEO and partner submissions, the partner is responsible for submitting the new company form through the dedicated portal. Once the form is submitted, the partner then selects the template and provides configurations and relevant company details.

As part of the survey and setup process, the customer or PEO is responsible for uploading the pay category list, the organizational hierarchy, and the setup survey, which includes business and overtime rules as well as policy details.

Regarding the Implementation team engagement, an implementation specialist is responsible for creating the client "shell" environment. Once created, thresholds, limits, labor levels, categories, and parameters are configured, and employee demographics are imported either by application programming interface (API) or CSV.

Once fully onboarded, the designated implementation specialist remains with the customer or PEO through one full payroll cycle. The customer is then transferred to the Support team and assigned a customer success manager (CSM) via Salesforce. Training resources and documentation are also established to provide additional support to new users. Live training sessions are recorded and delivered to the customer and PEO. Test accounts are also established to provide system demonstrations for external users, and documentation and process guides are published for reference.

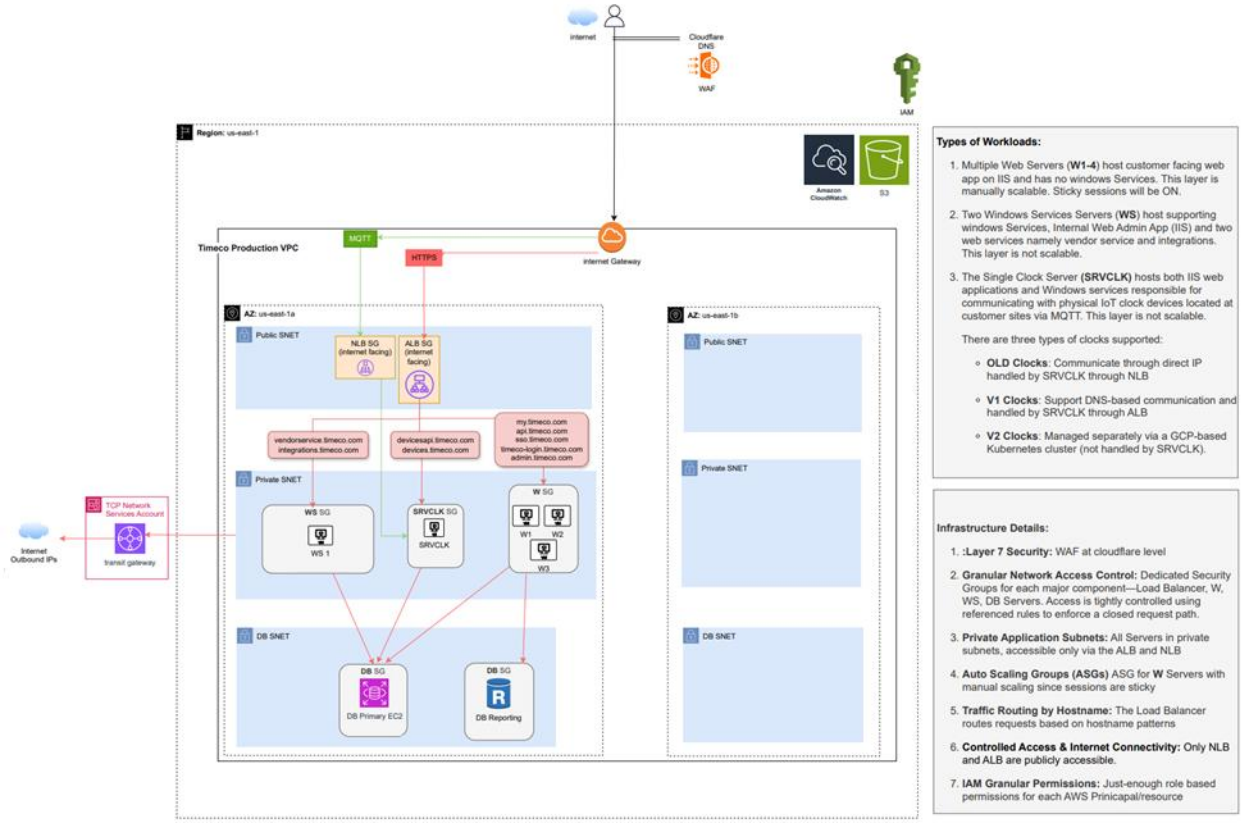
Customer Offboarding

The organization maintains a formal process for offboarding customers. Month-to-month subscriptions are provided to customers, and these subscriptions can be canceled at any time. The administrator portal allows for self-service cancellations,

and the portal tracks the reason for cancellation as well as the customer's signature. Humanity Time retains relevant customer data for 45 days, after which the data is permanently deleted. Customers may request data exports, and the Humanity Time team may run reports to temporarily reactivate accounts, if necessary.

Infrastructure

To outline the topology of its network, the organization maintains the network diagram below to illustrate its internal infrastructure.



Software

The organization maintains a software inventory that outlines the asset name/description, asset type, cost, owner, location, criticality, and purpose. The following critical software are in use:

- RabbitMQ
- VerneMQ
- HiveMQ
- New Relic

People

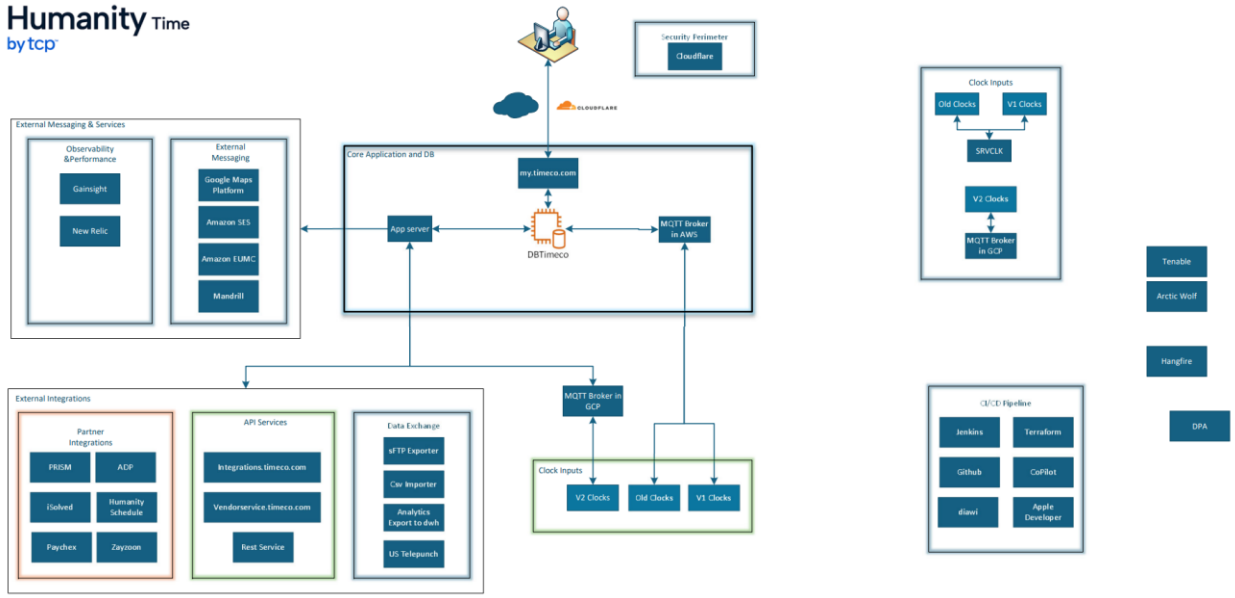
TCP has a hierarchical organizational structure with core vertical departments being led by C-level executives and directors. Functional components within each department are administered by managers and technical leads. An organizational chart is maintained to illustrate TCP's traditional structure and relevant reporting lines.

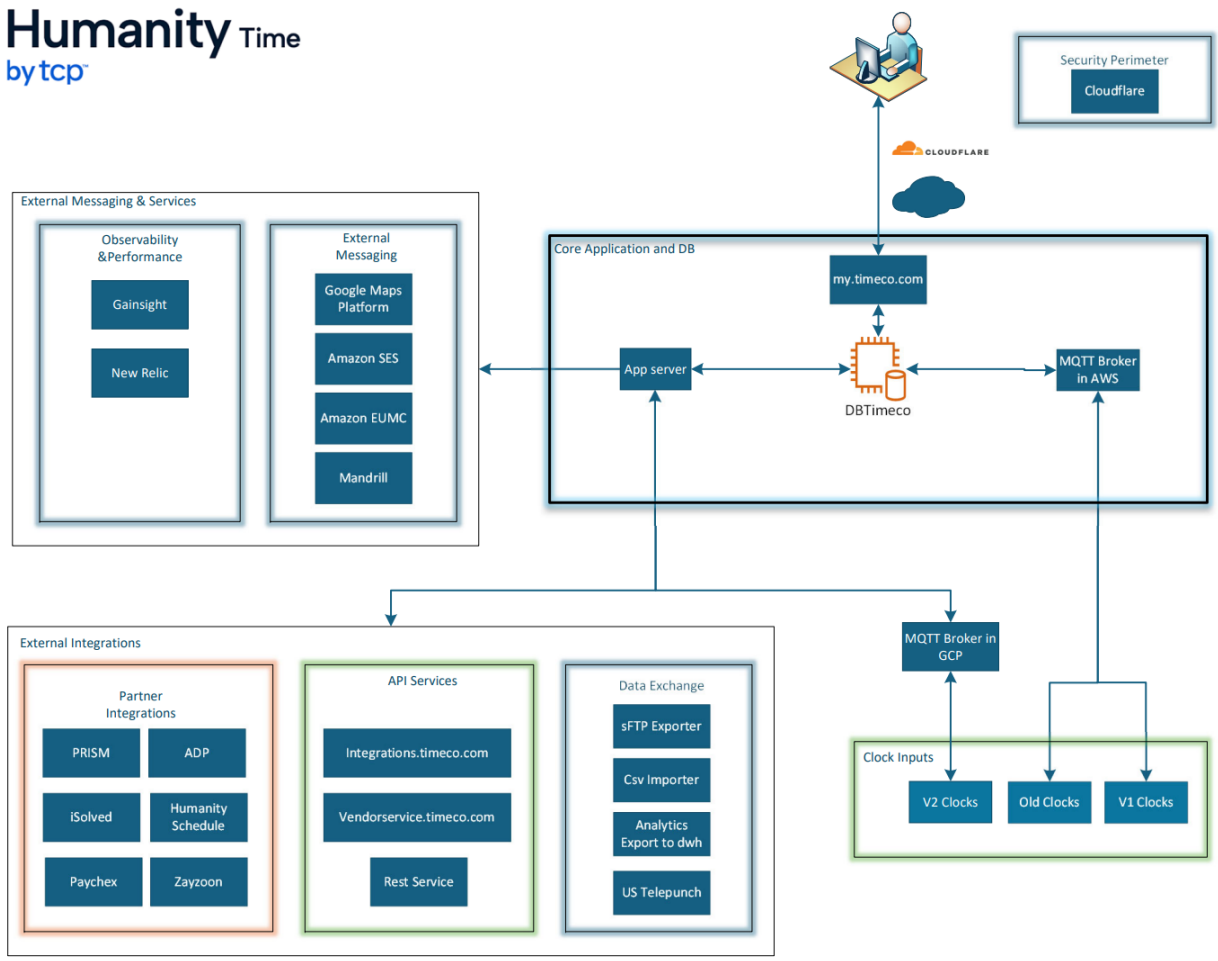
Additionally, the organization maintains a formal board of directors that consists of six members. The board meets quarterly, and executives present audit outcomes, security updates, and notable control topics during these sessions.

Data

The organization has established formal policies and procedures for securing sensitive data handled within the Humanity Time environment. Data is categorized into confidential, internal, and public, with handling requirements tied to these classifications. Confidential data, including personal, financial, and client information, requires special safeguards such as encryption both in transit and at rest, password salting, and hashing techniques.

Encryption standards include AES-256 for stored data, Transport Layer Security (TLS) v1.2 or higher for network communications, and full-disk encryption for workstations and laptops. Sensitive data resides primarily in Amazon S3 buckets, which are encrypted using server-side encryption (SSE-S3) with Amazon-managed keys. SQL databases hosted on EC2 instances use Transparent Data Encryption (TDE). All network traffic is routed through load balancers over TLS 1.2 or higher. Older protocols such as TLS 1.0 and 1.1 are disabled, and strong cipher suites are in place. Secure Shell (SSH) and IPsec are used for secure remote connections. Data at rest is encrypted using AES-256. The data flow diagrams below illustrate the secure movement of sensitive data throughout the Humanity Time environment.





Regarding encryption keys, key management is handled through a combination of AWS Key Management System (KMS) and Keeper. AWS KMS is used for rotating keys associated with storage services such as S3 and EBS, with automatic rotation enabled on a 365-day cycle. Customer-managed keys and AWS-managed keys are both present, and rotation is confirmed as active. TDE keys for Microsoft SQL databases are stored in Keeper.

The key and certificate inventory includes certificates managed through AWS Certificate Manager and Cloudflare. Certificates are renewed automatically, with Cloudflare certificates renewed every 90 days and AWS certificates renewed annually. Certificates in use for production load balancers have 2048-bit key strength and expiration dates clearly documented.

Access to sensitive data repositories is controlled. Only a limited group of users has access to production environments. Permissions are managed through AWS Identity and Access Management (IAM) roles, integrated with Okta for identity and access management. Multi-factor authentication (MFA) is enforced, and role-based access ensures developers typically have read-only access to production. Okta groups and ScaleFT (Advanced Server Access) are used for secure remote access to EC2 instances.

Access reviews are conducted biannually, and recent migration to AWS included a thorough security review of IAM roles and security groups.

Additionally, data retention and disposal follow prescribed schedules, with methods such as wiping and physical destruction applied to retired media.

Customer data is retained for 45 days after account termination. Once this period has passed, the data is purged from the system, and the deletion process is automated. A nightly job runs to identify companies that have been inactive for more than 45 days and purges their data. The process includes checks to confirm the company meets the criteria before deletion. The development team handles this process, and the script for purging is managed by a senior developer.

Processes and Procedures

Management has developed and communicated procedures to guide the provision of the organization's services. Changes to procedures are performed annually and authorized by management. These procedures cover the following key security life cycle areas:

- Data classification
- Categorization of information
- Assessment of the business impact resulting from proposed security approaches
- Selection, documentation, and implementation of security controls
- Performance of annual management self-assessments to assess security controls
- Authorization, changes to, and termination of information system access
- Monitoring security controls
- Management of access and roles
- Maintenance and support of the security system and necessary backup and offline storage
- Incident response
- Maintenance of restricted access to system configurations, user functionality, master passwords, powerful utilities, and security devices

Section B: Principal Service Commitments and System Requirements

Regulatory Commitments

Due to the nature of services TCP provides and the data types that it processes for service delivery, the organization operates under several regulatory requirements, including those from labor authorities such as the Equal Employment Opportunity Commission, the U.S. Department of Labor, and state-specific mandates like Texas labor practices. Privacy laws, including the General Data Protection Regulation (GDPR), Biometric Information Privacy Act (BIPA), the California Consumer Privacy Act (CCPA), and the Data Privacy Framework principles, guide how data is collected, processed, and protected across services.

The organization designs its security programs and business operations to maintain compliance with industry expectations and regulatory commitments. Internal policies are structured to align operational practices with these legal requirements, and legal oversight monitors jurisdictional obligations where employees are located. Regulatory expectations tied to biometric collection influence product features and customer guidance.

Contractual Commitments

The organization has established contracts and agreements with customers to communicate service offerings and commitments. TCP contracts establish the relationship between the service provider and the client by tying the order form directly to a licensing agreement. Terms specify that the provider grants access to services for the contracted period, with the order form prevailing in cases of conflict with general terms. Contracts also describe how amendments to the licensing agreement may occur, noting that changes must not reduce subscribed features or functions. Execution of an agreement requires authorized representatives from both sides, confirming that the contract is legally binding.

System Design

Humanity Time designs its Humanity Time SaaS solution system to meet its regulatory and contractual commitments. These commitments are based on the services that Humanity Time provides to its clients, the laws and regulations that govern the provision of those services, and the financial, operational, and compliance requirements that Humanity Time has established for its services. Humanity Time establishes operational requirements in its system design that support the achievement of its regulatory and contractual commitments. These requirements are communicated in Humanity Time's system policies and procedures, system design documentation, and contracts with clients.