TimeClock Plus, LLC

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 Management

Assertion of TimeClock Plus, LLC Management

We are responsible for designing, implementing, operating, and maintaining effective controls within TimeClock Plus, LLC's workforce management solution system (system) throughout the period January 1, 2025, to December 31, 2025, to provide reasonable assurance that TimeClock Plus, LLC'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'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'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'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's accompanying assertion titled "Assertion of TimeClock Plus, LLC Management" (assertion) that the controls within TimeClock Plus, LLC's workforce management solution system (system) were effective throughout the period January 1, 2025, to December 31, 2025, to provide reasonable assurance that TimeClock Plus, LLC'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 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's service commitments and system requirements were achieved. TimeClock Plus, LLC has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, TimeClock Plus, LLC 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'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'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.

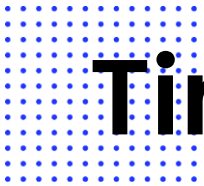
Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the 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's workforce management solution system were effective throughout the period January 1, 2025, to December 31, 2025, to provide reasonable assurance that TimeClock Plus, LLC'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

January 29, 2026



TimeClock Plus, LLC's Description of Its Workforce Management Solution System

Section A: TimeClock Plus, LLC's Description of the Boundaries of Its Workforce Management Solution System

Services Provided

Timeclock Plus, LLC (TCP) has more than 30 years of experience in providing workforce management, scheduling, and time and labor solutions. TCP's customer base spans across industries and verticals including food service, retail, education, and state and local government. The organization's workforce management, scheduling, and time and labor solutions include the following:

- Time Tracking Software
- Employee Scheduling Software
- Mobile Solutions
- Payroll Integrations
- Leave and Absence Management
- Document Management
- Substitute Management
- Advanced Scheduling
- Time Clocks – physical devices including temperature scanners, touchless badge readers, and fingerprint scanners

The above-listed solutions are provided as hardware (actual time clocks) or software that customers access through web interface or mobile applications. Additionally, TCP provides on-premises services for legacy customers or high-security companies that require it.

Onboarding and Implementation

The business development team in the sales department is responsible for engaging with prospects. Once the sales department identifies an interested prospect, an account executive and solutions consultant conducts a discovery call during which the team members gather information from the prospect, including general background and the issues that the prospect wants to solve with TCP services. Following the discovery call, the sales department conducts a demonstration of TCP's services for the prospect.

Once a prospect decides to contract with TCP for services, customer success manages the implementation process through the following phases:

- Initiation phase: During this phase, customer success develops a service strategy for the project, gathers project materials, and assigns resources to the project
- Discovery phase: During this phase, customer success coordinates with project stakeholders on both sides and conducts project kickoff activities, including a needs assessment, to determine build requirements and stores resulting documentation in Salesforce
- Planning phase: During this phase, customer success develops and approves a timeline, confirms deliverables, constructs a work breakdown structure, finalizes the project plan, and creates a communication plan and testing and training strategy

- Delivery phase: During this phase, customer success installs and configures software, ensures the software meets the customer's needs, and conducts training and a pilot test before going live
- Transition phase: During this phase, customer success finalizes agreements, closes the project, collects project feedback, and transitions customers to an ongoing support team

From a technical perspective, the cloud operations team is responsible for creating the customer database. The cloud operations team issues administrator IDs to the customer success team who then configures the environment according to the customer's requirements.

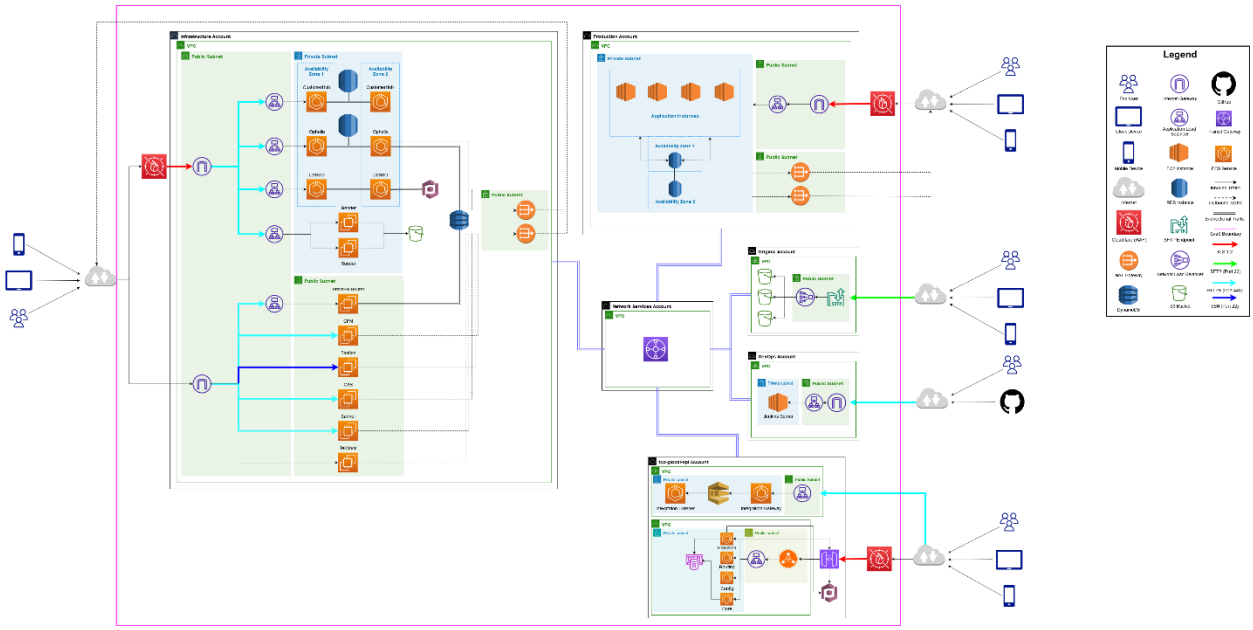
Customer Offboarding

If a customer wishes to terminate services provided by TCP, the customer must notify its customer success manager or account manager. When a customer success manager receives notice of termination, the manager notifies the cloud operations team, and the cloud operations team spins down the customer database. The cloud operations team retains records of customer spin downs.

After a customer terminates its relationship with TCP, the cloud operations team creates a backup of the customer's database and retains the backup for 45 days. After 45 days, the cloud operations team deletes the database schema. A customer may request a copy of their database within 30 days of notifying TCP of termination. The cloud operations team sends database files through a secure link (Liquid Files) that expires after seven days. The information security compliance team and cloud operations team periodically audits the database environment.

Infrastructure

The organization documents its network design for the purpose of showing its network inter-connectivity between its locations and the associated segmentation of various parts of network and perimeter security of its network via firewalls. To outline the topology of its network, the organization maintains the network diagram below to illustrate its internal infrastructure.



In addition, TCP maintains a detailed IT asset inventory that includes laptops, desktops, and servers with current operating system release and version information. Each asset is configured with disk encryption and antivirus software to protect data and reduce security risks.

Software

TCP maintains a documented software inventory that includes version numbers for all installed applications, confirmation of active licenses, and patch status. Each entry is reviewed to verify that licenses remain valid and that applications are not operating on expired agreements. Patch levels are monitored, and updates are applied so that the inventory reflects the current state of the software environment. The following software is deemed critical to the development and implementation of the organization's services:

- AWS Backups
- Cloud Protection Manager (CPM)
- GitHub
- New Relic
- Okta
- Salesforce
- SecureSend
- Tenable
- Mend.io
- Cloudflare
- GuardDuty
- Lumifi EventTracker
- Terraform
- Jenkins
- Veeam
- Windows Defender
- Intune
- SysAid
- Automox
- Pester

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

To provide its services, TCP stores, processes, and transmits customer and personal data related to calculating time and attendance. The types of protected data include employee records such as health information and payroll, authentication secrets, legal materials, and business reports. These datasets exist in multiple locations: production databases, S3 buckets in AWS, on-premises servers, backups on tape media, and endpoint devices.

The Data Classification Policy outlines the organization's standards for classifying data as confidential, internal, and public, with handling requirements tied to these classifications. Confidential data is classified and labeled in documents, folders, or presentations, and handled according to defined retention and disposal schedules. Processes also include anonymization scripts for removing personally identifiable information (PII) before moving databases into test environments, as well as policies for deleting or overwriting customer data once contracts end. Together, the people enforcing policy, the processes for classification, encryption, and disposal, and the technologies like AES, TLS, AWS KMS, and tape systems create a framework for protecting sensitive organizational and client data across its lifecycle.

Regarding data security, the IT Security Policy includes encryption standards for data in transit and at rest, secure workstation and server configurations, and controlled use of personal devices. Sensitive data must be encrypted in transit and at rest, and periodic audits are mandated to identify and correct compliance gaps. Data in transit is protected through TLS v1.2 or higher, with TLS 1.0 and 1.1 disabled, and strong cipher suites mandated for TLS, SSH, and IPsec connections. Corporate and guest wireless networks use WPA2-AES encryption, while application load balancers are configured with AWS security policies that only support TLS v1.2 and 1.3. For data at rest, production environments apply AES-based encryption, with AES-256 as the preferred standard for both databases and backups, and full-disk encryption is enabled on workstations and laptops.

Passwords and secrets are safeguarded with salted hashing algorithms, while storage volumes such as EC2 EBS disks demonstrate encryption enabled with AWS KMS-managed keys. S3 buckets storing sensitive data apply default server-side encryption. The data flow diagram illustrates the secure movement of data throughout the network environment.

Regarding data retention, the organization's data retention rules are determined by the nature of the data and align with applicable U.S. and international privacy frameworks. The IT Security Policy includes detailed data retention timelines, disposal requirements, and physical access controls for facilities and equipment. Personal data retention schedules are defined for corporate, legal, accounting, tax, payroll, employee, and client records, with retention periods ranging from months to permanent depending on the category.

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

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