TimeClock Plus, LLC

System and Organization Controls Report (SOC 3)

Independent Report of the Controls to meet the criteria for the Security, Availability, Processing Integrity, and Confidentiality categories for the period of January 1, 2023 through December 31, 2023.

KirkpatrickPrice

4235 Hillsboro Pike
Suite 300
Nashville, TN 37215

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, 2023, to December 31, 2023, to provide reasonable assurance that TimeClock Plus, LLC's service commitments and system requirements relevant to security, availability, processing integrity, and confidentiality 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, 2023, to December 31, 2023, 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, processing integrity, and confidentiality (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, 2023, to December 31, 2023, 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

Jaime Ellis
VP of IT & Information Security
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, 2023, to December 31, 2023, 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, processing integrity, and confidentiality (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, 2023, to December 31, 2023, 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 25, 2024

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

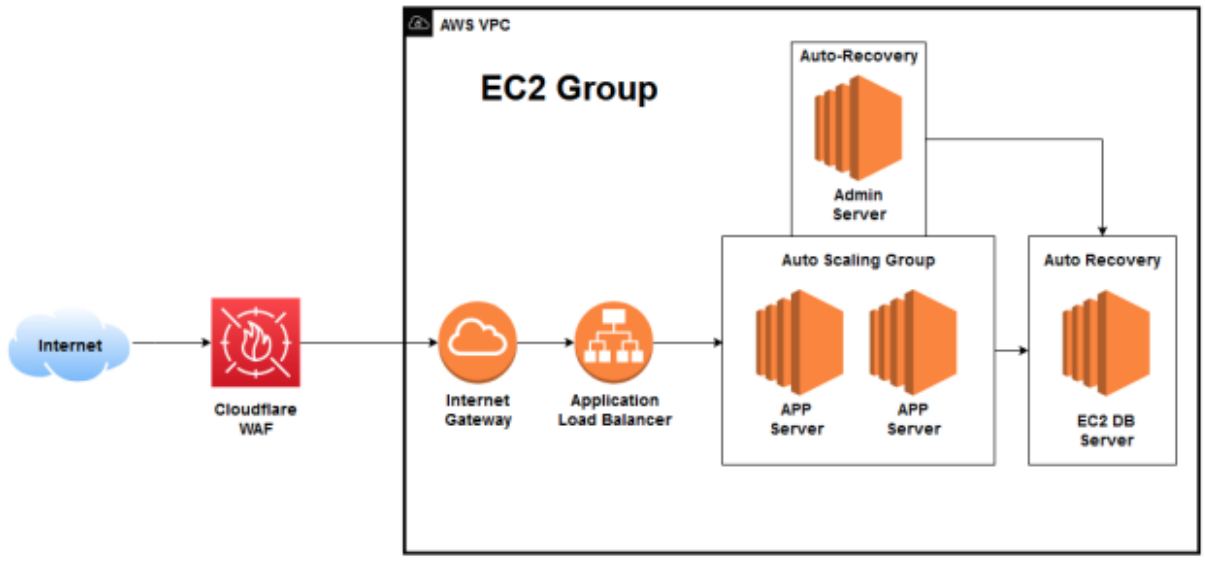
If a customer wishes to terminate services provided by TCP, the customer must notify its customer success manager or account manager. When a customer success manager receives notice of termination, the manager notifies the cloud operations team, and the cloud operations team spins down the customer database.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

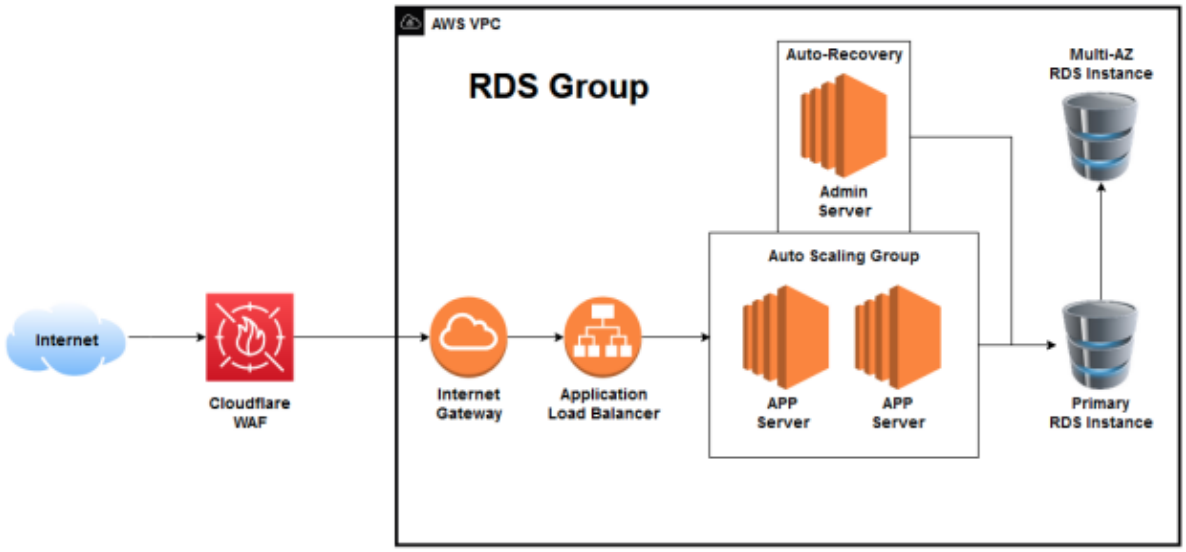
After a customer terminates its relationship with TCP, the cloud operations team creates a backup of the customer's database and retains the backup for 45 days. After 45 days, the cloud operations team deletes the database schema. A customer may request a copy of their database within 30 days of notifying 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

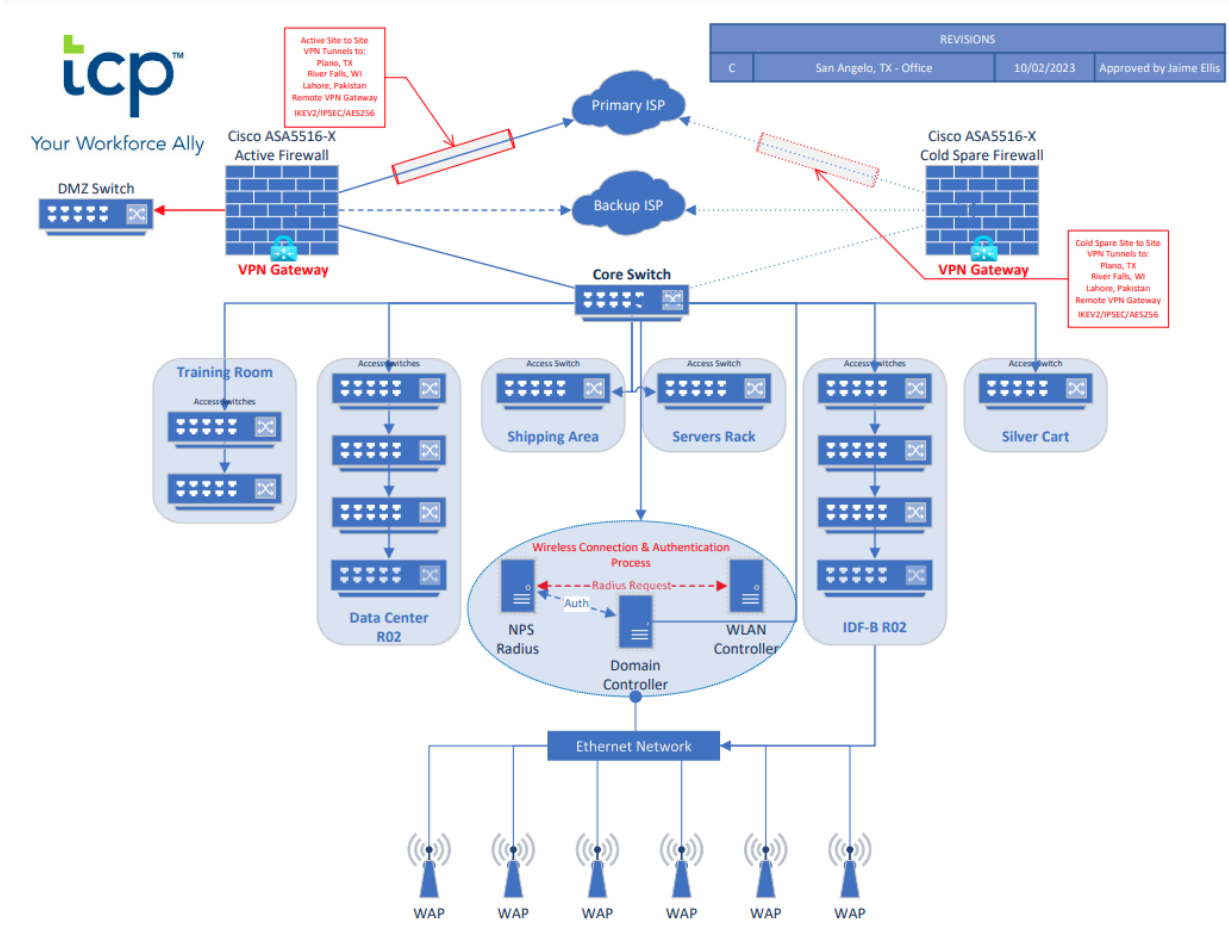
From San Angelo, there are active site-to-site virtual private network (VPN) tunnels to Plano, River Falls, and a remote VPN gateway. Each of the four offices are behind a firewall. The following diagrams depict TCP's infrastructure in Amazon Web Services (AWS), the San Angelo office, and the remote VPNs in all offices.

DATA STORAGE

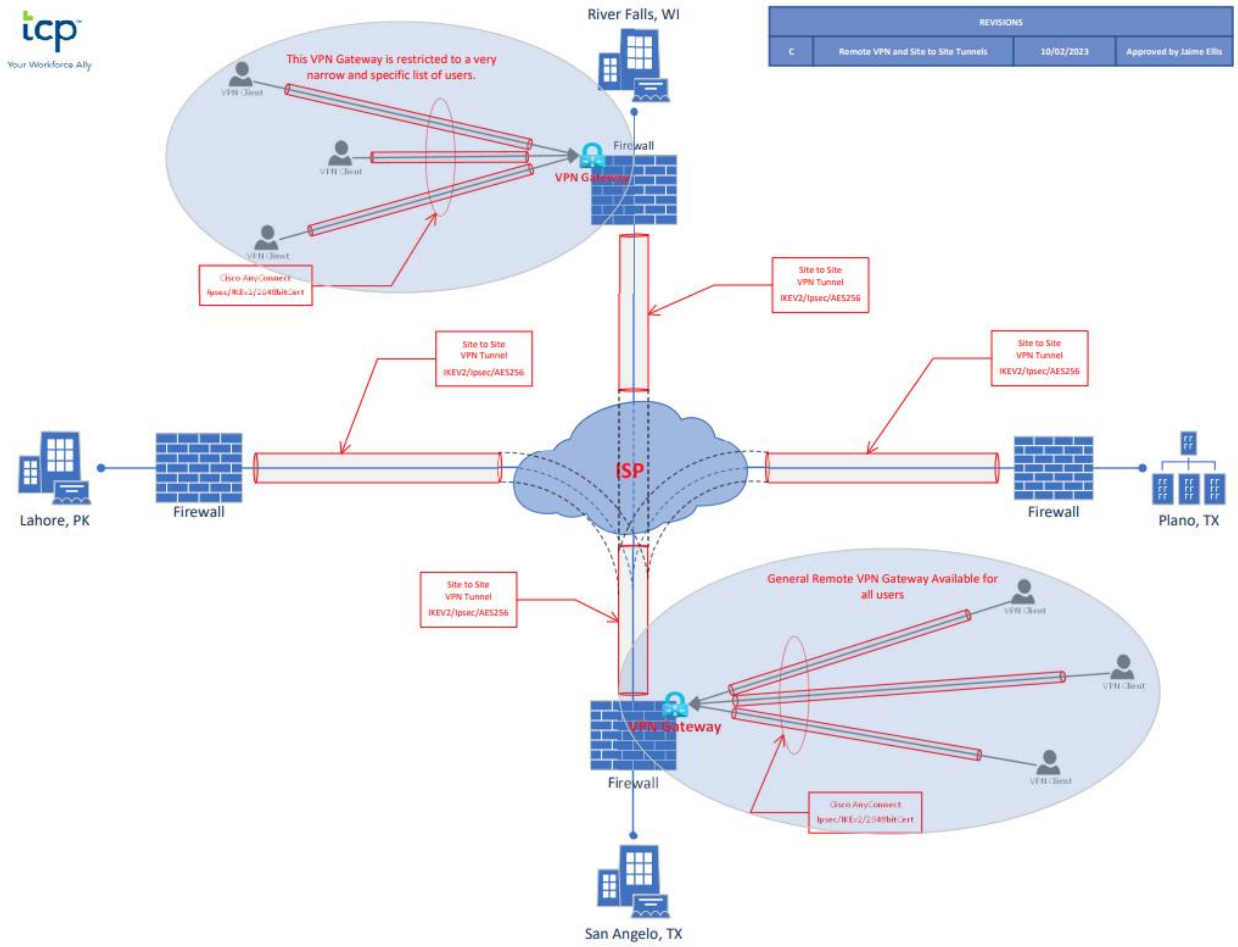




AWS Architecture Details



San Angelo Network Diagram



Remote VPN Infrastructure for All Offices Diagram

Software

TCP uses the following critical software to provide its services:

- Cloud Protection Manager (CPM)
- GitHub
- New Relic
- Okta
- Salesforce
- SecureSend Liquid Files
- Tenable

People

TCP is organized into a hierarchical structure with a Chief Executive Officer (CEO) at the head. The leadership team consists of C-level executives and the CEO, and the organization has established defined reporting lines up to the CEO. The Senior Vice President (VP) and chief executives report directly to the CEO.

Additionally, the TCP board of directors provides oversight to the organization. Quarterly board meetings are conducted during which the board reviews companywide performance and strategic initiatives. The board engages with an external company to conduct a third-party risk assessment that benchmarks TCP's security posture against other organizations, and the board reviews the results of the risk assessment and the risk maturity score.

Data

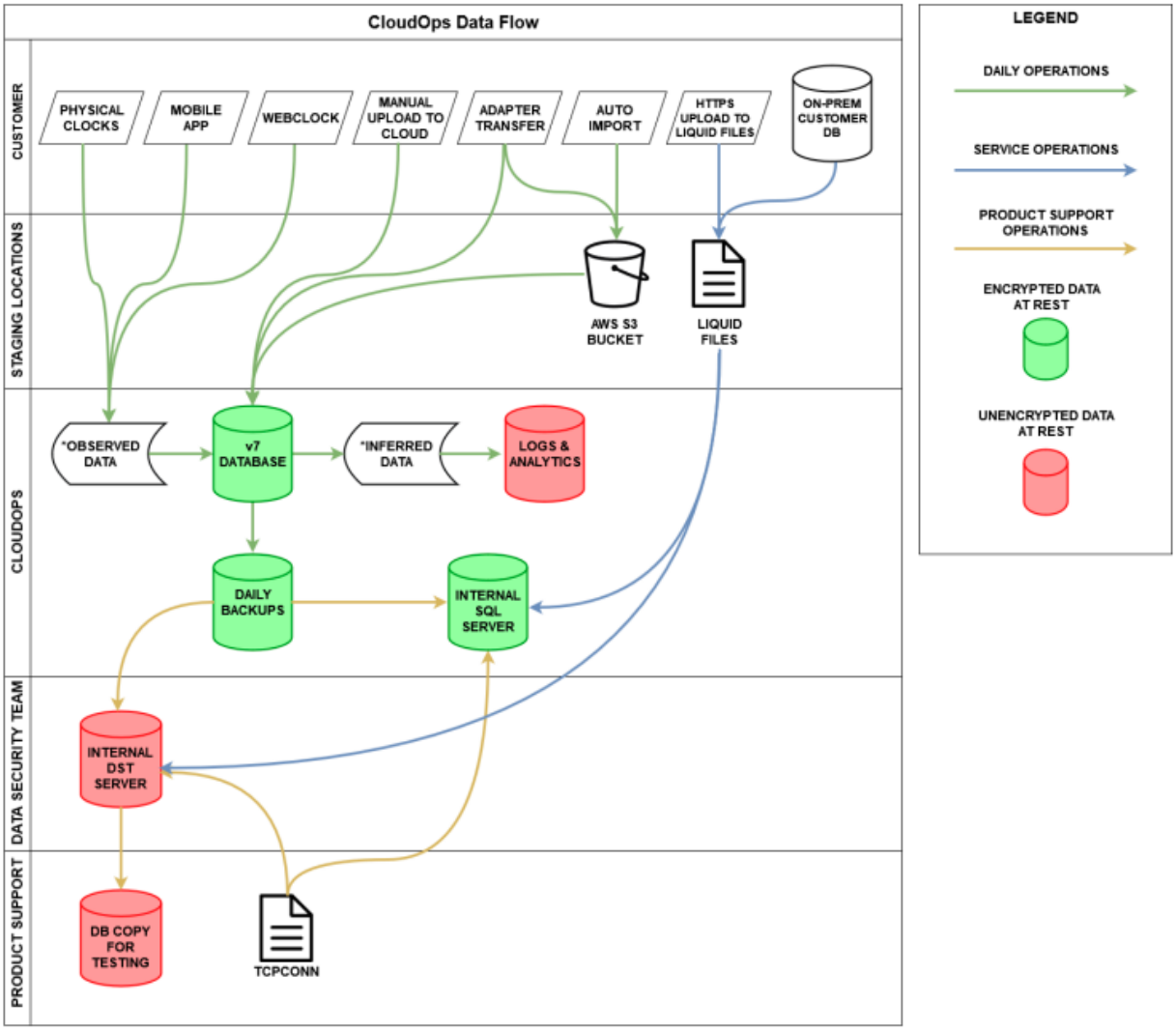
TCP handles a wide variety of customer and personal data related to calculating time and attendance. The data handled by the organization includes sensitive data, such as personal demographic and personal activity data. Personal demographic data may include the following:

- Username
- Password
- First and last name
- Social Security Number (SSN)
- Address
- Email
- Phone number
- Job title
- Employee ID
- Taxpayer ID
- Gender
- Date of birth
- Hire date
- Termination date
- Language preference
- Payroll classification
- Employment classification
- Pay rates
- Work schedules
- Employment contracts

Personal activity data may include the following:

- Clock-in/out time
- Clock-in/out location
- Leave requests, including vacation, sick, and other third-party defined leave reasons, leave accruals, Family and Medical Leave Act (FMLA) cases, and hours worked
- Special categories, such as trade union membership and biometric data

The diagram included below demonstrates the CloudOps data flow.



TCP employees do not receive access to customer data by default and must request and gain approved access from the Data Security Team through the TCP Security Portal, which serves as an internal identity management tool.

The Data Security Team is responsible for handling customer data. When testing must be conducted on a customer database, the Data Security Team scrubs the database to remove personally identifiable information (PII), and the database is hosted internally. The engineering team completes testing and support, and the database is deleted immediately. The Data Security Team uses a ticketing system and verifies that any database older than 45 days is removed.

The Global Data Privacy Policy governs data retention. The organization implements data retention policies for all types of personal data that TCP processes. When the retention period has expired, personal data is securely deleted or destroyed. The Data Disposal Policy and Procedures

document provides guidance for disposing of customer data in the TCP software-as-a-service (SaaS) environment.

The organization uses encryption to protect data. TCP follows industry best practices for encryption, including recommendations from Amazon, Payment Card Industry (PCI), and National Institute of Standards and Technology (NIST). Data in transit is encrypted using Transport Layer Security (TLS) 1.2 or higher and secure ciphers for communication sessions.

Additionally, TCP deploys a web application firewall (WAF) to protect data. The organization WAF is deployed with rules-based configurations to detect and block malicious traffic based on Open Web Application Security Project (OWASP) best practice guidelines. The WAF protects against distributed-denial-of-service (DDoS) attacks through real-time traffic inspection rules that are capable of detecting and blocking malicious behavior based on patterns.

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

TCP's operations are impacted by various privacy laws, including California Consumer Privacy Act (CCPA), General Data Protection Regulation (GDPR), and Biometric Information Privacy Act (BIPA). Privacy regulations form part of the set of regulations that have imposed changes to controls and procedures within the organization's operations and products. Regulations and laws provide a set of frameworks to which TCP aligns operational controls and procedures. The Global Data Privacy Policy outlines TCP's process of classifying, transmitting, storing, and processing sensitive and confidential data in compliance with applicable laws and regulations.

Contractual Commitments

When TCP reaches an agreement with a customer, the organization generates an order form in Salesforce. Order forms link to TCP's licensing, privacy, and data processing agreements. TCP and the customer may continue negotiating the terms of the agreement, and once all terms are determined, the customer signs the licensing agreement. The standard licensing agreement and data processing addendum communicate security standards and confidentiality commitments. Additionally, the data backup and retention portion of the licensing agreement lists a recovery point objective (RPO) of 24 hours. Although general license agreements do not contain uptime agreements, custom agreements may include uptime commitments. The organization has historically provided an SLA greater than 99.9% for customers.

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.