2. TCP Security & Risk Governance

TCP's primary security focus is to safeguard our customers' and users' data. This is the reason that TCP has invested in the appropriate resources, controls, and independent oversite to protect and service our customers around the world. This investment includes the implementation of a dedicated Security Team and Data Protection Officer (DPO). The Security Team and DPO are responsible for TCP's comprehensive security and risk management program and the governance process. The Security Team is focused on defining new and refining existing controls in accordance with industry best practices, implementing and managing the TCP security framework, maintaining legal compliance for our business and our customers, as well as providing a support structure to facilitate effective risk management. Our Data Protection Officer, who reports to the Vice President of Operations, oversees the Security Team.

3. Our Security & Risk Management Objectives

TCP has developed a security framework using industry best practices and widely adopted security principles. Our key objectives are:

- Trust and Data Protection – consistently deliver superior products and service to our customers while protecting the privacy and confidentiality of their data.
- Availability and Continuity of Service – ensure ongoing availability of the service and data to all authorized users and proactively minimize the security risks threatening service continuity.
- Compliance – implement process and controls to align with regulatory guidelines and industry best practices. We have designed our TCP Cloud security program around best-of-breed guidelines for cloud security. In particular, we leverage standards like SOC 2 Type II, Center for Internet Security (CIS), the EU General Data Protection Regulation (GDPR), and the California Consumer Protection Act (CCPA).

4. TCP Security Controls

In order to ensure we protect data entrusted to us, we have implemented an array of security controls. TCP's security controls are designed to allow for a high level of employee efficiency without artificial roadblocks, while minimizing risk.

TCP Product Infrastructure - Data Center Security

TCP outsources hosting of its TCP Cloud infrastructure to leading cloud infrastructure providers. TCP products leverage Amazon Web Services (AWS) for SaaS infrastructure hosting. These solutions are secure by design and provide high levels of physical and network security.

At present, TCP's AWS cloud server and instances reside only in US locations. Both providers maintain an audited security program, including SOC 2, NIST, ISO and FedRAMP compliance. TCP does not host any production software systems within its corporate offices. This world-class infrastructure provider leverages the most advanced facilities infrastructure such as power, networking, and security. Facilities uptime is guaranteed between 99.95% and 100%, and the facilities ensure a minimum of N+1 redundancy to all power, network, and HVAC services. Access to these providers' sites is highly restricted to both physical access as well as electronic access through public (internet) and private (intranet) networks in order to eliminate any unwanted interruptions in our service to our customers. The physical, environmental, and infrastructure security protections, including continuity and recovery plans, have been independently validated as part of their SOC 2 Type II certifications. More information and certificates are available at the AWS compliance and security site.

Amazon Compliance SOC 2 FAQs
Amazon Compliance Data Center Controls

Network Security & Perimeter Protection

The TCP Cloud infrastructure is built with internet-scale security protections in mind. In particular, network security protections are designed to prevent unauthorized network access to and within the internal product infrastructure. These security controls include enterprise-grade routing and network access control lists (firewalling). Network-level access control lists are implemented in AWS Virtual Private Cloud (VPC) security groups which applies port- and address-level protections to each of the server instances in the infrastructure. This allows for finely grained control for network traffic from a public network as well as between server instances on the interior of the infrastructure. Within the infrastructure, internal network restrictions allow a many-tiered approach to ensuring only the appropriate types of devices can communicate. Changes in the network security model are actively monitored, and controlled by standard change control processes. Rogue wireless access points are detected and reported continuously through the Wireless LAN controller deployed through the TCP offices. All existing rules and changes are evaluated for security risk by our Security Team, and captured appropriately.

Configuration Management

Automation drives TCP's ability to scale with our customers' needs. The TCP Cloud infrastructure is a highly automated environment that flexibly expands capacity and capability as needed. Server instances rely on configuration management utilities, meaning that every server's configuration is tightly controlled from spin-up through deprovisioning. All server type configurations are defined as attributes within environmental variables or bootstraps. Server-level configuration management is handled using these configuration scripts when the server is built.

Changes to the configuration are managed through a controlled change. Each server role includes its own hardened configuration, depending on the deployment of the instance. Patch management and configuration control is typically handled by removing server instances that are no longer compliant with the expected baseline and provisioning a replacement instance in its place. Rigorous and automated configuration management is baked into our day-to-day infrastructure processing.

Alerting & Monitoring

Not only does TCP fully automate its build procedures, we invest heavily in automated monitoring, alerting and response technologies to continuously address potential issues. The TCP Cloud infrastructure is instrumented to alert DevOps Engineers and SysOps Technicians when anomalies occur. In particular, error rates, server, outages, resource spikes, abuse scenarios, application attacks, and other anomalies trigger automatic responses and alerts to the appropriate teams for response, investigation, and correction. As unexpected or malicious activities occur, systems bring in the right people to ensure that the issue is rapidly addressed. Many automated triggers are also designed into the system to immediately respond to foreseen situations. Traffic blocking, quarantine, process termination, auto-scaling, and similar functions kick in at pre-defined thresholds to ensure that the TCP Cloud can protect itself against a wide variety of undesirable situations. The power behind TCP's ability to detect and respond to anomalies is our 24x7x365 monitoring program and extensive logging. Our systems capture and store logs that include all the technologies that comprise our products. At the application layer, all logins, operations, modifications, and other access to TCP databases are also logged. The production servers are configured to forward security events and syslogs to a Log Collection Appliance and onto a Security Operation Center(s) which monitors via a combination of AI and heuristic learning to trigger escalations as needed. In the infrastructure back-end, we log authentication attempts, horizontal and vertical permission changes, infrastructure health, and requests performed. Infrastructure and application events are monitored and categorized in real-time based on risk and the TCP team has access to online reporting including alerts and security event data to identify intrusion-behavior on the TCP production platform. Issues are escalated immediately at any hour of the day to developers, security professionals, and engineers to take appropriate action.

Infrastructure Access

Entire categories of potential security events are prevented with a stringent, consistent, and well-designed access control model. Along those lines, access to TCP's systems is strictly controlled. TCP employees are only granted access to product infrastructure based on their jobs, using a role-based access control model. For access to infrastructure tools, servers, and similar services, access is minimized to only the individuals whose jobs require it.

Additionally, connections to product infrastructure devices over SSH, RDP, or similar protocols is prohibited. Engineers are required to authenticate first through a centralized multi-factor authentication solution which grants a Single Sign On experience into the production Access Management Utility. The Access Management Utility then generates a short-lived certificate to the server to leverage certificate-based authentication in which all traffic is proxied through a bastion host.

Application Protection - Web Application Defenses

As part of its commitment to protecting customer data and websites, TCP implemented an industry recognized Web Application Firewall (WAF). The WAF automatically identifies and protects against attacks aimed at the TCP products hosted in the TCP Cloud. The rules used to detect and block malicious traffic are aligned to the best practice guidelines documented by the Open Web Application Security Project (OWASP) in the OWASP Top 10 and similar recommendations. Protections from Distributed Denial of Service (DDoS) attacks are also incorporated, helping to ensure that applications hosted in the TCP cloud are available continuously. The WAF is configured with a combination of industry standard and custom real-time traffic inspection rules. These rules are capable of detecting and automatically blocking malicious behavior based on behavior type and rate.

Development & Release Management

One of TCP's greatest advantages is a rapidly advancing feature set, and we provide constantly improving products through a modern, continuous delivery approach to software development. New code is promoted, tested, certified, and deployed monthly. Code reviews and quality assurance are performed, both manually and via automations, by specialized teams of engineers with intimate knowledge of the TCP product. Automated testing is performed on daily builds to ensure that bugs are identified well before a monthly release. Testing and certification are strictly controlled by quality assurance management under SOC 2 principles. Once certified, code is submitted to TCP's SaaS Team where additional testing occurs. If all passes, the new code is deployed in phases across all TCP Cloud environments. All code deployments create archives of existing production-grade code and full database backups in case failures are detected post-deployment. The SaaS Team manages notifications regarding the health of the applications. If a failure occurs, a roll-back is immediately engaged. Major feature changes, are communicated on our **Knowledgebase**, via email and through in-app messages and/or product update posts. Customers and users can sign up to receive updates notifications in advance.

Vulnerability Scanning, Penetration Testing

The TCP Security team manages a multi-layered approach to vulnerability scanning, using a variety of industry-recognized tools to ensure comprehensive coverage of our technology stack. We perform hundreds of vulnerability scanning and penetration testing activities against ourselves on a continuous basis. We perform vulnerability scanning against our internal networks, applications, and corporate infrastructure. Network-based and application-level vulnerability scans run at least daily to ensure that

we detect and respond to the latest vulnerabilities. Static code analysis automatically reviews the most current code to detect potential security flaws early in the development lifecycle. Web Application scans are conducted and reviewed prior to every version release as part of the validation process. Also, continually running scans, adaptive scanning inclusion lists, and continuously updating vulnerability signatures help TCP stay ahead of many security threats.

For a second opinion about our ability to identify and respond to security risks, we bring in industry-recognized third parties to perform regular penetration tests and security audits. The goal of these programs is to iteratively identify flaws that present security risks and rapidly address any issues. Penetration tests are performed against the application layers and network layers of the TCP technology stack, and penetration testers are given internal access to the TCP product and/or corporate networks in order to maximize the kinds of potential vectors that should be evaluated.

Customer Data Protection - TCP Products

TCP products are designed to process vast amounts of Personal Data. We process the personal data of our customers' employees and our business contacts. In order to provide the highest level of data protection, TCP has adopted the provisions of our Global Data Privacy Policy (Privacy Policy) for processing customers' employee. The information collected by our products is gathered directly from customers and users. TCP's products allow customers to define the type of information to be collected and processed on their behalf via our data-collection tools. Per the TimeClock Plus Service/Licensing Agreements, our customers ensure that they capture only appropriate information to support their business processes and do so in compliance with applicable data privacy regulations. The TCP products are not used to collect or capture sensitive data such as credit or debit card numbers or personal financial account information.

Please review the full **Global Data Privacy Policy here**

Encryption In-Transit & At-Rest

All sensitive interactions with the TCP products (e.g., API calls, login, authenticated sessions to the customer's portal, etc.) are encrypted in-transit with TLS 1.2 and 2,048 bit keys or better. TCP leverages several technologies to ensure stored data is encrypted at rest. The physical and virtualized hard drives used by TCP product server instances as well as long-term storage solutions use AES-256 encryption. Additionally, certain databases or field-level information is encrypted, based on the sensitivity of the information. For instance, user passwords are hashed and certain email features work by providing an additional level of both at-rest and in-transit encryption.

User Authentication & Authorization

The TCP products enforce a user-defined password policy that can be customized to match the client's existing security standards. TCP's TimeClockPlus software provides integrations with external Authentication services such as Active Directory and LDAP. The products compatibility with Identity Federation mechanisms such as SAML2 and CAS provide a Single Sign On experience for organizations who want to extend their security domain to the cloud-based Time and Attendance solution.

Customers can assign finely grained permissions to the users in their portals and limit access to the portal's content and features.

Privacy

The privacy of our customers' data is one of TCP's primary considerations. As described in our Privacy Policy, we never sell your Personal data to any third parties. The protections described in this document and other protections that we have been implemented are designed to ensure that your data stays private and unaltered. The TCP products are designed and built with customer needs and privacy considerations in the forefront. Our privacy program incorporates best practices, customers' and their employees' needs, as well as regulatory requirements. Along those lines, TCP is certified under the EU-US and Swiss-US Privacy Shield Frameworks and is a member of the U.S. Department of Commerce Privacy Shield. More information about our certification is available on the **Privacy Shield site**.

Please review the full **Global Data Privacy Policy here**

Data Retention Policy

Customer data is retained for as long as you remain a customer. Former customers' data is removed from live databases upon a customer's written request or after an established period following the termination of all customer agreements. In general, former customers' data, including information stored in replicas, snapshots, and backups, is purged 30 days after all customer relationships are terminated.

Please review the full **Data Retention Policy here**

Privacy Program Management
TCP's DPO, Legal, Security, and several other teams collaborate to ensure an effective and consistently implemented privacy program. Information about our commitment to the privacy of your data is described in greater detail in our Privacy Policy and Data Processing Agreements.

How to contact our DPO or lodge a complaint:

By Email:
Data Protection Officer
DPO@tcpsoftware.com

By Mail:
Data Management, Inc.
Attn: Data Protection Officer
1 Time Clock Dr.
San Angelo, TX 76904; USA

Business Continuity & Disaster Recovery
TCP maintains business continuity and disaster recovery plans focusing both on preventing outage through redundancy of telecommunications, systems and business operations, and on rapid recovery strategies in the event of an availability or performance issue. Whenever customer-impacting situations occur, TCP's goal is to quickly and transparently isolate and address the issue. Identified issues are published on TCP's status site and are subsequently updated until the issue is resolved.

System Resiliency & Recovery
Business continuity testing is part of TCP normal processing. TCP recovery processes are validated continuously through normal maintenance and support processes. We follow a monthly deployment lifecycle, and create or destroy many server instances as part of our regular daily maintenance and growth. We also use those procedures to recover from impaired instances and other failures, allowing us to practice our recovery process every day. TCP primarily relies on infrastructure redundancy, real time replication across multi-availability zones, and backups. All TCP product services are built with full redundancy. Server infrastructure is strategically distributed across multiple distinct availability zones and virtual private cloud networks within our infrastructure providers, and all web, application, and database components are deployed with a minimum of n+1 supporting server instances or containers.

Backup Strategy

TCP ensures data is replicated and backed up daily in multiple durable data-stores. The retention period of backups depends on the nature of the data, however customer database backups are stored for no less than 30 days. Customer database backups also replicated across availability zones and regions in order to provide fault-tolerance as well as scalability and responsive recovery, when necessary. In addition, the following policies have been implemented and enforced for data resilience:

- Customer (production) data is backed up at least daily. Thirty days' worth of backups are kept for any database in a way that ensures restoration can occur easily. Snapshots are taken and stored to a secondary service no less often than daily and where practicable, real time replication is used. All production data sets are stored on a distributed file storage facility like Amazon's S3.

- Because we leverage cloud services for hosting, backup and recovery, TCP does not implement physical infrastructure or physical storage media within its products. TCP does not generally produce or use other kinds of hard copy media (e.g., paper, tape, etc.) as part of making our products available to our customers.

- By default, all backups will be protected through access control restrictions on TCP product infrastructure networks, access control lists on the file systems storing the backup files and/or through database security protections.

- The fundamental Availability goal for the SaaS environment to provide an SLA of 99.9 (Historically it has been higher) outside of maintenance windows and if database loss occurs provide a recovery time objective of 24 hours and a recovery point objective of 24 hours.

TCP Corporate Security - Employee Authentication & Authorization

TCP enforces an industry-standard corporate password policy. That policy requires changing passwords at least every 180 days with corporate network perimeter access requiring multi-factor authentication. It also requires a minimum password length of 10 characters and complexity requirements including special characters, upper and lower case characters, numbers and enforcing greater complexity for accounts with administrator level access. TCP prohibits account and password sharing by multiple employees. Employees generally authenticate to TCP product infrastructure using SSH keys. Additionally, many of the capabilities we use to build the TCP products leverage multi-factor authentication or are protected by single sign on solutions.

Access Management

TCP has regimented and automated authentication and authorization procedures for employee access to TCP corporate and production systems. All access is logged. Most frequently, access is granted based on a role-based access control model. We built an extensive set of support systems and procedures to streamline and automate our security management and compliance activities. In addition to many other functions, our team sweeps our product and corporate infrastructure regularly to ensure that permission grants are appropriate, to manage employee events, to revoke accounts and access where needed, to compile logs of access requests, and to capture compliance evidence for each of our technology security controls.

Background Checks

TCP employees undergo an extensive 3rd party background check prior to formal employment offers. In particular, employment, education, and criminal checks are performed for all potential employees. Reference verification is performed at the hiring manager's discretion. All employees receive security training within the first week of employment as part of the TCP security program along with role-specific follow-up training. All employees must comply with Non-Disclosure Agreements and an Acceptable Use Policy as part of access to corporate and production networks.

Vendor Management

We leverage a small number of 3rd party service providers who augment the TCP products' ability to meet your needs. We maintain a vendor management program to ensure that appropriate security and privacy controls are in place. The program includes inventorying, tracking, and reviewing the security programs of the vendors who support TCP. Vendors must adhere to privacy policies no less restrictive than those adopted by TCP. Additionally, vendors must provide a certificate of insurance in accordance with the services being provided. Vendor employees must pass background checks and comply with Non-Disclosure Agreements and an Acceptable Use Policy to perform work on behalf of TCP. Vendor access to facilities and systems is granted in accordance the service being provided and the type of data being accessed. Ongoing compliance with expected protections is managed as part of our contractual relationship with them. Our Security team, Legal Department, and the business unit who owns each contract coordinate unique considerations for our providers as part of contract management.

Security Awareness & Security Policies

To help keep all our software engineers, support technicians, and other employees on the same page with regard to protecting your data, TCP developed and maintains an Information Security Policy and administers regular online and in-person security training. The policy covers data handling requirements, privacy considerations, and responses to violations, among many other topics. With this policy and the myriad of protections and standards in place, we also ensure TCP employees are well-trained for their roles. Multiple levels of security training are provided to TCP employees based on their roles and resulting access. General security awareness training is offered to all new employees and covers TCP security requirements. After initial training, different training tracks are available based on an employee's role. Developer-specific training is provided by and tailored to TCP's software engineering teams. In general, training sessions are held weekly, a portion of which include security materials. Recurring training is provided through regular updates, notices, and internal publications.

For more information about our training programs, contact **training@tcpsoftware.com.**

Incident Management

TCP provides 24x7x365 coverage to respond quickly to all security and privacy events. TCP's Incident Response Team (IRT) is responsible for triaging critical tickets, engaging the proper resources to correct an issue, and formulating a Root Cause/Correct Action report (RCCA). Pre-defined incident severity types are leveraged to facilitate timely incident tracking, consistent task assignment, escalation, and communication. Many automated processes feed into the incident response process, including malicious activity or anomaly alerts, vendor alerts, customer requests, privacy events, and others. In responding to any incident, we first confirm the exposure of the information and determine the source of the security problem, if possible. We communicate back to the customer (and any other affected customers) via email or phone (if email is not sufficient). We provide periodic updates as needed to ensure appropriate resolution of the incident. Our Chief Technology Officer and Security Team review all security-related incidents, either suspected or proven, and we coordinate with affected customers using the most appropriate means, depending on the nature of the incident and applicable disclosure regulations.

TCP utilizes 3rd party forensics and breach notification vendors to ensure that proper notice is given in accordance with applicable breach notification regulations. Additionally, these 3rd party services offer an additional layer of transparency to our customers.

5. Third Party Audits & Certifications Of TCP Security Controls

TCP is SOC 2 Type II certified and maintains compliance with the EU-US Privacy Shield. Our services are housed in the US with world-class cloud infrastructure providers Amazon Web Services. All TCP infrastructure providers are SOC 2 Type II, ISO 27001, NIST, and FedRAMP certified and maintain facilities secured against electronic and physical intrusion.

6. Document Scope & Use

TCP values transparency in the ways we provide solutions to our customers. This document is designed with that transparency in mind. We are continuously improving the protections that have been implemented and, along those lines, the information and data in this document (including any related communications) are not intended to create a binding or contractual obligation between TCP and any parties, or to amend, alter or revise any existing agreements between the parties.