SENTRY ASSURANCE

TESCHGlobal, LLC

SOC 2 Type 1

2024

REPORT ON TESCHGLOBAL, LLC's DESCRIPTION OF ITS SYSTEM RELEVANT TO COMMON CRITERIA/SECURITY, AVAILABILITY, CONFIDENTIALITY, AND PRIVACY

Pursuant to Reporting on System and Organization Controls 2 (SOC 2) Type 1 examination performed under AT-C 105 and AT-C 205

July 31, 2024

TABLE OF CONTENTS

SECTION 1
ASSERTION OF TESCHGLOBAL, LLC MANAGEMENT

ASSERTION OF TESCHGLOBAL, LLC MANAGEMENT

August 19, 2024

We have prepared the accompanying description of TESCHGlobal, LLC's ('TESCHGlobal' or 'service organization') HealthLX Platform services (description) based on the criteria for a description of a service organization's system set forth in DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance—2022) in AICPA, Description Criteria (description criteria). The description is intended to provide report users with information about the HealthLX Platform services that may be useful when assessing the risks arising from interactions with TESCHGlobal's system, particularly information about system controls that TESCHGlobal has designed and implemented to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Confidentiality, and Privacy (applicable trust services criteria) set forth in TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022) in AICPA, Trust Services Criteria and its compliance with the commitments in its Privacy Notice as of July 31, 2024.

TESCHGlobal uses subservice organizations to provide Cloud Hosting Services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at TESCHGlobal, to achieve TESCHGlobal's service commitments and system requirements based on the applicable trust services criteria and compliance with the commitments in the Privacy Notice. The description presents TESCHGlobal's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of TESCHGlobal's controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at TESCHGlobal, to achieve TESCHGlobal's service commitments and system requirements based on the applicable trust services criteria compliance with the commitments in the Privacy Notice. The description presents TESCHGlobal's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of TESCHGlobal's controls.

We confirm, to the best of our knowledge and belief, that—

a. The description presents TESCHGlobal's HealthLX Platform services that were designed and implemented as of July 31, 2024, in accordance with the description criteria.
b. The controls stated in the description were suitably designed as of July 31, 2024 to provide reasonable assurance that TESCHGlobal's service commitments and system requirements would be achieved based on the applicable trust services criteria.

Kelly Ross

_____

Kelly Ross
CISO
TESCHGlobal, LLC

SECTION 2
INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: TESCHGlobal, LLC

Scope

We have examined TESCHGlobal's accompanying description of its HealthLX Platform services found in Section 3 titled TESCHGlobal's Description of its HealthLX Platform services as of July 31, 2024 (description) based on the criteria for a description of a service organization's system set forth in DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance—2022) in AICPA, Description Criteria, (description criteria) and the suitability of the design of controls stated in the description as of July 31, 2024, to provide reasonable assurance that TESCHGlobal's service commitments and system requirements would be achieved based on the trust services criteria relevant to Security, Availability, Confidentiality, and Privacy ("applicable trust services criteria") set forth in TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022) (link) in AICPA, Trust Services Criteria.

TESCHGlobal uses subservice organizations to provide Cloud Hosting Services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at TESCHGlobal, to achieve TESCHGlobal's service commitments and system requirements based on the applicable trust services criteria. The description presents TESCHGlobal's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of TESCHGlobal's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls or the subservice organization's compliance with the commitments in its privacy notice.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at TESCHGlobal, to achieve TESCHGlobal's service commitments and system requirements based on the applicable trust services criteria and TESCHGlobal's compliance with the commitments in its privacy notice. The description presents TESCHGlobal's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of TESCHGlobal's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

TESCHGlobal is responsible for its service commitments and system requirements and for designing and implementing effective controls within the system to provide reasonable assurance that TESCHGlobal's service commitments and system requirements would be achieved. In Section 1, TESCHGlobal has provided the accompanying assertion titled Assertion of TESCHGlobal Management (assertion) about the description and the suitability of the design of controls stated therein. TESCHGlobal is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our

examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed to provide reasonable assurance that the service organization's service commitments and system requirements would be achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

An examination of a description of a service organization's system and the suitability of the design of controls involves—

- obtaining an understanding of the system and the service organization's service commitments and system requirements.
- assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed.
- performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
- performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization would achieve its service commitments and system requirements based on the applicable trust services criteria.
- evaluating the overall presentation of the description.

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

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual report users may consider important to meet their informational needs. There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. The projection to the future of any conclusions about the suitability of the design 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.

Other Matter

We did not perform any procedures regarding the operating effectiveness of controls stated in the description and, accordingly, do not express an opinion thereon.

Opinion

In our opinion, in all material respects—

a. the description presents TESCHGlobal's system that was designed and implemented as of July 31, 2024, in accordance with the description criteria.
b. the controls stated in the description were suitably designed as of July 31, 2024, to provide reasonable assurance that TESCHGlobal's service commitments and system requirements would be achieved based on the applicable trust services criteria.

Restricted Use
This report is intended solely for the information and use of TESCHGlobal; user entities of TESCHGlobal's HealthLX Platform services as of July 31, 2024; business partners of TESCHGlobal subject to risks arising from interactions with the HealthLX Platform services; practitioners providing services to such user

entities and business partners; prospective user entities and business partners; and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization.
- How the service organization's system interacts with user entities, business partners, and other parties.
- Internal control and its limitations.
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
- The applicable trust services criteria.
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

This report is not intended to be, and should not be, used by anyone other than these specified parties.

Sentry Assurance, LLC
Cleveland, Ohio
August 19, 2024

SECTION 3
TESCHGLOBAL LLC'S DESCRIPTION OF ITS HEALTHLX PLATFORM SERVICES AS OF JULY 31, 2024

OVERVIEW OF OPERATIONS

Company Background

TESCHGlobal LLC was founded in 2005 with the objective of providing data-driven solutions and consulting services. The company specializes in aligning business strategy with digital technologies to decrease costs, increase efficiency, and boost productivity. TESCHGlobal has earned recognition as one of the nation's fastest-growing private companies, showcasing its entrepreneurial spirit and dedication to customer success.

The organization is headquartered in Grafton, Wisconsin, with additional offices in Mexico and the Netherlands. TESCHGlobal's team is committed to continuous improvement and helping organizations overcome complex challenges through technology-agnostic solutions.

TESCHGlobal has partnered with several prominent companies, including HealthLX, Snowflake, and Alation, to deliver exceptional technology solutions.

TESCHGlobal serves a diverse range of industries, including but not limited to, Healthcare, Supply Chain, Marketing, Manufacturing, Data Management, and Web Development.

Description of Services Provided

services across various industries. The company specializes in aligning business strategy with digital technologies to increase efficiency, reduce costs, and boost productivity.

TESCHGlobal's core services include:

- Data Management: Transforming data into valuable assets for increased revenue, cost reduction, and risk mitigation.
- Managed Services: Managing cloud-based technology infrastructure with specialized staff.
- Software Development: Custom full-stack software development, including web and mobile applications.
- FHIR Interoperability: Implementing HealthLX Composable Automation Platform and FHIR Capability Suite.
- Enterprise Integration: Connecting disparate systems using technologies like Talend and Apache NiFi.

Trips are tracked throughout the order cycle, from initial ride assignment to completion or reassignment. Information is shared with user entities via telephone, fax, secure electronic exchange (FTP, email, EDI), and secured websites.

Principal Service Commitments and System Requirements

TESCHGlobal LLC designs its processes and procedures to meet its objectives for providing high-quality data-driven solutions and consulting services. These objectives are based on the service commitments TESCHGlobal makes to its clients, the laws and regulations that govern the provision of its services, and the financial, operational, and compliance requirements established for the services. TESCHGlobal's services are subject to various security and privacy requirements, including industry standards and relevant regulations.

Security commitments to clients are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the services offered. Key security commitments include:

- Access Control: Ensuring that users can access only the information necessary for their roles while preventing unauthorized access.
- Encryption: Using encryption technologies to protect client data both at rest and in transit.
- Regular Audits and Assessments: Conducting regular security audits and assessments to ensure compliance with security policies and procedures.
- Incident Response: Implementing a robust incident response plan to address and mitigate security incidents promptly.

Operational Requirements:
TESCHGlobal establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. These are communicated through policies, system design documentation, and contracts. Key operational requirements include:

- Organizational Policies: Developing organization-wide policies to protect systems and data, covering areas such as system design, operation, network management, and employee responsibilities.
- Training and Awareness: Ensuring all employees are trained on security policies and procedures and understand their roles in maintaining data security.
- Continuous Improvement: Regularly updating policies and procedures to address new security threats and improve existing security measures.
- Monitoring and Reporting: Implementing monitoring tools to track system performance and security incidents and providing regular reports to stakeholders.

These commitments and requirements are designed in order for TESCHGlobal's to meet client expectations, comply with regulatory standards, and maintain high levels of security and privacy.

Components of the System

The System description is comprised of the following components:

- Infrastructure – The collection of physical or virtual resources that supports an overall IT environment, including the physical environment and related structures, IT and hardware (for example, facilities, servers, storage, environmental monitoring equipment, data storage devices and media, mobile devices, and internal networks and connected external telecommunications networks) that the service organization used to provide the services.
- Software - The application programs and IT system software that supports application programs (operating systems, middleware, and utilities), the types of databases used, the nature of external facing web applications, and the nature of applications developed in-house, including details about whether the applications in use mobile applications or desktop or laptop applications are.
- People - The personnel involved in the governance, operation, security, and use of a system (business unit personnel, developers, operators, user entity personnel, vendor personnel, and managers).
- Data – The types of data used by the system, such as transaction streams, files, databases, tables, and output used or processed by the system.
- Procedures – The automated and manual procedures related to the services provided, including, as appropriate, procedures by which service activities are initiated, authorized, performed, and delivered, and reports and other information prepared.

Infrastructure

Primary Infrastructure	
Hardware	Purpose
Primarily AWS	Cloud Hosting Provider
PfSense Firewall	Perimeter firewall
Dell Power Edge Server	VDI instances and test environments

Software

Primary Software	
Software	Purpose
Apache Nifi v 1.25	Open-source Execution Engine

People

TESCHGlobal's organization consists of approximately 50 employees organized in the following functional areas:

- Executives. Executives are primarily responsible for the oversight and strategic direction of TESCHGlobal and organizational steering decisions.
- Developers. Responsible for the overall execution of system enhancements, maintenance and other feature improvements for the TESCHGlobal Interoperability services platform.
- Project Managers: Responsible for managing activities within the organization, prioritization of team allocation, maintaining and executing on end user use cases.

Data
Data, as defined by TESCHGlobal constitutes the following:

- Data captured and stored includes health data from various payers within the system.

All data ingested by the platform is subject to various methods of data validation, notably XSD, to confirm correct schema and expected formatting. Any inconsistencies or other noted errors are captured, and actions taken are documented via internal tracking tickets for follow up and resolution.

Processes, Policies and Procedures
Management has developed and communicated policies and procedures to manage the system's information security. reviews and updates are performed regularly and supported by the respective owners.

Physical Security
Formal IT policies and procedures exist that describe physical security, logical access, computer operations, change control and data communication standards. All teams are expected to adhere to the processes that define how services should be delivered. Guest logs are maintained for physical visits, and visitors are supervised onsite at all times.

Logical Access
TESCHGlobal uses role-based access management through Active Directory to authenticate users, requiring identification and authentication prior to the use of any system resources.

Resources are protected through the use of native system security and add-on software products that identify and authenticate users and validate access requests against the users' authorized roles in access control lists. TESCHGlobal additionally leverages Duo Multi-Factor Authentication (MFA) for system access.

Computer Operations – Backups
Customer data is backed up and monitored by operations personnel for completion and exceptions. In the event of an exception, operations personnel perform troubleshooting and analysis to identify the root cause and re-run the backup job immediately or as part of the next scheduled backup job. Backups are performed via AWS on a daily basis and encompass all production databases as well as EC2 instances.

Computer Operations – Availability
Incident response policies and procedures are in place to guide personnel in reporting and responding to information technology incidents. Procedures exist to identify, report, and act upon system security breaches and other incidents. Incident response procedures are in place to identify and respond to incidents on the network.

TESCHGlobal uses numerous tools to monitor system security, this includes many tools from AWS such as AWS Organizations, AWS Control Tower, and other tools to identify and then correct any outstanding issues.

Change Control
A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Quality assurance testing and User Acceptance Testing (UAT) results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers.

- TESCHGlobal has implemented a patch management process to ensure contracted customer and infrastructure systems are patched in accordance with vendor recommended operating system patches. Customers and system owners review proposed operating system patches to determine whether the patches are applied. TESCHGlobal's staff validate that all patches have been installed and if applicable that reboots have been completed.

Data Communication

Firewall systems are in place to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is otherwise not explicitly authorized. Network address translation (NAT) functionality is utilized to manage internal IP addresses. Admin access to the firewall is restricted to authorized users. TESCHGlobal leverages specific rules and whitelists through AWS to execute on traffic filtering. Access attempts are logged and reviewed for patterns or other inconsistencies, or potential threats as needed and incident tickets are raised for relevant events.

TESCHGlobal has VDI instances that are totally managed and require user privileges (vs admin privileges) for our users to use. This is to ensure that all users are compliant with all PHI and PII regulations and do not locally host any data of this nature.

BOUNDARIES OF THE SYSTEM

The scope of this report includes the HealthLX Platform services performed in the Ontario, Canada facilities.

This report does not include the data center hosting services provided by Amazon Web Services.

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION, AND MONITORING

Control Environment

Integrity and Ethical Values

TESCHGlobal LLC places a strong emphasis on integrity and ethical values, which are essential components of its control environment. These values influence the design, administration, and monitoring of all internal controls. TESCHGlobal's ethical standards are communicated through formal policies and reinforced through regular training and management practices.

Key aspects include:

- Management actions to mitigate risks associated with unethical behavior.
- Clear communication of organizational values through policies and codes of conduct.

Specific Control Activities:

- Documented Policies and Codes of Conduct: TESCHGlobal has formally documented policies that outline ethical standards and behavior expectations. These documents are communicated to all employees.
- Employee Acknowledgment: Employees are required to sign acknowledgment forms, confirming their understanding and commitment to adhere to the company's policies.
- Confidentiality Agreements: All employees sign confidentiality agreements to ensure that sensitive information is protected.
- Background Checks: Comprehensive background checks are conducted for all new hires to ensure the integrity of the workforce.

Commitment to Competence

TESCHGlobal LLC defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes considering the required competence levels for various jobs and ensuring that employees possess the requisite skills and knowledge.

Specific control activities that TESCHGlobal has implemented in this area are described below:

- Defined Competence Levels: Management at TESCHGlobal carefully considers the competence levels required for specific roles within the organization. These requirements are clearly documented in written job descriptions, ensuring that all employees understand the expectations and skills needed for their positions.
- Training Programs: TESCHGlobal is committed to continuous learning and skill development. The company provides ongoing training programs to help employees maintain and enhance their competencies. This includes professional development opportunities tailored to the needs of different roles within the organization.
- Performance Evaluations: Regular performance evaluations are conducted to assess the competence of employees. These evaluations help identify areas where additional training or support may be needed, ensuring that all team members can perform their duties effectively.
- Recruitment Practices: TESCHGlobal's recruitment process is designed to attract individuals with the necessary competencies for the roles they will fill. The company employs thorough vetting processes and competency-based interviewing techniques to ensure that new hires meet the required standards.
- Knowledge Sharing: TESCHGlobal fosters a culture of knowledge sharing through mentorship programs and collaborative projects. This approach ensures that expertise and skills are disseminated throughout the organization, supporting the overall competence of the team.

TESCHGlobal's commitment to competence is integral to its ability to provide high-quality services and maintain a strong control environment. By continuously investing in the skills and knowledge of its workforce, TESCHGlobal ensures that it can meet the evolving needs of its clients and maintain high standards of performance.

Management's Philosophy and Operating Style

TESCHGlobal LLC's management philosophy and operating style encompass a broad range of characteristics. These include the management's approach to taking and monitoring business risks, and their attitudes toward information processing, accounting functions, and personnel management. The company's management philosophy focuses on innovation, transparency, and a commitment to excellence, which are central to its success.

Specific control activities that TESCHGlobal has implemented in this area are described below:

- Regulatory and Industry Briefings: Management at TESCHGlobal is regularly briefed on regulatory and industry changes that could impact their services. This ensures that the company remains compliant with relevant laws and regulations and can quickly adapt to industry shifts. Regular updates and briefings help maintain a proactive approach to compliance and industry standards.
- Executive Management Meetings: Regular executive management meetings are held to discuss major initiatives and issues affecting the business as a whole. These meetings provide a platform for strategic planning, risk assessment, and decision-making, ensuring that all major business decisions are aligned with the company's overall strategy and objectives. These meetings facilitate clear communication and coordinate efforts across all levels of management.
- Approach to Risk Management: TESCHGlobal's management demonstrates a proactive approach to risk management by identifying potential risks early and implementing measures to mitigate them. This includes conducting regular risk assessments and developing comprehensive risk management plans. By maintaining a forward-thinking risk management strategy, TESCHGlobal ensures operational resilience and sustained performance.
- Attitudes Toward Information Processing: The management at TESCHGlobal places a high priority on the accuracy and reliability of information processing. This commitment is achieved through stringent data management practices, regular audits, and the use of advanced technology to ensure data integrity and security. Ensuring the quality and security of data is paramount to maintaining client trust and operational efficiency.

- Focus on Employee Development: Management at TESCHGlobal is deeply committed to the continuous development of its employees. This includes providing ongoing training and professional development opportunities, fostering a culture of continuous improvement, and encouraging knowledge sharing across the organization. Such practices ensure that employees remain competent and motivated, contributing to the company's overall success.

These control activities reflect TESCHGlobal's commitment to maintaining a robust control environment, ensuring operational efficiency, compliance with regulations, and the successful achievement of its business objectives.

Organizational Structure and Assignment of Authority and Responsibility

TESCHGlobal LLC's organizational structure provides the framework within which its activities for achieving company-wide objectives are planned, executed, controlled, and monitored. Management believes establishing a relevant organizational structure includes considering key areas of authority and responsibility. This organizational structure has been developed to suit TESCHGlobal's needs and is based, in part, on its size and the nature of its activities.

TESCHGlobal's assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

Specific control activities that TESCHGlobal has implemented in this area are described below:

- Organizational Charts: TESCHGlobal uses organizational charts to communicate key areas of authority and responsibility. These charts are regularly updated to reflect any changes in the organizational structure.
- Clear Reporting Lines: Reporting relationships and authorization hierarchies are clearly defined to ensure effective communication and decision-making within the company.
- Role-Specific Training: TESCHGlobal provides training and resources to ensure that employees have the necessary knowledge and skills to fulfill their roles and responsibilities effectively.
- Performance Management: Regular performance evaluations help ensure that employees understand their roles and how their performance contributes to the overall objectives of the company. These evaluations also help identify areas where additional support or training may be needed.
- Communication of Policies: TESCHGlobal communicates its policies and procedures clearly to all employees, ensuring that everyone understands the company's objectives and their role in achieving them.

These control activities help TESCHGlobal maintain a robust organizational structure that supports its business objectives and ensures effective governance and accountability.

Human Resources Policies and Practices

TESCHGlobal LLC's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top-quality personnel who ensure the organization operates at maximum efficiency. TESCHGlobal's human resource policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

Specific control activities that TESCHGlobal has implemented in this area are described below:

- New Employee Orientation: New employees are required to sign acknowledgment forms for the employee handbook and a confidentiality agreement following their orientation on their first day of employment. This ensures that all employees are aware of company policies and their responsibilities from the start.

- Annual Evaluations: Evaluations for each employee are performed on an annual basis. These evaluations help ensure that employees understand their roles, receive feedback on their performance, and identify areas for professional development.
- Termination Procedures: Employee termination procedures are in place to guide the termination process and are documented in a termination checklist. This ensures that all terminations are handled consistently and fairly, reducing the risk of legal issues and maintaining the organization's ethical standards.
- Training Programs: TESCHGlobal provides ongoing training and professional development opportunities to ensure that employees maintain the necessary skills to perform their roles effectively. This commitment to continuous learning helps the company adapt to new challenges and maintain a high standard of service.
- Compensation and Benefits: The company maintains transparent and competitive compensation and benefits policies to attract and retain top talent. Regular reviews of compensation structures ensure that they remain aligned with industry standards and organizational goals.
- Compliance and Ethics: TESCHGlobal has clear policies in place to ensure compliance with local, state, and federal regulations. This includes non-discrimination policies, safety guidelines, and procedures for addressing grievances and disciplinary issues. Regular training sessions are held to ensure all employees are aware of these policies and understand their importance.

These control activities reflect TESCHGlobal's commitment to maintaining a robust human resource environment that supports its business objectives and ensures operational efficiency and compliance with regulations.

Risk Assessment Process

TESCHGlobal LLC's risk assessment process identifies and manages risks that could potentially affect its ability to provide reliable services to user organizations. This ongoing process requires management to identify significant risks inherent in products or services as they oversee their areas of responsibility. TESCHGlobal identifies the underlying sources of risk, measures the impact to the organization, establishes acceptable risk tolerance levels, and implements appropriate measures to monitor and manage the risks.

This process has identified risks resulting from the nature of the services provided by TESCHGlobal, and management has implemented various measures designed to manage these risks. Risks identified in this process include the following:

- Operational Risk: Changes in the environment, staff, or management personnel.
- Strategic Risk: New technologies, changing business models, and shifts within the industry.
- Compliance Risk: Legal and regulatory changes.

TESCHGlobal has established an independent organizational business unit responsible for identifying risks to the entity and monitoring the operation of the firm's internal controls. This approach is intended to align the entity's strategy more closely with its key stakeholders, assist the organizational units with managing uncertainty more effectively, minimize threats to the business, and maximize its opportunities in the rapidly changing market environment. TESCHGlobal actively identifies and mitigates significant risks through the implementation of various initiatives and continuous communication with other leadership committees and senior management.

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of TESCHGlobal's system; as well as the nature of the components of the system result in risks that the criteria will not be met. TESCHGlobal addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meeting the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, TESCHGlobal's management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

Information and Communications Systems

Information and communication are integral components of TESCHGlobal LLC's internal control system. The process involves identifying, capturing, and exchanging information within the required timeframe to conduct, manage, and control the entity's operations. This process encompasses various aspects, including the dependency on and complexity of information technology.

At TESCHGlobal, information is identified, captured, processed, and reported through various information systems, as well as through conversations with clients, vendors, regulators, and employees.

Specific control activities that TESCHGlobal has implemented in this area are described below:

- Regular Meetings and Updates: Various weekly and bi-annual meetings are held to discuss operational efficiencies and disseminate new policies, procedures, controls, and strategic initiatives within the organization. For example, town hall meetings provide updates on key issues affecting the organization and its employees, ensuring everyone is informed and aligned with the company's goals.
- Automated Information Systems: Information gathered from formal automated information systems and informal databases is used to support decision-making processes. This includes data integration and management tools that help streamline operations and enhance communication across departments.
- Communication of Security Policies: General updates to security policies and procedures are communicated to TESCHGlobal personnel via e-mail messages and internal portals. This ensures all employees are aware of any changes and understand their role in maintaining security standards.
- Client and Stakeholder Engagement: TESCHGlobal engages with clients, vendors, and regulators through various channels to ensure that all relevant information is shared and feedback is incorporated into their processes. This helps in maintaining transparency and building trust with all stakeholders.

TESCHGlobal's approach to information and communication systems helps maintain a robust internal control environment, ensuring operational efficiency and compliance with industry standards.

Monitoring Controls

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. TESCHGlobal LLC performs continuous monitoring activities to assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

On-Going Monitoring

TESCHGlobal's management conducts quality assurance monitoring on a regular basis, and additional training is provided based upon the results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

Reporting Deficiencies

An internal tracking tool is utilized to document and track the results of on-going monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

These monitoring controls ensure that TESCHGlobal maintains a high standard of operational efficiency and compliance with industry standards and regulations.

Changes to the System in the Last 3 Months

No significant changes have occurred to the services provided to clients in the last 3 months preceding the end of the review date.

Incidents in the Last 3 Months

No significant incidents have occurred to the services provided to clients in the last 3 months preceding the end of the review date.

Trust Services Criteria Not Applicable to the System

Privacy		
Category	**Criteria**	**Description**
Privacy	P1.1	**Not Applicable** – TESCHGlobal acts as a data processor as a component of the in-scope services.
	P2.1	
	P3.1	
	P3.2	
	P5.2	
	P6.1	

Subservice Organizations

This report does not include the cloud hosting services provided by Amazon Web Services (AWS).

Subservice Description of Services

Amazon Web Services provides cloud hosting services.

Complementary Subservice Organization Controls

TESCHGlobal's services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all the trust services criteria related to TESCHGlobal's services to be solely achieved by TESCHGlobal's control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of TESCHGlobal.

The following subservice organization controls should be implemented by AWS to provide additional assurance that the trust services criteria are met.

Amazon Web Services (AWS)		
Category	Criteria	Control
Security	CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.
		Access to sensitive data center zones requires approval from authorized personnel and is controlled via badge access readers, biometric identification mechanism, and/or physical locks.
		Data center perimeters are defined and secured via physical barriers.
		Access lists to high security areas in data centers are reviewed on a defined basis and inappropriate access is removed in a timely manner.
		Visitors to data center facilities must gain approval from authorized personnel, have their identity verified at the perimeter, and remain with an escort for the duration of the visit.
		Security measures utilized in data centers are assessed annually and the results are reviewed by executive management.
		Data centers are continuously staffed and monitored by security personnel using real time video surveillance and/or alerts generated by security systems.
		The company reviews access to the data centers at least annually.
		The company has processes in place for granting, changing, and terminating physical access to company data centers based on an authorization from control owners.

TESCHGlobal utilizes subservice organizations to provide certain components of its service. To ensure that the subservice organization controls are necessary, in combination with controls at TESCHGlobal, to provide reasonable assurance that its service commitments and system requirements are achieved, TESCHGlobal management defines the scope and responsibility of these controls through written contracts, such as service level agreements.

TESCHGlobal conducts ongoing monitoring of the subservice organization controls, including the following procedures:

- Holding periodic discussions with vendors and subservice organizations
- Reviewing attestation reports over services provided by vendors and subservice organizations

TESCHGlobal documents the nature of the services provided by the subservice organization, relevant aspects of the subservice organization's infrastructure, software, people, procedures, and data, and the portions of the system that are attributable to the subservice organization when using the inclusive method. When using the carve-out method, TESCHGlobal documents the nature of the service provided by the subservice organization, each of the applicable trust services criteria that are intended to be met by controls at the subservice organization, and the types of controls that service organization management assumed would be implemented by the subservice organization that are necessary, in

combination with controls at TESCHGlobal, to provide reasonable assurance that its service commitments and system requirements are achieved (complementary subservice organization controls or CSOCs).

COMPLEMENTARY USER ENTITY CONTROLS

TESCHGlobal's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all the Trust Services Criteria related to TESCHGlobal's services to be solely achieved by TESCHGlobal's control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of TESCHGlobal's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to TESCHGlobal.
2. User entities are responsible for notifying TESCHGlobal of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record for content management.
4. User entities are responsible for ensuring the supervision, management, and control of the use of TESCHGlobal services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize TESCHGlobal's services.
6. User entities are responsible for providing TESCHGlobal with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying TESCHGlobal of any actual or suspected information security breaches, including compromised user accounts used for integrations and file transfers.

TRUST SERVICES CATEGORIES

In-Scope Trust Services Categories

Common Criteria (to the Security Category)
Security refers to the protection of: i. Information during its collection or creation, use, processing, transmission, and storage and; ii. Systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

Availability
i. Availability refers to the accessibility of information used by the entity's systems as well as the products or services provided to its customers. The availability objective does not, in itself, set a minimum acceptable performance level; it does not address system functionality (the specific functions a system performs) or usability (the ability of users to apply system functions to the performance of specific tasks or problems).

Confidentiality
i. Confidentiality addresses the entity's ability to protect information designated as confidential from its collection or creation through its final disposition and removal from the entity's control in accordance with management's objectives. Information is confidential if the custodian (for example, an entity that holds or stores information) of the information is required to limit its access, use, and retention and restrict its disclosure to defined parties (including those who may otherwise have authorized access within its system boundaries).

Privacy
Privacy. Personal information is collected, used, retained, disclosed, and disposed of to meet the entity's objectives. I. Notice and communication of objectives. The entity provides notice to data subjects about its objectives related to privacy. II. Choice and consent. The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to data subjects. III. Collection. The entity collects personal information to meet its objectives related to privacy. IV. Use, retention, and disposal. The entity limits the use, retention, and disposal of personal information to meet its objectives related to privacy. V. Access. The entity provides data subjects with access to their personal information for review and correction (including updates) to meet its objectives related to privacy. VI. Disclosure and notification. The entity discloses personal information, with the consent of the data subjects, to meet its objectives related to privacy. Notification of breaches and incidents is provided to data subjects, regulators, and others to meet its objectives related to privacy. VII. Quality. The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet its objectives related to privacy. VIII. Monitoring and enforcement. The entity monitors compliance to meet its objectives related to privacy, including procedures to address privacy-related inquiries, complaints, and disputes.

CONTROL ACTIVITIES SPECIFIED BY THE SERVICE ORGANIZATION

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Control Environment		
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	The company performs background checks on new employees.
		The company requires contractor agreements to include a code of conduct or reference to the company code of conduct.
		The company requires employees to acknowledge a code of conduct at the time of hire. Employees who violate the code of conduct are subject to disciplinary actions in accordance with a disciplinary policy.
		The company requires contractors to sign a confidentiality agreement at the time of engagement.
		The company requires employees to sign a confidentiality agreement during onboarding.
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The company's board of directors or a relevant subcommittee is briefed by senior management at least annually on the state of the company's cybersecurity and privacy risk. The board provides feedback and direction to management as needed.
		The company's board of directors has a documented charter that outlines its oversight responsibilities for internal control.
		The company's board members have sufficient expertise to oversee management's ability to design, implement and operate information security controls. The board engages third-party information security experts and consultants as needed.
		The company's board of directors meets at least annually and maintains formal meeting minutes. The board includes directors that are independent of the company.
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	The company's board of directors has a documented charter that outlines its oversight responsibilities for internal control.
		The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.
		The company maintains an organizational chart that describes the organizational structure and reporting lines.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Control Environment		
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**
		Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	The company performs background checks on new employees.
		Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.
		The company requires employees to complete security awareness training within thirty days of hire and at least annually thereafter.
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	The company requires employees to acknowledge a code of conduct at the time of hire. Employees who violate the code of conduct are subject to disciplinary actions in accordance with a disciplinary policy.
		Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Information and Communication		
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings. If the company has committed to an SLA for a finding, the corrective action is completed within that SLA.
		The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.
		Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.
		Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.
		The company requires employees to complete security awareness training within thirty days of hire and at least annually thereafter.
		The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.
		The company's information security policies and procedures are documented and reviewed at least annually.
		The company provides a description of its products and services to internal and external users.
		The company communicates system changes to authorized internal users.
		The company has established a formalized whistleblower policy, and an anonymous communication channel is in place for users to report potential issues or fraud concerns.
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company provides a description of its products and services to internal and external users.
		The company's security commitments are communicated to customers in Master Service Agreements (MSA) or Terms of Service (TOS).
		The company notifies customers of critical system changes that may affect their processing.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Information and Communication		
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**
		The company provides guidelines and technical support resources relating to system operations to customers.
		The company has an external-facing support system in place that allows users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel.
		The company has written agreements in place with vendors and related third-parties. These agreements include confidentiality and privacy commitments applicable to that entity.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Risk Assessment		
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	The company specifies its objectives to enable the identification and assessment of risk related to the objectives.
		The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.
CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.
		The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.
		The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.
		The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.
		The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.
CC3.4	COSO Principle 9: The entity identifies and assesses changes that	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Risk Assessment		
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**
	could significantly impact the system of internal control.	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.
		The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.
		The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Monitoring Activities		
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings. If the company has committed to an SLA for a finding, the corrective action is completed within that SLA.
		Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.
		The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.
		The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.
CC4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings. If the company has committed to an SLA for a finding, the corrective action is completed within that SLA.
		The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Control Activities		
CC5.0	**Criteria**	
CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	The company's information security policies and procedures are documented and reviewed at least annually.
		The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	The company's information security policies and procedures are documented and reviewed at least annually.
		The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.
		The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.
CC5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.
		The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.
		The company's information security policies and procedures are documented and reviewed at least annually.
		The company specifies its objectives to enable the identification and assessment of risk related to the objectives.
		The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.
		The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory;

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Control Activities		
CC5.0	**Criteria**	
		- vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.
		The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.
		The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.
		The company's data backup policy documents requirements for backup and recovery of customer data.
		The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Logical and Physical Access		
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.
		The company restricts privileged access to the application to authorized users with a business need.
		The company restricts privileged access to databases to authorized users with a business need.
		The company requires authentication to production datastores to use authorized secure authentication mechanisms, such as unique SSH key.
		The company restricts privileged access to encryption keys to authorized users with a business need.
		The company restricts privileged access to the firewall to authorized users with a business need.
		The company restricts privileged access to the operating system to authorized users with a business need.
		The company restricts privileged access to the production network to authorized users with a business need.
		The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.
		The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.
		The company restricts access to migrate changes to production to authorized personnel.
		The company has a data classification policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel.
		The company's datastores housing sensitive customer data are encrypted at rest.
		The company's network is segmented to prevent unauthorized access to customer data.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Logical and Physical Access		
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**
		The company requires passwords for in-scope system components to be configured according to the company's policy.
		The company maintains a formal inventory of production system assets.
		The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.
		The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.
		The company requires authentication to systems and applications to use unique username and password or authorized Secure Socket Shell (SSH) keys.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.
		The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.
		The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.
		The company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.
		The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system	The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Logical and Physical Access		
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**
	design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.
		The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.
		The company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.
		The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	**Not Applicable**: For additional information please refer to the subservice organization section above.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.
		The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.
		The company has electronic media containing confidential information purged or destroyed in accordance with best practices, and certificates of destruction are issued for each device destroyed.
		The company purges or removes customer data containing confidential information from the application environment, in accordance with best practices, when customers leave the service.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.
		The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Logical and Physical Access		
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**
		The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.
		The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.
		The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.
		The company reviews its firewall rulesets at least annually. Required changes are tracked to completion.
		The company uses firewalls and configures them to prevent unauthorized access.
		The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.
		The company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.
		The company encrypts portable and removable media devices when used.
		The company has a mobile device management (MDM) system in place to centrally manage mobile devices supporting the service.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.
		The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.
		The company deploys anti-malware technology to environments commonly susceptible to malicious attacks and configures this to be updated routinely, logged, and installed on all relevant systems.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
System Operations		
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.
		The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.
		The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.
		The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.
		The company's formal policies outline the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.
		Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.
		The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.
		The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.
		The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
System Operations		
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**
		The company's formal policies outline the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.
		An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.
		The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.
		The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.
		The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.
		The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.
		The company tests their incident response plan at least annually.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.
		The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
System Operations		
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**
		The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.
		The company tests their incident response plan at least annually.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Change Management		
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.
		The company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.
		The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.
		The company restricts access to migrate changes to production to authorized personnel.
		The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.
		Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Risk Mitigation		
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.
		The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	The company has written agreements in place with vendors and related third-parties. These agreements include confidentiality and privacy commitments applicable to that entity.
		The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.
		Management reviews SOC 2 reports for subservice organizations annually and assesses the impact of deficiencies as it relates to security and/or business risk.

TRUST SERVICES CRITERIA FOR THE AVAILABILITY CATEGORY		
Availability		
A1.0	**Criteria**	**Control Activity Specified by the Service Organization**
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.
		Production environments are monitored for performance, resource utilization and availability using log management and performance monitoring software and alerts are generated when specific, predefined thresholds are met. Processing capacity is expanded on demand to provide continuous availability of the system in accordance with service level commitments.
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.
		The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.
		Management reviews SOC 2 reports for subservice organizations annually and assesses the impact of deficiencies as it relates to security and/or business risk.
		Not Applicable: Part of this criterion is the responsibility of a third-party subservice organization. For additional information on this criterion, please refer to the subservice organizations within the system description, above.
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	The company's data backup policy documents requirements for backup and recovery of customer data.
		The company has Business Continuity and Disaster Recovery Plans in place that outline communication plans in order to maintain information security continuity in the event of the unavailability of key personnel.
		The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.

TRUST SERVICES CRITERIA FOR THE AVAILABILITY CATEGORY		
Availability		
A1.0	**Criteria**	**Control Activity Specified by the Service Organization**
		The company uses a firewall to provide continuous monitoring of the company's network and early detection of potential security breaches.

TRUST SERVICES CRITERIA FOR THE PROCESSING INTEGRITY CATEGORY		
Processing Integrity		
PI1.0	**Criteria**	**Control Activity Specified by the Service Organization**
PI1.1	The entity obtains or generates, uses, and communicates relevant, quality information regarding the objectives related to processing, including definitions of data processed and product and service specifications, to support the use of products and services.	The company's security commitments are communicated to customers in Master Service Agreements (MSA) or Terms of Service (TOS).
		The company provides guidelines and technical support resources relating to system operations to customers.
		The company provides a description of its products and services to internal and external users.
PI1.2	The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity's objectives.	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.
		The company's network is segmented to prevent unauthorized access to customer data.
PI1.3	The entity implements policies and procedures over system processing to result in products, services, and reporting to meet the entity's objectives.	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.
		An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.
		Production environments are monitored for performance, resource utilization and availability using log management and performance monitoring software and alerts are generated when specific, predefined thresholds are met. Processing capacity is expanded on demand to provide continuous availability of the system in accordance with service level commitments.
PI1.4	The entity implements policies and procedures to make available or deliver output completely,	The company's datastores housing sensitive customer data are encrypted at rest.
		The company prohibits confidential or sensitive customer data, by policy, from being used or stored in non-production systems/environments.

TRUST SERVICES CRITERIA FOR THE PROCESSING INTEGRITY CATEGORY		
Processing Integrity		
PI1.0	**Criteria**	**Control Activity Specified by the Service Organization**
	accurately, and timely in accordance with specifications to meet the entity's objectives.	Production environments are monitored for performance, resource utilization and availability using log management and performance monitoring software and alerts are generated when specific, predefined thresholds are met. Processing capacity is expanded on demand to provide continuous availability of the system in accordance with service level commitments.
		An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.
PI1.5	The entity implements policies and procedures to store inputs, items in processing, and outputs completely, accurately, and timely in accordance with system specifications to meet the entity's objectives.	The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.
		The company restricts privileged access to the production network to authorized users with a business need.
		Production environments are monitored for performance, resource utilization and availability using log management and performance monitoring software and alerts are generated when specific, predefined thresholds are met. Processing capacity is expanded on demand to provide continuous availability of the system in accordance with service level commitments.
		The company's data backup policy documents requirements for backup and recovery of customer data.
		The company's datastores housing sensitive customer data are encrypted at rest.

TRUST SERVICES CRITERIA FOR THE CONFIDENTIALITY CATEGORY		
Confidentiality		
C1.0	**Criteria**	**Control Activity Specified by the Service Organization**
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	The company has a data classification policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel.
		The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.
		The company has written agreements in place with vendors and related third-parties. These agreements include confidentiality and privacy commitments applicable to that entity.
		The company requires authentication to systems and applications to use unique username and password or authorized Secure Socket Shell (SSH) keys.
		The company prohibits confidential or sensitive customer data, by policy, from being used or stored in non-production systems/environments.
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	The company has electronic media containing confidential information purged or destroyed in accordance with best practices, and certificates of destruction are issued for each device destroyed.
		The company purges or removes customer data containing confidential information from the application environment, in accordance with best practices, when customers leave the service.

TRUST SERVICES CRITERIA FOR THE PRIVACY CATEGORY Notice and Communication of Objectives Related to Privacy		
P1.0	**Criteria**	**Control Activity Specified by the Service Organization**
P1.1	The entity provides notice to data subjects about its privacy practices to meet the entity's objectives related to privacy. The notice is updated and communicated to data subjects in a timely manner for changes to the entity's privacy practices, including changes in the use of personal information, to meet the entity's objectives related to privacy.	**Not Applicable:** TESCHGlobal is a Data Processor and as such is not required to provide notice to a data subject. For additional information please refer to the Criteria Not Applicable to the System.

TRUST SERVICES CRITERIA FOR THE PRIVACY CATEGORY Choice and Consent		
P1.0	**Criteria**	**Control Activity Specified by the Service Organization**
P2.1	The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice. Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons, if required. Such consent is obtained only for the intended purpose of the information to meet the entity's objectives related to privacy. The entity's basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented.	**Not Applicable:** TESCHGlobal is a Data Processor and as such is not required to provide notice to a data subject. For additional information please refer to the Criteria Not Applicable to the System.

TRUST SERVICES CRITERIA FOR THE PRIVACY CATEGORY		
Collection		
P3.0	**Criteria**	**Control Activity Specified by the Service Organization**
P3.1	Personal information is collected consistent with the entity's objectives related to privacy.	**Not Applicable:** TESCHGlobal is a Data Processor and as such is not required to determine the purposes and means for which personal information is collected. For additional information please refer to the Criteria Not Applicable to the System.
P3.2	For information requiring explicit consent, the entity communicates the need for such consent, as well as the consequences of a failure to provide consent for the request for personal information and obtains the consent prior to the collection of the information to meet the entity's objectives related to privacy.	**Not Applicable:** TESCHGlobal is a Data Processor and as such is not required to determine the purposes and means for which personal information is collected. For additional information please refer to the Criteria Not Applicable to the System.

TRUST SERVICES CRITERIA FOR THE PRIVACY CATEGORY Use, Retention, and Disposal		
P4.0	**Criteria**	**Control Activity Specified by the Service Organization**
P4.1	The entity limits the use of personal information to the purposes identified in the entity's objectives related to privacy.	TESCHGlobal's management and/or legal counsel reviews and approves the methods for the collection of personal information prior to implementation to ensure that information is obtained in a fair and lawful manner.
		TESCHGlobal's management reviews and approves the sources of personal information, other than the individual data subject (third-parties), to ensure that sources are reliable and that the information obtained by the third-parties has been collected in a fair and lawful manner.
		The company reviews policies and procedures as needed or when changes occur and updates them accordingly to ensure that personal information collected is: - identified as either essential or optional; - performed with consent (implicit or explicit) in accordance with legal and regulatory requirements; and - used in alignment with and limited to the purposes identified in the privacy notice.
P4.2	The entity retains personal information consistent with the entity's objectives related to privacy.	TESCHGlobal's retention requirements are documented, and personal information is retained, as required, for business purposes, including to fulfill the purposes related to its collection, and/or by applicable laws or regulations.
		TESCHGlobal's management reviews and approves the sources of personal information, other than the individual data subject (third-parties), to ensure that sources are reliable and that the information obtained by the third-parties has been collected in a fair and lawful manner.
		The company reviews policies and procedures as needed or when changes occur and updates them accordingly to ensure that personal information collected is: - identified as either essential or optional; - performed with consent (implicit or explicit) in accordance with legal and regulatory requirements; and - used in alignment with and limited to the purposes identified in the privacy notice.
P4.3	The entity securely disposes of personal information to meet the entity's objectives related to privacy.	TESCHGlobal's retention requirements are documented, and personal information is retained, as required, for business purposes, including to fulfill the purposes related to its collection, and/or by applicable laws or regulations.

TRUST SERVICES CRITERIA FOR THE PRIVACY CATEGORY		
Use, Retention, and Disposal		
P4.0	**Criteria**	**Control Activity Specified by the Service Organization**
		TESCHGlobal validates deletion requests and once confirmed are flagged and the requested information is deleted, in accordance with applicable laws and regulations.

TRUST SERVICES CRITERIA FOR THE PRIVACY CATEGORY		
Access		
P5.0	**Criteria**	**Control Activity Specified by the Service Organization**
P5.1	The entity grants identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, provides physical or electronic copies of that information to data subjects to meet the entity's objectives related to privacy. If access is denied, data subjects are informed of the denial and reason for such denial, as required, to meet the entity's objectives related to privacy.	The company has established a privacy policy that uses plain and simple language, is clearly dated, and provides information related to the company's practices and purposes for collecting, processing, handling, and disclosing personal information including: - organizational operating jurisdictions; - an individual's choice and consent for the collection, use, and disclosure of personal information; - an individual's right to access, update or remove personal information; - a process for individuals to exercise their rights; - requirements to only provide the essential information needed for the service; - types or categories of information collected; - purposes for the collection of information; - methods of collection (cookies or other tracking techniques, etc.); - consequences for not providing or withdrawing the essential information; - sources of information (third parties, direct collection, etc.); - types or categories of third parties (sources and disclosures); - the purpose for disclosure of information to third parties.
		TESCHGlobal provides requested information, after verification, in a timely manner in either a portable electronic format or by mail, in accordance with applicable law.
P5.2	The entity corrects, amends, or appends personal information based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity's objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and reason for such denial to meet the entity's objectives related to privacy.	**Not Applicable:** TESCHGlobal is a Data Processor and as such is not required to provide the data subject. For additional information please refer to the Criteria Not Applicable to the System.

TRUST SERVICES CRITERIA FOR THE PRIVACY CATEGORY Disclosure and Notification		
P6.0	**Criteria**	**Control Activity Specified by the Service Organization**
P6.1	The entity discloses personal information to third parties with the explicit consent of data subjects, and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy.	**Not Applicable:** TESCHGlobal is a Data Processor and as such is not required to collect explicit consent from the data subject. For additional information please refer to the Criteria Not Applicable to the System.
P6.2	The entity creates and retains a complete, accurate, and timely record of authorized disclosures of personal information to meet the entity's objectives related to privacy.	The company has established a privacy policy that uses plain and simple language, is clearly dated, and provides information related to the company's practices and purposes for collecting, processing, handling, and disclosing personal information including: - organizational operating jurisdictions; - an individual's choice and consent for the collection, use, and disclosure of personal information; - an individual's right to access, update or remove personal information; - a process for individuals to exercise their rights; - requirements to only provide the essential information needed for the service; - types or categories of information collected; - purposes for the collection of information; - methods of collection (cookies or other tracking techniques, etc.); - consequences for not providing or withdrawing the essential information; - sources of information (third parties, direct collection, etc.); - types or categories of third parties (sources and disclosures); - the purpose for disclosure of information to third parties.
		TESCHGlobal has personal information that is disclosed for legal purposes logged, tracked, and maintained in the company's designated tracking system for historical and audit purposes.
P6.3	The entity creates and retains a complete, accurate, and timely record of detected or reported unauthorized disclosures (including breaches) of personal information to meet the entity's objectives related to privacy.	The company has established a privacy policy that uses plain and simple language, is clearly dated, and provides information related to the company's practices and purposes for collecting, processing, handling, and disclosing personal information including: - organizational operating jurisdictions; - an individual's choice and consent for the collection, use, and disclosure of personal information; - an individual's right to access, update or remove personal information; - a process for individuals to exercise their rights; - requirements to only provide the essential information needed for the service;

TRUST SERVICES CRITERIA FOR THE PRIVACY CATEGORY Disclosure and Notification		
P6.0	**Criteria**	**Control Activity Specified by the Service Organization**
		- types or categories of information collected; - purposes for the collection of information; - methods of collection (cookies or other tracking techniques, etc.); - consequences for not providing or withdrawing the essential information; - sources of information (third parties, direct collection, etc.); - types or categories of third parties (sources and disclosures); - the purpose for disclosure of information to third parties.
		TESCHGlobal's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.
P6.4	The entity obtains privacy commitments from vendors and other third parties who have access to personal information to meet the entity's objectives related to privacy. The entity assesses those parties' compliance on a periodic and as-needed basis and takes corrective action, if necessary.	The company has established a privacy policy that uses plain and simple language, is clearly dated, and provides information related to the company's practices and purposes for collecting, processing, handling, and disclosing personal information including: - organizational operating jurisdictions; - an individual's choice and consent for the collection, use, and disclosure of personal information; - an individual's right to access, update or remove personal information; - a process for individuals to exercise their rights; - requirements to only provide the essential information needed for the service; - types or categories of information collected; - purposes for the collection of information; - methods of collection (cookies or other tracking techniques, etc.); - consequences for not providing or withdrawing the essential information; - sources of information (third parties, direct collection, etc.); - types or categories of third parties (sources and disclosures); - the purpose for disclosure of information to third parties.
		The company has written agreements in place with vendors and related third-parties. These agreements include confidentiality and privacy commitments applicable to that entity.
P6.5	The entity obtains commitments from vendors and other third parties with access to personal information to notify the entity in the event of actual or suspected unauthorized disclosures of personal information. Such notifications are reported to	The company has established a privacy policy that uses plain and simple language, is clearly dated, and provides information related to the company's practices and purposes for collecting, processing, handling, and disclosing personal information including: - organizational operating jurisdictions; - an individual's choice and consent for the collection, use, and disclosure of personal information; - an individual's right to access, update or remove personal information; - a process for individuals to exercise their rights;

TRUST SERVICES CRITERIA FOR THE PRIVACY CATEGORY Disclosure and Notification		
P6.0	**Criteria**	**Control Activity Specified by the Service Organization**
	appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's objectives related to privacy.	- requirements to only provide the essential information needed for the service; - types or categories of information collected; - purposes for the collection of information; - methods of collection (cookies or other tracking techniques, etc.); - consequences for not providing or withdrawing the essential information; - sources of information (third parties, direct collection, etc.); - types or categories of third parties (sources and disclosures); - the purpose for disclosure of information to third parties.
		The company has written agreements in place with vendors and related third-parties. These agreements include confidentiality and privacy commitments applicable to that entity.
P6.6	The entity provides notification of breaches and incidents to affected data subjects, regulators, and others to meet the entity's objectives related to privacy.	The company has established a privacy policy that uses plain and simple language, is clearly dated, and provides information related to the company's practices and purposes for collecting, processing, handling, and disclosing personal information including: - organizational operating jurisdictions; - an individual's choice and consent for the collection, use, and disclosure of personal information; - an individual's right to access, update or remove personal information; - a process for individuals to exercise their rights; - requirements to only provide the essential information needed for the service; - types or categories of information collected; - purposes for the collection of information; - methods of collection (cookies or other tracking techniques, etc.); - consequences for not providing or withdrawing the essential information; - sources of information (third parties, direct collection, etc.); - types or categories of third parties (sources and disclosures); - the purpose for disclosure of information to third parties.
		TESCHGlobal's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.
		TESCHGlobal has personal information that is disclosed for legal purposes logged, tracked, and maintained in the company's designated tracking system for historical and audit purposes.
P6.7	The entity provides data subjects with an accounting of the personal information held and disclosure of	The company has established a privacy policy that uses plain and simple language, is clearly dated, and provides information related to the company's practices and purposes for collecting, processing, handling, and disclosing personal information including:

TRUST SERVICES CRITERIA FOR THE PRIVACY CATEGORY Disclosure and Notification		
P6.0	**Criteria**	**Control Activity Specified by the Service Organization**
	the data subjects' personal information, upon the data subjects' request, to meet the entity's objectives related to privacy.	- organizational operating jurisdictions; - an individual's choice and consent for the collection, use, and disclosure of personal information; - an individual's right to access, update or remove personal information; - a process for individuals to exercise their rights; - requirements to only provide the essential information needed for the service; - types or categories of information collected; - purposes for the collection of information; - methods of collection (cookies or other tracking techniques, etc.); - consequences for not providing or withdrawing the essential information; - sources of information (third parties, direct collection, etc.); - types or categories of third parties (sources and disclosures); - the purpose for disclosure of information to third parties.
		TESCHGlobal, prior to granting an individual the ability to access and review personal information, authenticates the individuals or their authorized representative's identity, with an appropriate level of assurance, and verifies such access is not prohibited by law.
		TESCHGlobal provides requested information, after verification, in a timely manner in either a portable electronic format or by mail, in accordance with applicable law.

TRUST SERVICES CRITERIA FOR THE PRIVACY CATEGORY Quality		
P7.0	**Criteria**	**Control Activity Specified by the Service Organization**
P7.1	The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet the entity's objectives related to privacy.	The company has a privacy policy is in place that documents and clearly communicates to individuals the extent of personal information collected, the company's obligations, the individual's rights to access, update, or erase their personal information, and an up-to-date point of contact where individuals can direct their questions, requests or concerns.
		Individuals, customers, or designated account holders can update their personal information to ensure it is accurate and complete through the use of a customer web portal or by contacting the organization using the methods provided in the privacy policy.

TRUST SERVICES CRITERIA FOR THE PRIVACY CATEGORY Monitoring and Enforcement		
P8.0	**Criteria**	**Control Activity Specified by the Service Organization**
P8.1	The entity implements a process for receiving, addressing, resolving, and communicating the resolution of inquiries, complaints, and disputes from data subjects and others and periodically monitors compliance to meet the entity's objectives related to privacy. Corrections and other necessary actions related to identified deficiencies are made or taken in a timely manner.	The company has established a privacy policy that uses plain and simple language, is clearly dated, and provides information related to the company's practices and purposes for collecting, processing, handling, and disclosing personal information including: - organizational operating jurisdictions; - an individual's choice and consent for the collection, use, and disclosure of personal information; - an individual's right to access, update or remove personal information; - a process for individuals to exercise their rights; - requirements to only provide the essential information needed for the service; - types or categories of information collected; - purposes for the collection of information; - methods of collection (cookies or other tracking techniques, etc.); - consequences for not providing or withdrawing the essential information; - sources of information (third parties, direct collection, etc.); - types or categories of third parties (sources and disclosures); - the purpose for disclosure of information to third parties.
		The company has a privacy policy is in place that documents and clearly communicates to individuals the extent of personal information collected, the company's obligations, the individual's rights to access, update, or erase their personal information, and an up-to-date point of contact where individuals can direct their questions, requests or concerns.

SECTION 4

INFORMATION PROVIDED BY THE SERVICE AUDITOR

GUIDANCE REGARDING INFORMATION PROVIDED BY THE SERVICE AUDITOR

Sentry Assurance's examination of the controls of TESCHGlobal was limited to the Trust Services Criteria, related criteria and control activities specified by the management of TESCHGlobal and did not encompass all aspects of TESCHGlobal's operations or operations at user entities. Our examination was performed in accordance with American Institute of Certified Public Accountants (AICPA) AT-C 105 and AT-C 205.

Our examination of the control activities was performed using the following testing methods:

TEST	DESCRIPTION
Inquiry	The service auditor made inquiries from service organization personnel. Inquiries were made to obtain information and representations from the client to determine the client's knowledge of the control and corroborate policy or procedure information.
Observation	The service auditor observed application of the control activities by client personnel.
Inspection	The service auditor inspected among other items, source documents, reports, system configurations to determine performance of the specified control activity and in some instances the timeliness of the performance of control activities.
Re-performance	The service auditor independently executed procedures or controls that were originally performed by the service organization as part of the entity's internal control.

In determining whether the report meets the criteria, the user auditor should perform the following procedures:

- Understand the aspects of the service organization's controls that may affect the service commitments and system requirements based on the applicable trust services criteria.
- Understand the infrastructure, software, procedures, and data that are designed, implemented, and operated by the service organization.
- Determine whether the criteria are relevant to the user entity's assertions.
- Determine whether the service organization's controls are suitably designed to provide reasonable assurance that its service commitments and system were achieved based on the applicable trust services criteria.