Insight Assurance

SOC 2| ISO 27001 | PCI | HIPAA

System and Organization Controls Report (SOC 2® TYPE 1)

Report on Softworks AI LLC D/B/A TRUE's Description of Its TRUE Data Verification System and on the Suitability of Its Controls Relevant to Security as of July 14, 2023

TRUE

TABLE OF CONTENTS

SECTION 1: INDEPENDENT SERVICE AUDITOR'S REPORT

Insight Assurance
SOC 2| ISO 27001 | PCI | HIPAA

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Softworks AI LLC D/B/A TRUE

Scope

We have examined Softworks AI LLC D/B/A TRUE's ('TRUE' or 'the Service Organization') description of its TRUE Data Verification System found in Section 3 titled "Softworks AI LLC D/B/A TRUE's description of its TRUE Data Verification System" as of July 14, 2023 ("description") based on the criteria for a description of a service organization's system outlined 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 14, 2023, to provide reasonable assurance that TRUE's service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) outlined 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.*

TRUE uses Microsoft Azure to provide hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at TRUE, to achieve TRUE's service commitments and system requirements based on the applicable trust services criteria. The description presents TRUE's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of TRUE'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 designs or operating effectiveness of such complementary subservice organization controls.

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

TRUE is responsible for its service commitments and system requirements and designing, implementing, and operating effective controls within the system to provide reasonable assurance that TRUE's service commitments and system requirements were achieved. In Section 2, TRUE has provided the accompanying assertion titled "Softworks AI LLC D/B/A TRUE's Management

Assertion" (assertion) about the description and the suitability of the design of controls stated therein. TRUE 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 the suitability of the design of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and whether the controls stated therein were suitably designed to provide reasonable assurance that the service organization's service commitments and system requirements were 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 meet our other ethical responsibilities in accordance with 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 achieved 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. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, 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,

- the description presents TRUE's TRUE Data Verification System, which was designed and implemented as of July 14, 2023, in accordance with the description criteria.
- the controls stated in the description were suitably designed as of July 14, 2023, to provide reasonable assurance that TRUE's service commitments and system requirements would be achieved based on the applicable trust services criteria if its controls operated effectively throughout that period and if the subservice organization and user entities applied the complementary controls assumed in the design of TRUE's controls throughout that period.

Restricted Use

This report is intended solely for the information and use of TRUE, user entities of TRUE's TRUE Data Verification System as of July 14, 2023, business partners of TRUE subject to risks arising from interactions with the TRUE Data Verification System, 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.
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.
- 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 the specified parties.

Insight Assurance LLC

Tampa, Florida
August 30, 2023

SECTION 2: SOFTWORKS AI LLC D/B/A TRUE'S MANAGEMENT ASSERTION

SOFTWORKS AI LLC D/B/A TRUE'S MANAGEMENT ASSERTION

We have prepared the description of Softworks AI LLC D/B/A TRUE's ('TRUE' or 'the Service Organization') TRUE Data Verification System entitled "Softworks AI LLC D/B/A TRUE's description of its TRUE Data Verification System" as of July 14, 2023 ("description") based on the criteria for a description of a service organization's system outlined 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 TRUE Data Verification System that may be useful when assessing the risks arising from interactions with TRUE's system, particularly information about system controls that TRUE has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) outlined 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*.

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

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

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

- the description presents TRUE's TRUE Data Verification System which was designed and implemented as of July 14, 2023, in accordance with the description criteria.
- the controls stated in the description were suitably designed as of July 14, 2023, to provide reasonable assurance that TRUE's service commitments and system requirements would be achieved based on the applicable trust services criteria, and if the subservice organization and user entities applied the complementary controls assumed in the design of TRUE's controls.

Softworks AI LLC D/B/A TRUE

August 30, 2023

SECTION 3: SOFTWORKS AI LLC D/B/A TRUE'S DESCRIPTION OF ITS TRUE DATA VERIFICATION

SOFTWORKS AI LLC D/B/A TRUE'S DESCRIPTION OF ITS TRUE DATA VERIFICATION SYSTEM

COMPANY BACKGROUND

Softworks AI LLC D/B/A TRUE ('TRUE' or 'the Service Organization') is a software solutions company and AI lab that helps lenders harness the power of artificial intelligence to make accurately informed lending decisions. Since 2017, our technology has set the industry standard for intelligent lending technology, delivering results that provide a TRUE competitive advantage. Every day, lenders across the industry use TRUE to increase their revenue, reduce risk, and deliver a truly exceptional experience to their customers. Learn more at www.TRUE.ai.

DESCRIPTION OF SERVICES OVERVIEW

Specialties - Document Automation, Data Capture, Invoice Processing, Forms Processing, Mortgage Processing, EOB Processing, Lending Intelligence, and Artificial Intelligence

TRUE Data Intelligence

Document Classification - Built with models designed to accurately understand loan information, our lending document classification instantly organizes all incoming documents so your bankers can focus on revenue-generating activity.

Data Extraction - Using the pre-built document library, TRUE extracts over 8,500+ data points required for lending. This automated approach minimizes the need for human validation and reduces costly errors.

Document Versioning Automatically understands the linage of a document while ensuring decisions are being made with the correct document at the correct time.

TRUE Income Analysis (Add-on Solution) TRUE aggregates all financial documents, performs an automated analysis of a borrower's total income and extracts data points to complete required forms.

TRUE Data Verification

Provides a TRUE picture of borrowers by rapidly reviewing every document and every data point — for an incredibly precise assessment of risk. Whether you need to analyze an individual borrower or a large loan pool, TRUE helps you make fast, accurate, and informed lending decisions. Powered by our OCR and Document Classification and Data Extraction Engines, TRUE harnesses the power of machine learning to remove the need for sampling or humans in the loop. Uncover anomalies, inconsistencies, and risks, while drastically reducing audit costs. With TRUE Data Verification System, you can audit and verify loan packages at scale without settling for just sampling.

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

TRUE designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments that TRUE makes to user entities, the laws, and regulations that govern the provision of the services, and the financial, operational, and

compliance requirements that TRUE has established for the services. The system services are subject to the Security commitments established internally for its services.

TRUE's Privacy Policy Last updated June 23, 2022, this privacy policy has been compiled to better serve those who are concerned with how their 'Personally Identifiable Information' (PII) is being used online. PII, as described in US privacy law and information security, is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context. Please read our privacy policy carefully to get a clear understanding of how we collect, use, protect or otherwise handle your Personally Identifiable Information in accordance with our website. What personal information do we collect from the people who visit our blog, website, or app? When ordering or registering on our site, as proper, you may be asked to enter your name, email address, phone number, or other details to help you with your experience. When do we collect information? We collect information from you when you subscribe to a newsletter, fill out a form, or enter information on our site. How do we use your information? We may use the information we collect from you when you register, make a purchase, sign up for our newsletter, respond to a survey or marketing communication, surf the website, or use certain other site features in the following ways: To improve our website to better serve you. To send periodic emails regarding your order or other products and services. To follow up with them after correspondence (live chat, email, or phone inquiries)

Security Commitments

Security commitments include, but are not limited to, the following:

- System features and configuration settings are designed to authorize user access while restricting unauthorized users from accessing information not needed for their role.
- Use of intrusion detection systems to prevent and identify potential security attacks from users outside the boundaries of the system.
- Regular vulnerability scans over the system and network, and penetration tests over the production environment
- Operational procedures for managing security incidents and breaches, including notification procedures.
- Use encryption technologies to protect customer data both at rest and in transit.
- Use of data retention and data disposal
- Uptime availability of production systems

COMPONENTS OF THE SYSTEM USED TO PROVIDE SERVICES

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 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 are mobile applications or desktop or laptop applications.
- 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

TRUE maintains a system inventory that includes virtual machines, computers (desktops and laptops), and networking devices (switches and routers). The inventory documents the device name, inventory type, description, and owner. To outline the topology of its network, the organization maintains the following network diagram(s).

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Azure Platform	Azure	The managed cloud platform where services are hosted
Azure Virtual Machine	Azure	Virtual machine service for web hosting and backend service offerings
Azure Kubernetes	Azure	Container orchestration for deployment, scaling, and management
Azure Database	Azure	Transactional database with backups and redundancy

SOFTWARE

TRUE is responsible for managing the development and operation of the TRUE Data Verification System including infrastructure components such as servers, databases, and storage systems. The in-scope TRUE infrastructure and software components are shown in the table provided below:

Primary Software		
System/Application	**Operating System**	**Purpose**
Azure SDK	N/A	The SDK is used to communicate with Microsoft Azure web services
Bitbucket	N/A	Web-based version control platform designed source code management and collaboration.
Checkr	N/A	Facilitates efficient and reliable verification of qualifications, streamlining background checks and verification processes
Confluence	N/A	Wiki-style platform to create, share, and collaborate on documents, project plans, and other content.
Jira	N/A	Project management and issue tracking tool for planning, tracking, and managing tasks and projects
KnowBe4	N/A	Cloud Platform for security awareness training combined with simulated phishing attacks.
Microsoft Azure	N/A	Cloud computing platform to build, deploy, and manage applications and services, including virtual machines, databases, analytics, and user management

Microsoft Endpoint Manager	N/A	Unified platform for managing and securing endpoint devices within an organization.
Office 365	N/A	Suite of cloud-based productivity tools and services, including applications like Word, Excel, PowerPoint, and Outlook
Vanta	N/A	Platform designed to simplify and automate the process of achieving and maintaining security compliance certifications.

PEOPLE

The company employs dedicated team members to handle major product functions, including operations, and support. The IT/Engineering Team monitors the environment, as well as manages data backups and recovery. The Company focuses on hiring the right people for the right job as well as training them both in their specific tasks and on the ways to keep the company and its data secure.

TRUE has a staff organized in the following functional areas:

Management: Individuals who are responsible for enabling other employees to perform their jobs effectively and for maintaining security and compliance across the environment. This includes:

CEO - Handles the strategic direction of the organization. The CEO assigns authority and responsibility to key management personnel with the skills and experience necessary to carry out their assignments.

CFO - Responsible for overseeing financial operations, budgeting, and financial reporting

CTO - Responsible for the technological direction and advancements of the organization. Directs the operations, engineering, and support teams to efficiently create/present new services, maintain existing ones, and help support the TRUE customer base using the service

CRO - Accountable for driving better integration and alignment between all revenue-related functions, including marketing, sales, customer support, pricing, and revenue management.

Operations: Responsible for maintaining the availability of production infrastructure and managing access and security for production infrastructure. Only members of the Operations team have access to the production environment. Members of the Operations team may also be members of the Engineering team.

Information Technology: Responsible for managing laptops, software, and other technology involved in employee productivity and business operations.

Product Development: Responsible for the development, testing, deployment, and maintenance of the source code for the system. Responsible for the product life cycle, including adding additional product functionality.

DATA

Data as defined by TRUE, constitutes the following:

User and account data - this includes Personally Identifiable Information (PII) and other data from employees, customers, users (customers' employees), and other third parties such as suppliers, vendors, business partners, and contractors. This collection is permitted under the Terms of Service and Privacy Policy (as well as other separate agreements with vendors, partners, suppliers, and other relevant third parties). Access to PII is controlled through processes for provisioning system permissions, as well as ongoing monitoring activities, to ensure that sensitive data is restricted to employees based on job function.

Data is categorized into the following major types of data used by TRUE.

DATA		
Category	**Description**	**Examples**
Public	Public information is not confidential and can be made public without any implications for TRUE.	● Press releases ● Public website
Internal	Access to internal information is approved by management and is protected from external access.	● Internal memos ● Design documents ● Product specifications ● Correspondences
Customer data	Information received from customers for processing or storage by TRUE. TRUE must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information.	● Customer operating data ● Customer PII ● Customers' customers' PII ● Anything subject to a confidentiality agreement with a customer
Company data	Information collected and used by TRUE to operate the business. TRUE must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information.	● Legal documents ● Contractual agreements ● Employee PII ● Employee salaries

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer agreements, if any. Customer data is captured which is utilized by the company in delivering its services.

All employees and contractors of the company are obligated to respect and, in all cases, protect customer data. Additionally, TRUE has policies and procedures in place for proper and secure handling of customer data. These policies and procedures are reviewed on at least an annual basis.

PROCEDURES

Management has developed and communicated policies and procedures to manage the information security of the system. Changes to these procedures are performed annually and

authorized by management, the executive team, and control owners. These procedures cover the following key security life cycle areas:

- Physical Security
- Logical Access
- Availability
- Change Control
- Data Communications
- Risk Assessment
- Data Retention
- Vendor Management

Physical Security

TRUE's production servers are maintained by Microsoft Azure. The physical and environmental security protections are the responsibility of Microsoft Azure. TRUE reviews the attestation reports and performs a risk analysis of Microsoft Azure on at least an annual basis.

Logical Access

TRUE provides employees and contracts access to infrastructure via a role-based access control system, to ensure uniform, least privileged access to identified users and to maintain simple and reportable user provisioning and de-provisioning processes.

Access to these systems is split into admin roles, user roles, and no-access roles. User access and roles are reviewed on an annual basis to ensure the least privileged access.

IT Team with HR ad Flexible Systems is responsible for provision access to the system based on the employee's role and performing a background check. The employee is responsible for reviewing TRUE's policies and completing security training. These steps must be completed within 14 days of hire.

When an employee is terminated, IT Team with HR and Flexible Systems is responsible for de-provisioning access to all in-scope systems within 3 days of that employee's termination.

Change Management

TRUE maintains documented Systems Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

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 before 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.

Computer Operations - Backups

Customer data is backed up and monitored by the Flexible Systems monitors backup and reports are sent to TRUE Technical Team. for completion and exceptions. If there is an exception, Flexible Systems monitors backup and reports are sent to TRUE Technical Team. will perform troubleshooting to identify the root cause and either rerun the backup or as part of the next scheduled backup job.

Backup infrastructure is maintained in Microsoft Azure with physical access restricted according to the policies. Backups are encrypted, with access restricted to key personnel.

Computer Operations - Availability

TRUE maintains an incident response plan to guide employees on reporting and responding to any information security or data privacy events or incidents. Procedures are in place for identifying, reporting, and acting upon breaches or other incidents.

TRUE internally monitors all applications, including the web UI, databases, and cloud storage to ensure that service delivery matches SLA requirements.

TRUE utilizes vulnerability scanning software that checks source code for common security issues as well as for vulnerabilities identified in open-source dependencies and maintains an internal SLA for responding to those issues.

Data Communications

TRUE has elected to use a platform-as-a-service (PaaS) to run its production infrastructure in part to avoid the complexity of network monitoring, configuration, and operations. The PaaS simplifies our logical network configuration by providing an effective firewall around all the TRUE application containers, with the only ingress from the network via HTTPS connections to designated web frontend endpoints.

The PaaS provider also automates the provisioning and de-provisioning of containers to match the desired configuration; if an application container fails, it will be automatically replaced, regardless of whether that failure is in the application or on the underlying hardware.

True runs Vonahi Security Penetration Tests to perform a comprehensive security assessment to assist with evaluating the cyber risks presented within the tested environment(s). We run monthly Internal and External Pen Tests. The objective of this engagement is to determine if any identified threats could be used to mount an attack against the organization that could lead to the disclosure of sensitive information or access to critical information systems.

Vendor Management

The organization maintains a Vendor Management Policy that includes requirements for interacting with vendors/service providers. The policy includes requirements for performing due diligence measures before engaging with a new provider. Due diligence procedures include evaluating each material IT vendor’s cost-effectiveness, functionality/services, risk, financial viability, compliance, and performance. The organization is required to define service levels when

negotiating an arrangement with a new vendor or re-negotiating an existing arrangement, and all service levels are agreed upon and documented clearly. The organization monitors its providers' service levels to ensure each provider is providing the agreed-upon services and is compliant with all requirements. The organization executes non-disclosure agreements with third parties before any information is shared.

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

The security categories and applicable trust services criteria were used to evaluate the suitability of the design of controls stated in the description. Security criteria and the controls designed, implemented, and operated to meet them ensure that the system is protected against unauthorized access (both physical and logical). The controls supporting the applicable trust services security criteria are included in Section 4 of this report. Although the applicable trust services criteria and related controls are included in Section 4, they are an integral part of the TRUE description of its system.

CONTROL ENVIRONMENT

The control environment is the set of standards, processes, and structures that provide the basis for carrying out internal control across an organization. The organizational structure, separation of job responsibilities by departments and business function, documentation of policies and procedures, and internal audits are the methods used to define, implement, and assure effective operational controls. The Board of Directors and/or senior management establish the tone at the top regarding the importance of internal control and expected standards of conduct.

Boundaries of the System

The boundaries of the TRUE Data Verification System are the specific aspects of the Company's infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of the TRUE Data Verification System.

This report does not include the Cloud Hosting Services provided by Azure at multiple facilities.

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of TRUE's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of TRUE's ethical and behavioral standards, how they are communicated, and how they are reinforced in practice. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

Specific control activities that the service organization has implemented in this area are described below:

- Formally, documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel.

- Policies and procedures require employees to sign an acknowledgment form indicating they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual.
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties is a component of the employee handbook.
- Background checks are performed for employees as a component of the hiring process.

Management's Philosophy and Operating Style

The TRUE management team must balance two competing interests: continuing to grow and develop in a cutting-edge, rapidly changing technology space while remaining excellent and conservative stewards of the highly sensitive data and workflows our customers entrust to us.

The management team meets frequently to be briefed on technology changes that impact the way TRUE can help customers build data workflows, as well as new security technologies that can help protect those workflows, and finally, any regulatory changes that may require TRUE to alter its software to maintain legal compliance. Major planned changes to the business are also reviewed by the management team to ensure they can be conducted in a way that is compatible with our core product offerings and duties to new and existing customers.

Specific control activities that the service organization has implemented in this area are described below:

- Management is periodically briefed on regulatory and industry changes affecting the services provided.
- Executive management meetings are held to discuss major initiatives and issues that affect the business.

Commitment To Competence

TRUE's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for jobs and how those levels translate into the requisite skills and knowledge.

Specific control activities that the service organization has implemented in this area are described below:

- Management has considered the competence levels for jobs and translated required skills and knowledge levels into written position requirements.
- Training is provided to maintain the skill level of personnel in certain positions.

Human Resources Policies and Practices

TRUE'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 service organization is operating at maximum efficiency. TRUE's human resources policies and practices relating to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

Specific control activities that the service organization has implemented in this area are described below:

- New employees are required to sign acknowledgment forms for the employee handbook and a confidentiality agreement following new hire orientation on their first day of employment.
- Evaluations for each employee are performed on an annual basis.
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist.

RISK ASSESSMENT PROCESS

TRUE's risk assessment process identifies and manages risks that could potentially affect TRUE's ability to provide reliable and secure services to our customers. As part of this process, TRUE maintains a risk register to track all systems and procedures that could present risks to meeting the company's objectives. Risks are evaluated by likelihood and impact, and management creates tasks to address risks that score highly on both dimensions. The risk register is reevaluated annually, and tasks are incorporated into the regular TRUE product development process so they can be dealt with predictably and iteratively.

INTEGRATION WITH RISK ASSESSMENT

The environment in which the system operates; the commitments, agreements, and responsibilities of TRUE's system; as well as the nature of the components of the system result in risks that the criteria will not be met. TRUE 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 meet the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, TRUE's management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

INFORMATION AND COMMUNICATION SYSTEMS

Information and communication are an integral component of TRUE's internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations.

TRUE uses several information and communication channels internally to share information with management, employees, contractors, and customers. TRUE uses chat systems and email as the primary internal and external communications channels.

Structured data is communicated internally via SaaS applications and project management tools. Finally, TRUE uses in-person and video "all hands" meetings to communicate company priorities and goals from management to all employees.

MONITORING CONTROLS

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. TRUE's management performs monitoring activities to continuously 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

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

Management's close involvement in TRUE's operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control's weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. The goal of this process is to ensure legal compliance and maximize the performance of TRUE's personnel.

Reporting Deficiencies

Our internal risk management tracking tool is utilized to document and track the results of ongoing monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks, and instructions for escalation are supplied to employees in company policy documents. 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.

TRUST SERVICES CATEGORIES

The security categories and applicable trust services criteria were used to evaluate the suitability of the design of controls stated in the description. Criteria and controls designed, implemented, and operated to meet them ensure that information, systems, and access (physical and logical) are protected against unauthorized access, and systems are available for operation and use.

CONTROL ACTIVITIES AND CRITERIA

The Company's trust services criteria and related control activities are included in Section 4 of this report to eliminate the redundancies that would result from listing them here in Section 3 and repeating them in Section 4. Although the trust services criteria and related control activities are included in Section 4, they are, nevertheless, an integral part of TRUE's description of controls.

For specific criterion, which was deemed not relevant to the system, see Section 4 for the related explanation.

CHANGES TO THE SYSTEM AFTER THE REVIEW DATE

No significant changes have occurred to the services provided since the review date.

SYSTEM INCIDENTS AFTER THE REVIEW DATE

No significant incidents have occurred to the service provided since the review date.

COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS (CSOCs)

TRUE's controls related to the System cover only a portion of overall internal control for each user entity of TRUE. It is not feasible for the trust services criteria related to the System to be achieved solely by TRUE. Therefore, each user entity's internal controls should be evaluated in conjunction with TRUE's controls and the related tests and results described in Section 4 of this report, considering the related complementary subservice organization controls expected to be implemented at the subservice organization as described below.

	Complementary Subservice Organization Controls (CSOC)	Related Criteria
1	Microsoft Azure is responsible for maintaining physical security and environmental protection controls over the data centers hosting the TRUE infrastructure.	CC6.4
2	Microsoft Azure is responsible for the destruction of physical assets hosting the production environment.	CC6.5

COMPLEMENTARY USER ENTITY CONTROLS (CUECs)

TRUE's controls related to TRUE Data Verification System only cover a portion of the overall internal controls for each user entity. It is not feasible for the applicable trust service criteria related to the system to be achieved solely by TRUE control procedures. Accordingly, user entities, in conjunction with the services, should establish their internal controls or procedures to complement those of TRUE.

User auditors should determine whether the following controls have been in place in operation at the user organization:

- Controls to provide reasonable assurance that user access including the provisioning and de-provisioning are designed appropriately and operating effectively.
- User entities are responsible for reporting issues with TRUE systems and platforms.
- User entities are responsible for understanding and complying with their contractual obligations to TRUE.
- User entities are responsible for notifying TRUE of changes made to the administrative contact information.

SECTION 4: TRUST SERVICES CATEGORY, CRITERIA, AND RELATED CONTROLS

Trust Services Category, Criteria and Related Controls

This SOC 2 Type 1 report was prepared in accordance with the AICPA attestation standards and has been performed to examine the suitability of the design of controls to meet the criteria for the Security category 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* as of July 14, 2023.

The trust services category for the Security criteria and related controls specified by TRUE are presented in Section 4 of this report.

CONTROL ACTIVITIES SPECIFIED BY THE SERVICE ORGANIZATION

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CONTROL ENVIRONMENT		
Control Number	**Controls**	**Test Results**
Criteria: COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.		
CC1.1.1	The company has an approved Code of Conduct that is reviewed annually and updated as needed.	No exceptions noted.
CC1.1.2	The company requires employees to acknowledge the Code of Conduct at the time of hire and active employees to acknowledge the Code of Conduct at least annually.	No exceptions noted.
CC1.1.3	The company requires employees to review and acknowledge the information security policies at the time of hire.	No exceptions noted.
CC1.1.4	The company performs background checks on new employees.	No exceptions noted.
CC1.1.5	The company requires employees and contractors to sign a confidentiality agreement during onboarding.	No exceptions noted.
CC1.1.6	The company managers are required to complete performance evaluations for direct reports at least annually.	No exceptions noted.
Criteria: COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.		
CC1.2.1	The company's board members have sufficient expertise to oversee management's ability to design, implement and operate information security controls.	No exceptions noted.
CC1.2.2	The company's board of directors meets at least annually and maintains formal meeting minutes.	No exceptions noted.
CC1.2.3	The company has an Information Security Roles and Responsibilities Policy that outlines the board of directors' responsibilities for oversight of internal controls.	No exceptions noted.
CC1.2.4	The company's board of directors consists of members that are independent from the company.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CONTROL ENVIRONMENT		
Control Number	**Controls**	**Test Results**
Criteria: COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.		
CC1.3.1	The company has an Information Security Roles and Responsibilities policy that outlines the board of directors' responsibilities for oversight of internal controls.	No exceptions noted.
CC1.3.2	The company maintains an organizational chart that describes the organizational structure and reporting lines.	No exceptions noted.
CC1.3.3	The company requires employees to review and acknowledge the information security policies at the time of hire.	No exceptions noted.
CC1.3.4	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the Information Security Roles and Responsibilities Policy.	No exceptions noted.
Criteria: COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.		
CC1.4.1	The company performs background checks on new employees.	No exceptions noted.
CC1.4.2	The company managers are required to complete performance evaluations for direct reports at least annually.	No exceptions noted.
CC1.4.3	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the Information Security Roles and Responsibilities Policy.	No exceptions noted.
CC1.4.4	The company requires new employees and contractors to complete security awareness training at the time of hire and active employees to complete security training at least annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CONTROL ENVIRONMENT		
Control Number	**Controls**	**Test Results**
Criteria: COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.		
CC1.5.1	The company managers are required to complete performance evaluations for direct reports at least annually.	No exceptions noted.
CC1.5.2	The company requires employees to acknowledge the Code of Conduct at the time of hire and active employees to acknowledge the Code of Conduct at least annually.	No exceptions noted.
CC1.5.3	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the Information Security Roles and Responsibilities Policy.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
INFORMATION AND COMMUNICATION		
Control Number	**Controls**	**Test Results**
Criteria: COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.		
CC2.1.1	The company's information security policies and procedures are documented and reviewed at least annually.	No exceptions noted.
CC2.1.2	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.	No exceptions noted.
CC2.1.3	The company requires the use of a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.	No exceptions noted.
CC2.1.4	The company's penetration testing is required to be performed annually. A remediation plan is developed, and changes are implemented to remediate vulnerabilities in accordance with SLAs.	No exceptions noted.
CC2.1.5	Vulnerability scans are performed on a quarterly basis on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	No exceptions noted.
Criteria: COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.		
CC2.2.1	The company has security incident response policies and procedures that are documented and communicated to authorized users.	No exceptions noted.
CC2.2.2	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the Information Security Roles and Responsibilities Policy.	No exceptions noted.
CC2.2.3	The company requires new employees and contractors to complete security awareness training at the time of hire and active employees to complete security training at least annually.	No exceptions noted.
CC2.2.4	The company's information security policies and procedures are documented and reviewed at least annually.	No exceptions noted.
CC2.2.5	The company provides a description of its products and services to internal and external users.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
INFORMATION AND COMMUNICATION		
Control Number	**Controls**	**Test Results**
CC2.2.6	The company communicates system changes to authorized internal users.	No exceptions noted.
Criteria: COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.		
CC2.3.1	The company's security commitments are communicated to customers in the Terms of Service (TOS).	No exceptions noted.
CC2.3.2	The company provides a description of its products and services to internal and external users.	No exceptions noted.
CC2.3.2	The company provides a description of its products and services to internal and external users.	No exceptions noted.
CC2.3.3	The company notifies customers of critical system changes that may affect their processing.	No exceptions noted.
CC2.3.4	Contact information for users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel is available.	No exceptions noted.
CC2.3.5	The company has written agreements in place with vendors and related third parties. These agreements include confidentiality commitments applicable to that entity.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
RISK ASSESSMENT		
Control Number	**Controls**	**Test Results**
Criteria: COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.		
CC3.1.1	The company specifies its objectives to enable the identification and assessment of risk related to the objectives.	No exceptions noted.
CC3.1.2	The company has a documented risk management program 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.	No exceptions noted.
CC3.1.3	The company's risk assessments are performed regularly. 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.	No exceptions noted.
Criteria: 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.		
CC3.2.1	The company has a documented risk management program 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.	No exceptions noted.
CC3.2.2	The company has a third-party management program in place. Components of this program include: - vendor's security and privacy requirements; and - annual review of critical third-party vendors	No exceptions noted.
CC3.2.3	The company's risk assessments are performed regularly. 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.	No exceptions noted.
CC3.2.4	The company has a documented business continuity/disaster recovery (BC/DR) plan and requires that it be tested at least annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
RISK ASSESSMENT		
Control Number	**Controls**	**Test Results**
Criteria: COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.		
CC3.3.1	The company's risk assessments are performed regularly. 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	No exceptions noted.
CC3.3.2	The company has a documented risk management program 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.	No exceptions noted.
Criteria: COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.		
CC3.4.1	The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.	No exceptions noted.
CC3.4.2	The company's penetration testing is performed annually. A remediation plan is developed, and changes are implemented to remediate vulnerabilities in accordance with SLAs.	No exceptions noted.
CC3.4.3	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.	No exceptions noted.
CC3.4.4	The company has a documented risk management program 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.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
MONITORING ACTIVITIES		
Control Number	**Controls**	**Test Results**
Criteria: 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.		
CC4.1.1	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.	No exceptions noted.
CC4.1.2	The company's penetration testing is performed annually. A remediation plan is developed, and changes are implemented to remediate vulnerabilities in accordance with SLAs.	No exceptions noted.
CC4.1.3	The company has a third-party management program in place. Components of this program include: - vendor's security and privacy requirements; and - annual review of critical third-party vendors	No exceptions noted.
CC4.1.4	Vulnerability scans are performed on a quarterly basis on external-facing systems. Critical and high vulnerabilities are tracked to remediation.	No exceptions noted.
Criteria: 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.		
CC4.2.1	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.	No exceptions noted.
CC4.2.2	The company has a third-party management program in place. Components of this program include: - vendor's security and privacy requirements; and - annual review of critical third-party vendors	No exceptions noted.
CC4.2.3	The company's penetration testing is performed annually. A remediation plan is developed, and changes are implemented to remediate vulnerabilities in accordance with SLAs.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CONTROL ACTIVITIES		
Control Number	**Controls**	**Test Results**
Criteria: 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.		
CC5.1.1	The company has a documented risk management program 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.	No exceptions noted.
CC5.1.2	The company's information security policies and procedures are documented and reviewed at least annually.	No exceptions noted.
CC5.1.3	The company's risk assessments are performed regularly. 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	No exceptions noted.
CC5.1.4	Role-based access is configured within Azure and other supporting applications to enforce segregation of duties and restrict access to confidential information.	No exceptions noted.
Criteria: COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.		
CC5.2.1	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.	No exceptions noted.
CC5.2.2	The company has an Operations Security Policy and a Secure Development Policy in place that govern the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	No exceptions noted.
CC5.2.3	The company's information security policies and procedures are documented and reviewed at least annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CONTROL ACTIVITIES		
Control Number	**Controls**	**Test Results**
Criteria: COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.		
CC5.3.1	The company's information security policies and procedures are documented and reviewed at least annually.	No exceptions noted.
CC5.3.2	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.	No exceptions noted.
CC5.3.3	The company has an Operations Security Policy and a Secure Development Policy in place that govern the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	No exceptions noted.
CC5.3.4	The company has security incident response policies and procedures that are documented and communicated to authorized users.	No exceptions noted.
CC5.3.5	The company specifies its objectives to enable the identification and assessment of risk related to the objectives.	No exceptions noted.
CC5.3.6	The company has a documented risk management program 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.	No exceptions noted.
CC5.3.7	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the Information Security Roles and Responsibilities Policy.	No exceptions noted.
CC5.3.8	The company has a third-party management program in place. Components of this program include: - vendor's security and privacy requirements; and - annual review of critical third-party vendors	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CONTROL ACTIVITIES		
Control Number	**Controls**	**Test Results**
CC5.3.9	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.	No exceptions noted.
CC5.3.10	The company's Operations Security Policy documents requirements for backup and recovery of customer data.	No exceptions noted.
CC5.3.11	The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
LOGICAL AND PHYSICAL ACCESS CONTROLS		
Control Number	**Controls**	**Test Results**
Criteria: 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.		
CC6.1.1	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.	No exceptions noted.
CC6.1.2	The company has a Data Management Policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel.	No exceptions noted.
CC6.1.3	The company's databases housing sensitive customer data are encrypted at rest.	No exceptions noted.
CC6.1.4	The company restricts privileged access to encryption keys to authorized users with a business need.	No exceptions noted.
CC6.1.5	Role-based access is configured within Azure and other supporting applications to enforce segregation of duties and restrict access to confidential information.	No exceptions noted.
CC6.1.6	The company restricts privileged access to the application, databases, and supporting cloud infrastructure to authorized users with a business need.	No exceptions noted.
CC6.1.7	Firewalls are required to be configured in order to prevent unauthorized access.	No exceptions noted.
CC6.1.8	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.	No exceptions noted.
CC6.1.9	The company requires passwords for in-scope system components to be configured according to the company's policy.	No exceptions noted.
CC6.1.10	The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
LOGICAL AND PHYSICAL ACCESS CONTROLS		
Control Number	**Controls**	**Test Results**
CC6.1.11	The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	No exceptions noted.
CC6.1.12	The company maintains a formal inventory of production system assets.	No exceptions noted.
Criteria: 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.		
CC6.2.1	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.	No exceptions noted.
CC6.2.2	The company requires that access reviews be conducted quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	No exceptions noted.
CC6.2.3	Logical access to systems is revoked as a component of the termination process within the company’s SLAs.	No exceptions noted.
CC6.2.4	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.	No exceptions noted.
CC6.2.5	The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
LOGICAL AND PHYSICAL ACCESS CONTROLS		
Control Number	**Controls**	**Test Results**
Criteria: 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 design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.		
CC6.3.1	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.	No exceptions noted.
CC6.3.2	The company conducts quarterly access reviews for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	No exceptions noted.
CC6.3.3	Logical access to systems is revoked as a component of the termination process within the company's SLAs.	No exceptions noted.
CC6.3.4	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.	No exceptions noted.
CC6.3.5	The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	No exceptions noted.
Criteria: CC6.4: The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.		
CC6.4.1	Management contracts with Microsoft Azure to provide physical and logical access security of its production systems; therefore, this criterion is carved out.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
LOGICAL AND PHYSICAL ACCESS CONTROLS		
Control Number	**Controls**	**Test Results**
Criteria: 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.		
CC6.5.1	The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.	No exceptions noted.
CC6.5.2	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.	No exceptions noted.
CC6.5.3	Logical access to systems is revoked as a component of the termination process within the company's SLAs.	No exceptions noted.
CC6.5.4	The destruction of physical assets hosting the production environment is the responsibility of the subservice organization. Refer to the subservice organization's section above for controls managed by the subservice organization.	No exceptions noted.
Criteria: CC6.6: The entity implements logical access security measures to protect against threats from sources outside its system boundaries.		
CC6.6.1	The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	No exceptions noted.
CC6.6.2	The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.	No exceptions noted.
CC6.6.3	Firewalls are required to be configured to prevent unauthorized access.	No exceptions noted.
CC6.6.4	The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	No exceptions noted.
Criteria: 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.		
CC6.7.1	The company encrypts workstations to protect sensitive data.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
LOGICAL AND PHYSICAL ACCESS CONTROLS		
Control Number	**Controls**	**Test Results**
CC6.7.2	The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	No exceptions noted.
CC6.7.3	The company has a mobile device monitoring system (MDM) in place to centrally monitor mobile devices supporting the service.	No exceptions noted.
Criteria: 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.		
CC6.8.1	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.	No exceptions noted.
CC6.8.2	The company has an Operations Security Policy and a Secure Development Policy in place that govern the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
SYSTEM OPERATIONS		
Control Number	**Controls**	**Test Results**
Criteria: 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.		
CC7.1.1	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.	No exceptions noted.
CC7.1.2	The company's risk assessments are performed regularly. 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.	No exceptions noted.
CC7.1.3	The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.	No exceptions noted.
CC7.1.4	The company's formal policies outline the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.	No exceptions noted.
Criteria: 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.		
CC7.2.1	The company requires the use of a compliance tool to provide continuous monitoring of the company's network and early detection of potential security breaches.	No exceptions noted.
CC7.2.2	The company requires the use of a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.	No exceptions noted.
CC7.2.3	The company's formal policies outline the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
SYSTEM OPERATIONS		
Control Number	**Controls**	**Test Results**
CC7.2.4	An infrastructure monitoring tool is to be utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.	No exceptions noted.
CC7.2.5	The company's penetration testing is performed annually. A remediation plan is developed, and changes are implemented to remediate vulnerabilities in accordance with SLAs.	No exceptions noted.
CC7.2.6	Security incidents are reported to the IT personnel and tracked through to resolution in a ticketing system.	No exceptions noted.
CC7.2.7	Vulnerability scans are performed on a quarterly basis on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	No exceptions noted.
Criteria: 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.		
CC7.3.1	The company has security incident response policies and procedures that are documented and communicated to authorized users.	No exceptions noted.
CC7.3.2	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.	No exceptions noted.
Criteria: 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.		
CC7.4.1	The company has security incident response policies and procedures that are documented and communicated to authorized users.	No exceptions noted.
CC7.4.2	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.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
SYSTEM OPERATIONS		
Control Number	**Controls**	**Test Results**
CC7.4.3	The company requires that infrastructure supporting the service be patched or updated 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	No exceptions noted.
CC7.4.4	Vulnerability scans are performed on a quarterly basis on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	No exceptions noted.
CC7.4.5	The company tests their incident response plan at least annually.	No exceptions noted.
Criteria: CC7.5: The entity identifies, develops, and implements activities to recover from identified security incidents.		
CC7.5.1	The company has security incident response policies and procedures that are documented and communicated to authorized users.	No exceptions noted.
CC7.5.2	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.	No exceptions noted.
CC7.5.3	The company has a documented business continuity/disaster recovery (BC/DR) plan and requires that it be tested at least annually/tests it annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CHANGE MANAGEMENT		
Control Number	**Controls**	**Test Results**
Criteria: 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.		
CC8.1.1	The company has an Operations Security Policy and a Secure Development Policy in place that govern the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	No exceptions noted.
CC8.1.2	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.	No exceptions noted.
CC8.1.3	The company restricts access to migrate changes to production to authorized personnel.	No exceptions noted.
CC8.1.4	The company's penetration testing is performed annually. A remediation plan is developed, and changes are implemented to remediate vulnerabilities in accordance with SLAs.	No exceptions noted.
CC8.1.5	Vulnerability scans are performed on a quarterly basis on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	No exceptions noted.
CC8.1.6	The company's risk assessments are performed regularly. 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	No exceptions noted.
CC8.1.7	Vulnerability scans are performed on a quarterly basis on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	No exceptions noted.
CC8.1.8	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.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
RISK MITIGATION		
Control Number	**Controls**	**Test Results**
Criteria: CC9.1: The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.		
CC9.1.1	The company's risk assessments are required to be 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.	No exceptions noted.
CC9.1.2	The company has a documented risk management program 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.	No exceptions noted.
Criteria: CC9.2: The entity assesses and manages risks associated with vendors and business partners		
CC9.2.1	The company has written agreements in place with vendors and related third parties. These agreements include confidentiality commitments applicable to that entity.	No exceptions noted.
CC9.2.2	The company has a third-party management program in place. Components of this program include: - vendor's security and privacy requirements; and - annual review of critical third-party vendors.	No exceptions noted.