JOHANSON GROUP

System and Organization Controls (SOC) 2 Type I Report

And the Suitability of Design of Controls Relevant to the Trust Services Criteria for Security, Availability, and Confidentiality Categories

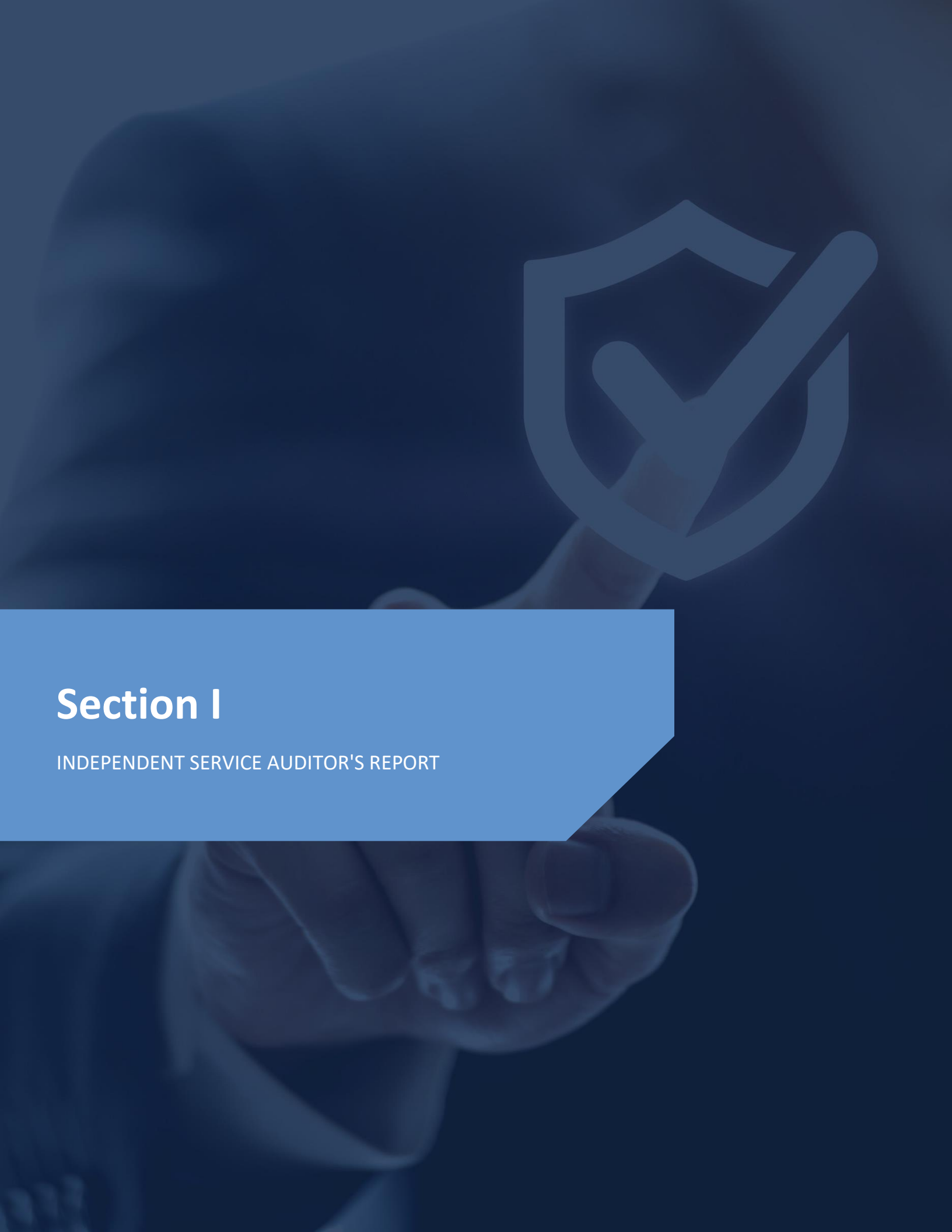
As of July 26, 2024

Together with Independent Service Auditor's Report

Report on Management's Description of

TRACE MACHINA

TABLE OF CONTENTS



Section I

INDEPENDENT SERVICE AUDITOR'S REPORT

Trace Machina, Inc.

Scope

We have examined Trace Machina, Inc.'s accompanying description of its Trace Services (system) titled "Description of Trace Services" as of July 26, 2024 (description) based on the criteria for a description of a service organization's system in the DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (AICPA, Description Criteria)*, (description criteria) and the suitability of the design of controls stated in the description as of July 26, 2024, to provide reasonable assurance that Trace Machina, Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*.

Service Organization's Responsibilities

Trace Machina, Inc. is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Trace Machina, Inc.'s service commitments and system requirements were achieved. Trace Machina, Inc. has provided the accompanying assertion titled "Assertion of Trace Machina, Inc.'s Management" (assertion) about the description and the suitability of the design of controls stated therein. Trace Machina, Inc. 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 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 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.

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

- 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.

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

Inherent Limitations

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 Trace Machina, Inc.'s Trace Services (system) that was designed and implemented as of July 26, 2024, in accordance with the description criteria.
b. The controls stated in the description were suitably designed as of July 26, 2024, to provide reasonable assurance that Trace Machina, Inc.'s service commitments and system requirements would be achieved based on the applicable trust services criteria if its controls operated effectively as of that date.

Restricted Use

This report is intended solely for the information and use of Trace Machina, Inc., user entities of Trace Machina, Inc.'s Trace Services (system) as of July 26, 2024, business partners of Trace Machina, Inc. subject to risks arising from interactions with the Trace Services (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, subservice organizations, 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.

JohansonGroup LLP
Colorado Springs, Colorado
August 12, 2024

Section II

ASSERTION OF TRACE MACHINA, INC. MANAGEMENT

We have prepared the accompanying description of Trace Machina, Inc.'s Trace Services (system) titled "Description of Trace Services as of July 26, 2024" (description) based on the criteria for a description of a service organization's system in the DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (AICPA, Description Criteria)*, (description criteria). The description is intended to provide report users with information about the Trace Services (system) that may be useful when assessing the risks arising from interactions with Trace Machina, Inc.'s system, particularly information about system controls that Trace Machina, Inc. 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, availability, and confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*.

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

a. The description presents Trace Machina, Inc.'s Trace Services (system) that was designed and implemented as of July 26, 2024, in accordance with the description criteria.
b. The controls stated in the description were suitably designed as of July 26, 2024, to provide reasonable assurance that Trace Machina, Inc.'s service commitments and system requirements would be achieved based on the applicable trust services criteria if its controls operated effectively as of that date.

Trace Machina, Inc. Management
August 12, 2024

Section III

DESCRIPTION OF TRACE SERVICES

COMPANY BACKGROUND

Trace Machina, Inc. (Trace) was founded in San Francisco in September 2023 and has employees based throughout the US as well as Germany and Peru.

Trace is the creator of the open-source project NativeLink (https://github.com/TraceMachina/nativelink), which is a build infrastructure tool written in Rust that facilitates testing and simulation and is specifically designed to allow rapid iteration with large complex codebases. Specifically, NativeLink integrates with all major build systems (such as Bazel and Buck 2) and allows users remote caching and remote execution dramatically reducing build times and flakiness.

In addition to the OSS product, Trace offers enterprise service level on a paid basis.

Trace was founded by two engineers with experience at Google, Toyota Research Institute, and MongoDB, and has since added veteran developers from Apple, Twitter, and Roblox. The company is backed by Wellington Management, Sequoia, Samsung Next, and a cadre of top-tier angel investors.

SERVICES PROVIDED

NativeLink makes it fast, reliable, and cost-effective to test large, complex projects written in multiple languages and across a variety of format structures (including monorepos). As an infrastructure tool, there are a variety of use cases, but NativeLink is particularly valuable for teams working on safety-critical software due to the complexity of simulating physical systems and the elevated reliability and compliance requirements.

The NativeLink OSS can be used locally but Trace also offers cloud hosting for remote execution, cashing, and building event protocol.

NativeLink is designed to be reliable and secure by default because of its Rust-based architecture, which identifies and removes unwanted dependencies and other security risks at the compile stage and removes race conditions at run-time.

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Trace designs its processes and procedures related to the use of NativeLink to meet its objectives. Those objectives are based on the service commitments that Trace makes to user entities, the laws and regulations that govern the provision of NativeLink, and the financial, operational, and compliance requirements that Trace has established for the use of the product. Use of NativeLink is subject to the security and privacy requirements of state and local privacy security laws and regulations in the jurisdictions in which Trace and its users operate.

Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online.

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

- Security principles within the fundamental designs of NativeLink that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role.
- Use of encryption technologies to protect customer data both at rest and in transit.

Trace has established operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Trace's system policies and procedures, system design documentation, and contracts with customers.

Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed,

and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the Trace Machina platform.

COMPONENTS OF THE SYSTEM

Infrastructure

The primary infrastructure used to provide NativeLink includes the following:

Primary Infrastructure		
Cloud Hardware	**Type**	**Purpose**
AWS EKS	ECS	Container runtime for web services, APIs, workers, and schedulers. Includes right-scaling and self-healing to replace failed containers.
AWS ECS	EKS	Container registry to store containers used in the K8s cluster's pods stored in EKS.
GitHub Actions	CI/CD runners	Our primary CI/CD system is used for the cloud and open-source repositories.
Redis	Storage/Pub-Sub	Provides a durable Redis instance for storage of small build artifacts, ETL pipelines, and as a pub-sub communication system for the scheduler.
AWS	Various Services, including VPC, Elastic IP, IAM, Lambda, Classic Load Balancer, CloudFront	Proxies for connections to NativeLink containers that allow all traffic to emanate from a set of IP addresses and also for safely exposing a CAS/metrics endpoint for users to send and pull down build artifacts from.
AWS	S3	Long-term storage for building artifacts and other miscellaneous files.
PostgreSQL	Storage	Relational database for cloud data.
MongoDB	Storage	Long-term no-SQL storage for non-sensitive user usage data.

Software

The primary software used to provide Trace Machina's Services system includes the following:

Primary Software		
Software	**Operating System**	**Purpose**
Rust	Linux	Primary development language for NativeLink remote execution service.
Go	Linux	Primary development language for NativeLink cloud.
Starlark	Linux	The primary language used to create build rules for bazel.
Nix	Linux	Language used to manage our Nix systems allows us to pin dependencies and have full control over the hermeticity of our infrastructure.
Typescript/JavaScript	Linux	Used to create the front-ends for our cloud application and internal API dashboards.

People

Trace has a staff of 19 employees and contractors organized into the following functional areas:

- Engineering: Software engineers who design and maintain the Trace product, including the web interface, remote execution, remote caching, and cloud. This team designs and implements new NativeLink functionality, assesses and remediates any issues or bugs found in NativeLink, and architects and deploys the underlying cloud infrastructure on which NativeLink can be run. Members of the engineering team are responsible for peer reviews of code and infrastructure designed and authored within the

team.

- Operations: The Chief of Staff and the Director of Business and Legal operations are responsible for the non-technical operations of Trace. This includes sourcing and interacting with vendors, facilitating internal communications, and legal operations including contracting with customers and directing outside counsel, finances, and overseeing the go-to-market team as well as special projects.

- Go to market: Individuals with commercial roles work to market, sell, and support NativeLink. At present these individuals work primarily in a developer relations or marketing capacity and are focused on developing assets and other content and disseminating this content through various channels, including social media and event planning to raise community awareness of and engagement with NativeLink.

Data

There are three major types of data used by Trace:

- **Configuration Data:** Data used to configure NativeLink on the NativeLink cloud.
- **Customer Data:** Data owned by Trace customers that are hosted on the NativeLink cloud during the use of the product.
- **Log Data:** Bazel Event Protocol data, Cloud Usage logs.

Configuration Data is stored in Trace's AWS Cloud account and includes:

- Trace customers' email addresses and usernames.
- Credentials for accessing NativeLink.
- The names of [databases, schemata, tables, columns, custom objects, and custom fields in customers' data warehouses and SaaS applications].
- Configuration objects that determine how data is copied between systems, including field mappings, update policies, and schedules.
- Audit logs covering changes to each of the above items.

Configuration Data is treated as sensitive by Trace. It is stored with a limited lifetime when possible. Access controls limit configuration data access to each customer's NativeLink account. Customers can invite other people in their company to access their NativeLink account and read and write configuration data. Trace operators may access configuration data to troubleshoot customer issues or to gather feedback for improving the NativeLink product.

Customer Data is the most sensitive data in the Trace system, and Trace does not store it. It is currently impossible for Trace to sync data from data warehouses directly to NativeLink without handling customer data, so we attempt to limit that handling as much as possible and offload as much processing to customer infrastructure as we can. When Trace does handle customer data, it does so using ephemeral (short-lived) worker instances and temporary storage managed by database vendors and our cloud providers. If an error occurs while running a sync, Trace can store a small sample of customer data in our cloud databases for ease of customer debugging. This data has a highly limited lifetime and size, and customers can elect to disable this debugging feature. Trace operators are permitted to access customer data to debug complex failures in the sync engine as a result of operational issues but are encouraged to use other tools and data sources to do this debugging when possible.

Log Data is produced by the sync engine to make it easier for Trace operators to monitor the health of the system and track down any issues. Log data is a trace of the actions performed by the system in the course of a sync. Log data will include snapshots of **Configuration Data** at the time the sync was performed, so operators can see what the sync engine was attempting to do. Log data also includes stack traces and samples of running code. Due to the nature of logging frameworks, there is a small possibility that log data can also include **Customer Data** captured by automatic tracers. Trace endeavors to "scrub" logs of any **Customer Data** before they are persisted. Log data may be stored by vendors that Trace has entrusted for purposes like indexing, monitoring, and trending. Regardless of whether log data is stored within Trace's own databases or by vendors, it is given a limited lifetime and automatically removed.

All data types processed by Trace are encrypted on the wire – no networking connections used by Trace for any purpose will ever send unencrypted data. In addition, all **Configuration Data** and **Log Data**, as well as samples of **Customer Data** stored by Trace are encrypted at rest, in our own databases, our caches, and our cloud storage.

PROCESSES AND PROCEDURES

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 Trace policies and procedures that define how services should be delivered. These are located on the Company's security compliance platform and can be accessed by any Trace team member.

Physical Security

All data is hosted by Amazon Web Services (AWS). AWS data centers do not allow Trace employees physical access. At present, Trace does not maintain any office space and all work is conducted remotely.

Logical Access

Trace employees and contractors are granted access to infrastructure via a role-based access control system, to ensure uniform, least-privilege access to identified users and to maintain simple and repeatable user provisioning and de-provisioning processes.

Trace infrastructure runs entirely on cloud and SaaS-based systems, and as such the resources used by employees to perform their roles are accounts and permissions within those systems. An employee can have one of their access levels to a SaaS or cloud service:

- Administrator – can alter policies and provision or de-provision users.
- User/Member – has full read/write access to the SaaS or cloud service (except for administration).
- No access

Trace currently does not have "read-only" roles in our SaaS or cloud applications or finer-grained policies on roles within those applications to avoid administrative complexity and friction for employees.

Roles are reviewed on an annual basis by management and the security team to ensure the least privileged access.

Trace identifies employees primarily by their G Suite account, which functions as our corporate directory and SSO provider. The Trace password policy mandates that employees and contractors use their G Suite accounts to sign in to SaaS and cloud tools when supported. When G Suite sign-in is not available, employees may authenticate using a strong, unique password, which must be stored in an approved password manager and includes two-factor identification.

The Trace G Suite tenant requires users to use a second factor for authentication. In addition, any SaaS applications used by the company that don't use G Suite sign-in must be configured to use a second factor when possible.

The operations team is responsible for onboarding new employees. The Chief of Staff is responsible for provisioning G Suite and other SaaS accounts as dictated by the employee's role and performing a background check, and the employee is responsible for reviewing Trace's policies, completing security training, and successfully gaining access to provisioned accounts (as well as enrolling a device for second-factor authentication). These steps must be completed within 14 days of hire.

When an employee is terminated, management is responsible for removing or disabling all of the employee's accounts within 1 day.

Trace employees may use a company-provided computer to perform their duties or may elect to "bring their own" device if that device is approved by the security team. Any computer (company-owned or BYOD) on which a Trace employee performs sensitive work must employ full-disk encryption and have an approved endpoint monitoring tool installed. On employee termination, management will ensure the return of company-owned devices and handle their de-provisioning or reprovisioning based on the company's Asset Management

policy.

Computer Operations – Backups

Customer data is backed up by Trace's cloud team. In the event of an exception, operations personnel perform troubleshooting to identify the root cause and then re-run the backup job immediately or as part of the next scheduled backup job.

Backup infrastructure is maintained in AWS, with physical access restricted according to applicable AWS policies. All backups are encrypted using KMS-managed encryption keys, with access restricted to key personnel via AWS IAM permissions.

Computer Operations – Availability

Trace maintains an Incident Response Policy that gives any Trace employee the ability to initiate a response to a potential security incident by notifying the internal security team through several channels and assisting in classifying the severity of the incident.

Customers are given a channel to send incident reports and responsibly disclose potential issues to the Trace security team.

Internally, the Trace operations team monitors the health of all applications, including vendor services, the NativeLink OSS, databases, and cloud storage. Critical incidents are routed to an on-call operator who is responsible for acknowledging them within one hour; if there is no acknowledgment, the incident is escalated to the rest of the operations team.

Trace employs 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.

Change Control

Trace maintains a documented Change Management policy as well as 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 pull request 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. The senior engineering team 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.

Data Communications

Trace's infrastructure is built on IaaS (Infrastructure as a Service) and PaaS (Platform as a Service). AWS is primarily an IaaS as it offers a wide range of services that allow users to rent virtualized computing resources over the Internet.

EKS (Elastic Kubernetes Services) is the core piece of Trace's data communications infrastructure.

BOUNDARIES OF THE SYSTEM

The scope of this report includes the services performed by NativeLink. This report does not include the data center hosting services provided by AWS.

THE APPLICABLE TRUST SERVICES CRITERIA AND THE RELATED CONTROLS

Common Criteria (to the Security, Availability, and Confidentiality Categories)
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 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
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). However, it does address whether systems include controls to support accessibility for operation, monitoring, and maintenance.

Confidentiality
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). Confidentiality requirements may be contained in laws or regulations or in contracts or agreements that contain commitments made to customers or others. The need for information to be confidential may arise for many different reasons. For example, the information may be proprietary and intended only for entity personnel. Confidentiality is distinguished from privacy in that privacy applies only to personal information, whereas confidentiality applies to various types of sensitive information. In addition, the privacy objective addresses requirements regarding the collection, use, retention, disclosure, and disposal of personal information. Confidential information may include personal information as well as other information, such as trade secrets and intellectual property.

CONTROL ENVIRONMENT

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 Trace's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Trace's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. 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.

Commitment to Competence

Trace'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.

Management and Security Team Philosophy and Operating Style

The Trace security 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 security team meets frequently to be briefed on technology changes that impact the way Trace 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 Trace to alter its software to maintain legal compliance. Major planned changes to the business are also reviewed by the security 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 NativeLink.
- Executive management meetings are held to discuss major initiatives and issues that affect the business as a whole.

Organizational Structure and Assignment of Authority and Responsibility

Trace is currently organized in the following management structure. All members of the engineering team report to the CTO or the senior Rust engineering manager. All members of the GTM team report to the Director of Business and Legal Operations. Managers report to the CIO and CEO respectively. As the team grows, management will elect to build an additional organizational structure that ensures that employees clearly understand their role in the organization, how they and their team are responsible for furthering company-wide initiatives, and channels for reporting upward and downward in the organizational hierarchy.

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

- Organizational charts are in place to communicate key areas of authority and responsibility.
- Organizational charts are communicated to employees and updated as needed.

Human Resource Policies and Practices

Trace'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. Trace's human resources policies and practices relate 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

Trace's risk assessment process identifies and manages risks that could potentially affect Trace's ability to provide reliable and secure services to our customers and users. As part of this process, Trace 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 Trace 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 Trace's product and internal system; as well as the nature of the components of the system result in risks that the criteria will not be met. Trace 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, Tra's security team 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 an integral component of Trace'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.

Trace uses several information and communication channels internally to share information with management, the security team, employees, contractors, and customers. Trace uses chat systems (Slack) and email as the primary internal and external communication channels. In addition, Trace communicates with customers via direct and group Slack and direct email, as well as various social media platforms.

Structured data is communicated internally via our SaaS applications (finance information in various applications and financial institutions such as Expensify and Mercury) and our project management tools (Jira). Finally, Trace uses video one-on-one and all-hands "standup" meetings to communicate company priorities and goals from management to all employees.

MONITORING CONTROLS

The security team monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. The security team 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 are also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

On-Going Monitoring

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

The security team's close involvement in Trace'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 to maximize the performance of Trace's personnel.

Reporting Deficiencies

Our risk management team documents and tracks 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.

INCIDENTS SINCE THE FOUNDING OF TRACE

No significant incidents have occurred to the services provided to user entities in the 9 months preceding the end of the review date, which period constitutes the current lifetime of Trace.

CRITERIA NOT APPLICABLE TO THE SYSTEM

All relevant trust services criteria were applicable to the Trace Services system.

SUBSERVICE ORGANIZATIONS

Trace'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 of the trust services criteria related to Trace's services to be solely achieved by Trace control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of Trace.

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

Subservice Organization – AWS		
Category	**Criteria**	**Control**
Common Criteria / Security	CC6.4	Physical access to data centers is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
		Physical access points to server locations are recorded by closed-circuit television cameras (CCTV). Images are retained for 90 days unless limited by legal or contractual obligations.
		Physical access points to server locations are managed by electronic access control devices.
		Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.
Availability	A1.2	Amazon-owned data centers are protected by fire detection and suppression systems.
		Amazon-owned data centers are air-conditioned to maintain appropriate atmospheric conditions. Personnel and systems monitor and control air temperature and humidity at appropriate levels.
		Uninterruptible Power Supply (UPS) units provide backup power in the event of an electrical failure in Amazon-owned data centers.
		Amazon-owned data centers have generators to provide backup power in case of electrical failure.
		Contracts are in place with third-party colocation service providers which include provisions to provide fire suppression systems, air conditioning to maintain appropriate atmospheric conditions, Uninterruptible Power Supply (UPS) units, and redundant power supplies.
		Critical AWS system components are replicated across multiple Availability Zones and backups are maintained.
		Backups of critical AWS system components are monitored for successful replication across multiple Availability Zones.

Trace management, along with the subservice organization, defines the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, Trace performs monitoring of the subservice organization controls, including the following procedures

- Reviewing attestation reports over services provided by vendors and subservice organizations.
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organization.

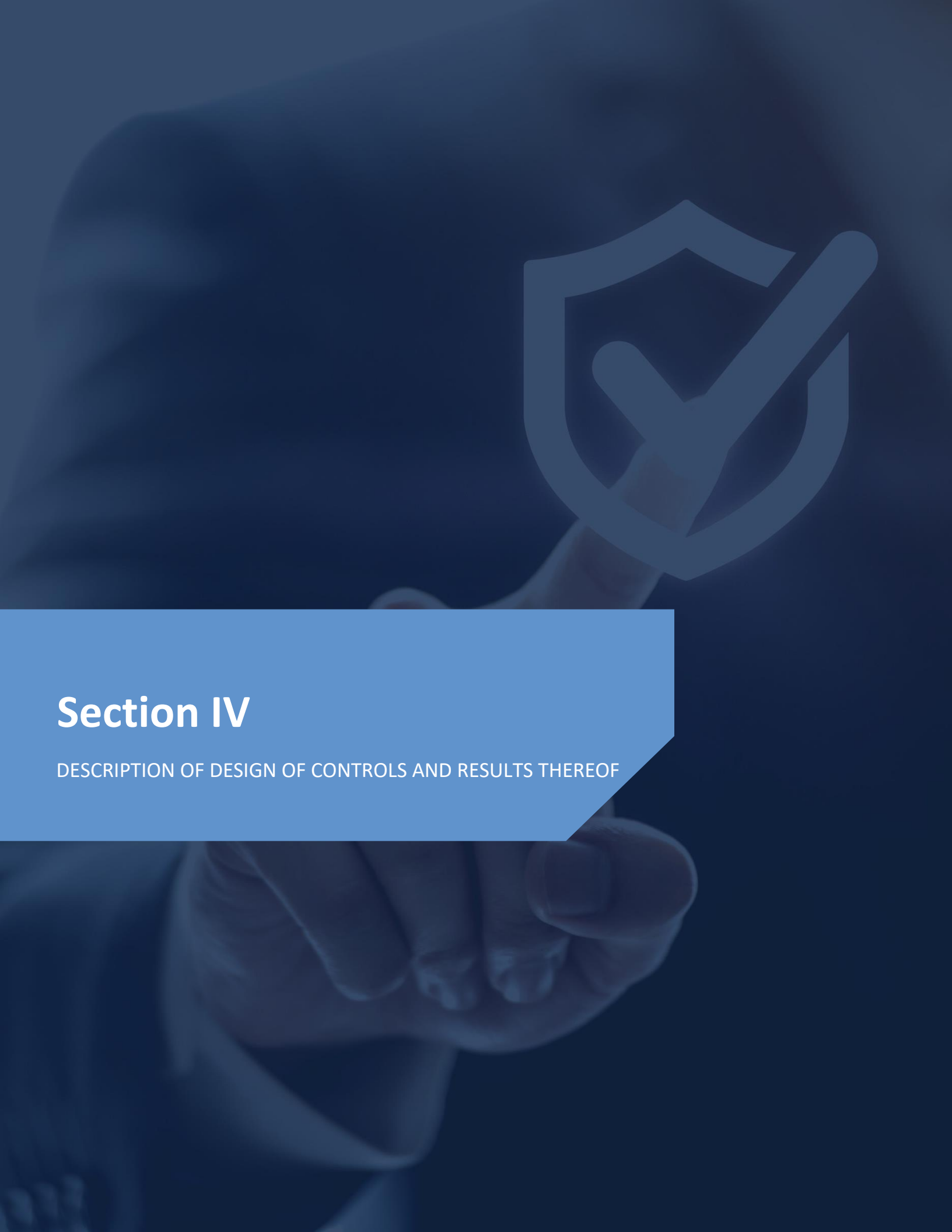
COMPLEMENTARY USER ENTITY CONTROLS

Trace'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 Trace's services to be solely achieved by Trace control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Trace.

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 Trace.
2. User entities are responsible for maintaining their own system(s) of record.
3. User entities are responsible for ensuring the supervision, management, and control of the use of Trace services by their personnel.
4. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Trace services.
5. Any paid customer entities are responsible for providing Trace with a list of approvers for security and system configuration changes for data transmission.

6. Customer entities are responsible for immediately notifying Trace of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.



Section IV

DESCRIPTION OF DESIGN OF CONTROLS AND RESULTS THEREOF

Relevant trust services criteria and Trace Machina, Inc.-related controls are an integral part of management's system description and are included in this section. Johanson Group LLP assessed if Trace Machina, Inc.'s controls were suitably designed to meet the specified criteria for the security, availability, and confidentiality categories set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*, as of July 26, 2024.

Assessment of control design included inquiry of appropriate management, supervisory, and staff personnel and the inspection of Trace Machina, Inc.'s policy and procedure documentation. The results of those assessments were considered in the planning, the nature, timing, and extent of Johanson LLP's review of the controls designed to address the relevant trust services criteria. Being a Type I SOC 2 report, there were no tests performed to determine the operational effectiveness of each designed control.

Criteria Number	Trust Services Criteria	Description of Trace Machina, Inc.'s Controls	Result
CONTROL ENVIRONMENT			
CC 1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	A Code of Conduct outlines ethical expectations, behavior standards, and ramifications of noncompliance.	Control determined to be suitably designed.
		Internal personnel are evaluated via a formal performance review at least annually.	Control determined to be suitably designed.
		Personnel who violate information security policies are subject to disciplinary action and such disciplinary action is clearly documented in one or more policies.	Control determined to be suitably designed.
		An Internal Control Policy identifies how a system of controls should be maintained to safeguard assets, promote operational efficiency, and encourage adherence to prescribed managerial policies.	Control determined to be suitably designed.
CC 1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The board of directors or equivalent entity function includes senior management and external advisors, who are independent of the company's operations. An information security team has also been established to govern cybersecurity.	Control determined to be suitably designed.
		Senior management and/or board of directors meets at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters. The information security team meets at least annually to discuss security risks, roles and responsibilities, controls, changes, audit results, and/or other matters as necessary.	Control determined to be suitably designed.
CC 1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	The board of directors or equivalent entity function includes senior management and external advisors, who are independent of the company's operations. An information security team has also been established to govern cybersecurity.	Control determined to be suitably designed.
		Senior management and/or board of directors meets at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters. The information security team meets at least annually to discuss security risks, roles and responsibilities, controls, changes, audit results, and/or other matters as necessary.	Control determined to be suitably designed.

Criteria Number	Trust Services Criteria	Description of Trace Machina, Inc.'s Controls	Result
		Management maintains a formal organizational chart to clearly identify positions of authority and the lines of communication and publishes the organizational chart to internal personnel.	Control determined to be suitably designed.
		Roles and responsibilities related to security, availability, and confidentiality for all personnel and executive roles are outlined in job descriptions and policies, as applicable.	Control determined to be suitably designed.
		Vendor SOC 2 reports (or equivalent) are collected and reviewed on at least an annual basis.	Control determined to be suitably designed.
		New vendors are assessed in accordance with the Vendor Risk Management Policy prior to engaging with the vendor. Reassessment occurs at least annually.	Control determined to be suitably designed.
CC 1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	A Code of Conduct outlines ethical expectations, behavior standards, and ramifications of noncompliance.	Control determined to be suitably designed.
		Internal personnel are evaluated via a formal performance review at least annually.	Control determined to be suitably designed.
		Background checks or their equivalent are performed before or promptly after a new hire's start date, as permitted by local laws.	Control determined to be suitably designed.
		Hiring managers screen new hires or internal transfers to assess their qualifications, experience, and competency to fulfill their responsibilities. New hires sign confidentiality agreements or equivalents upon hire.	Control determined to be suitably designed.
		Internal personnel complete annual training programs for information security to help them understand their obligations and responsibilities related to security.	Control determined to be suitably designed.
		An Information Security Policy establishes the security requirements for maintaining the security, confidentiality, integrity, and availability of applications, systems, infrastructure, and data.	Control determined to be suitably designed.
		An Internal Control Policy identifies how a system of controls should be maintained to safeguard assets, promote operational efficiency, and encourage adherence to prescribed managerial policies.	Control determined to be suitably designed.
		A Performance Review Policy provides personnel context and transparency into their performance and career development processes.	Control determined to be suitably designed.
		Vendor SOC 2 reports (or equivalent) are collected and reviewed on at least an annual basis.	Control determined to be suitably designed.
CC 1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Senior management and/or board of directors meets at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters. The information security team meets at least annually to discuss security risks, roles and responsibilities, controls, changes, audit results, and/or other matters as necessary.	Control determined to be suitably designed.
		Internal personnel are evaluated via a formal performance review at least annually.	Control determined to be suitably designed.

Criteria Number	Trust Services Criteria	Description of Trace Machina, Inc.'s Controls	Result
		A continuous monitoring solution monitors internal controls used in the achievement of service commitments and system requirements.	Control determined to be suitably designed.
		Management maintains a formal organizational chart to clearly identify positions of authority and the lines of communication and publishes the organizational chart to internal personnel.	Control determined to be suitably designed.
		Personnel who violate information security policies are subject to disciplinary action and such disciplinary action is clearly documented in one or more policies.	Control determined to be suitably designed.
		An Internal Control Policy identifies how a system of controls should be maintained to safeguard assets, promote operational efficiency, and encourage adherence to prescribed managerial policies.	Control determined to be suitably designed.
		A Performance Review Policy provides personnel context and transparency into their performance and career development processes.	Control determined to be suitably designed.
COMMUNICATION AND INFORMATION			
CC 2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	A continuous monitoring solution monitors internal controls used in the achievement of service commitments and system requirements.	Control determined to be suitably designed.
		An Information Security Policy establishes the security requirements for maintaining the security, confidentiality, integrity, and availability of applications, systems, infrastructure, and data.	Control determined to be suitably designed.
		Formal risk assessments are performed, which include the identification of relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	Control determined to be suitably designed.
		Vulnerability scanning is performed on production infrastructure systems, and identified deficiencies are remediated on a timely basis.	Control determined to be suitably designed.
		A 3rd party is engaged to conduct a network and application penetration test of the production environment at least annually. Critical and high-risk findings are tracked through resolution.	Control determined to be suitably designed.
CC 2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Descriptions of the company's services and systems are available to both internal personnel and external users.	Control determined to be suitably designed.
		A confidential reporting channel is made available to internal personnel and external parties to report security and other identified concerns.	Control determined to be suitably designed.
		An Incident Response Plan outlines the process of identifying, prioritizing, communicating, assigning, and tracking confirmed incidents through to resolution.	Control determined to be suitably designed.

Criteria Number	Trust Services Criteria	Description of Trace Machina, Inc.'s Controls	Result
		A Network Security Policy identifies the requirements for protecting information and systems within and across networks.	Control determined to be suitably designed.
		Senior management and/or board of directors meets at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters. The information security team meets at least annually to discuss security risks, roles and responsibilities, controls, changes, audit results, and/or other matters as necessary.	Control determined to be suitably designed.
		Internal personnel complete annual training programs for information security to help them understand their obligations and responsibilities related to security.	Control determined to be suitably designed.
		Roles and responsibilities related to security, availability, and confidentiality for all personnel and executive roles are outlined in job descriptions and policies, as applicable.	Control determined to be suitably designed.
CC 2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	Descriptions of the company's services and systems are available to both internal personnel and external users.	Control determined to be suitably designed.
		Security commitments and expectations are communicated to both internal personnel and external users via the company's website.	Control determined to be suitably designed.
		Terms of Service or the equivalent are published or shared with external users.	Control determined to be suitably designed.
		Critical information is communicated to external parties, as applicable.	Control determined to be suitably designed.
		A confidential reporting channel is made available to internal personnel and external parties to report security and other identified concerns.	Control determined to be suitably designed.
		A Privacy Policy is established for external users describing the company's privacy commitments.	Control determined to be suitably designed.
		Senior management and/or board of directors meets at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters. The information security team meets at least annually to discuss security risks, roles and responsibilities, controls, changes, audit results, and/or other matters as necessary.	Control determined to be suitably designed.
		New vendors are assessed in accordance with the Vendor Risk Management Policy prior to engaging with the vendor. Reassessment occurs at least annually.	Control determined to be suitably designed.
RISK ASSESSMENT			
CC 3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	Senior management and/or board of directors meets at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters. The information security team meets at least annually to discuss security risks, roles and responsibilities, controls, changes, audit results, and/or other matters as necessary.	Control determined to be suitably designed.

Criteria Number	Trust Services Criteria	Description of Trace Machina, Inc.'s Controls	Result
		A Risk Assessment and Treatment Policy governs the process for conducting risk assessments to account for threats, vulnerabilities, likelihood, and impact with respect to assets, team members, customers, vendors, suppliers, and partners. Risk tolerance and strategies are also defined in the policy.	Control determined to be suitably designed.
		Formal risk assessments are performed, which include the identification of relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	Control determined to be suitably designed.
CC 3.2	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.	A Risk Assessment and Treatment Policy governs the process for conducting risk assessments to account for threats, vulnerabilities, likelihood, and impact with respect to assets, team members, customers, vendors, suppliers, and partners. Risk tolerance and strategies are also defined in the policy.	Control determined to be suitably designed.
		Formal risk assessments are performed, which include the identification of relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	Control determined to be suitably designed.
		A risk register is maintained, which records the risk mitigation strategies for identified risks, and the development or modification of controls consistent with the risk mitigation strategy.	Control determined to be suitably designed.
		New vendors are assessed in accordance with the Vendor Risk Management Policy prior to engaging with the vendor. Reassessment occurs at least annually.	Control determined to be suitably designed.
		Vulnerability scanning is performed on production infrastructure systems, and identified deficiencies are remediated on a timely basis.	Control determined to be suitably designed.
CC 3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	Formal risk assessments are performed, which include the identification of relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	Control determined to be suitably designed.
CC 3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	Formal risk assessments are performed, which include the identification of relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	Control determined to be suitably designed.
		New vendors are assessed in accordance with the Vendor Risk Management Policy prior to engaging with the vendor. Reassessment occurs at least annually.	Control determined to be suitably designed.
MONITORING ACTIVITIES			
CC 4.1	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.	A continuous monitoring solution monitors internal controls used in the achievement of service commitments and system requirements.	Control determined to be suitably designed.

Criteria Number	Trust Services Criteria	Description of Trace Machina, Inc.'s Controls	Result
		An Internal Control Policy identifies how a system of controls should be maintained to safeguard assets, promote operational efficiency, and encourage adherence to prescribed managerial policies.	Control determined to be suitably designed.
		Vulnerability scanning is performed on production infrastructure systems, and identified deficiencies are remediated on a timely basis.	Control determined to be suitably designed.
		A 3rd party is engaged to conduct a network and application penetration test of the production environment at least annually. Critical and high-risk findings are tracked through resolution.	Control determined to be suitably designed.
CC 4.2	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.	Senior management and/or board of directors meets at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters. The information security team meets at least annually to discuss security risks, roles and responsibilities, controls, changes, audit results, and/or other matters as necessary.	Control determined to be suitably designed.
		A continuous monitoring solution monitors internal controls used in the achievement of service commitments and system requirements.	Control determined to be suitably designed.
		Vulnerability scanning is performed on production infrastructure systems, and identified deficiencies are remediated on a timely basis.	Control determined to be suitably designed.
		A 3rd party is engaged to conduct a network and application penetration test of the production environment at least annually. Critical and high-risk findings are tracked through resolution.	Control determined to be suitably designed.
CONTROL ACTIVITIES			
CC 5.1	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.	An Internal Control Policy identifies how a system of controls should be maintained to safeguard assets, promote operational efficiency, and encourage adherence to prescribed managerial policies.	Control determined to be suitably designed.
		Formal risk assessments are performed, which include the identification of relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	Control determined to be suitably designed.
		A Vendor Risk Management Policy defines a framework for the onboarding and management of the vendor relationship lifecycle.	Control determined to be suitably designed.
CC 5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	A Secure Development Policy defines the requirements for secure software and system development and maintenance.	Control determined to be suitably designed.
		A continuous monitoring solution monitors internal controls used in the achievement of service commitments and system requirements.	Control determined to be suitably designed.

Criteria Number	Trust Services Criteria	Description of Trace Machina, Inc.'s Controls	Result
		An Internal Control Policy identifies how a system of controls should be maintained to safeguard assets, promote operational efficiency, and encourage adherence to prescribed managerial policies.	Control determined to be suitably designed.
		Roles and responsibilities related to security, availability, and confidentiality for all personnel and executive roles are outlined in job descriptions and policies, as applicable.	Control determined to be suitably designed.
CC 5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and procedures that put policies into action.	An Access Control and Termination Policy governs authentication and access to applicable systems, data, and networks.	Control determined to be suitably designed.
		An Encryption and Key Management Policy supports the secure encryption and decryption of app secrets and governs the use of cryptographic controls.	Control determined to be suitably designed.
		Business Continuity and Disaster Recovery Policy governs the required processes for restoring the service or supporting infrastructure after suffering a disaster or disruption.	Control determined to be suitably designed.
		A Data Classification Policy details the security and handling protocols for sensitive data.	Control determined to be suitably designed.
		A Data Retention and Disposal Policy specifies how customer data is to be retained and disposed of based on compliance requirements and contractual obligations.	Control determined to be suitably designed.
		A Configuration and Asset Management Policy governs configurations for new sensitive systems.	Control determined to be suitably designed.
		A Change Management Policy governs the documenting, tracking, testing, and approving of system, network, security, and infrastructure changes.	Control determined to be suitably designed.
		A Secure Development Policy defines the requirements for secure software and system development and maintenance.	Control determined to be suitably designed.
		A Privacy Policy is established for external users describing the company's privacy commitments.	Control determined to be suitably designed.
		An Incident Response Plan outlines the process of identifying, prioritizing, communicating, assigning, and tracking confirmed incidents through to resolution.	Control determined to be suitably designed.
		A Network Security Policy identifies the requirements for protecting information and systems within and across networks.	Control determined to be suitably designed.
		A continuous monitoring solution monitors internal controls used in the achievement of service commitments and system requirements.	Control determined to be suitably designed.
		An Acceptable Use Policy defines standards for the appropriate and secure use of company hardware and electronic systems including storage media, communication tools, and internet access.	Control determined to be suitably designed.
		Personnel who violate information security policies are subject to disciplinary action and such disciplinary action is clearly documented in one or more policies.	Control determined to be suitably designed.

Criteria Number	Trust Services Criteria	Description of Trace Machina, Inc.'s Controls	Result
		An Information Security Policy establishes the security requirements for maintaining the security, confidentiality, integrity, and availability of applications, systems, infrastructure, and data.	Control determined to be suitably designed.
		An Internal Control Policy identifies how a system of controls should be maintained to safeguard assets, promote operational efficiency, and encourage adherence to prescribed managerial policies.	Control determined to be suitably designed.
		A Performance Review Policy provides personnel context and transparency into their performance and career development processes.	Control determined to be suitably designed.
		Policies and procedures are reviewed and updated by management at least annually.	Control determined to be suitably designed.
		Internal personnel review and accept applicable information security policies at least annually.	Control determined to be suitably designed.
		Roles and responsibilities related to security, availability, and confidentiality for all personnel and executive roles are outlined in job descriptions and policies, as applicable.	Control determined to be suitably designed.
		A Risk Assessment and Treatment Policy governs the process for conducting risk assessments to account for threats, vulnerabilities, likelihood, and impact with respect to assets, team members, customers, vendors, suppliers, and partners. Risk tolerance and strategies are also defined in the policy.	Control determined to be suitably designed.
		A Vendor Risk Management Policy defines a framework for the onboarding and management of the vendor relationship lifecycle.	Control determined to be suitably designed.
		A Vulnerability Management and Patch Management Policy outlines the processes to efficiently respond to identified vulnerabilities.	Control determined to be suitably designed.
LOGICAL AND PHYSICAL ACCESS			
CC 6.1	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.	A list of system assets, components, and respective owners is maintained and reviewed at least annually.	Control determined to be suitably designed.
		Personnel are assigned unique IDs to access sensitive systems, networks, and information.	Control determined to be suitably designed.
		Personnel are required to use strong, complex passwords and a second form of authentication to access sensitive systems, networks, and information.	Control determined to be suitably designed.
		An Access Control and Termination Policy governs authentication and access to applicable systems, data, and networks.	Control determined to be suitably designed.
		Non-console access to production infrastructure is restricted to users with a unique SSH key or access key.	Control determined to be suitably designed.
		Service data is encrypted at rest.	Control determined to be suitably designed.

Criteria Number	Trust Services Criteria	Description of Trace Machina, Inc.'s Controls	Result
		An Encryption and Key Management Policy supports the secure encryption and decryption of app secrets and governs the use of cryptographic controls.	Control determined to be suitably designed.
		A Configuration and Asset Management Policy governs configurations for new sensitive systems.	Control determined to be suitably designed.
		Company endpoints are managed and configured with a strong password policy, anti-virus, and hard drive encryption.	Control determined to be suitably designed.
		Configurations ensure available networking ports, protocols, services, and environments are restricted as necessary, including firewalls.	Control determined to be suitably designed.
CC 6.2	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.	An Access Control and Termination Policy governs authentication and access to applicable systems, data, and networks.	Control determined to be suitably designed.
		Administrative access to production infrastructure is restricted based on the principle of least privilege.	Control determined to be suitably designed.
		Users are provisioned access to systems based on the principle of least privilege.	Control determined to be suitably designed.
		Upon termination or when internal personnel no longer require access, system access is removed, as applicable.	Control determined to be suitably designed.
		System owners conduct scheduled user access reviews of production servers, databases, and applications to validate that internal user access is commensurate with job responsibilities.	Control determined to be suitably designed.
CC 6.3	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.	An Access Control and Termination Policy governs authentication and access to applicable systems, data, and networks.	Control determined to be suitably designed.
		Non-console access to production infrastructure is restricted to users with a unique SSH key or access key.	Control determined to be suitably designed.
		Users are provisioned access to systems based on the principle of least privilege.	Control determined to be suitably designed.
		Upon termination or when internal personnel no longer require access, system access is removed, as applicable.	Control determined to be suitably designed.
		System owners conduct scheduled user access reviews of production servers, databases, and applications to validate that internal user access is commensurate with job responsibilities.	Control determined to be suitably designed.

Criteria Number	Trust Services Criteria	Description of Trace Machina, Inc.'s Controls	Result
CC 6.4	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.	The entity does not operate any physical hardware such as servers and network devices but rather uses subservice organizations and relies on its own controls for physical access.	Control determined to be suitably designed.
CC 6.5	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.	Vendor SOC 2 reports (or equivalent) are collected and reviewed on at least an annual basis.	Control determined to be suitably designed.
CC 6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Personnel are required to use strong, complex passwords and a second form of authentication to access sensitive systems, networks, and information.	Control determined to be suitably designed.
		Service data transmitted over the internet is encrypted in transit.	Control determined to be suitably designed.
		An Encryption and Key Management Policy supports the secure encryption and decryption of app secrets and governs the use of cryptographic controls.	Control determined to be suitably designed.
		Security tools are implemented to provide monitoring of network traffic to the production environment.	Control determined to be suitably designed.
		Configurations ensure available networking ports, protocols, services, and environments are restricted as necessary, including firewalls.	Control determined to be suitably designed.
		A Network Security Policy identifies the requirements for protecting information and systems within and across networks.	Control determined to be suitably designed.
CC 6.7	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.	Service data is encrypted at rest.	Control determined to be suitably designed.
		Service data transmitted over the internet is encrypted in transit.	Control determined to be suitably designed.
		Company endpoints are managed and configured with a strong password policy, anti-virus, and hard drive encryption.	Control determined to be suitably designed.
		An Acceptable Use Policy defines standards for the appropriate and secure use of company hardware and electronic systems including storage media, communication tools, and internet access.	Control determined to be suitably designed.
CC 6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	Baseline configurations and codebases for production infrastructure, systems, and applications are securely managed.	Control determined to be suitably designed.

Criteria Number	Trust Services Criteria	Description of Trace Machina, Inc.'s Controls	Result
		Software changes are tested prior to being deployed into production.	Control determined to be suitably designed.
		System changes are approved by at least 1 independent person prior to deployment into production.	Control determined to be suitably designed.
		A Configuration and Asset Management Policy governs configurations for new sensitive systems.	Control determined to be suitably designed.
		A Change Management Policy governs the documenting, tracking, testing, and approving of system, network, security, and infrastructure changes.	Control determined to be suitably designed.
		Company endpoints are managed and configured with a strong password policy, anti-virus, and hard drive encryption.	Control determined to be suitably designed.
		An Acceptable Use Policy defines standards for the appropriate and secure use of company hardware and electronic systems including storage media, communication tools, and internet access.	Control determined to be suitably designed.
SYSTEM OPERATIONS			
CC 7.1	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.	Baseline configurations and codebases for production infrastructure, systems, and applications are securely managed.	Control determined to be suitably designed.
		A Configuration and Asset Management Policy governs configurations for new sensitive systems.	Control determined to be suitably designed.
		Security tools are implemented to provide monitoring of network traffic to the production environment.	Control determined to be suitably designed.
		Logging and monitoring software is used to collect data from infrastructure to detect potential security threats, and unusual system activity, and monitor system performance, as applicable.	Control determined to be suitably designed.
		Alerting software is used to notify impacted teams of potential security events.	Control determined to be suitably designed.
		A Vulnerability Management and Patch Management Policy outlines the processes to efficiently respond to identified vulnerabilities.	Control determined to be suitably designed.
		Vulnerability scanning is performed on production infrastructure systems, and identified deficiencies are remediated on a timely basis.	Control determined to be suitably designed.
		A 3rd party is engaged to conduct a network and application penetration test of the production environment at least annually. Critical and high-risk findings are tracked through resolution.	Control determined to be suitably designed.

Criteria Number	Trust Services Criteria	Description of Trace Machina, Inc.'s Controls	Result
CC 7.2	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.	Security tools are implemented to provide monitoring of network traffic to the production environment.	Control determined to be suitably designed.
		Logging and monitoring software is used to collect data from infrastructure to detect potential security threats, and unusual system activity, and monitor system performance, as applicable.	Control determined to be suitably designed.
		Alerting software is used to notify impacted teams of potential security events.	Control determined to be suitably designed.
		A Network Security Policy identifies the requirements for protecting information and systems within and across networks.	Control determined to be suitably designed.
CC 7.3	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.	An Incident Response Plan outlines the process of identifying, prioritizing, communicating, assigning, and tracking confirmed incidents through to resolution.	Control determined to be suitably designed.
		Identified incidents are documented, tracked, and analyzed according to the Incident Response Plan.	Control determined to be suitably designed.
CC 7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Business Continuity and Disaster Recovery Policy governs the required processes for restoring the service or supporting infrastructure after suffering a disaster or disruption.	Control determined to be suitably designed.
		Critical information is communicated to external parties, as applicable.	Control determined to be suitably designed.
		An Incident Response Plan outlines the process of identifying, prioritizing, communicating, assigning, and tracking confirmed incidents through to resolution.	Control determined to be suitably designed.
		Identified incidents are documented, tracked, and analyzed according to the Incident Response Plan.	Control determined to be suitably designed.
		After any identified security incident has been resolved, management provides a "Lessons Learned" document to the team in order to continually improve the company's security and operations.	Control determined to be suitably designed.
		The Incident Response Plan is periodically tested via tabletop exercises or equivalents. When necessary, Management makes changes to the Incident Response Plan based on the test results.	Control determined to be suitably designed.
		Personnel who violate information security policies are subject to disciplinary action and such disciplinary action is clearly documented in one or more policies.	Control determined to be suitably designed.

Criteria Number	Trust Services Criteria	Description of Trace Machina, Inc.'s Controls	Result
CC 7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Backed-up data is restored to a non-production environment at least annually to validate the integrity of backups.	Control determined to be suitably designed.
		The Business Continuity and Disaster Recovery Plan is periodically tested via tabletop exercises or equivalents. When necessary, Management makes changes to the Business Continuity and Disaster Recovery Plan based on the test results.	Control determined to be suitably designed.
		Critical information is communicated to external parties, as applicable.	Control determined to be suitably designed.
		An Incident Response Plan outlines the process of identifying, prioritizing, communicating, assigning, and tracking confirmed incidents through to resolution.	Control determined to be suitably designed.
		Identified incidents are documented, tracked, and analyzed according to the Incident Response Plan.	Control determined to be suitably designed.
		After any identified security incident has been resolved, management provides a "Lessons Learned" document to the team in order to continually improve the company's security and operations.	Control determined to be suitably designed.
		The Incident Response Plan is periodically tested via tabletop exercises or equivalents. When necessary, Management makes changes to the Incident Response Plan based on the test results.	Control determined to be suitably designed.
CHANGE MANAGEMENT			
CC 8.1	The entity authorizes, designs, develops acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Non-console access to production infrastructure is restricted to users with a unique SSH key or access key.	Control determined to be suitably designed.
		Baseline configurations and codebases for production infrastructure, systems, and applications are securely managed.	Control determined to be suitably designed.
		Software changes are tested prior to being deployed into production.	Control determined to be suitably designed.
		System changes are approved by at least 1 independent person prior to deployment into production.	Control determined to be suitably designed.
		Development, staging, and production environments are segregated.	Control determined to be suitably designed.
		Production data is not used in the development and testing environments unless required for debugging customer issues.	Control determined to be suitably designed.
		A Configuration and Asset Management Policy governs configurations for new sensitive systems.	Control determined to be suitably designed.
		A Change Management Policy governs the documenting, tracking, testing, and approving of system, network, security, and infrastructure changes.	Control determined to be suitably designed.
		A Secure Development Policy defines the requirements for secure software and system development and maintenance.	Control determined to be suitably designed.

Criteria Number	Trust Services Criteria	Description of Trace Machina, Inc.'s Controls	Result
RISK MITIGATION			
CC 9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Business Continuity and Disaster Recovery Policy governs the required processes for restoring the service or supporting infrastructure after suffering a disaster or disruption.	Control determined to be suitably designed.
		An Incident Response Plan outlines the process of identifying, prioritizing, communicating, assigning, and tracking confirmed incidents through to resolution.	Control determined to be suitably designed.
		A Risk Assessment and Treatment Policy governs the process for conducting risk assessments to account for threats, vulnerabilities, likelihood, and impact with respect to assets, team members, customers, vendors, suppliers, and partners. Risk tolerance and strategies are also defined in the policy.	Control determined to be suitably designed.
		Formal risk assessments are performed, which include the identification of relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	Control determined to be suitably designed.
		A risk register is maintained, which records the risk mitigation strategies for identified risks, and the development or modification of controls consistent with the risk mitigation strategy.	Control determined to be suitably designed.
CC 9.2	The entity assesses and manages risks associated with vendors and business partners.	A Vendor Risk Management Policy defines a framework for the onboarding and management of the vendor relationship lifecycle.	Control determined to be suitably designed.
		Vendor SOC 2 reports (or equivalent) are collected and reviewed on at least an annual basis.	Control determined to be suitably designed.
ADDITIONAL CRITERIA FOR AVAILABILITY			
A 1.1	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.	System tools monitor for uptime and availability based on predetermined criteria.	Control determined to be suitably designed.
		The system is configured for high availability to support continuous availability, when applicable.	Control determined to be suitably designed.
A 1.2	The entity authorizes, designs, develops acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.	System tools monitor for uptime and availability based on predetermined criteria.	Control determined to be suitably designed.
		The system is configured for high availability to support continuous availability, when applicable.	Control determined to be suitably designed.
		Full backups are performed and retained in accordance with the Business Continuity and Disaster Recovery Policy.	Control determined to be suitably designed.

Criteria Number	Trust Services Criteria	Description of Trace Machina, Inc.'s Controls	Result
		Formal risk assessments are performed, which include the identification of relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	Control determined to be suitably designed.
		Vendor SOC 2 reports (or equivalent) are collected and reviewed on at least an annual basis.	Control determined to be suitably designed.
A 1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	Business Continuity and Disaster Recovery Policy governs the required processes for restoring the service or supporting infrastructure after suffering a disaster or disruption.	Control determined to be suitably designed.
		Backed-up data is restored to a non-production environment at least annually to validate the integrity of backups.	Control determined to be suitably designed.
		The Business Continuity and Disaster Recovery Plan is periodically tested via tabletop exercises or equivalents. When necessary, Management makes changes to the Business Continuity and Disaster Recovery Plan based on the test results.	Control determined to be suitably designed.
ADDITIONAL CRITERIA FOR CONFIDENTIALITY			
C 1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	Business Continuity and Disaster Recovery Policy governs the required processes for restoring the service or supporting infrastructure after suffering a disaster or disruption.	Control determined to be suitably designed.
		Procedures are in place to retain customer data based on agreed-upon customer requirements or in line with information security policies.	Control determined to be suitably designed.
		Access to, erasure of, or destruction of customer data is restricted to personnel that need access based on the principle of least privilege.	Control determined to be suitably designed.
		A Data Classification Policy details the security and handling protocols for sensitive data.	Control determined to be suitably designed.
		A Data Retention and Disposal Policy specifies how customer data is to be retained and disposed of based on compliance requirements and contractual obligations.	Control determined to be suitably designed.
		Company endpoints are managed and configured with a strong password policy, anti-virus, and hard drive encryption.	Control determined to be suitably designed.
C 1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	Procedures are in place to retain customer data based on agreed-upon customer requirements or in line with information security policies.	Control determined to be suitably designed.
		Upon customer request, the Company requires that data that is no longer needed from databases and other file stores be removed in accordance with agreed-upon customer requirements.	Control determined to be suitably designed.
		A Data Classification Policy details the security and handling protocols for sensitive data.	Control determined to be suitably designed.
		A Data Retention and Disposal Policy specifies how customer data is to be retained and disposed of based on compliance requirements and contractual obligations.	Control determined to be suitably designed.