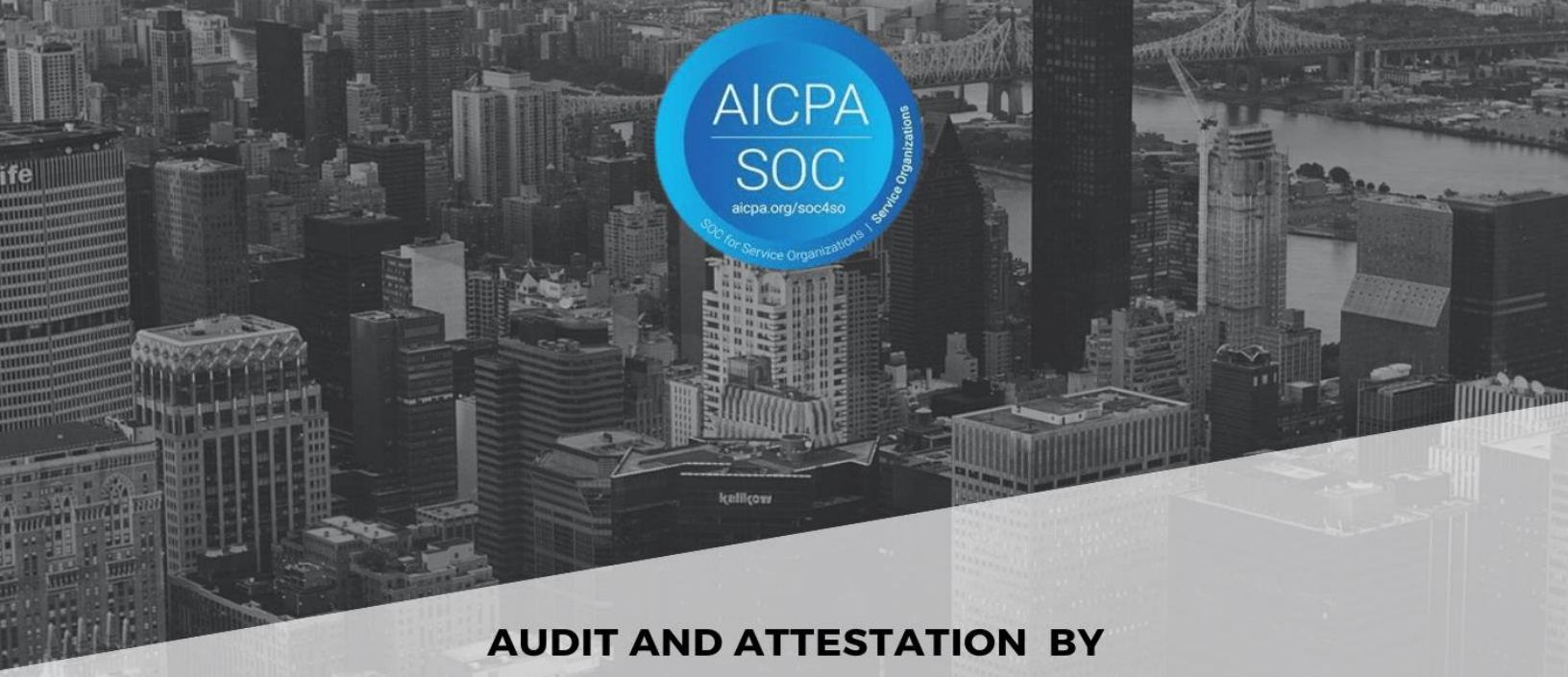
January 6, 2023 to July 6, 2023

Keebo Inc

SOC 3 Report

An Independent Service Auditor's Report on Controls Relevant to Security



AUDIT AND ATTESTATION BY

PRESCIENT ASSURANCE

CPA

Prescient Assurance LLC.
1100 Market Street Suite 600
Chattanooga, TN 37402

www.prescientassurance.com
info@prescientassurance.com
+1 646 209 7319

Table of Contents

SECTION 1

Management's Assertion

Management's Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within Keebo Inc's system (the system) throughout the period January 6, 2023, to July 6, 2023, to provide reasonable assurance that Keebo Inc's service commitments and system requirements relevant to Security were achieved. Our description of the boundaries of the system is presented in Attachment A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of controls within the system throughout the period January 6, 2023, to July 6, 2023, to provide reasonable assurance that Keebo Inc's service commitments and system requirements were achieved based on the trust services criteria relevant to Security (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). Keebo Inc's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Attachment B.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

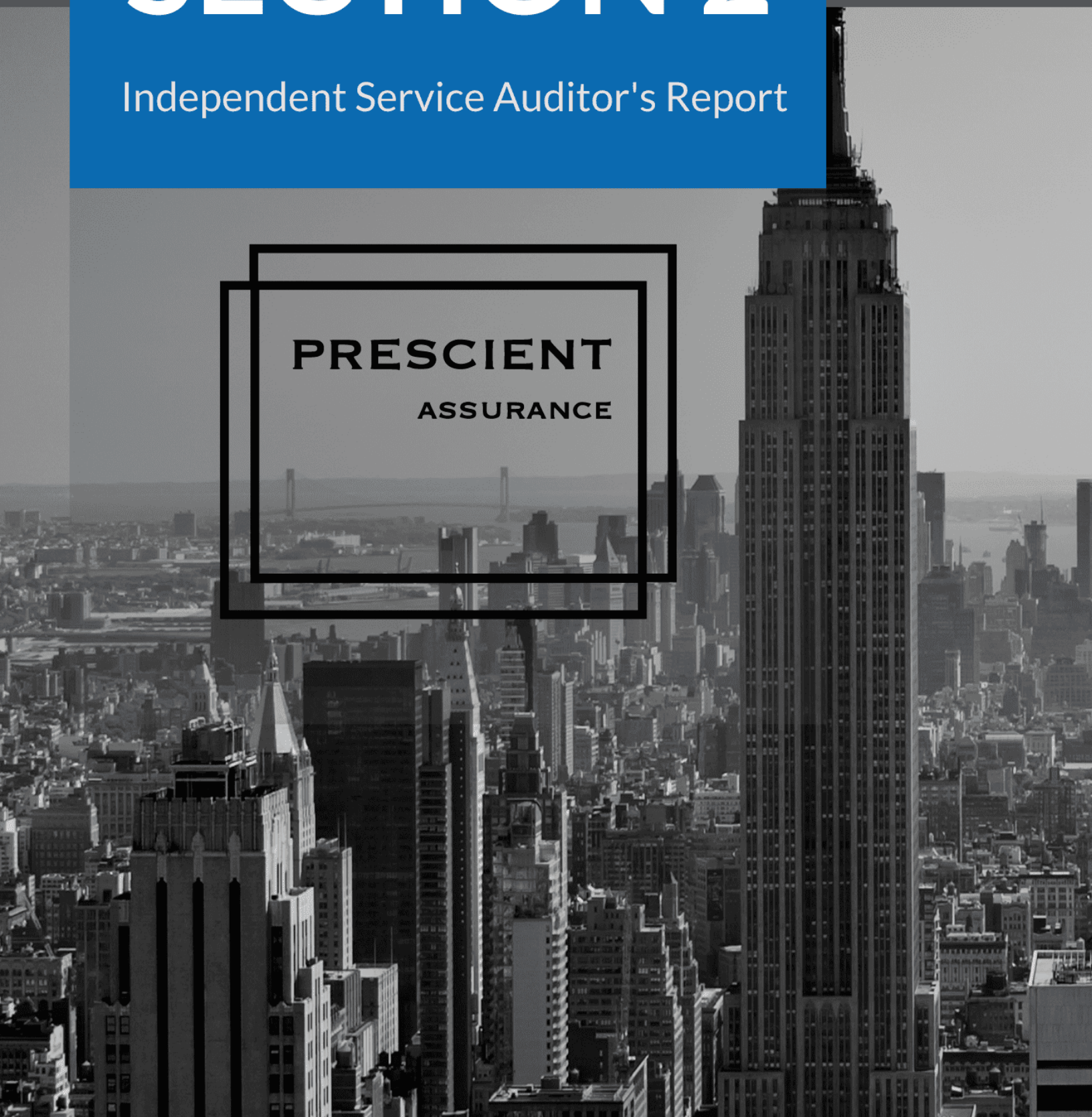
We assert that the controls within the system were effective throughout the period January 6, 2023, to July 6, 2023, to provide reasonable assurance that Keebo Inc's service commitments and system requirements were achieved based on the applicable trust services criteria.

DocuSigned by:
Nicholas Richardson
8F7A13438DB2402...

Nicholas Richardson
VP of Engineering
Keebo Inc

SECTION 2

Independent Service Auditor's Report



Independent Service Auditor's Report

To: Keebo Inc

Scope

We have examined Keebo Inc's (Keebo Inc) accompanying assertion in Section I, titled "Management's Assertion that the controls within Keebo Inc's system were effective throughout the period January 6, 2023, to July 6, 2023, to provide reasonable assurance that Keebo Inc's service commitments and system requirements were achieved based on the trust services criteria relevant to Security (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

Keebo 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 Keebo Inc's service commitments and system requirements were achieved. In Section I, Keebo Inc has provided the accompanying assertion about the effectiveness of the controls within the system. When preparing its assertion, Keebo Inc is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the controls are not effective to achieve Keebo Inc's service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Keebo Inc's service commitments and system requirements based on the applicable trust services criteria

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

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

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risks that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Keebo Inc's system were effective throughout the period January 6, 2023, to July 6, 2023, to provide reasonable assurance that Keebo Inc's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

DocuSigned by:
John D Wallace
F5ADFA3569EA450...

John D. Wallace, CPA
Chattanooga, TN
July 13, 2023

ATTACHMENT A

System Description

DC 1: Company Overview and Types of Products and Services Provided

We are a SaaS provider of cloud data services built on top of automatic data learning models (AI/ML). Aimed at simplifying data warehouse management. Using data learning we optimize your warehouses both to save money, and to speed up your queries, additionally, we provide increased visibility into your data workload patterns.

DC 2: The Principal Service Commitments and System Requirements

Keebo Inc designs its processes and procedures to meet the objectives of our board and our customers. Those objectives are based on the service commitments that Keebo Inc makes to user entities, the laws and regulations that govern the provision of services, and the financial, operational, and compliance requirements that Keebo Inc has established for the services. The platform of Keebo Inc is subject to the federal and state privacy and security laws and regulations in the jurisdictions in which Keebo Inc operates.

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. The Privacy Policy and Terms and Conditions can be found at Keebo Inc. Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of the platform 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.
- Maintain commercially reasonable administrative, technical, and organizational measures that are designed to protect customer data processed.
- Encryption of data at rest and in transit.
- Maintain security procedures that are consistent with applicable industry standards.
- Document and enforce confidentiality agreements with third parties prior to sharing confidential data.
- Review documentation from third-party providers to help ensure that they are in compliance with security and confidentiality policies.
- Maintain business continuity and disaster recovery programs.
- Restrict system access to authorized personnel only.
- Regularly assess security programs and processes.
- Identification and remediation of security incidents/events.

Keebo Inc establishes systems and operational requirements that support the achievement of service commitments, relevant laws and regulations, and other security and privacy requirements. Such requirements are communicated in Keebo Inc's Terms and Conditions (https://keebo.ai/trial-terms-of-use/) 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 platform.

Support SLA

Severity	Response Time
Severity 1, Critical: • Access to Keebo Inc platform in production is down. • Production APIs/microservice is down or severely impacted such that routine operation is impossible. More than 50% of containers and hosts in the application are in an unhealthy state.	Within 1 business hours
Severity 2, High: • Production issue where the system is functioning but in degraded or restricted capacity. • At least 25% of containers and hosts in the application are in an unhealthy state.	Within 2 hours during business hours
Severity 3, Medium: • Production issue where minor functionality is impacted or a development issue.	Within 4 hours during business hours
Severity 4, Low: • Request for information with no impact to business operations	Within 3 business days

DC 3: The Components of the System Used to Provide the Services

Primary Infrastructure

Primary Infrastructure		
Hardware	**Type**	**Purpose**
GCP	Load Balancers Cloud Run API Gateway	Allow for the servicing, processing, and directing of network traffic and data.
GCP	IAM	Allow the management of user accounts internally.
GCP	VPC Firewalls, Network Services Load Balancing	Protects the network traffic against denial of service and web attacks.
GCP	Cloud Storage Buckets	Cloud-hosted storage solution with encryption capabilities used to store objects created during development and business operations i.e. artifacts, backups, and authentication files.
GCP	Cloud Logging Audit Logs	Used for monitoring network resources, alerting based on preconfigured metric-based alarms, and application logs for all of the services.
GCP	Firestore DB Instances	Used to store user and customer data.
GCP	Firebase Authentication	User for API management and access control
GCP	Artifact Registry	Repository for all product containers
Google Workspace	User Authentication	Used for user management and access control
Github	Codebase & CICD/Pipeline	Codebase used for versioning, testing, and deployment of changes to the environments.
Jira/Confluence	Communication Services	Internal business communications, storage of organizational documents, and project management.

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Drata Compliance Automation Platform	Client/Dashboard	Monitors infrastructure for common vulnerabilities and aids in ensuring compliance.

Primary Software

Primary Software		
Software	**Type**	**Purpose**
NodeJS	Server Side Logic	Web application framework used to power backend services such as APIs
Firestore NoSQL DB	Database	Transactional database for customer login data
Cloud Pub/Sub	Functions	Queue management software for job queue.
Airflow/Composer	Job management	Batch job management
Angular	Frontend UI	Front end UI
Postgres	Database	Transactional database for customer deployments
Java	Server Side Logic	Primary development language/runtime for all applications
Python	Model Logic	Primary development language for ML models

People

Keebo Inc has a staff of approximately 14 full time, 3 contractors and 3 part-time employees organized in the following functional areas:

- **Management:** Individuals who are responsible for enabling other employees to perform their jobs effectively and for maintaining security and compliance across the environment.
- **Product Development:** Product managers and software engineers who design and maintain the platform, including the web interface, the APIs, the databases, and the integrations with data sources. This team designs and implements new functionality, assesses, and remediates any issues or bugs found in the platform, and architects and deploys the underlying cloud

infrastructure on which the platform runs. Members of the product team are responsible for peer reviews of code and infrastructure designed and authored within the team.

- **Sales:** Sales provides active sales development activities for new customers and trial customers to develop Keebo's customer base
- **Marketing:** Employees or outsourced Individuals responsible for providing ongoing marketing of Keebo's products and services

Security Processes and Procedures

The company employs a set of procedures in order to obtain its objectives for network and data security. These procedures are executed by qualified and experienced team members. Procedures are in place in the following areas:

- Keebo Inc's backend application runs in Google Cloud Platform on Kubernetes utilizing Google's Storage and Database services, and local Postgres instances.
- Each platform instance (production, customer test, Quality Assurance "QA") is contained within a separate Keebo utilizes Local, Staging, Demo, and Production environments. The project infrastructure provides granular access control to all aspects of the infrastructure. Access from external locations is controlled through configuration and firewall rules. Access to internal components of the platform is only possible via MFA-controlled access utilizing Secure Shell ("SSH") protocol. Access is granted on a project and component within each project (i.e., pods, storage, and database) basis.
- Data is persisted in Bigquery within GCP, and Postgres within Kubernetes clusters. These systems utilize Advanced Encryption Standard ("AES") 256 encrypted disks for all data stored at rest. Each customer instance in production establishes a database and data storage bucket that is allocated for use solely for that customer. Customer data is never co-mingled in the application.
- User entities access their instance using standard web browsers utilizing Transport Layer Security ("TLS") 1.2 or above for encrypted communications.
- *Security Policy Administration:* The company's policies concerning various security, availability, processing integrity, confidentiality, and privacy matters are reviewed at least annually by the Security Team.
- *Risk Assessment:* At least annually the VP of Engineering, Development, Security, and IT Teams collaborate on an overall risk assessment for the company and the system.
- *Communication:* The company opportunistically and continually uses a mixture of intranet services, email, and in-person meeting opportunities for the communication of security policies and procedures. Regular confirmation of this communication is captured in annual attestations from each team member that they have read general internal policies.
- *Logical Access:* All team members must have unique credentials as well as established authorization to access the Company's information assets. Access to systems and information is restricted based on the responsibilities of the individual and their role.
- *Change Management:* The company has a Software Development Life Cycle Policy. The policy covers the planning, assignment, development, design, code review, impact considerations, infrastructure assignments, quality assurance, security testing, implementation, and maintenance of both the system software and infrastructure.

Data

There are three major types of data used by Keebo Inc: Configuration Data, Customer Data, and Log Data. Other types of data include: Service data, Data in transit, Data at rest, and Usernames and Passwords.

Principal Data Types	
Data Types	**Protection and Breach Notification during the lifecycle of Data**
Configuration Data: Data used to configure the system	Configuration Data is stored in and includes credentials for accessing web-based software applications, including usernames and passwords; the names of databases, schema, tables, columns, custom objects, and custom fields; and models stored by customers to provide custom analysis views, and routines in the web-based software application.
Customer Data: Data owned by Keebo Inc's customers that is copied from edge compute devices to web-based software application	Customer Data is stored. It is encrypted both in-transit and at-rest and is protected with daily backups/versioning controls. Only authorized Keebo Inc operators are permitted to access customer data and only for justifiable business use cases, such as debugging failures or other operational issues.
Log Data: Logs produced by the system	Log Data is produced by the various services to make it easier for Keebo Inc operators to monitor the health of the system and track down any issues. Log data may be stored by vendors that Keebo Inc has entrusted for purposes like indexing, monitoring, and trending. Log data is retained for 30 days for log data.
Service Data	Service Data is user and account metadata, troubleshooting, accounts receivable and billing, and related information necessary for the company to know in order to service accounts and provide the service.
Data in transit	To protect data in transit between our app and our servers, Keebo Inc'supports the latest recommended secure cipher suites to encrypt all traffic in transit, including the use of TLS 1.2 protocols, AES256 encryption, and SHA2 signatures, whenever supported by the clients.
Data at rest	Data at rest in Keebo Inc's production network is encrypted using industry-standard 256-bit Advanced Encryption Standard (AES256), which applies to all types of data at rest within Keebo Inc's systems—relational databases, file stores, database backups, etc.
Usernames and passwords	Keebo Inc encrypts customer usernames and passwords used to access the Keebo Inc platform using cryptographic hash functions.

Third Party Access

Third Party Access	
Name of Third Party/ Vendor	**Type of Access and Connectivity to Keebo Inc data**
N/A	N/A

System Boundaries

There are no business processes not within the boundaries of the description of the system in scope.

DC 4: Disclosures About Identified Security Incidents

Name of incident	Timing	Impact
N/A	N/A	N/A

DC 5: The Applicable Trust Services Criteria and the Related Controls Designed to Provide Reasonable Assurance that the Service Organization's Service Commitments and System Requirements were Achieved

Integrity and Ethical Values

Keebo Inc uses its Code of Conduct, which is read and signed by all employees as part of the onboarding process, to define and lay out our values. Keebo Inc has also instituted a number of technical controls to prevent and disincentivize illegal and unethical actions by Keebo Inc employees. These controls include but are not limited to:

- Limiting access to confidential information based on clearly defined roles and following the principle of least privilege.
- Rigorously upholding the standards of ethical behavior laid out in our Code of Conduct especially as they pertain to discrimination and harassment of any kind.
- Performing background checks on domestic employees as part of the hiring process.
- Protecting and valuing individuals who bring concerns to the attention of Keebo Inc management.

Use of NDAs to prevent the disclosure of confidential information to unauthorized parties.

Commitment to Competence

Keebo Inc'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 have been 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.
- The company periodically provides training to its new hires

Management's Philosophy and Operating Style

Keebo Inc S management team is committed to creating a productive and encouraging work environment as well as providing a secure product to our customers and users. To accomplish this Keebo Inc has instituted a number of processes:

- A rigorous QA program ensuring that development on the Keebo Inc application meets industry security standards.
- Meetings are held between managers on a weekly basis to prioritize objectives and tasks.
- Employees are encouraged to reach out to each other when facing obstacles.
- Weekly team meetings where any concerns or challenges are shared

Organizational Structure and Assignment of Authority and Responsibility

During normal operations Keebo Inc has a simple organizational structure. Employees report directly to the CEO or VP of Engineering who ultimately provide direction. Keebo Inc has clearly defined job descriptions and as the organization grows, we have in place roles and responsibilities which will allow for dissemination of managerial responsibilities as necessary. Keebo Inc has taken the following steps to achieve this goal:

- Regularly updated organization chart fully accessible by employees.
- Responsibilities of roles are clearly defined in policies and job descriptions.

Human Resource Policies and Practices

Keebo Inc consistently strives to hire and retain the most qualified individuals for the job. To meet this goal, Keebo Inc has in place onboarding requirements and a Human Resource Security Policy which cover employee security training, performance reviews, competency assessments, and the terms of employment.

Specifically, Keebo Inc has the following controls in place:

- Bi-Annual Performance Reviews
- Annual employee security training
- New employees are required to sign a non-disclosure or confidentiality agreement.
- Clearly defined disciplinary process
- A "New Employee Checklist" or "30/60/90 Plan" which is given to new hires and is fully accessible to all Keebo Inc employees

Lastly, Keebo Inc recognizes that policies and procedures often need to change to serve the needs of the organization. To accomplish this, all security procedures are reviewed at least annually.

Security Management

Keebo Inc uses a VP of Engineering who is responsible for the management of information security throughout the organization. This individual and their team maintains security credentials, performs the technical onboarding/off-boarding work, and updates, maintains, and annually signs to acknowledge their review of the information security policies. They are responsible for enforcing the information security policies, configuring, monitoring, and maintaining preventative, corrective, and detective controls within the Keebo Inc environment, and ensuring user awareness training is conducted.

As the team maintains security, it monitors known incidents and patches as well as results from recent vulnerability assessments and addresses necessary changes to the policies and procedures. Such changes can include a reclassification of data, a reassessment of risk, changes in incident response plans, and a verification of responsibilities for authorizing and monitoring accesses. Changes are reviewed and communicated during weekly IT maintenance meetings, via internal Slack messages, emails, or through system alerts.

During annual security training and awareness programs, management ensures communication of the latest security policies as well as written job descriptions for security management.
Additionally, management is responsible for ensuring business associate agreements are current for third parties and for updating the annual IT risk assessment.

Security Policies

- Acceptable Use Policy
- Asset Management Policy
- Backup Policy
- Business Continuity Policy
- Code of Conduct
- Data Classification Policy
- Data Protection Policy
- Data Retention Policy
- Disaster Recovery Plan
- Encryption Policy
- Incident Management Policy

- Incident Response Plan
- Information Security Policy
- Password Policy
- Responsible Disclosure Policy
- Risk Assessment Policy
- Software Development Lifecycle Policy
- Vendor Management Policy
- Vulnerability Management Policy

Personnel Security

Keebo Inc has several personnel security procedures in place specifically during the onboarding process. These include:

- Background checks for new domestic employees.
- Employees must read and agree to all security policies.
- Roles within the organization have been clearly defined and are reflected in the organizational chart.
- Employees are granted access/authorization based on their role and in accordance with the principle of least privilege.
- Employees are required to sign an NDA.
- Upon hire and annually thereafter security awareness training is completed by all Keebo Inc employees.
- Employees are directed to report any potential security incidents to the IT Manager.

Violations of Keebo Inc Security policies have clearly defined repercussions.

Physical Security and Environmental Controls

Keebo Inc is a fully remote company with no centralized headquarters or physical network. Because of this, physical and environmental security procedures have been deemed unnecessary. There are specific considerations taken, however, regarding remote work and the security risks inherent specific to companies that are fully remote. These can be found in our BYOD policy, our Business Continuity and Disaster Recovery plan, and our Information Security Policy.

Change Management

Keebo Inc's change management procedures are detailed in the Software Development Life Cycle Policy. There are five requirements for all changes to the organization, business processes, information processing facilities, and systems that affect information security in Keebo Inc's production environment. They are as follows:

- The change must include processes for planning and testing of changes, including remediation measures.
- Documented managerial approval and authorization before proceeding with changes that may have a significant impact on information security, operations, or the production platform.

- Advance communication/warning of changes, including schedules and a description of reasonably anticipated effects, provided to all relevant internal and external stakeholders.
- Documentation of all emergency changes and subsequent review.
- A rollback process for unsuccessful deployments must be in place.

System Monitoring

Keebo Inc uses a combination of services to monitor its network and systems. These include GCP Cloud Logging, the Drata Client, Web Application Firewall (WAF) or VPC Firewalls, and GCP Audit Logs.

- GCP Cloud Logging: Used for monitoring of network usage, availability, and overall performance and health of network resources. Also logs metrics for fine-tuning alarms and alerts as usage data is received. GCP Cloud Logging is used in conjunction with GCP Audit Logs to monitor for failed and successful authorization attempts.
- Compliance Automation Platform Client: Compliance Automation Platform allows us to monitor multiple aspects of our attack surface including employee devices (ensuring anti-malware, HDD encryption, etc. are in place), monitoring GCP resources for potential configuration vulnerabilities, and tracking necessary patches/updates.
- GCP Audit Logs: Used to log actions taken by users and services within our GCP account.
- WAF or VPC Firewalls: Provide metrics regarding attempted and successful requests to the application.

Keebo Inc is constantly striving to improve our security monitoring capabilities and uses GCP's documentation on best practices to inform the alarming and logging measures we take.

Incident Management

Keebo Inc's incident response procedures are detailed in its Incident Response Plan. Our primary goals will be to investigate, contain any exploitations, eradicate any threats, recover Keebo Inc'systems, and remediate any vulnerabilities. Throughout this process, thorough documentation will be required as well as a post-mortem report.

Specific steps that Keebo Inc will take are:

- The Security Manager will manage the incident response effort.
- Once an incident is confirmed, all internal correspondence will take place within a dedicated Keebo Inc Slack channel.
- A recurring Incident Response Meeting will be held at regular intervals until the incident is resolved.
- Keebo Inc will inform all necessary parties of the incident without undue delay.

Data Backup and Recovery

Keebo Inc uses Google Workflows to ensure full backup recovery of its database. Keebo Inc has a shared google drive which acts as a backup for any non-system documentation. Access to Keebo Inc databases is heavily restricted using user and role-based authorization controls.

System Account Management

Keebo Inc's access management procedures are documented in its System Access Control Policy. Keebo Inc uses Role-based authorization to control access to its network infrastructure. Keebo Inc uses the principle of least privilege to determine the type and level of access to grant users. A number of standards are in place which Keebo Inc uses when granting access to its systems:

- Technical access to Keebo Inc networks must be formally documented.
- Background checks will be performed on domestic persons granted access to Keebo Inc networks.
- Only authorized Keebo Inc employees and third parties working off a signed contract or statement of work, with a business need, shall be granted access to the Keebo Inc production network.

With regards to access provisioning, Keebo Inc uses the following controls:

- New employees and/or contractors are not to be granted access to any Keebo Inc production systems until after they have completed all HR onboarding tasks, which includes receiving and passing a background check (as applicable), review and signing of all company policies, signing of Keebo Inc's NDA, and completion of cybersecurity awareness training.
- Access is restricted to only what is necessary to perform job duties.
- No access may be granted earlier than the official employee start date to anything other than email, which may be granted up to 72 hours prior to the start date to aid in first-day onboarding.
- Access requests and rights modifications beyond initial setup shall be documented in an access request ticket, slack channel, or email. No permissions shall be granted without approval from the system/data owner or management.
- Records of all permission and privilege changes shall be maintained for no less than one year.
- Access rights of users must be removed promptly within 72 hours of notification being given to the IT Manager.
- If current access rights are no longer needed due to transfer or change of role, termination of those rights must be performed promptly within 72 hours of notification being given to the IT Manager.

Risk Management Program

Data Classification

Keebo Inc has four classifications for the data it uses, processes, and produces. The classifications are:

- Confidential
- Restricted
- Public
- Internal Use

Confidential Data is sensitive business information and the level of protection is dictated internally by Keebo Inc. Examples include:

- PII
- Customer Data
- Keebo Inc financial and banking data
- Incident Reports
- Risk Assessment Reports
- Technical Vulnerability Reports
- Secret and Private Keys
- Source Code

Restricted Data is defined as proprietary information requiring thorough protection. Access to this data is restricted to employees on a "need-to-know" basis. Approval is required for distribution. Examples include:

- Internal Policies
- Legal Documents
- Internal Reports
- Slack Messages
- Emails
- Contracts
- Bug Reports and Maintenance

Public Data is defined as: Documents intended for public consumption which can be freely distributed outside of Keebo Inc. Examples include:

- Marketing Materials
- Product Descriptions
- Release Notes
- External Facing Policies

Internal Use Data is information originating within or owned by Keebo Inc or entrusted to it by others. Internal Use information may be shared with authorized employees, contractors, and business partners who have a business need, but may not be released to the general public, due to the negative impact it might have on the company's business interests. By default, all data that is not explicitly classified as Restricted, Confidential, or Public data should be treated as Internal Use data.

Risk Management Responsibilities

Keebo Inc's Risk Assessment Policy details the primary responsibilities.

Role	Responsibility
CEO	Ultimately responsible party for the acceptance and/or treatment of any risks to the organization.

VP of Engineering	Can approve the avoidance, remediation, transference, or acceptance of any risk cited in the Risk Register. This person shall be responsible for communicating risks to top management and the board and adopting risk treatments in accordance with the executive direction.
VP of Engineering or Security Officer	Shall be responsible for adherence to the Risk Management Policy.

Risk Management Program Activities

On a practical level, Keebo Inc's Risk Management process involves 3 stages:

- Identification of risks
- Assessment of their potential impact
- Keebo Inc's risk treatment towards the risk

Identification of risks involves categorization and investigation. Examples of categories used are

- Technical
- Legal
- Human Resources
- Information Security
- Finance
- Sales

The risk assessment focuses on the likelihood and potential impact of risks to Keebo Inc. Likelihood can be assessed as not likely, somewhat likely, or very likely. Impact can be assessed as not impactful, somewhat impactful, and very impactful. These factors together will give an overall risk ranking. Keebo Inc's stance towards any given risk is based on the assessment described above. Where Keebo Inc chooses a risk response other than "Accept," it shall develop a Risk Treatment Plan. Keebo Inc's stance will fall into one of the following categories:

- **Mitigate:** Keebo Inc may take actions or employ strategies to reduce the risk.
- **Accept**: Keebo Inc may decide to accept and monitor the risk at the present time. This may be necessary for some risks that arise from external events.
- **Transfer**: Keebo Inc may decide to pass the risk on to another party. For example, contractual terms may be agreed to ensure that the risk is not borne by Keebo Inc, or insurance may be appropriate for protection against financial loss.
- **Eliminate**: The risk may be such that Keebo Inc could decide to cease the activity or to change it in such a way as to end the risk.

Keebo Inc'sdetails our key business processes and critical services.

Risk Assessment

Keebo Inc's Risk Assessment process takes into account a number of factors each of which contributes to both the likelihood and potential impact of a given risk. These include:

- The criticality of potentially impacted business processes as laid out in the Business Continuity and Disaster Recovery Plan.
- Whether a risk could potentially impact the confidentiality, availability, integrity, or privacy of customer data or PII.
- Potential monetary loss.
- The ability of the risk to impact Keebo Inc's business objectives.
- Potential impact to Keebo Inc customers or vendors.

Keebo Inc uses Risk Treatment Plans for any response to risks other than "Accept."

Risk Analysis

Keebo Inc's Risk Analysis Method is as follows:

	RISK = LIKELIHOOD * IMPACT	LIKELIHOOD		
		Very likely: 3	Somewhat likely: 2	Not likely: 1
IMPACT	Very impactful: 3	9	6	3
	Somewhat impactful: 2	6	4	2
	Not impactful: 1	3	2	1

RISK LEVEL	RISK DESCRIPTION
Low (1-2)	A threat event could be expected to have a limited adverse effect on organizational operations, mission capabilities, assets, individuals, customers or other organizations.
Moderate (3)	A threat event could be expected to have a serious adverse effect on organizational operations, mission capabilities, assets, individuals, customers or other organizations
High (7-9)	A threat event could be expected to have a severe adverse effect on organizational operations, mission capabilities, assets, individuals, customers or other organizations.

IMPACT LEVEL	IMPACT DESCRIPTION
Not impactful (1)	A threat event could be expected to have a limited adverse effect, meaning: degradation of mission capability yet primary functions can still be performed; minor damage; minor financial loss; or range of effects is limited to some cyber resources but no critical resources.
Somewhat impactful (2)	A threat event could be expected to have a serious adverse effect, meaning: significant degradation of mission capability yet primary functions can still be performed at a reduced capacity; minor damage; minor financial loss; or range of effects is significant to some cyber resources and some critical resources.
Very impactful (3)	A threat event could be expected to have a severe or catastrophic adverse effect, meaning: severe degradation or loss of mission capability and one or more primary functions cannot be performed; major damage; major financial loss; or range of effects is extensive to most cyber resources and most critical resources.

LIKELIHOOD LEVEL	LIKELIHOOD DESCRIPTION
Not likely (1)	Adversary is unlikely to initiate a threat event; non-adversarial threat event (e.g., nature, error, accident) is unlikely to occur; or threat is unlikely to have adverse impacts.
Somewhat likely (2)	Adversary is somewhat unlikely to initiate a threat event; non-adversarial threat event (e.g., nature, error, accident) is somewhat unlikely to occur; or threat is somewhat unlikely to have adverse impacts.
Very likely (3)	Adversary is highly likely to initiate a threat event; non-adversarial threat event (e.g., nature, error, accident) is highly likely to occur; or threat is highly likely to have adverse impacts.

Risk Response

In accordance with Keebo Inc's , risks will be prioritized and mapped according to the descriptions listed above. The following responses to risk should be employed. Where Keebo Inc chooses a risk response other than "Accept," it shall develop a risk treatment plan.

- Mitigate: Keebo Inc may take actions or employ strategies to reduce the risk.
- Accept: Keebo Inc may decide to accept and monitor the risk at the present time. This may be necessary for some risks that arise from external events.

- Transfer: Keebo Inc may decide to pass the risk on to another party. For example, contractual terms may be agreed to ensure that the risk is not borne by Keebo Inc, or insurance may be appropriate for protection against financial loss.

- Eliminate: The risk may be such that Keebo Inc could decide to cease the activity or to change it in such a way as to end the risk.

Integration with Risk Assessment

Keebo Inc is committed to handling and remediating risks inherent in any commitments, agreements, or responsibilities it may enter into or take on during the operation of the company. Due to the nature of these risks it may be necessary for Keebo Inc to develop specialized controls. Keebo Inc takes into account all relevant factors; contractual, legal, and regulatory when designing these controls. Keebo Inc S Head of Engineering has the final say on the design and implementation of these controls.
In general, Keebo Inc's Risk Assessment procedure is still applicable to risks inherent in Keebo Inc S commitments and contractual responsibilities and should be applied to determining the severity of risks.

Information and Communications Systems

Keebo Inc uses Slack, Gmail for restricted internal communications. Keebo Inc also uses video conferencing tools and a company Gmail for both internal and external communications.
For workflow, project management, and sharing of internal documents Keebo Inc uses Google Docs, Jira, and Confluence.

Data Communication

All traffic within the network is redirected from HTTP to HTTPS. Access Control to the production code base is limited via the following controls:

- The production code branch is protected, requiring a merge request and approval before any changes can be made. This also protects the branch from being deleted.
- RBAC approach is used for accessing the application code repository.
- All default regular-user accounts have been removed.

Monitoring Controls

Keebo Inc takes a dual approach to continuous monitoring using both internal monitoring and relying on third parties.

Internal Monitoring

Keebo Inc has a highly interconnected business process allowing for visibility and insight by management into the operations of each department. Corrective action is initiated through direct conference calls. Within departments, code reviews and Keebo Inc's quality assurance program help ensure internal controls are being followed and implemented.

Third Party Monitoring

Keebo Inc contracts a third party to perform annual penetration tests and uses the Drata client to monitor for new vulnerabilities. The process for reporting of any deficiencies with regards to Keebo Inc policies and procedures is clearly spelled out in each relevant policy.

DC 6: Complementary User Entity Controls (CUECs)

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

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.

- User entities are responsible for understanding and complying with their contractual obligations to Keebo Inc.
- User entities are responsible for notifying Keebo Inc of changes made to technical or administrative contact information.
- User entities are responsible for maintaining their own system(s) of record.
- User entities are responsible for ensuring the supervision, management, and control of the use of Keebo Inc's services by their personnel.
- User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Keebo Inc's services.
- User entities are responsible for immediately notifying Keebo Inc of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.

The user entity controls presented should not be regarded as a comprehensive list of all controls that should be employed by user entities. Management of user entities are responsible for the following:

Trust Services Criteria	Complementary User Entity Controls
CC2.1	User entities are responsible for the security and integrity of data housed under user entity control, particularly the data utilized by Keebo Inc's systems and services.

CC6.2	Determination of personnel who need specific functionality and the granting of such functionality is the responsibility of authorized personnel at the user entity. This includes allowing access to Keebo Inc's application keys and API keys for access to the web service API.
CC6.3	Authorized users and their associated access are reviewed periodically.
CC6.6	User entities will ensure protective measures are in place for their data as it traverses from user entity to Keebo Inc.
CC6.6	User entities should establish adequate physical security and environmental controls of all devices and access points residing at their operational facilities, including remote employees or at-home agents for which the user entity allows connectivity in order to provide authorized information to Keebo Inc.

DC 7: Complementary Subservice Organization Controls (CSOCs)

Keebo Inc uses Google Cloud Platform as a subservice organization for data center colocation services. Keebo Inc's controls related to their system cover only a portion of the overall internal control for each user entity of the System. The description does not extend to the services provided by the subservice organization that provides colocation services for IT infrastructure. Section 4 of this report and the description of the system only cover the Trust Services Criteria and related controls of the Company and exclude the related controls of GCP.

Although the subservice organization has been "carved out" for the purposes of this report, certain Trust Services Criteria are intended to be met by controls at the subservice organization. Complementary Subservice Organization Controls (CSOCs) are expected to be in place at GCP related to physical security and environmental protection, as well as backup, recovery, and redundancy controls related to availability. GCP physical security controls mitigate the risk of fires, power loss, climate, and temperature variabilities. Management of Keebo Inc receives and reviews the GCP SOC 2 report annually. In addition, through its operational activities, Keebo Inc management monitors the services performed by GCP to determine whether operations and controls expected to be implemented at the subservice organization are functioning effectively. Management also has communication with the subservice organization to monitor compliance with the service agreement, stay abreast of changes planned at the hosting facility, and relay any issues or concerns to GCP management.

It is not feasible for the criteria related to the System to be achieved solely by Keebo Inc. Therefore, each user entity's internal control must be evaluated in conjunction with Keebo Inc's controls and related tests, and results described in Section 4 of this report, considering the related CSOCs expected to be implemented at the subservice organization as described below.

Google Cloud Platform (GCP)

Criteria	Complementary Subservice Organization Controls
CC6.4	GCP is responsible for restricting data center access to authorized personnel.
CC6.4	GCP is responsible for the 24/7 monitoring of data centers by closed circuit cameras and security personnel.
CC7.2	GCP is responsible for the installation of fire suppression and detection, and environmental monitoring systems at the data centers.
CC7.2	GCP is responsible for protecting data centers against disruption in power supply to the processing environment by an uninterruptible power supply.
CC7.2	GCP is responsible for overseeing the regular maintenance of environmental protections at data centers.

DC 8: Any Specific Criterion of the Applicable Trust Services Criteria that is Not Relevant to the System and the Reasons it is Not Relevant

There are no trust services criteria that are not relevant to the system in scope.

DC 9: Disclosures of Significant Changes in Last 1 Year

No significant changes have occurred in the last 1 year.