As of January 25, 2022

System and Organization Controls (SOC) 2 Type 1 Report for

Report on Replicated, Inc.'s description of its Replicated System and on the suitability of the design of its controls relevant to security and confidentiality as of January 25, 2022.

Table of Contents

Section I: Independent Service Auditors Report Provided by Laika Compliance LLC

Section I: Independent Service Auditor's Report Provided by Laika Compliance LLC

To: Replicated, Inc.

Scope

We have examined Replicated's accompanying description of its Replicated System found in Section 3 titled "Replicated's Description of its Replicated System as of January 25, 2022" (description), based on the criteria for a description of a service organization's system set forth in 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 January 25, 2022, to provide reasonable assurance that Replicated's service commitments and system requirements were achieved based on the trust services criteria relevant to security 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).

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

Replicated uses a subservice organization for data center colocation services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Replicated to achieve Replicated's service commitments and system requirements based on the applicable trust services criteria. The description presents Replicated's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Replicated's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

Replicated 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

Replicated's service commitments and system requirements were achieved. In Section 2, Replicated has provided the accompanying assertion titled "Assertion of Replicated, Inc. 's Management" (assertion) about the description and the suitability of design of controls stated therein. Replicated is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the 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 a description of a service organization's system and the suitability of the design of controls involves—

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

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

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual 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 the Replicated System that was designed and implemented as of January 25, 2022, in accordance with the description criteria.

b. The controls stated in the description were suitably designed as of January 25, 2022, to provide reasonable assurance that Replicated'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 and if the subservice organization and user entities applied the complementary controls assumed in the design of Replicated's controls as of that date.

Restricted Use

This report is intended solely for the information and use of Replicated; user entities of the Replicated System as of January 25, 2022, business partners of Replicated subject to risks arising from interactions with the Replicated 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.

- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
- The applicable trust services criteria.
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

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

Laika Compliance LLC

Arlington, Virginia
February 10, 2022

Section II: Assertion of Replicated, Inc.'s Management

Section II: Assertion of Replicated Inc.'s Management

We have prepared the accompanying description of the Replicated System "Replicated's Description of its Replicated System as of January 25, 2022" (description), based on the criteria for a description of a service organization's system set forth in 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 Replicated System that may be useful when assessing the risks arising from interactions with the Replicated System, particularly information about system controls that Replicated 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 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).

Replicated uses a subservice organization for data center colocation services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Replicated, to achieve Replicated's service commitments and system requirements based on the applicable trust services criteria. The description presents Replicated's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Replicated's controls. The description does not disclose the actual controls at the subservice organization.

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

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

a. The description presents the Replicated System that was designed and implemented as of January 25, 2022, in accordance with the description criteria.

b. The controls stated in the description were suitably designed as of January 25, 2022, to provide reasonable assurance that Replicated'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, and if the subservice organization and user entities applied the complementary controls assumed in the design of Replicated's controls as of that date.

Replicated, Inc.

Section III: Replicated's Description of its Replicated System as of January 25, 2022

Section III: Replicated's Description of its Replicated System as of January 25, 2022

Overview of Operations

Replicated, Inc. ("Replicated" or "the Company") is a software as a service company. Replicated offers the Replicated System, a software as a service application that provides software vendors a container-based platform for quickly deploying cloud native applications inside technical environments, enabling greater security and control.

The system description in this section of the report details the Replicated System. Any other Company services are not within the scope of this report. The accompanying description includes only the policies, procedures, and control activities at the Company and does not include the policies, procedures, and control activities at any subservice organizations (see below for further discussion of the subservice organization).

Service Commitments and System Requirements

Commitments are declarations made by management to customers regarding the performance of the Replicated System. Replicated's Security Page and Data Processing Addendum (DPA) includes the communication of the Company's commitments to its customers. Changes to any commitments are communicated to customers.

System requirements are specifications regarding how Replicated should function to meet the Company's principal commitments to user entities. System requirements are specified in the Company's policies and procedures.

The Company's principal service commitments and system requirements related to the Replicated System include the following:

Trust Services Category	Service Commitments	System Requirements
Security	• Replicated will implement commercially reasonable technical and organisational measures, as further described at the Security Page, that are designed to	• Identity and access control • Security monitoring and reporting • Threat management • Security incident response • Security awareness training

	protect against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data.	• Third party provider controls (vendor risk management) • Change control procedures
Confidentiality	• Replicated will require Replicated's personnel who access Customer Personal Data to commit to protect the confidentiality of Customer Personal Data. • Replicated may engage sub-Processors to Process Customer Personal Data on Customer's behalf.	• Data Retention and Disposal • Data Classification

The Components of the System Used to Provide the Service

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

The components that directly support the services provided to customers are described in the subsections below.

INFRASTRUCTURE

The Company utilizes Amazon Web Services (AWS) to provide the resources to host the Replicated System. The Company leverages the experience and resources of AWS to quickly and securely scale as necessary to meet current and future demand. However, the Company is responsible for designing and configuring the architecture within AWS to ensure security and resiliency requirements are met.

The in-scope hosted infrastructure also consists of multiple supporting tools, as shown in the table below:

Infrastructure		
Production Tool	**Business Function**	**Hosted Location**
Amazon Elasticsearch Service	Analytics	AWS
Amazon RDS	Data Storage	AWS
Amazon Elastic Container Service (ECS)	Container management service	AWS
Amazon Elastic Kubernetes Service (Amazon EKS)	Container management service	AWS
AWS Application Load Balancer (ALB)	Load distribution	AWS
Amazon Simple Storage Solution (S3)	Data Storage	AWS
Virtual Private Cloud (VPC)	Private Cloud	AWS
AWS Security Groups	Network traffic control	AWS
Cloudflare	Content delivery network and web application firewall	Cloudflare

SOFTWARE

Software consists of the programs and software that support the Replicated System. The list of software and ancillary software used to build, support, secure, maintain, and monitor the Replicated System include the following applications, as shown in the table below:

Software	
Production Application	**Business Function**
Detectify	Vulnerability Scanning
Github	Source Code Repository
Okta	Authentication

1Password	Password Manager
Falco	Runtime Security Tool
Cylance	Antivirus/Antimalware for Endpoints
Google	Email and Productivity
Terraform	Configuration Management
DataDog	Logging and Monitoring
Slack	Error and Incident Monitoring and Communication
Shortcut	Ticketing System
Zendesk	Customer Support Ticketing System
Salesforce	CMS for Managing Customer and Support Information

PEOPLE

The Company develops, manages, and secures the Replicated System via separate departments. The responsibilities of these departments are defined in the following table:

People	
Group/Role Name	**Function**
Chief Technology Officer (CTO)	Responsibilities include providing overall direction, guidance, leadership, and support on methods and tools for the implementation of a program that governs the acceptable use of sensitive information in the environment. The CTO will conduct resource and investment planning to implement the management, operational, and technical privacy requirements of the Privacy program.
	Responsibilities include providing overall direction, guidance, leadership, and support for the entire information systems environment while supporting methods and tools for secure storage, retention, and disposal of Confidential & Sensitive Data. The CTO is also guiding annual BCP testing, supporting the

	entire incident response platform and reporting any events that are categorized as breach events to the Risk Committee.
Chief Executive Officer (CEO)	Responsibilities include managing relationships with critical vendors and overseeing the implementation of the Business Contingency Plan. The CEO is also responsible for communications to the client in the event of a significant business disruption.
Risk and Compliance Officer	Responsibilities include chairing the Risk Committee and will provide insight and guidance on the risk posture of the organization directly to the CEO or the Board of Directors. At least twice a year, the Risk and Compliance Officer will provide a report and recommendations to the Executive Committee.
Senior Security Engineer	Responsibilities for this individual include daily operational oversight of all incident response initiatives.
Operations	Responsible for finance and accounting.
Engineering	Responsible for the development, testing, deployment, and maintenance of new code for the Replicated System .
People	Responsible for human resources functions.

The following organization chart reflects the Company's internal structure related to the groups discussed above:

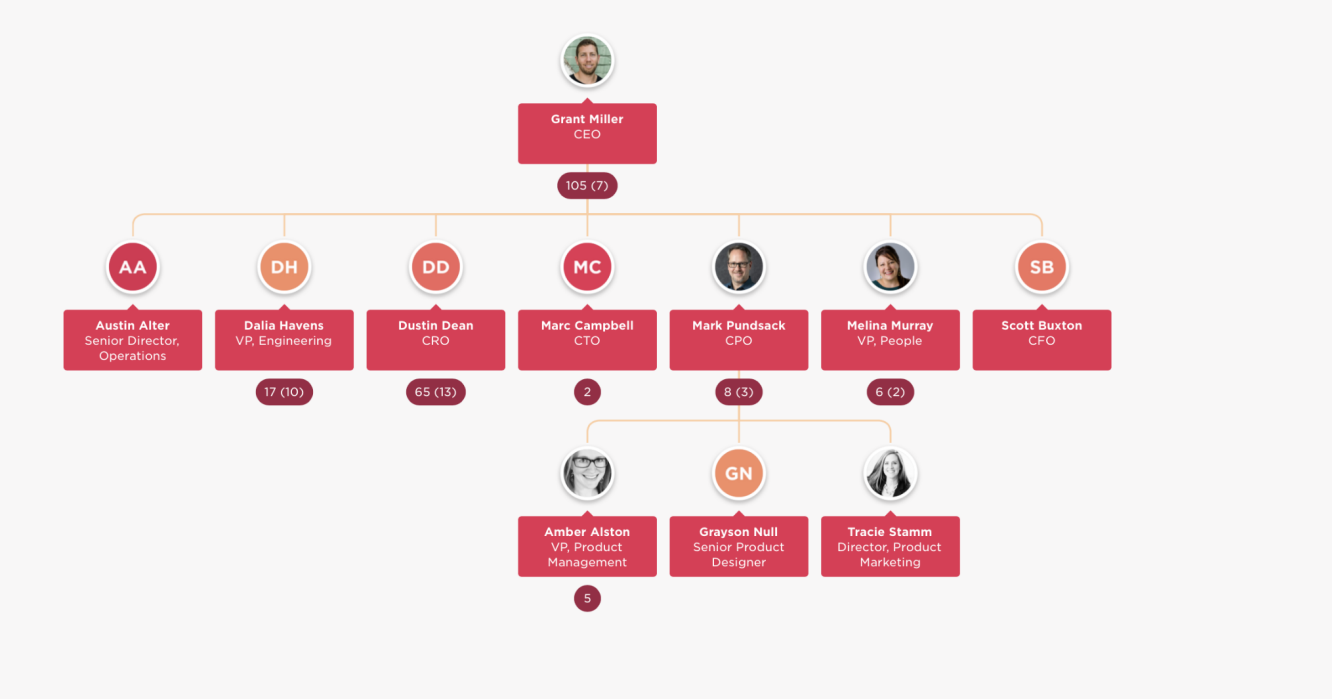

Figure 1: Replicated Organization Chart

PROCEDURES

Procedures include the automated and manual procedures involved in the operation of the Replicated System. Procedures are developed and documented by the respective teams for a variety of processes. These procedures are drafted in alignment with the overall information security policies and are updated and approved as necessary for changes in the business, but no less than annually.

The following table details the procedures as they relate to the operation of Replicated System:

Procedure	Description
Logical and Physical Access	How the Company restricts logical and physical access, provides and removes that access, and prevents unauthorized access.
System Operations	How the Company manages the operation of the system and detects and mitigates processing deviations, including logical and physical security deviations.

Configuration and Change Management	How the Company identifies the need for changes, makes the changes using a controlled change management process, and prevents unauthorized changes from being made.
Risk and Compliance	How the entity identifies, selects, and develops risk mitigation activities arising from potential business disruptions and the use of vendors and business partners.
Data Backup and Storage	How the Company manages data backups to allow for data restorations to occur if needed.
Business Continuity and Disaster Recovery (BC/DR)	How the Company identifies the steps to be taken in the event of a disaster to help resume business operations.
Data Classification and Handling	How the company classifies data included in the service and the procedures for handling the data.
Incident Response Plan	How the company identifies the steps to be taken in the event of a security incident.

DATA

Data refers to transaction streams, files, data stores, tables, and output used or processed by the Company. Through the application programming interface (API), the customer or end-user defines and controls the data they load into and store in the Replicated System production network. Once stored in the environment, the data is accessed remotely from customer systems via the Internet.

Customer data is managed, processed, and stored in accordance with relevant data protection and other regulations and with specific requirements formally established in client contracts.

The Company has deployed secure methods and protocols for transmission of confidential or sensitive information over public networks. Database's housing sensitive customer data are encrypted at rest.

SYSTEM INCIDENTS

There were no identified significant system incidents that (a) were the result of controls that were not suitably designed or operating effectively to achieve one or more of the service commitments and system requirements or (b) otherwise resulted in a significant failure in the achievement of one or more of those service commitments and system requirements as of January 25, 2022.

The Applicable Trust Services Criteria and Related Controls

APPLICABLE TRUST SERVICES CRITERIA

The Trust Services Categories that are in scope for the purposes of this report are as follows:

- **Security:** Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the confidentiality of information or systems and affect the entity's ability to meet its objectives.
- **Confidentiality:** Information designated as confidential is protected to meet the entity's objectives.

Many of the criteria used to evaluate a system are shared amongst all categories; for example, the criteria related to risk assessment apply to the security and confidentiality categories. As a result, the criteria for the security and confidentiality categories are organized into (a) the criteria that are applicable to all categories (common criteria) and (b) criteria applicable only to a single category. The common criteria constitute the complete set of criteria for the security category. For the categories of security and confidentiality , a complete set of criteria is comprised of all the common criteria and all the criteria applicable to the category being reported on.

The common criteria are organized as follows:

1. Control environment: The criteria relevant to how the entity is structured and the processes the entity has implemented to manage and support people within its operating units. This includes criteria addressing accountability, integrity, ethical values, qualifications of personnel, and the environment in which they function.

2. Communication and information: The criteria relevant to how the entity communicates its policies, processes, procedures, commitments, and requirements to authorized users and other parties of the system and the obligations of those parties and users to the effective operation of the system.

3. Risk assessment: The criteria relevant to how the entity (i) identifies potential risks that would affect the entity’s ability to achieve its objectives, (ii) analyzes those risks, (iii) develops responses to those risks including the design and implementation of controls and other risk mitigating actions, and (iv) conducts ongoing monitoring of risks and the risk management process.

4. Monitoring activities: The criteria relevant to how the entity monitors the system, including the suitability and design and operating effectiveness of the controls, and acts to address deficiencies identified.

5. Control activities: The criteria relevant to the actions established through policies and procedures that help ensure that management’s directives to mitigate risks to the achievement of objectives are carried out.

6. Logical and physical access controls: The criteria relevant to how the entity restricts logical and physical access, provides and removes that access, and prevents unauthorized access.

7. System operations: The criteria relevant to how the entity manages the operation of system(s) and detects and mitigates processing deviations, including logical and physical security deviations.

8. Change management: The criteria relevant to how the entity identifies the need for changes, makes the changes using a controlled change management process, and prevents unauthorized changes from being made.

9. Risk mitigation: The criteria relevant to how the entity identifies, selects, and develops risk mitigation activities arising from potential business disruptions and the use of vendors and business partners.

This report is focused solely on the security and confidentiality categories. The Company has elected to exclude the availability, processing integrity, and privacy categories.

CONTROL ENVIRONMENT

INTEGRITY AND ETHICAL VALUES

Replicated places emphasis on ethics and communication within the organization. Management communicates and oversees the implementation of the Code of Business Ethics and Conduct to new and current employees via the Employee Handbook. The Employee Handbook contains Code of Conduct information and defines employee expectations. Employees receive the handbook upon hire and sign the Employee Acknowledgement form to confirm that they have received, read, and understand the contents, including the Code of Conduct.

The handbook contains employment provisions, including details on confidential information, internet and email use, job fulfillment of duties, and conduct. Use of company property and conflict of interest are also covered in the document.

Replicated commits to the highest level of integrity in dealing with its customers, vendors, and workforce. This commitment to integrity is promulgated with established policies that cover a variety of business and integrity objectives.

As part of the compliance effort, Replicated maintains a complete inventory list of all third parties. Such third parties are contractually required to maintain relevant elements of information security policy requirements, and to report cyber security incidents, in a timely manner.

OVERSIGHT AND AUTHORITY

Replicated has a risk and privacy committee tasked with governance and oversight. The risk and privacy committee meets at least quarterly and maintains formal meeting minutes. The risk and privacy committee includes directors that are independent of the internal control function. The committee is chaired by the Chief Risk Officer and comprised of members as determined by the Board of Directors.

ORGANIZATIONAL STRUCTURE

Replicated's organizational structure provides a framework for planning, executing and controlling business operations. The organizational structure assigns roles and responsibilities to provide for adequate staffing, efficiency of operations and the segregation of duties. Roles and responsibilities are formally documented

and include responsibilities for the oversight and implementation of the security and control environment. Management has also established authority and appropriate lines of reporting for key personnel. Replicated follows a structured on-boarding process to assist new employees as they become familiar with processes, systems, policies and procedures. Replicated places emphasis on ethics and communication within the organization.

MANAGEMENT'S PHILOSOPHY AND OPERATING STYLE

Replicated's senior management takes a hands-on approach to running the business. Senior management is heavily involved in all phases of the business operations. The senior management team remains in close contact with all personnel and consistently emphasizes appropriate behavior to all personnel and key vendor personnel.

AUTHORITY AND RESPONSIBILITY

Management and employees are assigned appropriate levels of authority and responsibility to facilitate effective internal control.

HUMAN RESOURCES

Upon hiring, and annually thereafter, all employees must successfully complete training courses covering basic information security practices that support the functioning of an effective risk management program. The training courses are designed to assist employees in identifying and responding to social engineering attacks (phishing, pharming, and tailgating) and in avoiding inappropriate security practices (for example, writing down passwords or leaving sensitive material unattended).

If an employee is found to be violating company policies, additional training is provided, or other disciplinary actions are taken.

Employees with job responsibilities that fall directly within the incident response program have additional requirements to complete technical and job-specific training throughout the year. Additionally, those employees who have direct access to customer and employee data will receive specific training around incident management, information handling, and data protection.

When onboarding new personnel, background checks are performed by Replicated management, where available.

COMMUNICATION AND INFORMATION

Replicated has various IT policies such as the IT security policy to ensure that employees understand their individual roles and responsibilities concerning processing as well as controls to ensure that significant events are communicated in a timely manner. These policies include formal and informal training programs and the use of email, instant messaging, and other mechanisms to communicate time-sensitive information and processes for security and system availability purposes that notify key personnel in the event of problems. Policies and supporting documents (and any changes to those documents) help users

understand how the System relates to their roles and responsibilities and are communicated to all users by the Company's Security organization.

Replicated has also published documentation describing the security features of the service, internal security-related processes and controls, and conformity to regulatory requirements.

RISK ASSESSMENT AND MITIGATION

Replicated's Risk Committee has performed a risk assessment during the design and implementation of the control objectives and related controls described in this report. As part of its risk assessment, the Risk Committee identified the threats and vulnerabilities relevant to the security of Replicated business operations and rated the risk posed by each identified vulnerability. This rating allowed for the design and implementation of controls to mitigate the most significant risks to the security of Replicated's service.

The risk assessments are performed by the Risk Committee annually, at a minimum, or in response to any major updates to the product, client base, or business plan.

When conducting a risk assessment, the Risk Committee first identifies threats and vulnerabilities relevant to the security of business operations. The Risk Committee then – for each identified vulnerability – considers:

- The likelihood of impact (i.e., the likelihood of the vulnerability being exploited), and
- The severity of impact (i.e., how damaging an exploitation of the vulnerability would be).

These estimations of impact potential and impact severity are then used in conjunction to establish a risk ranking for each vulnerability.

MONITORING

The systems within the boundary are configured to prevent and detect vulnerabilities. In addition to daily oversight and monthly reviews of logs and other usage of virtual infrastructure, management provides monitoring and audit logging in the form of preventive, detective, and corrective reporting. Relevant output from monitoring and detection mechanisms are distributed at monthly meetings with executive and management personnel. Security testing, both automated and manual, occurs at regular intervals. Vulnerability scans are performed quarterly to identify, quantify, and prioritize vulnerabilities. Penetration testing is performed at least annually to identify vulnerabilities that could be exploited to gain access to the production environment. Vulnerabilities identified are ranked by the security team and management and remediated based on the Company's vulnerability management policies and procedures.

Anti-malware technology is deployed for environments commonly susceptible to malicious attack and is configured to be updated routinely, logged, and installed on all relevant endpoints.

The Company utilizes a distributed approach in order to scale the security monitoring function by using a combination of commercially available tools, custom code, and an instant messaging platform. The Company has created a system that provides for the determination of attributions for most critical security-relevant events and target notifications to the staff with the authority and the context necessary

to vet that security alert. The interface of this system allows the targeted staff member to either resolve the security alert if they can do so safely or to escalate to the security team if response is required.

CONTROL ACTIVITIES

Information Security: An Information Security Policy has been formally documented and implemented to provide policies and procedures governing the protection of confidential and sensitive information. The Information Security Policy is communicated and distributed to employees upon hire. In the event of a significant change to the Information Security Policy, a communication is sent to all new and existing employees regarding the changes.

The Information Security Policy is reviewed and updated on an annual basis. The Information Security Policy defines information security responsibilities for all personnel. Where security responsibilities apply, roles are related to the policy and procedures that define their activity within their associated responsibilities. Security awareness training is provided to all employees upon hire and on an annual basis thereafter to ensure that personnel understand their security roles and responsibilities.

Replicated also communicates security roles and responsibilities to vendors and other third parties. Marketing and contractual materials that describe the services and scope of work provided to clients are documented and maintained to ensure that employees, contractors, vendors, and clients understand their roles and responsibilities.

LOGICAL AND PHYSICAL ACCESS

Access management processes exist so that Replicated employee and contractor user accounts are added, modified, or disabled in a timely manner and are reviewed on a quarterly basis. In addition, password configuration settings for user authentication to Replicated System are managed in compliance with Replicated's Password Policy which is part of the Information Security Policy.

Users must be approved for logical access by senior management prior to receiving access to the Replicated System. Management authorization is required before employment is offered and access is provided. Users must also be assigned a unique ID before being allowed access to system components. User IDs are authorized and implemented as part of the new hire onboarding process. Access rights and privileges are granted to user IDs based on the principle of least privilege and Role-Based Access Control (RBAC) protocols. Access is limited to that which is required for the performance of job duties for individual users, and generic access by Replicated employees is not allowed.

SYSTEM OPERATIONS

An Incident Response Policy and Procedures manual has been formally documented and implemented to guide preparation, detection, response, analysis and repair, communication, follow-up, and training for any class of security breach or incident. The responsibilities in the event of a breach, the steps of a breach, and the importance of information security are defined for all employees. The Incident Response Team employs industry-standard diagnosis procedures (such as incident identification, registration and verification, as well as initial incident classification and prioritizing actions) to drive resolution during business-impacting events.

Replicated reviews, triages, and communicates all incident alerts to Replicated whereupon the Incident Response Team starts the incident response process. Post-mortems are convened after any significant operational issue, regardless of external impact. Documentation of the investigation is conducted to determine that the root cause is captured and that preventative actions may be taken for the future.

CHANGE MANAGEMENT

A Configuration and Change Management Policy has been formally documented and implemented to guide the processes of change request, documentation, review, evaluation, approval, scheduling, testing, and implementation. Changes that may affect system availability and system security are communicated to management and any partners who may be affected via email.

System configuration standards are formally documented and implemented to ensure that all systems and network devices are properly and securely configured. CIS and NIST hardening standards, as well as configurations in AWS are used as a basis for Replicated's system configuration standards.

Secure Software Development: Replicated applies a systematic approach to software development so that changes to customer impacting services are reviewed, tested, approved, and well communicated. Prior to deployment to production environments, changes are:

- Developed: in a development environment that is segregated from the production environment. Customer content is not used in test and development environments.
- Reviewed: reviewed by peers for technical aspects and appropriateness.
- Tested: to confirm the changes will behave as expected when applied and not adversely impact performance.
- Approved: by authorized team members to provide appropriate oversight and understanding of business impact.

CONFIDENTIALITY

The confidentiality category refers to the protection of customer information as committed by the Company's service level agreements. The confidentiality of the Replicated System is dependent on many aspects of the Company's operations. The risks that would prevent the Company from meeting its confidentiality commitments and requirements are diverse. The Company has designed its controls to address both internal and external confidentiality risks specifically related to protection from improper use and disclosure (including the monitoring of vendor services), as well as the proper retention and disposal of confidential customer information.

Confidentiality risks are addressed through policies and procedures covering the use, retention, and disposal of confidential data, data classification policies and procedures, confidentiality and information sharing agreements, remote access and transmission restrictions, and vendor risk assessments.

In evaluating the suitability of the design of confidentiality controls, the Company considers the likely causes of improper disclosure or handling of confidential information and the commitments and requirements related to confidentiality.

COMPLEMENTARY USER ENTITY CONTROLS (CUECs)

The Company's controls related to Replicated cover only a portion of overall internal control for each user entity of Replicated. It is not feasible for the service commitments, system requirements, and applicable criteria related to the system to be achieved solely by the Company. Therefore, each user entity's internal control should be evaluated in conjunction with the Company's controls and the related tests and results described in Section 4 of this report, taking into account the related complementary user entity controls (CUECs) identified for the specific criterion. In order for user entities to rely on the controls reported herein, each user entity must evaluate its own internal control environment to determine whether the identified CUECs have been implemented and are operating effectively.

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

Criteria	Complementary User Entity Controls (CUECs)
CC2.1	• User entities have policies and procedures to report any material changes to their overall control environment that may adversely affect services being performed by the Company according to contractually specified time frames • Controls to provide reasonable assurance that the Company is notified of changes in: - User entity vendor security requirements - The authorized user list
CC2.3	• It is the responsibility of the user entity to have policies and procedures to: - Inform their employees and users that their information or data is being used and stored by the Company - Determine how to file inquiries, complaints, and disputes to be passed on to the Company
CC6.1	• User entities grant access to the Company's system to authorized and trained personnel • User entities deploy physical security and environmental controls for all devices and access points residing at their operational facilities, including remote employees or at-home agents for which the user entity allows connectivity
CC6.6	• Controls to provide reasonable assurance that policies and procedures are deployed over user IDs and passwords that are used to access services provided by the Company.

SUBSERVICE ORGANIZATIONS AND COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS (CSOCs)

The Company uses Amazon Web Services (AWS) as a subservice organization(s) for data center colocation services. The Company's controls related to Replicated cover only a portion of the overall internal control for each user entity of Replicated. The description does not extend to the colocation services for IT infrastructure provided by the subservice organization. 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 AWS.

Although the subservice organization has been carved out for the purposes of this report, certain service commitments, system requirements, and applicable criteria are intended to be met by controls at the subservice organization. Complementary subservice organization controls (CSOCs) are expected to be in place at AWS related to physical security and environmental protection, as well as backup, recovery, and redundancy controls related to availability. AWS physical security controls mitigate the risk of fires, power loss, climate, and temperature variabilities.

The Company management receives and reviews the AWS SOC 2 report annually. In addition, through its operational activities, Company management monitors the services performed by AWS to determine whether operations and controls expected to be implemented are functioning effectively. Management also has communication with the subservice organization to monitor compliance with the service agreement, stay informed of changes planned at the hosting facility, and relay any issues or concerns to AWS management.

It is not feasible for the service commitments, system requirements, and applicable criteria related to Replicated to be achieved solely by the Company. Therefore, each user entity's internal control must be evaluated in conjunction with the Company's controls and related tests and results described in Section 4 of this report, taking into account the related CSOCs expected to be implemented at AWS as described below.

Criteria	Complementary Subservice Organization Controls (CSOCs)
CC6.4	• AWS is responsible for restricting data center access to authorized personnel • AWS is responsible for the 24/7 monitoring of data centers by closed circuit cameras and security personnel
CC6.5	• AWS is responsible for securely decommissioning and physically destroying production assets in its control

CC7.2	• AWS is responsible for the installation of fire suppression and detection and environmental monitoring systems at the data centers • AWS is responsible for protecting data centers against a disruption in power supply to the processing environment by an uninterruptible power supply (UPS) • AWS is responsible for overseeing the regular maintenance of environmental protections at data centers.

SPECIFIC CRITERIA NOT RELEVANT TO THE SYSTEM

There were no specific Security and Confidentiality Trust Services Criteria as set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, Trust Services Criteria) that were not relevant to the system as presented in this report.

REPORT USE

The description does not omit or distort information relevant to Replicated while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to their particular needs.

Section IV: Trust Services Criteria and Related Controls Relevant to the Security and Confidentiality Categories

Section IV: Trust Services Criteria and Related Controls Relevant to the Security and Confidentiality Categories

Control Environment			
TSC Reference	**Trust Services Criteria**	**Control No.**	**Applicable Control Activities**
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	LCL-1	Upon hire, employees must acknowledge that they have read and agree to a code of conduct that describes their responsibilities and expected behavior regarding data and information system usage.
		LCL-2	Employees are required to sign a confidentiality agreement upon hire. This agreement prohibits any disclosure of information and other data to which the employee has been granted access.
		LCL-3	New personnel offered employment are subject to background checks prior to their start dates.
		LCL-10	Managers are required to complete performance appraisals for direct reports quarterly.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	LCL-4	The risk and privacy committee has documented oversight responsibilities relative to internal control.
		LCL-5	The risk and privacy committee meets at least quarterly and maintains formal meeting minutes. The risk and privacy committee includes directors that are independent of the internal control function.

CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	LCL-5	The risk and privacy committee meets at least quarterly and maintains formal meeting minutes. The risk and privacy committee includes directors that are independent of the internal control function.
		LCL-6	An organization chart is documented and defines the organizational structure and reporting lines.
		LCL-7	Management has established defined roles and responsibilities to oversee the implementation of the security and control environment.
		LCL-8	Job descriptions are documented for employees supporting the service and include authorities and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	LCL-8	Job descriptions are documented for employees supporting the service and include authorities and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system.
		LCL-9	Employees complete security awareness training upon hire and annually thereafter.
		LCL-10	Managers are required to complete performance appraisals for direct reports quarterly.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	LCL-1	Upon hire, employees must acknowledge that they have read and agree to a code of conduct that describes their responsibilities and expected behavior regarding data and information system usage.
		LCL-8	Job descriptions are documented for employees supporting the service and include authorities and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system.

		LCL-10	Managers are required to complete performance appraisals for direct reports quarterly.

Communication and Information			
TSC Reference	**Trust Services Criteria**	**Control No.**	**Applicable Control Activities**
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	LCL-11	Control self-assessments are performed by management at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings and tracked to resolution.
		LCL-46	Vulnerability scans are performed quarterly to identify, quantify, and prioritize vulnerabilities.
		LCL-47	A remediation plan is developed and changes are implemented to remediate all critical and high vulnerabilities at a minimum identified during quarterly vulnerability scans.
		LCL-48	A log management tool is utilized to identify trends that may have a potential impact on the Company's ability to achieve its security objectives.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	LCL-7	Management has established defined roles and responsibilities to oversee the implementation of the security and control environment.
		LCL-8	Job descriptions are documented for employees supporting the service and include authorities and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system.

		LCL-9	Employees complete security awareness training upon hire and annually thereafter.
		LCL-12	System changes are communicated to authorized internal users.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	LCL-13	Replicated's Security Page and Data Processing Addendum (DPA) includes the communication of the Company's commitments to its customers.
		LCL-14	Formal information sharing agreements are in place with critical vendors. These agreements include confidentiality commitments applicable to that entity.
		LCL-15	Guidelines and technical support resources related to system operations are provided on the Company's website.

Risk Assessment			
TSC Reference	**Trust Services Criteria**	**Control No.**	**Applicable Control Activities**
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	LCL-16	The Company specifies its objectives in its annual risk assessment to enable the identification and assessment of risk related to the objectives.
		LCL-17	A documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes	LCL-17	A documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance

	risks as a basis for determining how the risks should be managed.		of the risks associated with the identified threats, and mitigation strategies for those risks.
		LCL-18	A risk assessment is performed at least annually. As part of this process, threats and changes to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	LCL-17	A documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.
		LCL-18	A risk assessment is performed at least annually. As part of this process, threats and changes to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	LCL-17	A documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.
		LCL-18	A risk assessment is performed at least annually. As part of this process, threats and changes to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.
		LCL-19	A configuration management tool is in place to ensure that system configurations are deployed consistently throughout the environment.

		LCL-20	Penetration testing is performed at least annually to identify vulnerabilities that could be exploited to gain access to the production environment.
		LCL-21	A remediation plan is developed and changes are implemented to remediate all critical and high vulnerabilities at a minimum identified during the annual penetration test.

Monitoring Activities			
TSC Reference	**Trust Services Criteria**	**Control No.**	**Applicable Control Activities**
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	LCL-11	Control self-assessments are performed by management at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings and tracked to resolution.
		LCL-20	Penetration testing is performed at least annually to identify vulnerabilities that could be exploited to gain access to the production environment.
		LCL-21	A remediation plan is developed and changes are implemented to remediate all critical and high vulnerabilities at a minimum identified during the annual penetration test.
		LCL-46	Vulnerability scans are performed quarterly to identify, quantify, and prioritize vulnerabilities.
		LCL-47	A remediation plan is developed and changes are implemented to remediate all critical and high vulnerabilities at a minimum identified during quarterly vulnerability scans.

		LCL-55	Third-party attestation report review or a vendor risk assessment is performed at least annually for all critical vendors. Exceptions noted in the reports or risk assessments are evaluated to determine their impact on the service.
CC4.2	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.	LCL-11	Control self-assessments are performed by management at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings and tracked to resolution.
		LCL-55	Third-party attestation report review or a vendor risk assessment is performed at least annually for all critical vendors. Exceptions noted in the reports or risk assessments are evaluated to determine their impact on the service.

Control Activities			
TSC Reference	**Trust Services Criteria**	**Control No.**	**Applicable Control Activities**
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	LCL-17	A documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.
		LCL-22	As part of its annual risk assessment, management selects and develops manual and IT general control activities that contribute to the mitigation of identified risks.
CC5.2	The entity also selects and develops general control	LCL-17	A documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance

	activities over technology to support the achievement of objectives.		of the risks associated with the identified threats, and mitigation strategies for those risks.
		LCL-22	As part of its annual risk assessment, management selects and develops manual and IT general control activities that contribute to the mitigation of identified risks.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	LCL-17	A documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.
		LCL-23	Security incident response policies and procedures are documented and provide guidance for detecting, responding to, and recovering from security events and incidents. The policies and procedures are communicated to authorized users.
		LCL-24	Formal procedures are documented that outline the process the Company's staff follows to perform the following access control functions: - Adding new users - Modifying an existing user's access - Removing an existing user's access - Restricting access based on separation of duties and least privilege The procedures are reviewed at least annually.
		LCL-25	Information security policies and procedures are documented and define the information security rules and requirements for the service environment. These policies and procedures are reviewed at least annually and updated as needed.

		LCL-26	Formal procedures are documented that outline requirements for vulnerability management and system monitoring. The procedures are reviewed at least annually.
		LCL-27	A vendor management program is in place. Components of this program include: - Maintaining a list of critical third-party vendors. - Requirements for third-party vendors to maintain their own security practices and procedures. - Annually reviewing critical third-party attestation reports or performing a vendor risk assessment.
		LCL-28	A formal systems development life cycle (SDLC) methodology is in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.
		LCL-29	Network and system hardening standards are documented and reviewed at least annually.
		LCL-30	Formal data retention and disposal procedures are in place to guide the secure retention and disposal of Company and customer data.
		LCL-62	A data classification policy is in place to help ensure that confidential data is properly secured and restricted to authorized personnel.

Logical and Physical Access			
TSC Reference	**Trust Services Criteria**	**Control No.**	**Applicable Control Activities**
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	LCL-31	Authentication to the following in-scope production system components requires unique usernames and passwords or authorized Secure Shell (SSH) keys: - Network - Replicated System - OS - Data stores - AWS console - Encryption keys - Firewalls - Log data
		LCL-32	Privileged access to the following in-scope production system components is restricted to authorized users with a business need: - Network - Replicated System - OS - Data stores - AWS console - Encryption keys - Firewalls - Log data
		LCL-33	Passwords for in-scope system components are configured according to the Company's policy. Company policy requires the following (unless there is a system limitation): - 8-character minimum - Complexity enabled

			- 90-day password change
		LCL-34	The network is segmented to prevent unauthorized access to customer data.
		LCL-35	Encryption is enabled for data stores housing sensitive customer data.
		LCL-39	A formal inventory of production system assets is maintained by management.
		LCL-54	Access to migrate changes to production is restricted to authorized personnel.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	LCL-36	User access to in-scope system components is based on job role and function and requires a documented access request form and manager approval prior to access being provisioned.
		LCL-37	Termination checklists are completed to track employee terminations, and access is revoked for employees within 24 hours of termination as part of the termination process.
		LCL-38	Quarterly access reviews are conducted by management for the in-scope system components to help ensure that access is restricted appropriately. Tickets are created to remove or modify access as necessary in a timely manner.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration	LCL-36	User access to in-scope system components is based on job role and function and requires a documented access request form and manager approval prior to access being provisioned.
		LCL-37	Termination checklists are completed to track employee terminations, and access is revoked for employees within 24 hours of termination as part of the termination process.

	to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	LCL-38	Quarterly access reviews are conducted by management for the in-scope system components to help ensure that access is restricted appropriately. Tickets are created to remove or modify access as necessary in a timely manner.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	N/A	Not applicable.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	LCL-30	Formal data retention and disposal procedures are in place to guide the secure retention and disposal of Company and customer data.
		LCL-39	A formal inventory of production system assets is maintained by management.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	LCL-40	Remote access to production systems is restricted to authorized employees with a valid multi-factor authentication (MFA) token.
		LCL-41	AWS security groups are used and configured to prevent unauthorized access to the production environment.
		LCL-42	A runtime security tool is used to provide continuous monitoring of the Company's production clusters and early detection of potential security breaches.

		LCL-43	Infrastructure supporting the service is patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.
		LCL-44	Secure data transmission protocols are used to encrypt confidential and sensitive data when transmitted over public networks.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	LCL-44	Secure data transmission protocols are used to encrypt confidential and sensitive data when transmitted over public networks.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	LCL-43	Infrastructure supporting the service is patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.
		LCL-45	Anti-malware technology is deployed for environments commonly susceptible to malicious attack and is configured to be updated routinely, logged, and installed on all relevant endpoints.

System Operations			
TSC Reference	**Trust Services Criteria**	**Control No.**	**Applicable Control Activities**
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	LCL-18	A risk assessment is performed at least annually. As part of this process, threats and changes to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.
		LCL-19	A configuration management tool is in place to ensure that system configurations are deployed consistently throughout the environment.
		LCL-46	Vulnerability scans are performed quarterly to identify, quantify, and prioritize vulnerabilities.
		LCL-47	A remediation plan is developed and changes are implemented to remediate all critical and high vulnerabilities at a minimum identified during quarterly vulnerability scans.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	LCL-20	Penetration testing is performed at least annually to identify vulnerabilities that could be exploited to gain access to the production environment.
		LCL-21	A remediation plan is developed and changes are implemented to remediate all critical and high vulnerabilities at a minimum identified during the annual penetration test.
		LCL-42	A runtime security tool is used to provide continuous monitoring of the Company's production clusters and early detection of potential security breaches.

		LCL-43	Infrastructure supporting the service is patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.
		LCL-46	Vulnerability scans are performed quarterly to identify, quantify, and prioritize vulnerabilities.
		LCL-47	A remediation plan is developed and changes are implemented to remediate all critical and high vulnerabilities at a minimum identified during quarterly vulnerability scans.
		LCL-48	A log management tool is utilized to identify trends that may have a potential impact on the Company's ability to achieve its security objectives.
		LCL-49	An infrastructure monitoring tool is utilized to monitor system or infrastructure availability and performance and generates alerts when specific, predefined thresholds are met.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	LCL-20	Penetration testing is performed at least annually to identify vulnerabilities that could be exploited to gain access to the production environment.
		LCL-21	A remediation plan is developed and changes are implemented to remediate all critical and high vulnerabilities at a minimum identified during the annual penetration test.
		LCL-23	Security incident response policies and procedures are documented and provide guidance for detecting, responding to, and recovering from security events and incidents. The policies and procedures are communicated to authorized users.

		LCL-46	Vulnerability scans are performed quarterly to identify, quantify, and prioritize vulnerabilities.
		LCL-47	A remediation plan is developed and changes are implemented to remediate all critical and high vulnerabilities at a minimum identified during quarterly vulnerability scans.
		LCL-50	Security events are logged, tracked, resolved, and communicated to affected parties by management according to the Company's security incident response policies and procedures. All events are evaluated to determine whether they could have resulted in a failure to meet security commitments and objectives.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	LCL-23	Security incident response policies and procedures are documented and provide guidance for detecting, responding to, and recovering from security events and incidents. The policies and procedures are communicated to authorized users.
		LCL-43	Infrastructure supporting the service is patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.
		LCL-51	All incidents related to security are logged, tracked, evaluated and communicated to affected parties by management until the Company has recovered from the incidents.
		LCL-52	The incident response plan is tested at least annually to assess the effectiveness of the incident response program.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	LCL-23	Security incident response policies and procedures are documented and provide guidance for detecting, responding to, and recovering from security events and incidents. The policies and procedures are communicated to authorized users.

		LCL-51	All incidents related to security are logged, tracked, evaluated and communicated to affected parties by management until the Company has recovered from the incidents.
		LCL-52	The incident response plan is tested at least annually to assess the effectiveness of the incident response program.

Change Management			
TSC Reference	**Trust Services Criteria**	**Control No.**	**Applicable Control Activities**
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	LCL-43	Infrastructure supporting the service is patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.
		LCL-53	Changes to software and infrastructure components of the service are authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.
		LCL-54	Access to migrate changes to production is restricted to authorized personnel.

Risk Mitigation			
TSC Reference	**Trust Services Criteria**	**Control No.**	**Applicable Control Activities**
CC9.1	The entity identifies, selects, and develops risk mitigation	LCL-17	A documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance

	activities for risks arising from potential business disruptions.		of the risks associated with the identified threats, and mitigation strategies for those risks.
		LCL-23	Security incident response policies and procedures are documented and provide guidance for detecting, responding to, and recovering from security events and incidents. The policies and procedures are communicated to authorized users.
		LCL-52	The incident response plan is tested at least annually to assess the effectiveness of the incident response program.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	LCL-14	Formal information sharing agreements are in place with critical vendors. These agreements include confidentiality commitments applicable to that entity.
		LCL-55	Third-party attestation report review or a vendor risk assessment is performed at least annually for all critical vendors. Exceptions noted in the reports or risk assessments are evaluated to determine their impact on the service.

Additional Criteria for Confidentiality			
TSC Reference	**Trust Services Criteria**	**Control No.**	**Applicable Control Activities**
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	LCL-14	Formal information sharing agreements are in place with critical vendors. These agreements include confidentiality commitments applicable to that entity.
		LCL-30	Formal data retention and disposal procedures are in place to guide the secure retention and disposal of Company and customer data.

		LCL-62	A data classification policy is in place to help ensure that confidential data is properly secured and restricted to authorized personnel.
		LCL-63	Confidential or sensitive customer data is prohibited by policy from being used or stored in non-production systems or environments.
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	LCL-64	Customer data containing confidential information is purged or removed from the application environment at the customer's request or when a customer leaves the service if contractual obligations are in place.