Insight Assurance

Delivering Quality, Assuring Trust.

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

Report on Mohrer Associates LLC's Description of Its Wave Platform and on the Suitability of the Design of Its Controls Relevant to Security as of March 1, 2025

TABLE OF CONTENTS

SECTION 1: INDEPENDENT SERVICE AUDITOR'S REPORT

Insight Assurance
Delivering Quality, Assuring Trust.

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Mohrer Associates LLC

Scope

We have examined Mohrer Associates LLC's ("Wave" or "the Service Organization") accompanying description of its Wave Platform found in Section 3 titled "Mohrer Associates LLC's description of its Wave Platform" as of March 1, 2025 ("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 With Revised Implementation Guidance—2022)* in AICPA, *Description Criteria*, (description criteria) and the suitability of the design of controls stated in the description as of March 1, 2025, to provide reasonable assurance that Wave's service commitments and system requirements would be 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 (With Revised Points of Focus—2022)* in AICPA, *Trust Services Criteria.*

Wave uses Google Cloud Platform (GCP), Vercel and Firebase to provide hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Wave, to achieve Wave's service commitments and system requirements based on the applicable trust services criteria. The description presents Wave's controls, the applicable trust services criteria and the types of complementary subservice organization controls assumed in the design of Wave's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

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

Service Organization's Responsibilities

Wave is responsible for its service commitments and system requirements and designing, implementing, and operating effective controls within the system to provide reasonable assurance that Wave's service commitments and system requirements would be achieved. In Section 2, Wave has provided the accompanying assertion titled "Mohrer Associates LLC's Management

Assertion" (assertion) about the description and the suitability of the design of controls stated therein. Wave is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria, and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and the suitability of the design of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed to provide reasonable assurance that the service organization's service commitments and system requirements would be achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

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

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

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

Inherent Limitations

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

to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Other Matter – No Tests of Operating Effectiveness Performed

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

Opinion

In our opinion, in all material respects,

- the description presents Wave's Platform that was designed and implemented as of March 1, 2025, in accordance with the description criteria.
- the controls stated in the description were suitably designed as of March 1, 2025, to provide reasonable assurance that Wave'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 organizations and user entities applied the complementary controls assumed in the design of Wave's controls as of that date.

Restricted Use

This report is intended solely for the information and use of Wave, user entities of Wave's Platform as of March 1, 2025, business partners of Wave subject to risks arising from interactions with the Wave Platform, 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 the specified parties.

Insight Assurance LLC

Tampa, Florida
May 13, 2025

SECTION 2: MOHRER ASSOCIATES LLC'S MANAGEMENT ASSERTION

MOHRER ASSOCIATES LLC'S MANAGEMENT ASSERTION

We have prepared the description of Mohrer Associates LLC's ('Wave' or 'the Service Organization') Wave Platform entitled "Mohrer Associates LLC's description of its Wave Platform" as of March 1, 2025 ("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 (With Revised Implementation Guidance—2022)* in AICPA, *Description Criteria*, (description criteria). The description is intended to provide report users with information about the Wave Platform that may be useful when assessing the risks arising from interactions with Wave's system, particularly information about system controls that Wave has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* in AICPA*, Trust Services Criteria*.

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

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

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

- the description presents Wave's Platform that was designed and implemented as of March 1, 2025, in accordance with the description criteria.
- the controls stated in the description were suitably designed as of March 1, 2025, to provide reasonable assurance that Wave'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 organizations and user entities applied the complementary controls assumed in the design of the Wave's controls as of that date.

Mohrer Associates LLC
May 13, 2025

SECTION 3: MOHRER ASSOCIATES LLC'S DESCRIPTION OF ITS WAVE PLATFORM

MOHRER ASSOCIATES LLC'S DESCRIPTION OF ITS WAVE PLATFORM

Company Background

Wave is a technology company headquartered in New York, NY that provides transcription and text summary services to customers via the Wave AI Note Taker App for iOS and Android devices.

Description of Services Overview

The Wave Platform provides customers with a personal AI note-taker, turning lectures, business meetings, or doctor's appointments into clear, concise notes on your iOS device. An essential tool for capturing and understanding critical information, anytime, anywhere.

Wave is the AI-powered transcription and summarization app for audio recordings and phone calls. The app transcribes the recorded audio and then uses AI to create summaries of the text.

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Wave designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments that Wave makes to user entities, the laws, and regulations that govern the provision of the services, and the financial, operational, and compliance requirements that Wave has established for the services. The system services are subject to the Security commitments established internally for its services.

Wave's Security commitments to its users are communicated through the privacy policy.

Security Commitments

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

- Security principles within the fundamental designs of services are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role.
- Use of encryption technologies to protect customer data both at rest and in transit
- Use of data retention and data disposal
- Implementation of a robust incident response plan that outlines procedures for addressing security breaches, including notification processes for affected parties.
- Regular security assessments and penetration testing to identify vulnerabilities and ensure timely remediation.
- Adoption of a zero-trust security model, ensuring strict verification of all individuals and devices before granting access to system resources.
- Continuous monitoring and anomaly detection to quickly identify and mitigate unauthorized or suspicious activities.
- Application of security patches and updates in a timely manner to mitigate known vulnerabilities.
- Employee security awareness training programs to educate staff about the latest security threats and best practices.

- Vendor risk management to ensure third-party service providers comply with security standards and contractual obligations.

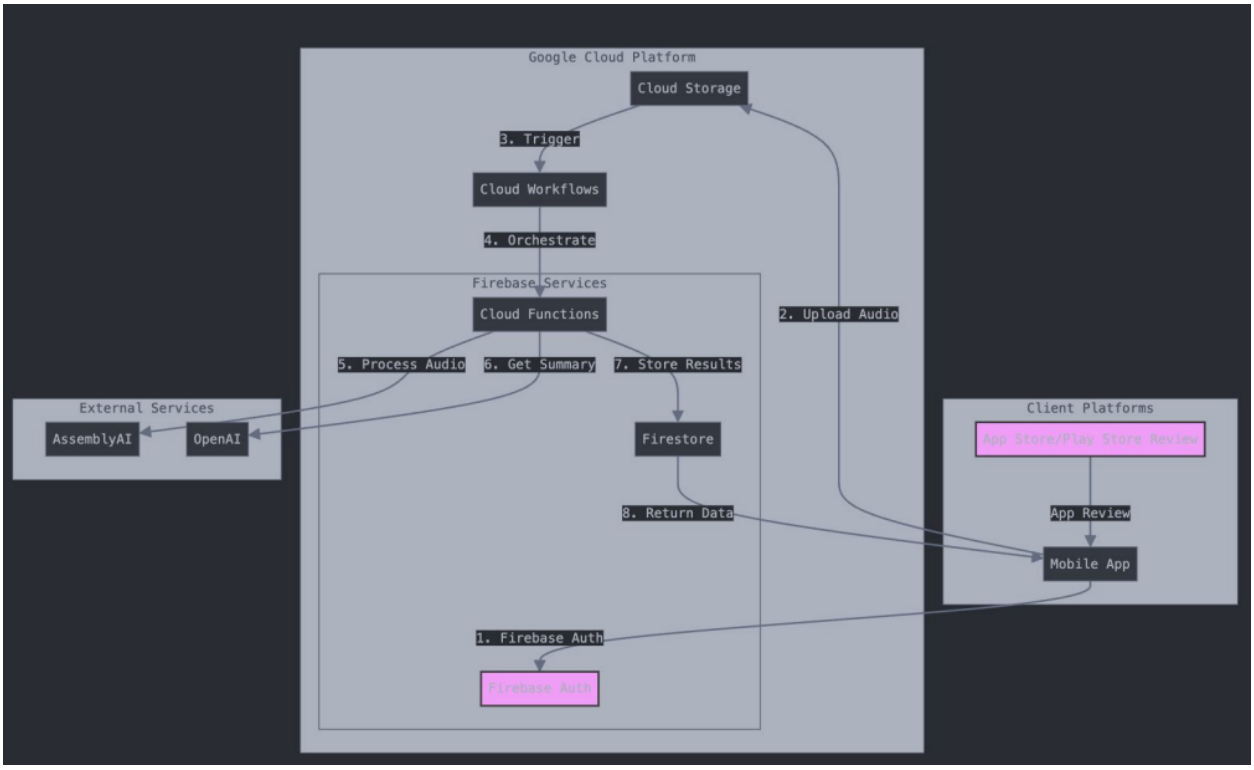
COMPONENTS OF THE SYSTEM USED TO PROVIDE THE SERVICES

The System description is comprised of the following components:

- ***Infrastructure*** – The servers, databases, computers, firewalls, routers, and other equipment (both physical and virtual) that work together to store, process, transmit, and protect data and that form the foundation of the system functions and services provided.
- ***Software*** - The application programs and IT system software that supports application programs (operating systems, middleware, and utilities), the types of databases used, the nature of external facing web applications, and the nature of applications developed in-house, including details about whether the applications in use are mobile applications or desktop or laptop applications.
- ***People*** - The personnel involved in the governance, operation, security, and use of a system (business unit personnel, developers, operators, user entity personnel, vendor personnel, and managers).
- ***Data*** – The types of information used by the system, such as transaction streams, files, databases, tables, and output used or processed by the system.
- ***Procedures*** – The automated and manual processes related to the services provided, including, as appropriate, procedures by which service activities are initiated, authorized, performed, and delivered, and reports and other information prepared.

INFRASTRUCTURE

Wave maintains a system inventory that includes virtual machines, computers (desktops and laptops), and networking devices (switches and routers). The inventory documents device name, inventory type, description and owner.



The in-scope Wave infrastructure components are shown in the table provided below:

Primary Infrastructure		
Asset	**Type**	**Purpose**
Google Cloud Platform	Hosting	Outsourced hosting provider
Vercel	Cloud services	Cloud platform that enables developers to deploy, manage, and scale web applications
Firebase	Database	Database and User Management

SOFTWARE

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

Primary Software	
System/Application	**Purpose**
Vanta	Trust management platform
GitHub	Version control and collaboration platform which allows developers to host and review code.
Google Drive	Document management
Google Workspace	Identity provider
Intercom	Communication platforms
Adapty	Payment Interface Management
Sentry	Application monitoring and error tracking tool that helps developers identify, diagnose, and fix issues in real-time within their software applications
Customer.io	Customer Data Platform

PEOPLE

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

Wave has a staff of approximately 1 organized in the following functional areas:

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

- **Chief Executive Officer (CEO)** – Responsible for setting the strategic direction of the company, ensuring operational alignment with business goals, and maintaining overall accountability for company performance, security, and compliance.

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

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

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

DATA

Data as defined by Wave, constitutes the following:

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

Data is categorized in the following major types of data used by Wave:

Data		
Category	**Description**	**Examples**
Public	Public information is not confidential and can be made public without any implications for Wave.	• Press releases • Public website • Marketing materials • Product descriptions • Change Release notes
Internal Use	Non-sensitive Information originating within or owned by Wave or entrusted to it by others. May be shared with authorized employees, contractors, and business partners who have a business need, but may not be released to the public, due to the negative impact it might have on the company's business interests	• Financial reports • Source Code • Internal communications • Training Material • Business Strategy Documents • Security Information
Confidential	Highly sensitive data requires the highest levels of protection; access is restricted to specific employees or departments, and these records can only be passed to others with approval by Management. Wave must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information.	• Customer data • PII data • PHI data • Test results

Data		
Category	**Description**	**Examples**
Restricted	Wave provides proprietary information requiring thorough protection; access is restricted to employees with a "need-to-know" based on business requirements. This data can only be distributed outside the company with management approval. This is default for all company information unless stated otherwise.	• Internal policies • Employee PII • Employee compensation • Legal documents • Meeting minutes and internal presentations • Contracts • Internal reports • Slack messages • Email

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

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

PROCEDURES

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

Physical Security

Wave's production servers are maintained by GCP, Firebase and Vercel. The physical and environmental security protections are the responsibility of GCP, Firebase and Vercel. Wave reviews the attestation reports and performs a risk analysis of GCP, Firebase and Vercel on at least an annual basis.

Logical Access

Wave provides employees and contracts access to infrastructure via a role-based access control system, to ensure uniform, least privilege access to identified users and to maintain simple and reparable user provisioning and deprovisioning processes.

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

Management is responsible for provision access to the system based on the employee's role and performing a background check. The employee is responsible for reviewing Wave's policies, completing security training. These steps must be completed within 14 days of hire.

When an employee is terminated, Management is responsible for deprovisioning access to all in scope systems within 3 days for that employee's termination.

Change Management

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

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

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

Patch Management

Software patches and updates are applied to systems in a timely manner. Infrastructure supporting the services provided is patched as a part of the change management process to help ensure that servers supporting the service are hardened against security threats. Routine updates are applied after thorough testing. In the case of updates to correct known vulnerabilities, priority will be given to testing to speed the time to production. Critical security patches are applied within three days from identification and non-critical security patches are applied within seven days after identification.

Computer Operations

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

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

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

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

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

Data Communications

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

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

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

System Monitoring

The Network Security and Vulnerability Management Policy describes the organization's policies and procedures related to network logging and monitoring as well as vulnerability identification and remediation. The organization uses Cloud Monitoring for system logging within the SSO environment, and the organization collects logs from the office router and firewall. Cloud Monitoring logs and the office router and firewall logs document source IP, destination IP, destination port, protocol type, and timestamp. The organization monitors system capacity using Cloud Monitoring.

Cloud Armor is used for threat detection purposes, and the tool generates logs, VPC flow logs, and DNS logs for intrusion detection.

The vulnerability assessment process involves the execution of CIS testing, implementation of antivirus software, and system patching. The organization uses Cloud Armor anti-malware and has configured the software to run updates daily and prohibit end-users from disabling or altering the software. Alerts are sent immediately when a potential virus is detected, and logs are generated and retained for at least one year with at least three months readily available. Cloud Armor is used to identify newly emerging vulnerabilities, and the organization monitors vendors for patch updates to correct vulnerabilities.

Vendor Management

The organization maintains a Vendor Management Policy that includes requirements for interacting with vendors/service providers. The policy includes requirements for performing due diligence measures prior to engaging with a new provider. Due diligence procedures include evaluating each material IT vendors' cost-effectiveness, functionality/services, risk, financial

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

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

CONTROL ENVIRONMENT

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

Integrity and Ethical Values

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

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

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

Commitment to Competence

Wave's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to

competence includes management's consideration of the competence levels for jobs and how those levels translate into the requisite skills and knowledge.

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

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

Management Philosophy and Operating Style

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

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

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

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

Organizational Structure and Assignment of Authority and Responsibilities

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

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

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

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

Human Resources Policies and Procedures

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

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

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

RISK ASSESSMENT PROCESS

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

Integration with risk assessment

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

CONTROL ACTIVITIES

Control activities are the actions established by policies and procedures to help ensure that management directives to mitigate risks to the achievement of objectives are executed. Control activities are performed at all levels of the organization and various stages within business processes, and over the technology environment.

INFORMATION AND COMMUNICATION SYSTEMS

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

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

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

MONITORING CONTROLS

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

Ongoing Monitoring

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

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

Monitoring of the Subservice Organizations

Wave uses GCP, Vercel and Firebase subservice organizations to provide hosting services.

The management of Wave receives and reviews the SOC 2 report of GCP, Vercel and Firebase and on an annual basis. In addition, through its daily operational activities, the management of Wave monitors the services performed by GCP, Vercel and Firebase to ensure that operations and controls expected to be implemented at the subservice organizations are functioning effectively.

Reporting Deficiencies

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

CHANGES TO THE SYSTEM

No significant changes have occurred to the services provided to user entities since the exam date.

SYSTEM INCIDENTS

No significant incidents have occurred to the services provided to user entities since the exam date.

COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS (CSOCs)

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

#	Complementary Subservice Organization Controls (CSOC)	Related Criteria
1	GCP, Vercel and Firebase are responsible for maintaining physical security and environmental protection controls over the data centers hosting the Wave infrastructure.	CC6.4
2	GCP, Vercel and Firebase are responsible for the destruction of physical assets hosting the production environment.	CC6.5

COMPLEMENTARY USER ENTITY CONTROLS (CUECs)

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

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

1. User entities should have controls in place to provide reasonable assurance that user access including the provisioning and de-provisioning are designed appropriately and operating effectively.
2. User entities are responsible for reporting issues with Wave systems and platforms.

3. User entities are responsible for understanding and complying with their contractual obligations to Wave.
4. User entities are responsible for notifying Wave of changes made to the administrative contact information.

TRUST SERVICES CATEGORY, CRITERIA, AND RELATED CONTROLS

The Security category and applicable trust services criteria were used to evaluate the suitability of the design of controls stated in the description. The criteria and controls designed, implemented, and operated to meet them ensure that information, systems, and access (physical and logical) are protected against unauthorized access, and systems are available for operation and use. The controls supporting the applicable trust services criteria are included in Section 4 of this report and are an integral part of the description of the system.

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

Trust Services Category, Criteria, and Related Controls

This SOC 2 Type 1 report was prepared in accordance with the AICPA attestation standards and has been performed to examine the suitability of the design of controls to meet the criteria for the Security category set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* in AICPA*, Trust Services Criteria* as of March 1, 2025.

The applicable trust services criteria and related controls specified by Wave are presented in Section 4 of this report.

On the pages that follow, the applicable trust services criteria and the control activities to achieve the applicable trust services criteria have been specified by and are the responsibility of Wave.

CONTROL ACTIVITIES SPECIFIED BY THE SERVICE ORGANIZATION

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY	
CONTROL ENVIRONMENT	
Control Number	**Controls**
CC1.1 – COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	
CC1.1.1	The company has an approved Code of Conduct that is reviewed annually and updated as needed. Sanction policies are documented within the information security policies and procedures.
CC1.1.2	The company requires employees and contractors to acknowledge the Code of Conduct at the time of hire and active employees and contractors to acknowledge the Code of Conduct at least annually.
CC1.1.3	The company requires employees and contractors to acknowledge the Code of Conduct at the time of hire and active employees and contractors to acknowledge the Code of Conduct at least annually.
CC1.1.4	The company's managers are required to complete performance evaluations for direct reports at least annually.
CC1.1.5	The company requires employees and contractors to review and acknowledge the information security policies at the time of hire and active employees and contractors to acknowledge the information security policies at least annually.
CC1.1.6	Employees are required to review and acknowledge the confidentiality agreement at the time of hire.
CC1.2 – COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	
CC1.2.1	Wave does not have an independent Board of Directors; therefore, this criteria is not applicable.
CC1.3 – COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	
CC1.3.1	The company maintains an organizational chart that describes the organizational structure and reporting lines.
CC1.3.2	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the Information Security Roles and Responsibilities Policy.
CC1.3.3	The company requires employees to review and acknowledge the information security policies at the time of hire and active employees to acknowledge the information security policies at least annually.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY	
CONTROL ENVIRONMENT	
Control Number	**Controls**
CC1.4 – COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	
CC1.4.1	The company requires to perform background checks on new employees.
CC1.4.2	The company's managers are required to complete performance evaluations for direct reports at least annually.
CC1.4.3	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the Information Security Roles and Responsibilities Policy.
CC1.4.4	The company requires new employees to complete security awareness training at the time of hire and active employees to complete security training at least annually.
CC1.5 – COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	
CC1.5.1	The company has an approved Code of Conduct that is reviewed annually and updated as needed. Sanction policies are documented within the information security policies and procedures.
CC1.5.2	The company requires employees and contractors to acknowledge the Code of Conduct at the time of hire and active employees to acknowledge the Code of Conduct at least annually.
CC1.5.3	The company's managers are required to complete performance evaluations for direct reports at least annually.
CC1.5.4	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the Information Security Roles and Responsibilities Policy.
CC1.5.5	The company requires new employees and contractors to complete security awareness training at the time of hire and active employees to complete security training at least annually.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY	
INFORMATION AND COMMUNICATION	
Control Number	**Controls**
CC2.1 – COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	
CC2.1.1	The company's information security policies and procedures are documented and reviewed at least annually.
CC2.1.2	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.
CC2.1.3	The company utilizes a log management tool to identify events that may potentially impact the company's ability to achieve its security objectives.
CC2.2 – COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	
CC2.2.1	The company has security incident response policies and procedures that are documented and communicated to authorized users.
CC2.2.2	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the Information Security Roles and Responsibilities Policy.
CC2.2.3	The company requires new employees and contractors to complete security awareness training at the time of hire and active employees and contractors to complete security training at least annually.
CC2.2.4	The company's information security policies and procedures are documented and reviewed at least annually.
CC2.2.5	The company describes its products and services to internal and external users.
CC2.2.6	The company communicates system changes to authorized internal users.
CC2.3 – COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	
CC2.3.1	The company's security commitments are communicated to customers in the Privacy Policy and Terms of Use.
CC2.3.2	The company provides guidelines and technical support resources relating to system operations to customers.
CC2.3.3	The company describes its products and services to internal and external users.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY	
INFORMATION AND COMMUNICATION	
Control Number	**Controls**
CC2.3.4	The company has contact information on its website to allow users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel.
CC2.3.5	The company has written agreements in place with vendors and related third parties. These agreements include security and confidentiality commitments applicable to that entity.
CC2.3.6	The company notifies customers of critical system changes that may affect their processing.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY	
RISK ASSESSMENT	
Control Number	**Controls**
CC3.1 – COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	
CC3.1.1	The company specifies its objectives to enable the identification and assessment of risk related to the objectives.
CC3.1.2	The company has a documented risk management program that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.
CC3.1.3	The company's risk assessments are performed at least annually. As part of this process, threats, and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes consideration of the potential for fraud and how fraud may impact the achievement of objectives.
CC3.2 – COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	
CC3.2.1	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.
CC3.2.2	The company has a third-party management program in place. Components of this program include: - critical vendor inventory. - vendor's security requirements; and - annual review of vendors and subservice organizations.
CC3.2.3	The company's risk assessments are performed at least annually. As part of this process, threats, and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.
CC3.2.4	The company has a documented business continuity plan and tests it at least annually.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY	
RISK ASSESSMENT	
Control Number	**Controls**
CC3.3 – COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	
CC3.3.1	The company's risk assessments are performed at least annually. As part of this process, threats, and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.
CC3.3.2	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.
CC3.4 – COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	
CC3.4.1	The company's risk assessments are performed at least annually. As part of this process, threats, and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.
CC3.4.2	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY	
MONITORING ACTIVITIES	
Control Number	**Controls**
CC4.1 – COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	
CC4.1.1	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.
CC4.1.2	Vulnerability scans are performed quarterly on in-scope systems. Critical and high vulnerabilities are tracked to remediation.
CC4.1.3	The company has a third-party management program in place. Components of this program include: - critical vendor inventory. - vendor's security requirements; and - annual review of critical vendors and subservice organizations.
CC4.2 – COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	
CC4.2.1	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.
CC4.2.2	The company has a third-party management program in place. Components of this program include: - critical vendor inventory; - vendor's security requirements; and - annual review of critical vendors and subservice organizations.
CC4.2.3	Vulnerability scans are performed quarterly on in-scope systems. Critical and high vulnerabilities are tracked to remediation.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY	
CONTROL ACTIVITIES	
Control Number	**Controls**
CC5.1 – COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	
CC5.1.1	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.
CC5.1.2	The company's information security policies and procedures are documented and reviewed at least annually.
CC5.1.3	The company's risk assessments are performed at least annually. As part of this process, threats, and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.
CC5.1.4	Role-based access is configured within GCP, Vercel, Firebase, GitHub, and other supporting applications to enforce the segregation of duties and restrict access to confidential information.
CC5.2 – COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	
CC5.2.1	The company's Access Control Policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.
CC5.2.2	The company has a formal secure development policy in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.
CC5.2.3	The company's information security policies and procedures are documented and reviewed at least annually.
CC5.3 – COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	
CC5.3.1	The company's information security policies and procedures are documented and reviewed at least annually.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY	
CONTROL ACTIVITIES	
Control Number	**Controls**
CC5.3.2	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved before being implemented in the production environment.
CC5.3.3	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.
CC5.3.4	The company has security incident response policies and procedures that are documented and communicated to authorized users.
CC5.3.5	The company specifies its objectives to enable the identification and assessment of risk related to the objectives.
CC5.3.6	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.
CC5.3.7	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and the Information Security Roles and Responsibilities Policy.
CC5.3.8	The company has a third-party management program in place. Components of this program include: - critical vendor inventory; - vendor's security requirements; and - annual review of critical vendors and subservice organizations.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY	
LOGICAL AND PHYSICAL ACCESS CONTROLS	
Control Number	**Controls**
CC6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	
CC6.1.1	The company's Access Control Policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.
CC6.1.2	The company has a Data Management Policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel.
CC6.1.3	The company's databases housing sensitive customer data are encrypted at rest.
CC6.1.4	The company restricts privileged access to encryption keys to authorized users with a business need.
CC6.1.5	Role-based access is configured within GCP, Vercel, Firebase, GitHub, and other supporting applications to enforce the segregation of duties and restrict access to confidential information.
CC6.1.6	The company restricts privileged access to the network, application, databases, and supporting cloud infrastructure to authorized users with a business need.
CC6.1.7	The company restricts privileged access to the firewall to authorized users with a business need.
CC6.1.8	The firewall is configured to prevent unauthorized access to the company's network.
CC6.1.9	The company ensures that user access to in-scope system components is based on job role and function.
CC6.1.10	The company requires passwords for in-scope system components to be configured according to the company's policy.
CC6.1.11	The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.
CC6.1.12	The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.
CC6.1.13	The company maintains a formal inventory of production system assets.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY	
LOGICAL AND PHYSICAL ACCESS CONTROLS	
Control Number	**Controls**
CC6.1.14	The company's network is segmented to prevent unauthorized access to customer data.
CC6.2: Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	
CC6.2.1	The company's Access Control Policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.
CC6.2.2	The company conducts quarterly access reviews for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.
CC6.2.3	Logical access to systems is revoked as a component of the termination process within the company's SLAs.
CC6.2.4	The company ensures that user access to in-scope system components is based on job role and function.
CC6.3: The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	
CC6.3.1	The company's Access Control Policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.
CC6.3.2	The company conducts quarterly access reviews for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.
CC6.3.3	Logical access to systems is revoked as a component of the termination process within the company's SLAs.
CC6.3.4	The company ensures that new user access to in-scope system components is based on job role and function.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY	
LOGICAL AND PHYSICAL ACCESS CONTROLS	
Control Number	**Controls**
CC6.4: The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	
CC6.4.1	Management contracts with GCP, Vercel and Firebase to provide physical access security of its production systems.
CC6.5: The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	
CC6.5.1	The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.
CC6.5.2	The company has electronic media containing confidential information purged or destroyed in accordance with best practices.
CC6.5.3	The destruction of physical assets hosting the production environment is the responsibility of GCP, Vercel and Firebase.
CC6.6: The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	
CC6.6.1	The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.
CC6.6.2	The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.
CC6.6.3	The firewall is configured to prevent unauthorized access to the company's network.
CC6.6.4	The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.
CC6.6.5	The company uses an Intrusion Detection System (IDS) to provide continuous monitoring of the company's network and early detection of potential security breaches.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY	
LOGICAL AND PHYSICAL ACCESS CONTROLS	
Control Number	**Controls**
CC6.7: The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	
CC6.7.1	The company encrypts portable and removable media devices when used.
CC6.7.2	The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.
CC6.7.3	The company has a mobile device monitoring system in place to centrally monitor mobile devices supporting the service.
CC6.8: The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	
CC6.8.1	The company deploys anti-malware technology to environments commonly susceptible to malicious attacks. The anti-malware software is configured to scan workstations daily and install updates as new updates/signatures are available.
CC6.8.2	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY	
SYSTEM OPERATIONS	
Control Number	**Controls**
CC7.1: To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	
CC7.1.1	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved before being implemented in the production environment.
CC7.1.2	The company's risk assessments are performed at least annually. As part of this process, threats, and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.
CC7.1.3	Vulnerability scans are performed quarterly on in-scope systems. Critical and high vulnerabilities are tracked to remediation.
CC7.1.4	The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.
CC7.1.5	The company's formal policies outline the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.
CC7.2: The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	
CC7.2.1	The company uses an Intrusion Detection System (IDS) to provide continuous monitoring of the company's network and early detection of potential security breaches.
CC7.2.2	The company utilizes a log management tool to identify events that may potentially impact the company's ability to achieve its security objectives.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY	
SYSTEM OPERATIONS	
Control Number	**Controls**
CC7.2.3	The company's formal policies outline the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.
CC7.2.4	An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.
CC7.2.5	Vulnerability scans are performed quarterly on in-scope systems. Critical and high vulnerabilities are tracked to remediation in accordance with SLAs.
CC7.2.6	Security incidents are reported to the IT personnel and tracked through to resolution in a ticketing system.
CC7.3: The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	
CC7.3.1	The company has security incident response policies and procedures that are documented and communicated to authorized users.
CC7.3.2	The company's security incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.
CC7.4: The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	
CC7.4.1	The company has security incident response policies and procedures that are documented and communicated to authorized users.
CC7.4.2	The company's security incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.
CC7.4.3	The company tests its incident response plan at least annually.
CC7.5: The entity identifies, develops, and implements activities to recover from identified security incidents.	
CC7.5.1	The company has security incident response policies and procedures that are documented and communicated to authorized users.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY	
SYSTEM OPERATIONS	
Control Number	**Controls**
CC7.5.2	The company's security incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.
CC7.5.3	The company's risk assessments are performed at least annually. As part of this process, threats, and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.
CC7.5.4	The company has a documented business continuity/disaster recovery (BC/DR) Plan and tests it at least annually.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY	
CHANGE MANAGEMENT	
Control Number	**Controls**
CC8.1: The entity authorizes, designs, develops, or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	
CC8.1.1	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.
CC8.1.2	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved before being implemented in the production environment.
CC8.1.3	Segregation of duties is in place within the SDLC process.
CC8.1.4	The company restricts access to the production environment to authorized personnel.
CC8.1.5	The company's risk assessments are performed at least annually. As part of this process, threats, and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.
CC8.1.6	Vulnerability scans are performed quarterly on in-scope systems. Critical and high vulnerabilities are tracked to remediation in accordance with SLAs.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY	
RISK MITIGATION	
Control Number	**Controls**
CC9.1: The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	
CC9.1.1	The company's risk assessments are performed at least annually. As part of this process, threats, and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.
CC9.1.2	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.
CC9.2: The entity assesses and manages risks associated with vendors and business partners	
CC9.2.1	The company has written agreements in place with vendors and related third parties. These agreements include security and confidentiality commitments applicable to that entity.
CC9.2.2	The company has a third-party management program in place. Components of this program include: - critical vendor inventory; - vendor's security requirements; and - annual review of critical vendors and subservice organizations.