

INTENTWISE INC.

SOC 2 REPORT

FOR

Intentwise Ad Optimizer, Intentwise Analytics Cloud and Intentwise Explore Software Application

TYPE 2 INDEPENDENT SERVICE AUDITOR'S REPORT ON
CONTROLS RELEVANT TO SECURITY, CONFIDENTIALITY AND AVAILABILITY

December 23, 2024 – December 22, 2025

Attestation and Compliance Services

CertPro

Proprietary & Confidential
Reproduction or distribution in whole or in part without prior written consent is strictly prohibited.

This report is intended solely for use by the management of Intentwise Inc., user entities of Intentwise Inc.’s services, and other parties who have sufficient knowledge and understanding of Intentwise Inc.’s services covered by this report (each referred to herein as a “specified user”).

If report recipient is not a specified user (herein referred to as a "non-specified user"), use of this report is the non-specified user's sole responsibility and at the non-specified user's sole and exclusive risk. Non-specified users may not rely on this report and do not acquire any rights against CertPro and the service auditor as a result of such access. Further, CertPro and the service auditor do not assume any duties or obligations to any non-specified user who obtains this report and/or has access to it.

Unauthorized use, reproduction, or distribution of this report, in whole or in part, is strictly prohibited.

Table of Contents

SECTION 1 INDEPENDENT SERVICE AUDITOR'S REPORT 1

SECTION 2 MANAGEMENT'S ASSERTION 6

SECTION 3 DESCRIPTION OF THE SYSTEM 9

SECTION 4 TESTING MATRICES 28

Section 1

Independent Service Auditor's Report

INDEPENDENT SERVICE AUDITOR'S REPORT

To Board of Directors
Intentwise Inc.

Scope

We have examined the accompanying "Description of Intentwise Ad Optimizer, Intentwise Analytics Cloud and Intentwise Explore Software Application" provided by Intentwise Inc. throughout the period December 23, 2024 to December 22, 2025 (the description) based on the criteria for the description of service organizations system in DC section 200, *2018 Description Criteria* for a description of a service organization systems in a *SOC 2 report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period December 23, 2024 to December 22, 2025 to provide reasonable assurance that Intentwise Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Confidentiality and Availability (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Confidentiality, Availability, Processing Integrity and Privacy* (AICPA, Trust Services Criteria).

Intentwise Inc. uses Amazon Web Services Inc. (AWS), a subservice organization, to provide cloud Software-as-a-Service (SaaS), Microsoft Azure, a cloud computing service operated by Microsoft for application management, Google Cloud Platform Inc. (GCP), a subservice organization, to provide cloud Software-as-a-Service (SaaS), Heroku, Inc., a subservice organization, to provide cloud Platform-as-a-Service (PaaS) for building, running, and scaling applications, supporting multiple programming languages and integrated add-on services, GitHub, a cloud computing service operated by GitHub Inc. (GitHub), a subservice organization, to provide and host the GitHub application and Google Workspace, a collection of cloud computing, productivity and collaboration tools, software, and products such as Gmail, Calendar, Drive, Docs, Sheets, Slides, Meet, and many more. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Intentwise Inc., to achieve Intentwise Inc.'s service commitments and system requirements based on the applicable trust services criteria. The description presents Intentwise Inc.'s controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Intentwise Inc.'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 presents Intentwise Inc.'s controls, the applicable trust services criteria, and the types of complementary user entity controls assumed in the design of Intentwise Inc.'s controls. The description does not disclose the actual controls at the user entity organizations. Our examination did not include the services provided by the user entity organizations and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

Intentwise Inc. has provided the accompanying assertion titled "Intentwise Inc.'s Management Assertion throughout the period December 23, 2024 to December 22, 2025" about the fairness of the presentation of the description based on the description criteria and suitability of the design and operating effectiveness of the controls described therein to meet Intentwise Inc.'s service commitments and system requirements based on the applicable trust services criteria. Intentwise Inc. responsible for: (1) preparing the description and assertion; (2) the completeness, accuracy and method of presentation of the description and assertion; (3) providing the services covered by the description; (4) identifying the risks that would prevent the applicable trust services criteria from being met; (5) specifying the controls that meet Intentwise Inc.'s service commitments and system requirements based on the applicable trust services criteria and stating them in the description; (6) designing,

implementing, maintaining and documenting controls to meet Intentwise Inc.'s service commitments and system requirements based on the applicable trust services criteria stated in the description.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description based on the description criteria set forth in Intentwise Inc.'s assertion and on the suitability of the design and operating effectiveness of the controls to provide reasonable assurance that the service organization commitments and system requirements were met based on applicable trust services criteria.

We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA). Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, (1) the description is fairly presented based on the description criteria, (2) the controls were suitably designed to provide reasonable assurance that the service organization's commitments and system requirements would be achieved if controls operated effectively based on the applicable trust services criteria and (3) the controls operated effectively to provide reasonable assurance that the service organization's commitments and system requirements were achieved based on the applicable trust services criteria throughout the period December 23, 2024 to December 22, 2025.

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

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively.
- 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.
- Testing the operating effectiveness of controls stated in the description 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 users and may not therefore include every aspect of the system that each individual user may consider important to its own particular needs. Because of their nature and inherent limitations, controls at a service organization may not always operate effectively to meet the applicable trust services criteria.

Also, the projection to the future of any evaluation of the fairness of the presentation of the description or conclusions about the suitability of the design of the controls to meet the applicable trust services criteria is subject to the risks that the system may change or that controls at a service organization may become inadequate or fail.

Description of tests of controls

The specific controls were tested and the nature, timing, and results of those tests are listed in Section 4.

Opinion

In our opinion, in all material respects, based on the description criteria described in Intentwise Inc.'s assertion and the applicable trust services criteria:

a. The description presents Intentwise Inc.'s Intentwise Ad Optimizer, Intentwise Analytics Cloud and Intentwise Explore Software Application that was designed and implemented throughout the period December 23, 2024 to December 22, 2025, in accordance with the description criteria.

b. The controls stated in the description were suitably designed to provide reasonable assurance that the service organizations commitments and system requirements would be achieved if the controls operated effectively based on the applicable trust services criteria and if sub-service organizations and user entities applied the controls contemplated in the design of Intentwise Inc.'s controls throughout the period December 23, 2024 to December 22, 2025.

c. The controls stated in the description operated effectively throughout the period December 23, 2024 to December 22, 2025, to provide reasonable assurance that Intentwise Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Intentwise Inc.'s controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in the description of tests and results is intended solely throughout information and use of user entities of Intentwise Inc.'s Intentwise Ad Optimizer, Intentwise Analytics Cloud and Intentwise Explore Software Application throughout the period December 23, 2024 to December 22, 2025, and prospective user entities, 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 organizations' system interacts with the user entities, subservice organizations, or other parties.
- Internal controls and their limitations.
- Complementary subservice organizations and complementary user entity controls and how those controls interact with the controls at the service organizations 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 applicable trust services criteria 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.

CertPro CPA LLC

Certified Public Accountants
License Number: CF-0010928
State of Delaware
February 20, 2026

Section 2

Management's Assertion

MANAGEMENT'S ASSERTION

Intentwise Inc.'s Management Assertion throughout the period December 23, 2024 to December 22, 2025

We have prepared the attached description titled "Description of Intentwise Inc.'s Intentwise Ad Optimizer, Intentwise Analytics Cloud and Intentwise Explore Software Application" throughout the period December 23, 2024 to December 22, 2025 (the description), based on the criteria in items (a) (i)–(ii) below, which are the criteria for a description of a service organization's system given in DC section 200 prepared by AICPA's Assurance Services Executive Committee (ASEC), through its Trust Information Integrity Task Force's SOC 2 Guide Working Group to be used in conjunction with the AICPA Guide Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (the description criteria). The description is intended to provide users with information about Intentwise Ad Optimizer, Intentwise Analytics Cloud and Intentwise Explore Software Application provided by Intentwise Inc., that may be useful when assessing the risks from interactions with the system throughout the period December 23, 2024 to December 22, 2025 particularly information about the suitability of the design and operating effectiveness of controls to meet Intentwise Inc.'s service commitments and system requirements based on the criteria related to Security, Confidentiality and Availability (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).*

Intentwise Inc. uses Amazon Web Services Inc. (AWS), a subservice organization, to provide cloud Software-as-a-Service (SaaS), Microsoft Azure, a cloud computing service operated by Microsoft for application management, Google Cloud Platform Inc. (GCP), a subservice organization, to provide cloud Software-as-a-Service (SaaS), Heroku, Inc., a subservice organization, to provide cloud Platform-as-a-Service (PaaS) for building, running, and scaling applications, supporting multiple programming languages and integrated add-on services, GitHub, a cloud computing service operated by GitHub Inc. (GitHub), a subservice organization, to provide and host the GitHub application and Google Workspace, a collection of cloud computing, productivity and collaboration tools, software, and products such as Gmail, Calendar, Drive, Docs, Sheets, Slides, Meet, and many more. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Intentwise Inc., to achieve Intentwise Inc.'s service commitments and system requirements based on the applicable trust services criteria. The description presents Intentwise Inc.'s controls, the applicable trust services criteria and the types of complementary subservice organization controls assumed in the design of Intentwise Inc.'s controls. The description does not disclose the actual controls at the subservice organizations.

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

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

1. The description of Intentwise Ad Optimizer, Intentwise Analytics Cloud and Intentwise Explore Software Application provided by Intentwise Inc. throughout the period December 23, 2024 to December 22, 2025. The criteria for description are identified below under the heading "Description Criteria".

2. The controls stated in the description were suitably designed and operated effectively to meet Intentwise Inc.'s service commitments and system requirements based on the applicable trust services criteria throughout the period December 23, 2024 to December 22, 2025, to meet the applicable trust services criteria.

Description Criteria:

i. The description contains the following information:

1. The types of services provided.
2. The principal service commitments and system requirements.
3. The components of the system used to provide the services, which are the following:
    - Infrastructure - The physical and hardware components of a system (facilities, equipment, and networks).
    - Software - The programs and operating software of a system (systems, applications, and utilities).
    - People - The personnel involved in the operation and use of a system (developers, operators, users, and managers).
    - Procedures - The automated and manual procedures involved in the operation of a system.
    - Data - The information used and supported by a system (transaction streams, files, databases, and tables).
4. The boundaries or aspects of the system are covered by the description.
5. The applicable trust services criteria and the related controls are designed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved.
6. Other aspects of the service organization's control environment, risk assessment process, communication and information systems and monitoring of controls that are relevant to the services provided and the applicable trust services criteria.

ii. The description does not omit or distort information relevant to the service organizations' system 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 his or her own needs.

For Intentwise Inc.



Raghu Kashyap - CTO & Founder

Authorized Signatory

02 / 19 / 2026

Section 3

Description of the System

Overview of Operations

Types of Services Provided

Intentwise Ad Optimizer, Intentwise Analytics Cloud and Intentwise Explore Software Application built by Intentwise Inc.

Intentwise Inc. helps worldwide brands accelerate their ecommerce growth on marketplaces such as Amazon, Walmart, Instacart, and Target. Intentwise Inc.'s technology platform empowers professional advertisers, large-scale aggregators, and high-volume agencies with recommendations, automation, competitive intelligence, and data infrastructure for Amazon, Instacart, Target, Walmart, and more. Intenwise Inc. assist brands, agencies and aggregators in harnessing the data across the retail platforms and assist them with retail aware ad optimization by leveraging Intentwise products.

Any other services provided by Intentwise Inc. are not in the scope of this report.

Principal Service Commitments and System Requirements

Intentwise Inc. designs its processes and procedures to meet objectives for its software application. Those objectives are based on the service commitments that Intentwise Inc. makes to customers and the compliance requirements that Intentwise Inc. has established for their services.

Security commitments to user entities are documented and communicated in Intentwise Inc.'s customer agreements, as well as in the description of the service offering provided online. Intentwise Inc.'s security commitments are standardized and based on some common principles.

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

- The fundamental design of Intentwise Inc.'s software application addresses security concerns such that system users can access the information based on their role in the system and are restricted from accessing information not needed for their role.
- Intentwise Inc. implements various procedures and processes to control access to the production environment and the supporting infrastructure.
- Monitoring of key infrastructure components is in place to collect and generate alerts based on utilization metrics.
- Regular vulnerability scans over the system and network, and penetration tests over the production environment.
- Operational procedures for managing security incidents and breaches, including notification procedures.

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

- The use of encryption technologies to protect system data both at rest and in transit.
- Confidentiality and non-disclosure agreements with employees, contractors, and third parties.
- Confidential information must be used only for the purposes explicitly stated in agreements between Intentwise Inc. and user entities.

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

- System performance and availability monitoring mechanisms to help ensure the consistent delivery of the system and its components.
- Responding to customer requests in a reasonably timely manner.
- Business Continuity and Disaster Recovery Plans are tested on a periodic basis.
- Operational procedures supporting the achievement of availability commitments to user entities.

Such requirements are communicated in Intentwise Inc.'s system policies and procedures, system design documentation, and contracts with customers. System controls and design are aligned with applicable legal and contractual obligations, including data protection requirements under ISO 27001:2022 & GDPR and security commitments defined in customer SLAs.

Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures are documented on how to carry out specific manual and automated processes required in the operation and development of the system.

Components of the System Used to Provide Services

Infrastructure

The production infrastructure for the Intentwise Ad Optimizer, Intentwise Analytics Cloud and Intentwise Explore Software Application is hosted on Amazon Web Services, Microsoft Azure, Google Cloud Platform and Heroku in their various regions across US-West-2.

Intentwise Ad Optimizer, Intentwise Analytics Cloud and Intentwise Explore Software Application use a virtual and secure network environment on top of Amazon Web Services, Microsoft Azure, Google Cloud Platform and Heroku infrastructure to ensure that the software application is always protected. This is achieved by hosting the application inside a Virtual Private Cloud (VPC) and accompanying firewalls on the infrastructure provider. Intentwise Ad Optimizer, Intentwise Analytics Cloud and Intentwise Explore Software Application ensures there are only specific authorized points of entry, and filters traffic to the private networks that support the application.

When a customer's client device connects to the application over the internet, their data is encrypted and secured over HTTPS. It then passes through the software application Internet Gateway, over to a Virtual Private Cloud that:

1. Houses the entire application runtime.
2. Protects the application runtime from any external networks.

The internal networks of Amazon Web Services, Microsoft Azure, Google Cloud Platform and Heroku are protected by deny-by-default security groups and firewalls to ensure that only deliberately allowed traffic can pass through.

Further, all VPC network flow logs, DNS logs, and other AWS console events are continuously monitored by AWS Guard duty to spot malicious activity and unauthorized behavior. Specifically, AWS Guard Duty uses machine learning, anomaly detection, and integrated threat intelligence to identify potential threats.

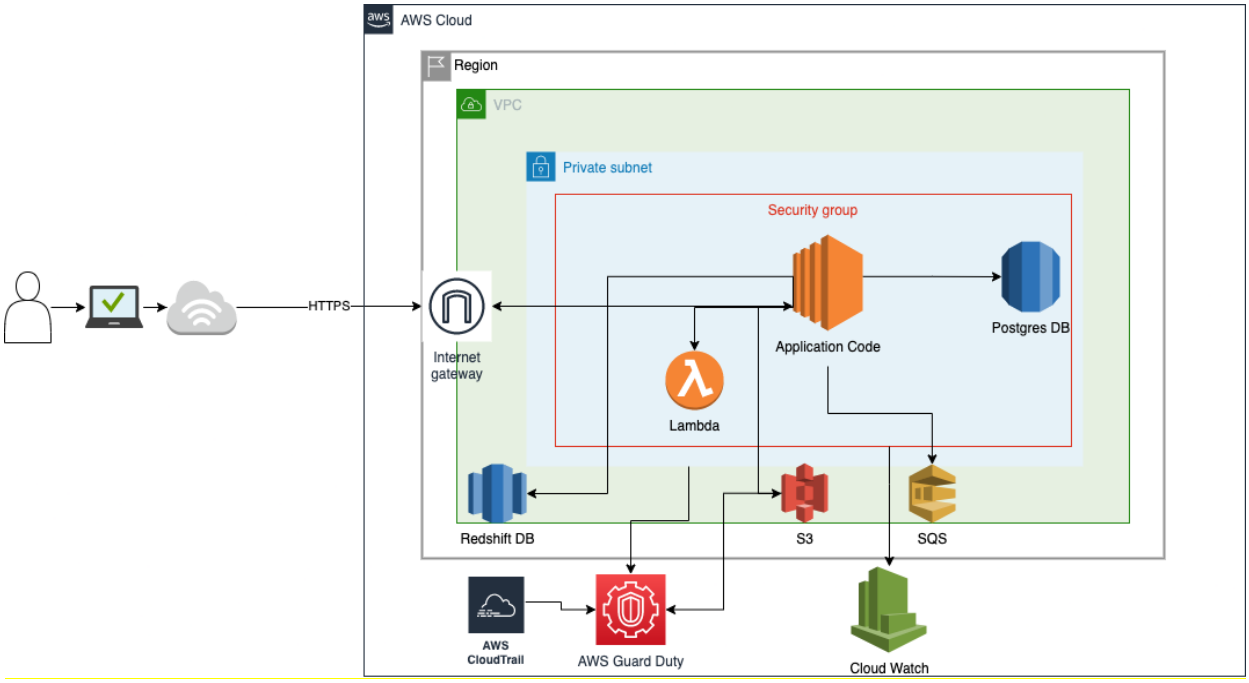
Software

Intentwise Inc. is responsible for managing the development and operation of the Intentwise Ad Optimizer, Intentwise Analytics Cloud and Intentwise Explore Software Application including infrastructure components such as servers, databases, and storage systems. The in-scope Intentwise Ad Optimizer, Intentwise Analytics Cloud and Intentwise Explore Software Application infrastructure and software components are shown in the table below:

Primary Infrastructure and Software			
System / Application	**Business Function / Description**	**Underlying Operating System & Storage**	**Physical Location**
Intentwise Ad Optimizer, Intentwise Analytics Cloud and Intentwise Explore application	Access to the Intentwise Ad Optimizer, Intentwise Analytics Cloud and Intentwise Explore SaaS application is through a web/mobile interface and user authentication.	Linux, Ubuntu with Postgres, Redshift, Big Query	Amazon Web Services, Microsoft Azure, Google Cloud Platform, Heroku US-West-2
Amazon Web Services, Microsoft Azure, Google Cloud Platform, Heroku IAM	Identity and access management console for AWS resources.	Amazon Web Services, Microsoft Azure, Google Cloud Platform, Heroku Proprietary	Amazon Web Services, Microsoft Azure, Google Cloud Platform, Heroku
Amazon Web Services, Microsoft Azure, Google Cloud Platform, Heroku Firewalls	Front-end firewalls protect the network perimeter with rule-based ACLs and back-end firewalls segregate the database servers from internal traffic.	Amazon Web Services, Microsoft Azure, Google Cloud Platform, Heroku Proprietary	Amazon Web Services, Microsoft Azure, Google Cloud Platform, Heroku
GitHub	Source code repository, version control system, and build software.	GitHub Proprietary	GitHub Cloud
Google Workspace and Office 365	Identity/Email provider for all Intentwise Inc. employees.	Google Workspace Proprietary and Office 365 Proprietary	Google Workspace and Office 365

Supporting Tools	
System / Application	**Business Function / Description**
Java, Python and JavaScript	Programming Language used for Intentwise Ad Optimizer, Intentwise Analytics Cloud and Intentwise Explore application.
Sprinto	Provide continuous compliance monitoring of the company's system.
Google Workspace and Office 365	Office communication services.

Network Architecture Diagram



People

Intentwise Inc.'s staff have been organized into various functions like Sales, Support, Engineering, Product Management, etc. The personnel have also been assigned to the following key roles:

Senior Management: Senior management carries the ultimate responsibility for achieving the mission and objectives of the organization. They ensure that the necessary resources are effectively applied to develop the capabilities needed to accomplish the organization's mission. They also assess and incorporate the results of the risk assessment activity into the decision-making process. The senior management understands that their support and involvement is required in order to run an effective risk management program that assesses and mitigates IT-related mission risks.

Information Security Officer: The Senior Management assigns the role of Information Security Officer to one of its staff members who is responsible for the performance of the information security program of the organization. Decisions made in these areas are based on an effective risk management program. The Information Security Officer is responsible for identifying risks, threats, and vulnerabilities, and adding controls to mitigate these risks. Additionally, they also summarize remaining residual risks and report the same to Senior Management in a timely manner.

Compliance Program Manager: The company assigns the role of Compliance Program Manager to a staff member who would be responsible for the smooth functioning of the Information Security Program. The Compliance Program Manager takes care of the effective and timely completion of tasks required for the functioning of all information security controls, across all functions/departments of the organization.

System Users: The organization's staff members are the users of the IT systems. The organization understands that use of the IT systems and data according to an organization's policies, guidelines, and rules of behavior is critical to mitigating risk and protecting the organization's IT resources. To minimize risk to the IT systems, staff members that access IT resources are provided with annual security awareness training.

Procedures and Policies

Formal policies and procedures have been established to support the Intentwise Ad Optimizer, Intentwise Analytics Cloud and Intentwise Explore Software Application. These policies cover:

- Code of Business Conduct
- Change Management
- Data Retention
- Data Backup
- Information Security
- Vendor Management
- Physical Security
- Risk Management
- Media Disposal
- Incident Management
- Endpoint Security
- Encryption
- Disaster Recovery
- Data Classification
- Confidentiality
- Business Continuity
- Access Control
- Acceptable Usage
- Vulnerability Management

Via the Sprinto platform, all policies are made available to all staff members to provide direction regarding the staff members' responsibilities related to the functioning of internal control. All staff members are expected to adhere to the policies and procedures that define how services should be delivered. Specifically, staff members are required to acknowledge their understanding of these policies upon hiring (and annually thereafter).

Intentwise Inc. also provides information to clients and staff members on how to report failures, incidents, concerns, or complaints related to the services or systems provided by the Intentwise Ad Optimizer, Intentwise Analytics Cloud and Intentwise Explore Software Application, in the event there are problems and takes actions within an appropriate timeframe as and when issues are raised.

Data

Data, as defined by Intentwise Inc., constitutes the following:

- Transaction Data
- Electronic Interface Files
- Output Reports
- Input Reports
- System Files
- Error Logs

All data that is managed, processed and stored as a part of the Intentwise Ad Optimizer, Intentwise Analytics Cloud and Intentwise Explore Software Application are classified as per the Data Classification Policy which establishes a framework for categorizing data based on its sensitivity, value, and criticality to achieving the objectives of the organization. All data is to be assigned one of the following sensitivity levels:

Data Sensitivity	Description	Examples
Customer Confidential	Highly valuable and sensitive information where the level of protection is dictated internally through policy and externally by legal and/or contractual requirements. Access to confidential information is limited to authorized employees, contractors, and business partners with a specific need.	• Customer system and operating data. • Customer PII. • Anything subject to a confidentiality agreement with a customer.
Company Confidential	Information that originated or is owned internally or was entrusted to Intentwise Inc. by others. Company confidential information may be shared with authorized employees, contractors, and business partners but not released to the general public.	• Intentwise Inc.'s PII. • Unpublished financial information. • Documents and processes explicitly marked as confidential. • Unpublished goals, forecasts, and initiatives marked as confidential. • Pricing/marketing and other undisclosed strategies.
Public	Information that has been approved for release to the public and is freely shareable both internally and externally.	• Press releases. • Public website.

Further, all customer data is treated as confidential. The availability of this data is also limited by job function. All customer data storage and transmission follow industry-standard encryption. The data is also regularly backed up as documented in the Data Backup Policy.

System Boundaries

A system is designed, implemented, and operated to achieve specific business objectives in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which includes the services and commitments outlined in the overview of operations and the five components described above: infrastructure, software, people, processes and procedures, and data.

Disclosure of Incidents

During the observation period from December 23, 2024 to December 22, 2025, incidents were recorded. Each incident was promptly addressed in accordance with established incident management procedures. None of the incidents resulted from a control failure, involved unauthorized access or data impact, or affected the achievement of service commitments or system requirements. No other incidents requiring disclosure were noted.

Relevant aspects of the Control Environment, Risk Assessment, Control Activities, Information and Communication and Monitoring Controls

The applicable trust services criteria were used to evaluate the suitability of design and operating effectiveness of controls stated in the description. Although the applicable trust services criteria and related controls are included in Section IV, they are an integral part of Intentwise Inc.'s description of the system. This section provides information about the five interrelated components of internal control at Intentwise Inc., including:

- Control Environment
- Risk Assessment
- Control Activities
- Information and Communication
- Monitoring Controls

Trust Services Categories

The following Trust Service Categories are in scope: **Common Criteria (to the Security, Confidentiality and Availability Categories).**

1. **Security** refers to the protection of:
    a. Information during its collection or creation, use, processing, transmission, and storage.
    b. Systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or another unauthorized removal of information or system resources, misuse of the software, and improper access to or use of, alteration, destruction, or disclosure of information.

2. **Confidentiality** addresses the entity's ability to protect information designated as confidential from its collection or creation through its final disposition and removal from the entity's control in accordance with management's objectives. Information is confidential if the custodian (for example, an entity that holds or stores information) of the information is required to limit its access, use, and retention and restrict its disclosure to defined parties (including those who may otherwise have authorized access within its system boundaries). Confidentiality requirements may be contained in laws or regulations or in contracts or agreements that contain commitments made to customers or others. The need for information to be confidential may arise for many different reasons. For example, the information may be proprietary and intended only for entity personnel. Confidentiality is distinguished from privacy in that privacy applies only to personal information, whereas confidentiality applies to various types of sensitive information. In addition, the privacy objective addresses requirements regarding the collection, use, retention, disclosure, and disposal of personal information. Confidential information may include personal information as well as other information, such as trade secrets and intellectual property.

3. **Availability** refers to the accessibility of information used by the entity's systems, as well as the products or services provided to its customers. The availability objective does not, in itself, set a minimum acceptable performance level; it does not address system functionality (the specific functions a system performs) or usability (the ability of users to apply system functions to the performance of specific tasks or problems). However, it does address whether systems include controls to support accessibility for operation, monitoring, and maintenance.

Any applicable trust services criteria that are not addressed by control activities at Intentwise Inc. are described within the sections titled **"Complementary User Entity Controls"** and **"Complementary Subservice Organization Controls".**

Control Environment

Integrity & 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 Intentwise Inc.'s control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical

behavior are the product of Intentwise Inc.'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.

Intentwise Inc. and its management team have established the following controls to incorporate ethical values throughout the organization:

- A formally documented "Code of Business Conduct" communicates the organization's values and behavioral standards to staff members.
- Staff members are required to acknowledge (upon hiring and annually thereafter) comprehensive policies and procedures covering the areas of Information Security, Change Management, Incident Management, and Access Control. Staff Members also acknowledge that they understand their responsibility for adhering to the policies and procedures.
- All new employees go through background checks as a part of the hiring process.

Commitment to Competence

Intentwise Inc.'s management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. The following controls have been established in order to incorporate the commitment to competence throughout the organization:

- Management outlines the roles and responsibilities of technical staff to ensure that they are clear about their responsibilities in the organization. These roles and responsibilities are reviewed annually by the senior management.
- Annual Security Awareness Training is provided to all staff which focuses on maintaining the security of the proprietary and customer-servicing systems and related data.
- Employees receive periodic reviews by their supervisors inclusive of discussing any deficiencies noted in the execution of their job responsibilities.
- Employees are evaluated for competence in performing their job responsibilities at the time of hiring.

Management Philosophy and Operating Style

Intentwise Inc.'s management philosophy and operating style encompasses a broad range of characteristics. Such characteristics include management's approach to monitoring business risks, and management's attitudes toward personnel and the processing of information.

Intentwise Inc.'s information security function, composed of senior management and the Information Security Officer, meets frequently and includes at least an annual meeting to review policies and procedures and set the information security program roadmap. The security function, under the direction of senior management, oversees the security activities and communication of its policies and procedures.

Specific control activities that the Intentwise Inc. has implemented in this area are described below:

- Senior management meetings are held to discuss major initiatives and issues that affect the business as a whole.
- Senior management reviews the functioning of internal controls, vendor risk assessment, risk assessment and high severity security incidents annually.
- Senior management meets frequently and includes at least an annual meeting to review policies and procedures and set the information security program roadmap.

Organizational Structure and Assignment of Authority and Responsibility

Intentwise Inc.'s organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes that 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.

The management is committed to maintaining and improving its framework for how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. This 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. Organizational charts are in place to communicate key areas of authority and responsibility. These charts are accessible to all employees of the company and are updated as required.

Human Resources

Intentwise Inc.'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 the management's ability to hire and retain top-quality personnel who ensure the service organization operates at maximum efficiency.

Specific control activities that the Intentwise Inc. has implemented in this area are described below:

- Background checks are performed on new hires, who are evaluated for competence in performing their job responsibilities at the time of hiring.
- Job positions are supported by job descriptions.
- New employees are required to acknowledge company policy and confidentiality-related agreements upon hire and annually thereafter.
- Upon hire and annually thereafter, all employees must complete training courses covering basic information security practices.
- Performance evaluations for each employee are performed on an annual basis.
- If an employee violates the Code of Business Conduct in the employee handbook or the company's policies or otherwise acts in a manner deemed contrary to the mission and objectives of the company, the employee is subject to sanctions up to and including termination of employment.
- When a person is relieved of duties from the company, access to critical systems is made inaccessible in a timely manner.

Risk Assessment

Intentwise Inc.'s risk assessment process identifies and manages risks that could potentially affect its ability to provide reliable services to its customers. The management is expected to identify significant risks inherent in products and services as they oversee their areas of responsibility. Intentwise Inc. identifies the underlying sources of risk, measures the impact on the organization, establishes acceptable risk tolerance levels and implements appropriate measures to monitor and manage the risks.

This process identifies risks to the services provided by the Intentwise Inc. and the management has implemented various measures designed to manage these risks.

Intentwise Inc. believes that effective risk management is based on the following principles:

1. Senior management's commitment to the security of Intentwise Ad Optimizer, Intentwise Analytics Cloud and Intentwise Explore Software Application.
2. The involvement, cooperation, and insight of all Intentwise Inc. staff.
3. Initiating risk assessments with discovery and identification of risks.
4. A thorough analysis of identified risks.
5. Commitment to the strategy and treatment of identified risks.
6. Communicating all identified risks to the senior management.
7. Encouraging all Intentwise Inc. staff to report risks and threat vectors.

Scope

The Risk Assessment and Management program applies to all systems and data that are a part of the Intentwise Ad Optimizer, Intentwise Analytics Cloud and Intentwise Explore Software Application. The Intentwise Inc. risk assessment exercise evaluates infrastructure such as computer infrastructure, containing networks, instances, databases, systems, storage, and services. The risk assessments also include an analysis of business/IT practices, procedures, and physical spaces as needed.

Risk assessments may be high-level or detailed to a specific organizational or technical change as the stakeholders and technologists see fit.

Overall, the execution, development, and implementation of risk assessment and remediation programs is the joint responsibility of Intentwise Inc.'s Information Security Officer and the department or individuals responsible for the area being assessed. All Intentwise Inc. staff are expected to cooperate fully with any risk assessment being conducted on systems and procedures for which they are responsible. Staff is further expected to work with the risk assessment project lead in the development of a remediation plan per risk assessment performed.

Potential for Fraud

Management considers the potential for fraud when assessing the risks Intentwise Inc.’s objectives. Management realizes that the potential for fraud can occur in several forms including when employees are motivated by certain pressures or incentivized to commit fraud. The absence of controls, or ineffective controls, provides an opportunity for fraud when combined with an incentive to commit fraud. Documented policies and procedures are in place to guide personnel in identifying the potential for fraud when performing the risk assessment process. The annual risk assessment process considers the potential for fraud. Identified risks are rated using a risk evaluation process and are formally documented, with mitigation strategies, for management review.

Vendor Risk Assessment

Intentwise Inc. uses a number of vendors to meet its business objectives. Intentwise Inc. understands that risks exist when engaging with vendors and as a result, continuously assesses those risks that could potentially affect the Company's ability to meet its business objectives.

Intentwise Inc. employs several activities to effectively manage their vendors. Firstly, the Information Security Officer performs an annual exercise of thoroughly examining the nature and extent of risks involved with each vendor relationship. For critical vendors, Intentwise Inc. assesses vendor compliance commitments through the review of available information security assessment reports and determines whether compliance levels adequately support Intentwise Inc.'s commitments to its customers. If a critical vendor is unable to provide a third-party security report or assessment, Intentwise Inc. management meets with such vendors periodically to assess their performance, security concerns, and their services. Any vendor risks identified are recorded in the risk assessment matrix, which is reviewed annually by the Senior Management of the company.

Integration with Risk Assessment

As part of the design and operation of the system, Intentwise Inc. identifies the specific risks that service commitments may not be met, and designs control necessary to address those risks. Intentwise Inc.'s management performs an annual Risk Assessment Exercise to identify and evaluate internal and external risks to the Company, as well as their potential impacts, likelihood, severity, and treatment.

Control Activities

Intentwise Inc.'s control activities are defined through its established policies and procedures which address individual risks associated with the achievement of the company's objectives. Such statements may be documented, explicitly stated in communications, or implied through actions and decisions.

Policies serve as the basis for procedures. Control activities are deployed through policies that establish what is expected and procedures that put policies into action.

Logical Access Control

The Intentwise Ad Optimizer, Intentwise Analytics Cloud and Intentwise Explore Software Application use role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. User access, which is role-based, is controlled in the platform and authenticates the database.

Intentwise Inc. has identified certain systems that are critical to meet its service commitments. All-access to critical systems is under the principle of least required privilege (wherein a staff member is granted the minimum necessary access to perform their function) and controlled by the role of the staff member as well as a role-based access matrix prior to being issued system credentials and granted the ability to access the system. When a person is relieved of duties from the company, access to critical systems is made inaccessible in a timely manner.

The Information Security Officer is responsible for performing quarterly reviews of everyone who has access to the system and assessing the appropriateness of the access and permission levels and making modifications based on the principle of least privilege, whenever necessary.

Access to critical systems requires Multi Factor Authentication (MFA) wherever possible. Staff members must use complex passwords, wherever possible, for all of their accounts that have access to Intentwise Inc. customer data. Staff are encouraged to use passwords that have at least 10 characters, are randomly generated, alphanumeric, and are special-character based. Password configuration settings are configured on each critical system. Additionally, company owned endpoints are configured to auto-screen-lock after 15 minutes of inactivity.

Physical Access and Environmental Controls

The in-scope system and supporting infrastructure are hosted by Amazon Web Services, Microsoft Azure, Google Cloud Platform and Heroku. As such, Amazon Web Services, Microsoft Azure, Google Cloud Platform and Heroku is responsible for the Physical Security controls of the in-scope system. Intentwise Inc. reviews the SOC 2 report provided by Amazon Web Services, Microsoft Azure, Google Cloud Platform and Heroku on an annual basis, to ensure their controls are in accordance with standards expected by the customers of the Intentwise Ad Optimizer, Intentwise Analytics Cloud and Intentwise Explore Software Application.

Incident Management

Intentwise Inc. has an incident management framework that includes defined processes, roles, communications, responsibilities, and procedures for detection, escalation, and response to incidents internally and to customers. Customers are directed to contact Intentwise Inc. via the support email address provided during onboarding to report failures, incidents, concerns, or other complaints in the event there were problems.

Incident response procedures and centralized tracking tools consist of different channels for reporting production system incidents and weaknesses. Production infrastructure is configured to generate audit events for actions of interest related to operations and security. Security alerts are tracked, reviewed, and analyzed for anomalous or suspicious activity.

Where required, security incidents are escalated to privacy, legal, customer, or senior management team(s) and assigned to a severity rating. Operational events are automatically resolved by the self-healing system.

- **Low severity incidents** are those that do not require immediate remediation. These typically include a partial service of Intentwise Inc. being unavailable (for which workarounds exist). This does not require someone to be paged or woken up beyond normal work hours.

- **Medium severity incidents** are similar to low but could include scenarios like suspicious emails or unusual activity on a staff laptop. Again, these do not require immediate remediation or trigger automatic calls outside work hours. Low and medium-severity incidents usually cover the large majority of incidents found.

- **High severity incidents** are problems an active security attack has not yet happened but is likely. This includes situations like backdoors, malware, and malicious access to business data (e.g., passwords, payment information, vulnerability data, etc.). In such cases, the information security team must be informed, and immediate remediation steps should begin.

- **Critical severity incidents** are those where a security attack was successful and something important was lost (or irreparable damage caused to production services). Again, in such cases, immediate actions need to be taken to limit the damage.

Post-mortem activities are conducted for incidents with critical severity ratings. Results of post-mortems may include updates to the security program or changes to systems required as a result of incidents.

Network Operations Monitoring

Web applications are protected by deploying network firewalls and security groups that inspect traffic flowing to the web application for common attacks. The network is segmented based on the label or classification level of the information stored on the servers. This includes filtering between Virtual Private Cloud (VPC) environments to help ensure only authorized systems are able to communicate with other systems necessary to fulfill their specific responsibilities. Operations and security functions use a variety of security utilities to identify and detect possible security threats and incidents. These utilities include, but are not limited to, firewall notifications, Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) alerts, vulnerability assessment reports, and operating system event logs.

Incidents and alerts from the security utilities are reviewed by Intentwise Inc. management. Security events requiring further investigation are tracked using internal ticketing systems and monitored until resolved.

Intentwise Inc. only uses network ports, protocols, and services listening on a system with validated business need to run on each system. Default-deny rules drop traffic except those services and ports that are explicitly allowed.

Cryptography

User requests to Intentwise Inc.'s systems are encrypted using Transport Layer Security (TLS) using certificates from an established third-party certificate authority. Remote system administration access to Intentwise Inc. web and application servers are available through cryptographic network protocols (i.e., SSH) or an encrypted Virtual Private Network (VPN) connection. Data at rest is encrypted using Advanced Encryption Standard (AES) 256 bit.

Change Management

A documented Change Management Policy guides all staff members in documenting and implementing application and infrastructure changes. It outlines how changes to the Intentwise Ad Optimizer, Intentwise Analytics Cloud and Intentwise Explore system are reviewed, deployed, and managed. The policy covers all changes made to the Intentwise Ad Optimizer, Intentwise Analytics Cloud and Intentwise Explore regardless of their size, scope, or potential impact.

The Change Management Policy is designed to mitigate the risks of:

- Corrupted or destroyed information.
- Degraded or disrupted platform performance.
- Productivity loss.
- Introduction of software bugs, configuration errors, vulnerabilities, etc.

A change to the Intentwise Ad Optimizer, Intentwise Analytics Cloud and Intentwise Explore can be initiated by a staff member with an appropriate role. Intentwise Inc. uses a version control system to manage and record activities related to the change management process.

The version control system maintains source code versions and migrates source code through the development and testing process to the production environment. The version control software maintains a history of code changes to support rollback capabilities. It also facilitates the code review process which is mandated for all changes.

To initiate a change, the developer first creates a feature branch with the updated code. Once the code change is ready for review, the developer submits the code for peer review and automated testing, known as a pull request. For all code changes, the reviewer must be different from the author. Once a pull request is approved, the change can be released to production.

The ability to implement changes in the production infrastructure is restricted to only those individuals who require the ability to implement changes as part of their responsibilities.

Software Security Assurance

Secure coding practices are established based on the programming language and development environment used. In-house developed software includes explicit error checking and documented inputs, including for size, data type, and acceptable ranges or formats. Security analysis is performed to verify secure coding practices are followed during change control. Vulnerabilities identified, if any, are tracked to resolution.

Asset Management (Hardware and Software)

Assets used in the system are inventoried or tagged to include business descriptions, asset ownership, versions, and other configuration levels, as appropriate, to help ensure assets are classified appropriately, patched, and tracked as part of configuration management. Intentwise Inc. uses tagging tools to automatically facilitate the company's hardware and software asset inventory. This helps to ensure a complete and accurate inventory of technology assets with the potential to store or process information is maintained.

Vulnerability Management

Vulnerability scanning tools are used to automatically scan systems on the network at least monthly to identify potential vulnerabilities. Automated software update tools are used to help ensure operating systems are running the most recent security updates provided by the software vendor. Vulnerabilities identified are risk- ranked to prioritize the remediation of discovered vulnerabilities.

External penetration tests are performed at least annually and include a full scope of blended attacks, such as client-based and web application attacks.

Endpoint Management

Endpoint management solutions are in place that include policy enforcement on company-issued devices, as well as bring-your-own devices that could connect to or access data within the system boundaries. Policies enforced on endpoints include but are not limited to enabling screen lock, OS updates, and encryption at rest on critical devices/workstations.

To help prevent malware, the following are implemented within the organization:

- Email attachments entering the organization's email gateway are scanned for viruses.
- Anti-malware software to continuously monitor and defend each of the organization's workstations and servers.

Availability

Intentwise Inc. has a documented Business Continuity Plan (BCP) and testing performed against the Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs). At least daily backup schedules are maintained to protect sensitive data from loss in the event of a system failure. Backups are restored at least annually as part of operational activities and are included as part of the BCP test plan.

Information and Communication

Pertinent information must be identified, captured, and communicated in a form and timeframe that enables people to carry out their responsibilities. Policies and procedures are in place to guide employees in providing effective communication to both internal and external parties. Information systems also produce reports that make it possible to run and control the business. Intentwise Inc. deals not only with internally generated data, but also information about external events, activities, and conditions necessary to inform business decision-making and external reporting. Effective communication must occur throughout the organization and between external parties to achieve objectives and principal service commitments. Personnel must receive a clear message from top management that control responsibilities must be taken seriously. They must understand their own role in the internal control system, as well as how individual activities relate to the work of others.

Internal Communications

Intentwise Inc. has implemented various methods of internally communicating information including objectives and responsibilities for internal control necessary to support the functioning of internal control. Specific control activities that Intentwise Inc. have implemented in this area are described below:

- Documented policies and procedures are in place to guide personnel in areas including, but not limited to, the following:
  - Information Security
  - Access Control
  - Data Retention
  - Change Management
- Internal control responsibilities regarding security are documented within the organization's policies. Employees are required to acknowledge that they have read and understand their responsibilities upon hire and annually thereafter.
- Employees are required to complete security awareness training upon hire, and annually thereafter, to understand their obligations and responsibilities to comply with the corporate security policies.
- Documented job descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs, and are communicated to employees through the Intentwise Inc. intranet.
- Documented escalation procedures for reporting security incidents are provided to internal users to guide them in identifying and reporting failures, incidents, concerns, and other complaints.
- Employees are required to acknowledge, upon hire and at least annually thereafter, that they have been given access to the employee handbook and code of conduct and understand their responsibility for adhering to Intentwise Inc.'s behavioral standards.
- Executive management meetings are held with operational management at least annually to discuss and align internal control responsibilities, performance measures, and incentives with company objectives.
- Reporting procedures are in place to facilitate the reporting of complaints, unethical behaviors, and fraudulent activities.

External Communications

Intentwise Inc. has also implemented various methods of communicating with external parties regarding matters affecting the functioning of internal control. Specific control activities that Intentwise Inc. has implemented in this area are described below:

- Intentwise Inc.'s security commitments and the associated system requirements are documented in the enterprise hosting terms.
- System components, planned outages, and known issues are communicated to external parties via the company website.
- Vendors and third parties are required to enter an agreement with Intentwise Inc. for services provided that includes statements of confidentiality.
- Communication channels are in place to enable external parties to report security incidents, concerns, and complaints.
- Intentwise Inc. contact information and relevant communication channels are available to external parties via the public-facing website.

Monitoring Controls

Intentwise Inc.'s management monitors control to ensure that they are operating as intended and that the controls are modified as conditions change. Monitoring activities are undertaken 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. Staff activity and adherence to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, independent evaluations, or a combination of the two.

Ongoing Monitoring

Intentwise Inc. has selected, developed, and implemented ongoing monitoring procedures to ascertain whether the components of internal controls are present and functioning. TechOwl's vulnerability assessments of in-scope systems are performed on a continuous basis to identify threats and assess their potential impact to system security. Identified security findings classified as 'critical' are triaged by the security team and monitored through to resolution. Security applications are in place to monitor and analyze the in-scope systems for security vulnerabilities to production images and the intentwise website, including any possible or actual security breaches. Identified security vulnerabilities are triaged by the security team and monitored through resolution.

Independent Evaluations

Security and compliance personnel obtain a penetration testing report annually as evidence that a third-party specialist performed penetration testing. Management reviews the results of the penetration tests and remediation plans are proposed and monitored through resolution. The audit committee, composed of executive management personnel, performs an internal audit annually to identify potential control gaps and weaknesses. Management reviews result of third-party audits at least annually. Intentwise Inc. process owners and management are continuously developing processes, controls, and policies to address risks that threaten service commitments.

Complementary User Entity Controls

Intentwise Inc.'s controls were designed with the assumption that certain internal controls would be in place at user entity. The application of such internal controls by user entity is necessary to achieve certain trust services criteria identified in this report. In addition, there may be control activities that are not identified in this report that would be appropriate for processing of transactions for Intentwise Inc. user entity.

For user entity to rely on the information processed through the Intentwise Inc.'s software application, each user entity is expected to evaluate its own internal controls to ensure appropriate control activities are in place. The following general procedures and controls should be considered. They should not, however, be regarded as a comprehensive list of all controls that should be implemented by user entity.

- User entity is responsible for managing their organization's Intentwise Inc.'s software application account as well as establishing any customized security solutions or automated processes through the use of setup features.
- User entity is responsible for protecting established user IDs and passwords within their organizations.
- User entity is responsible for reviewing customer access to the Intentwise Inc.'s software application periodically to validate appropriateness of access levels.
- User entity is responsible for approving and creating new user access to the Intentwise Inc.'s software application.
- User entity is responsible for removing terminated employee access to the Intentwise Inc.'s software application.
- User entity is responsible for implementing policies and procedures over the types of data that are allowed to be entered into the Intentwise Inc.'s software application.
- User entity is responsible for sending data to Intentwise Inc.'s software application via a secure connection and/or the data should be encrypted.

- User entity is responsible for notifying Intentwise Inc.'s software application if they detect or suspect a security incident related to the Intentwise Inc.
- User entity is responsible for reviewing email and other forms of communications from Intentwise Inc., related to changes that may affect Intentwise Inc. customers and users, and their security or availability obligations.
- User entity is responsible for establishing, monitoring, and maintaining controls over the security for system-generated outputs and reports from the system.
- User entity is responsible for endpoint protection of workstations used to access the system.
- User entity is responsible for developing their own Business Continuity and Disaster Recovery Plan.

The list of complementary user entity control considerations presented above does not represent a comprehensive list of all the controls that should be deployed by user organizations. Other controls may be required at the user organization in order to achieve adequate internal control.

Complementary Subservice Organization Controls

Intentwise Inc. uses subservice organizations in support of its system. Intentwise Inc.'s controls related to the system cover only a portion of overall internal control for user entities. It is not feasible for the trust services criteria over the Intentwise Inc. to be achieved solely by Intentwise Inc. Therefore, user entity controls must be evaluated in conjunction with Intentwise Inc.'s controls described in Section IV of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organization as described below.

Intentwise Inc. periodically reviews the quality of the outsourced operations by various methods including:

- Review of subservice organizations' SOC reports.
- Regular meetings to discuss performance.
- Non-disclosure agreements.

Control Activity Expected to be Implemented by Subservice Organization	Subservice Organization	Applicable Criteria
Logical access to the underlying network and virtualization management software for the cloud architecture is appropriate.	Amazon Web Services, Microsoft Azure, Google Cloud Platform and Heroku	CC6.1, CC6.2, CC6.3, CC6.5, CC7.2
Physical access and security to the data center facility are restricted to authorized personnel.	Amazon Web Services, Microsoft Azure, Google Cloud Platform and Heroku	CC6.5
Environmental protection, including monitoring and alarming mechanisms, are implemented to address Physical & Environmental Security and environmental control requirements.	Amazon Web Services, Microsoft Azure, Google Cloud Platform and Heroku	A1.2
Business Continuity and Disaster Recovery Procedures are developed, reviewed, and tested periodically.	Amazon Web Services, Microsoft Azure, Google Cloud Platform and Heroku	A1.3

Control Activity Expected to be Implemented by Subservice Organization	Subservice Organization	Applicable Criteria
Policies and procedures to document repairs and modifications to the physical components of a facility including, but not limited to, hardware, walls, doors, locks, and other Physical & Environmental Security components.	Amazon Web Services, Microsoft Azure, Google Cloud Platform and Heroku	A1.2
A defined Data Classification Policy specifies classification levels and control requirements in order to meet the company's commitments related to confidentiality.	Amazon Web Services, Microsoft Azure, Google Cloud Platform and Heroku	C1.1
A defined process is in place to sanitize and destroy hard drives and backup media containing customer data prior to leaving company facilities.	Amazon Web Services, Microsoft Azure, Google Cloud Platform and Heroku	C1.2
Encryption methods are used to protect data in transit and at rest.	Amazon Web Services, Microsoft Azure, Google Cloud Platform and Heroku	CC6.1

Criteria Not Applicable to the System

All common and specific criteria under the Security, Availability, and Confidentiality categories of the 2017 Trust Services Criteria (TSP Section 100) were evaluated for applicability to the Intentwise Ad Optimizer, Intentwise Analytics Cloud and Intentwise Explore Software Application.

The Intentwise Inc. has determined that Processing Integrity and Privacy trust service categories are not relevant to the system as described in this report.

Significant Changes during the Observation Period

There were no significant changes that are likely to affect report users' understanding of how the in-scope system is used to provide the services covered by this examination during the observation period.

SECTION 4

TESTING MATRICES

TESTS OF OPERATING EFFECTIVENESS AND RESULTS OF TESTS

Scope of Testing

This report is on the controls relating to Intentwise Ad Optimizer, Intentwise Analytics Cloud and Intentwise Explore Software Application provided by Intentwise Inc. The scope of the testing was restricted to Intentwise Ad Optimizer, Intentwise Analytics Cloud and Intentwise Explore Software Application, and its boundaries as defined in Section 3. CertPro conducted the examination testing throughout the period December 23, 2024 to December 22, 2025.

Tests of Operating Effectiveness

The tests applied to test the operating effectiveness of controls are listed alongside each of the respective control activities within the Testing Matrices. Such tests were considered necessary to evaluate whether the controls were sufficient to provide reasonable, but not absolute, assurance that the applicable trust services criteria were achieved during the review period. In selecting the tests of controls, CertPro considered various factors including, but not limited to, the following:

- The nature of the control and the frequency with which it operates.
- The control risk is mitigated by the control.
- The effectiveness of entity-level controls, especially controls that monitor other controls.
- The degree to which the control relies on the effectiveness of other controls.
- Whether the control is manually performed or automated.

The types of tests performed with respect to the operational effectiveness of the control activities detailed in this section are briefly described below:

Test Approach	Description
Inquiry	Inquired of relevant personnel with the requisite knowledge and experience regarding the performance and application of the related control activity. This included in-personinterviews, telephone calls, e-mails, web-based conferences, or a combination of the preceding.
Observation	Observed the relevant processes or procedures during fieldwork. This included, butwas not limited to, witnessing the performance of controls or evidence of control performance with relevant personnel, systems, or locations relevant to the performance of control policies and procedures.
Inspection	Inspected the relevant audit records. This included, but was not limited to, documents,system configurations and settings, or the existence of sampling attributes, such as signatures, approvals, or logged events. In some cases, inspection testing involved tracing events forward to consequent system documentation or processes (e.g. resolution, detailed documentation, alarms, etc.) or vouching backwards for prerequisite events (e.g. approvals, authorizations, etc.).

Sampling

Consistent with American Institute of Certified Public Accountants (AICPA) authoritative literature, CertPro utilizes professional judgment to consider the tolerable deviation rate, the expected deviation rate, the audit risk, the characteristics of the population, and other factors, in order to determine the number of items to be selected in a sample for a particular test. CertPro, in accordance with AICPA authoritative literature, selected samples in such a way that the samples were expected to be representative of the population. This included judgmental selection methods, where applicable, to ensure representative samples were obtained.

System-generated population listings were obtained whenever possible to ensure completeness prior to selecting samples. In some instances, full populations were tested in cases including but not limited to, the uniqueness of the event or low overall population size.

Test Results

The results of each test applied are listed alongside each respective test applied within the Testing Matrices. Test results not deemed as control deviations are noted by the phrase “No exceptions noted” in the test result column of the Testing Matrices. Any phrase other than the aforementioned, constitutes either a test result that is the result of non-occurrence, a change in the application of the control activity, or a deficiency in the operating effectiveness of the control activity. Testing deviations identified within the Testing Matrices are not necessarily weaknesses in the total system of controls, as this determination can only be made after consideration of controls in place at user entities and subservice organizations, if applicable, and other factors.

SECURITY PRINCIPLE AND CRITERIA TABLE

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.0: CONTROL ENVIRONMENT			
CC1.1: COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
CC1.1.1	Entity has a documented policy to define behavioral standards and acceptable business conduct.	Inspected the company policies & Code of Business Conduct to determine the behavioral standards and acceptable business conduct. Observed that it has been reviewed and acknowledged by staff members.	No exceptions noted.
CC1.1.2	Entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.	Inspected the company policies to determine that the entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding. Observed that the policies have been reviewed and acknowledged by new staff members.	No exceptions noted.
CC1.1.3	Entity has established procedures for staff to acknowledge applicable company policies periodically.	Inspected the company policies to determine that the entity has established procedures for staff to acknowledge applicable company policies periodically. Observed records that the policies have been reviewed and acknowledged by staff members.	No exceptions noted.
CC1.1.4	Entity requires that new staff members review and acknowledge the Code of Business Conduct upon hire, and that all staff members review and acknowledge it annually.	Inspected evidence of employee acknowledgement of the Code of Business Conduct for a sample of new employees to determine that the new staff members review and acknowledge the Code of Business Conduct upon hire, and that all staff members review and acknowledge it annually.	No exceptions noted.
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	Entity's Senior Management reviews and approves all company policies annually.	Inspected annual records that the company policies have been reviewed and approved by the Senior Management.	No exceptions noted.
CC1.2.2	Entity's Senior Management reviews and approves the "Risk Assessment Report" annually.	Inspected annual records showing that the Senior Management has reviewed and approved the "Risk Assessment Report".	No exceptions noted.
CC1.2.3	Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.	Inspected annual records showing that the Senior Management has reviewed and approved the “Vendor Risk Assessment Report”.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.2.4	Entity's Senior Management reviews and approves the Organizational Chart for all employees annually.	Inspected annual records showing that Senior Management has reviewed and approved the entity's Organizational Chart.	No exceptions noted.
CC1.2.5	Entity's Senior Management reviews and approves the state of the Information Security program including policies, standards, and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.	Inspected the Management Review Meeting minutes showing review of relevant policies to determine that the Senior Management reviews and approves the state of the Information Security program including policies, standards, and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.	No exceptions noted.
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	Entity has established procedures to communicate with staff about their roles and responsibilities.	Inspected job descriptions for various job roles to determine that the entity has established procedures to communicate with staff about their roles and responsibilities.	No exceptions noted.
CC1.3.2	Entity's Senior Management assigns the role of Information Security Officer who is delegated to centrally manage, coordinate, develop, implement, and maintain an enterprise-wide cybersecurity and privacy program.	Inspected the Organizational Chart showing that the role of Information Security Officer has been appropriately assigned to an employee to determine that the Senior Management assigns the role of Information Security Officer who is delegated to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity and privacy program.	No exceptions noted.
CC1.3.3	Entity maintains an Organizational Structure to define authorities, facilitate information flow and establish responsibilities.	Inspected the company Organizational Structure which shows reporting structure by role to determine that the entity maintains an Organizational Structure to define authorities, facilitate information flow and establish responsibilities.	No exceptions noted.
CC1.3.4	Entity appoints a Compliance Program Manager who is delegated the responsibility of planning and implementing the internal control environment.	Observed that a Compliance Program Manager has been appointed who is delegated the responsibility of planning and implementing the internal control environment.	No exceptions noted.
CC1.3.5	Entity has set up mechanisms to assign and manage asset ownership responsibilities and establish a common understanding of asset protection requirements.	Observed that an Infrastructure Operations Person has been appointed to assign and manage asset ownership responsibilities and establish a common understanding of asset protection requirements.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.3.6	Entity appoints a People Operations Officer to develop and drive all personnel related security strategies.	Observed that a People Operations Officer has been appointed to develop and drive all personnel related security strategies.	No exceptions noted.
CC1.3.7	Entity's Senior Management reviews and approves the state of the Information Security program including policies, standards, and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.	Inspected the Management Review Meeting minutes showing review of relevant policies to determine that the Senior Management reviews and approves the state of the Information Security program including policies, standards, and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.	No exceptions noted.
CC1.4: COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
CC1.4.1	Entity has procedures to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.	Inspected new hire evaluation with applicant background and competencies for a sample of new hires to determine that the entity has procedures to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.	No exceptions noted.
CC1.4.2	Entity has established procedures to perform security risk screening of individuals prior to authorizing access.	Inspected background check details with details of the official documents collected as part of the onboarding process for a sample of new hires to determine that the entity has established procedures to perform security risk screening of individuals prior to authorizing access.	No exceptions noted.
CC1.5: COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
CC1.5.1	Entity has established procedures for new staff to complete security and privacy literacy training as a part of their onboarding.	Inspected the Security Awareness Training material provided to onboarded employees to determine that the entity has established procedures for new staff to complete security and privacy literacy training as a part of their onboarding.	No exceptions noted.
CC1.5.2	Entity has established procedures for staff to acknowledge applicable company policies periodically.	Inspected the company policies to determine that the entity has established procedures for staff to acknowledge applicable company policies periodically. Observed records that the policies have been reviewed and acknowledged by staff members.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.5.3	Entity requires that all employees in client serving, IT, Engineering, and Information Security roles are periodically evaluated regarding their job responsibilities.	Inspected the HR Security Policy and Procedure to determine that the entity requires that all employees are periodically evaluated regarding their Job responsibilities.	No exceptions noted.
CC1.5.4	Entity documents, monitors, and retains individual training activities and records.	Inspected the Information Security Training records to determine that the entity documents, monitors and retains individual training activities and records.	No exceptions noted.
CC1.5.5	Entity provides information security and privacy training to staff that is relevant to their job function.	Inspected the Information Security Training document to determine that the entity provides information security and privacy training to staff that is relevant for their job function.	No exceptions noted.
CC1.5.6	Entity requires that all staff members complete Information Security Awareness training annually.	Inspected annual records of Security Awareness Training completion for a sample of employees to determine that the entity requires that all staff members complete Information Security Awareness training.	No exceptions noted.
CC1.5.7	Entity requires that new staff members complete Information Security Awareness training upon hire, and that all staff members complete Information Security Awareness training annually.	Inspected records of Security Awareness Training completion for a sample of employees to determine the company requires that new staff members complete Information Security Awareness training annually.	No exceptions noted.
CC2.0: COMMUNICATION AND INFORMATION			
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	Entity systems generate information that is reviewed and evaluated to determine impacts on the functioning of internal controls.	Inspected the production infrastructure health monitoring records to determine that the entity systems generate information that is reviewed and evaluated to determine impacts to the functioning of internal controls.	No exceptions noted.
CC2.1.2	Entity makes all policies and procedures available to all staff members for their perusal.	Inspected the list of policies to determine that the entity makes all policies and procedures available to all staff members for their perusal.	No exceptions noted.
CC2.1.3	Entity displays the most current information about its services on its website, which is accessible to its customers.	Inspected the company's website to determine that the entity displays the most current information about its services on its website, which is accessible to its customers.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.1.4	Entity has a documented policy outlining guidelines for the disposal and retention of information.	Inspected the Data Retention Policy to determine that the entity has a documented policy outlining guidelines for the disposal and retention of information.	No exceptions noted.
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	Entity has established procedures for new staff to complete security and privacy literacy training as a part of their onboarding.	Inspected the Security Awareness Training material provided to onboarded employees to determine that the entity has established procedures for new staff to complete security and privacy literacy training as a part of their onboarding.	No exceptions noted.
CC2.2.2	Entity has established procedures for staff to acknowledge applicable company policies periodically.	Inspected the company policies to determine that the entity has established procedures for staff to acknowledge applicable company policies periodically. Observed records that the policies have been reviewed and acknowledged by staff members.	No exceptions noted.
CC2.2.3	Entity makes all policies and procedures available to all staff members for their perusal.	Inspected the list of policies to determine that the entity makes all policies and procedures available to all staff members for their perusal.	No exceptions noted.
CC2.2.4	Entity documents, monitors, and retains individual training activities and records.	Inspected the Information Security Training records to determine that the entity documents, monitors and retains individual training activities and records.	No exceptions noted.
CC2.2.5	Entity has provided information to employees, via various Information Security Policies/procedures, on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the entity in the event there are problems.	Inspected the Incident Management Policy and Procedure and the section that describes how to report incidents to determine that the entity has provided information to employees, on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the entity in the event there are problems.	No exceptions noted.
CC2.2.6	Entity has a documented policy to define behavioral standards and acceptable business conduct.	Inspected the company policies & Code of Business Conduct to determine the behavioral standards and acceptable business conduct. Observed that it has been reviewed and acknowledged by staff members.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.2.7	Entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.	Inspected the company policies to determine that the entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding. Observed that the policies have been reviewed and acknowledged by new staff members.	No exceptions noted.
CC2.2.8	Entity requires that all staff members complete Information Security Awareness training annually.	Inspected the Information Security Training document to determine that the entity provides information security training annually.	No exceptions noted.
CC2.2.9	Entity requires that new staff members complete Information Security Awareness training upon hire, and that all staff members complete Information Security Awareness training annually.	Inspected records of Security Awareness Training completion for a sample of employees to determine the company requires that new staff members complete Information Security Awareness training annually.	No exceptions noted.
CC2.3: COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.			
CC2.3.1	Entity displays the most current information about its services on its website, which is accessible to its customers.	Inspected the company's website to determine that the entity displays the most current information about its services on its website, which is accessible to its customers.	No exceptions noted.
CC2.3.2	Entity has provided information to customers on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the Entity in the event there are problems.	Inspected the customer support page in the company website to determine that the entity has provided information to customers on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the entity in the event there are problems.	No exceptions noted.
CC3.0: RISK ASSESSMENT			
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	Entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.	Inspected the annual formal risk assessment exercise records to determine that the entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.	No exceptions noted.
CC3.1.2	Entity has formally documented policies and procedures to govern risk management.	Inspected Risk Management Policy to determine that the entity has formally documented policies and procedures to govern risk management's.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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	Entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.	Inspected the annual formal risk assessment exercise records to determine that the entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.	No exceptions noted.
CC3.2.2	Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability, and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.	Inspected the risk assessment documentation to determine that each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability, and confidentiality of the Company platform. Observed that Risks are mapped to mitigating factors that address some or all of the risk.	No exceptions noted.
CC3.2.3	Entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.	Inspected the company policies to determine that the entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding. Observed that the policies have been reviewed and acknowledged by new staff members.	No exceptions noted.
CC3.2.4	Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.	Inspected the vendor risk assessment documentation to determine that the entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.	No exceptions noted.
CC3.3: COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
CC3.3.1	Entity considers the potential for fraud when assessing risks. This is an entry in the risk matrix.	Inspected the risk assessment documentation to determine that the entity considers the potential for fraud when assessing risks. Observed an entry in the risk matrix.	No exceptions noted.
CC3.4: COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
CC3.4.1	Entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.	Inspected the annual formal risk assessment exercise records to determine that the entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.4.2	Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability, and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.	Inspected the risk assessment documentation to determine that each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability, and confidentiality of the Company platform. Observed that risks are mapped to mitigating factors that address some or all of the risk.	No exceptions noted.
CC3.4.3	Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.	Inspected the vendor risk assessment documentation to determine that the entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.	No exceptions noted.
CC4.0: MONITORING ACTIVITIES			
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	Entity's Senior Management assigns the role of Information Security Officer who is delegated to centrally manage, coordinate, develop, implement, and maintain an enterprise-wide cybersecurity and privacy program.	Inspected the Organizational Structure showing that the role of Information Security Officer has been appropriately assigned to an employee to determine that the Senior Management assigns the role of Information Security Officer who is delegated to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity and privacy program.	No exceptions noted.
CC4.1.2	Entity has set up mechanisms to assign and manage asset ownership responsibilities and establish a common understanding of asset protection requirements.	Observed that an Infrastructure Operations Person has been appointed to assign and manage asset ownership responsibilities and establish a common understanding of asset protection requirements.	No exceptions noted.
CC4.1.3	Entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.	Inspected the Internal Audit Report on Sprinto compliance automation tool to determine that the entity continuously monitors, tracks, and reports the health of the information security program to the Information Security Officer and other stakeholders.	No exceptions noted.
CC4.1.4	Entity's Senior Management reviews and approves all company policies annually.	Inspected annual records that the company policies have been reviewed and approved by the Senior Management.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC4.1.5	Entity periodically updates and reviews the inventory of systems as a part of installations, removals, and system updates.	Inspected the Internal Audit Report to determine that the entity periodically updates and reviews the inventory of systems as a part of installations, removals, and system updates.	No exceptions noted.
CC4.1.6	Entity's Senior Management reviews and approves the "Risk Assessment Report" annually.	Inspected annual records showing that the Senior Management has reviewed and approved the "Risk Assessment Report".	No exceptions noted.
CC4.1.7	Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.	Inspected annual records showing that the Senior Management has reviewed and approved the “Vendor Risk Assessment Report”.	No exceptions noted.
CC4.1.8	Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to entity's customers can be met.	Inspected the vendor risk assessment documentation to determine that the entity reviews and evaluates all subservice organizations periodically, to ensure commitments to entity's customers can be met.	No exceptions noted.
CC4.1.9	Entity's Senior Management reviews and approves the Organizational Chart for all employees annually.	Inspected annual records showing that Senior Management has reviewed and approved the entity’s Organizational Chart.	No exceptions noted.
CC4.1.10	Entity's Senior Management reviews and approves the state of the Information Security program including policies, standards, and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.	Inspected the Management Review Meeting minutes showing review of relevant policies to determine that the Senior Management reviews and approves the state of the Information Security program including policies, standards, and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.	No exceptions noted.
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	Entity has provided information to employees, via various Information Security Policies/procedures, on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the entity in the event there are problems.	Inspected the Incident Management Policy and the section that describes how to report incidents to determine that the entity has provided information to employees, on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the entity in the event there are problems.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC4.2.2	Entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.	Inspected the Internal Audit Report on Sprinto compliance automation tool to determine that the entity continuously monitors, tracks, and reports the health of the information security program to the Information Security Officer and other stakeholders.	No exceptions noted.
CC4.2.3	Entity's Senior Management reviews and approves all company policies annually.	Observed that the company policies have been reviewed and approved by the Senior Management annually.	No exceptions noted.
CC4.2.4	Entity's Senior Management reviews and approves the state of the Information Security program including policies, standards, and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.	Inspected the Management Review Meeting minutes showing review of relevant policies to determine that the Senior Management reviews and approves the state of the Information Security program including policies, standards, and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.	No exceptions noted.
CC5.0: CONTROL ACTIVITIES			
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	Entity has developed a set of policies and procedures that establish expected behavior with regard to the Company’s control environment.	Inspected the Code of Business Conduct Policy and list of policies made available to employees to determine that the entity has developed a set of policies that establish expected behavior with regard to the company’s control environment.	No exceptions noted.
CC5.1.2	Entity establishes guidelines for acceptable and unacceptable technology usage behaviors, including outlining consequences for unacceptable actions.	Inspected the Acceptable Usage Policy to determine that the entity establishes guidelines for acceptable and unacceptable technology usage behaviors, including outlining consequences for unacceptable actions.	No exceptions noted.
CC5.1.3	Entity's Senior Management segregates responsibilities and duties across the organization to mitigate risks to the services provided to its customers.	Inspected the Organizational Chart and the roles/responsibilities defined by management to determine that the entity's Senior Management segregates responsibilities and duties across the organization to mitigate risks to the services provided to its customers.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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	Entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.	Inspected the Internal Audit Report on Sprinto compliance automation tool to determine that the entity continuously monitors, tracks, and reports the health of the information security program to the Information Security Officer and other stakeholders.	No exceptions noted.
CC5.2.2	Entity's Senior Management reviews and approves all company policies annually.	Observed that the company policies have been reviewed and approved by Senior Management annually.	No exceptions noted.
CC5.2.3	Entity's Senior Management reviews and approves the "Risk Assessment Report" annually.	Inspected annual records showing that the Senior Management has reviewed and approved the "Risk Assessment Report".	No exceptions noted.
CC5.2.4	Entity's Infosec officer reviews and approves the list of people with access to production consoles annually.	Inspected records where the access to critical systems has been reviewed and approved by the Infosec Officer.	No exceptions noted.
CC5.2.5	Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.	Inspected annual records showing that the Senior Management has reviewed and approved the “Vendor Risk Assessment Report”.	No exceptions noted.
CC5.2.6	Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to entity's customers can be met.	Inspected the vendor risk assessment documentation to determine that the entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.	No exceptions noted.
CC5.2.7	Entity has developed a set of policies and procedures that establish expected behavior with regard to the Company’s control environment.	Inspected the Code of Business Conduct Policy and list of policies made available to employees to determine that the entity has developed a set of policies that establish expected behavior with regard to the company’s control environment.	No exceptions noted.
CC5.2.8	Entity's Senior Management reviews and approves the state of the Information Security program including policies, standards, and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.	Inspected the Management Review Meeting minutes showing review of relevant policies to determine that the Senior Management reviews and approves the state of the Information Security program including policies, standards, and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.	No exceptions noted.
CC5.2.9	Entity's Senior Management reviews and approves the Organizational Chart for all employees annually.	Observed that the Organization chart has been reviewed and approved by senior management for all employees annually.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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	Entity makes all policies and procedures available to all staff members for their perusal.	Inspected the list of policies to determine that the entity makes all policies and procedures available to all staff members for their perusal.	No exceptions noted.
CC5.3.2	Entity has established procedures for staff to acknowledge applicable company policies periodically.	Inspected the company policies to determine that the entity has established procedures for staff to acknowledge applicable company policies periodically. Observed records that the policies have been reviewed and acknowledged by staff members.	No exceptions noted.
CC5.3.3	Entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.	Inspected the company policies to determine that the entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding. Observed that the policies have been reviewed and acknowledged by new staff members.	No exceptions noted.
CC5.3.4	Entity has developed a set of policies that establish expected behavior with regard to the Company's control environment.	Inspected the Code of Business Conduct Policy and list of policies made available to employees to determine that the entity has developed a set of policies that establish expected behavior with regard to the company's control environment.	No exceptions noted.
CC6.0: LOGICAL AND PHYSICAL ACCESS 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	Entity has documented policies and procedures to manage Access Control and an accompanying process to register and authorize users for issuing system credentials which grant the ability to access the critical systems.	Inspected the Access Control Policy to determine that the entity manages an accompanying process to register and authorize users for issuing system credentials which grant the ability to access the critical systems.	No exceptions noted.
CC6.1.2	Entity has documented guidelines to manage passwords and secure login mechanisms and makes them available to all staff members on the company employee portal.	Inspected the Access Control Policy to determine that the entity has documented guidelines to manage passwords and secure login mechanisms and makes them available to all staff members on the company employee portal.	No exceptions noted.
CC6.1.3	Entity uses Sprinto, a continuous monitoring system, to alert the security team to update the access levels of team members whose roles have changed.	Inspected the Sprinto compliance automation tool that continuously monitors and alerts the security team to update the access levels of team members whose roles have changed.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.1.4	Entity ensures that the production databases access and Secure Shell access to infrastructure entities are protected from public internet access.	Inspected the public access for infrastructure assets which ensures that access to infrastructure assets has been restricted from the public.	No exceptions noted.
CC6.1.5	Entity's Senior Management or the Information Security Officer periodically reviews and ensures that access to the critical systems is restricted to only those individuals who require such access to perform their job functions.	Inspected that the users of the critical system have been identified and their access has been reviewed by the entity's Senior Management or the Information Security Officer periodically.	No exceptions noted.
CC6.1.6	Entity's Senior Management or the Information Security Officer periodically reviews and ensures that administrative access to the critical systems is restricted to only those individuals who require such access to perform their job functions.	Inspected that the users of the critical system have been identified and their administrative access has been reviewed by the entity's Senior Management or the Information Security Officer periodically.	No exceptions noted.
CC6.1.7	Entity ensures that logical access provisioning to critical systems requires approval from authorized personnel on an individual need or for a predefined role.	Inspected records where Role Based Access to critical systems has been set up and validated to determine that the entity ensures that logical access provisioning to critical systems requires approval from authorized personnel on an individual need or for a predefined role.	No exceptions noted.
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	Entity ensures logical access that is no longer required in the event of termination is made inaccessible in a timely manner.	Inspected offboarded employee's access records to determine that the entity ensures logical access that is no longer required in the event of a termination is made inaccessible in a timely manner.	No exceptions noted.
CC6.2.2	Entity has documented policies and procedures to manage Access Control and an accompanying process to register and authorize users for issuing system credentials which grant the ability to access the critical systems.	Inspected the Access Control Policy to determine that the entity manages an accompanying process to register and authorize users for issuing system credentials which grant the ability to access the critical systems.	No exceptions noted.
CC6.2.3	Entity ensures that logical access provisioning to critical systems requires approval from authorized personnel on an individual need or for a predefined role.	Inspected records where Role Based Access to critical systems has been set up and validated to determine that the entity ensures that logical access provisioning to critical systems requires approval from authorized personnel on an individual need or for a predefined role.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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	Entity ensures that logical access provisioning to critical systems requires approval from authorized personnel on an individual need or for a predefined role.	Inspected records where Role Based Access to critical systems has been set up and validated to determine that the entity ensures that logical access provisioning to critical systems requires approval from authorized personnel on an individual need or for a predefined role.	No exceptions noted.
CC6.3.2	Entity ensures that access to the production databases is restricted to only those individuals who require such access to perform their job functions.	Inspected records where the users of the critical system have been identified and their access to production database has been restricted to only those individuals who require such access to perform their job functions.	No exceptions noted.
CC6.3.3	Entity has documented policies and procedures to manage Access Control and an accompanying process to register and authorize users for issuing system credentials which grant the ability to access the critical systems.	Inspected the Access Control Policy to determine that the entity has documented policy to manage Access Control and an accompanying process to register and authorize users for issuing system credentials which grant the ability to access the critical systems.	No exceptions noted.
CC6.3.4	Entity ensures logical access that is no longer required in the event of termination is made inaccessible in a timely manner.	Inspected offboarded employee's access records to determine that the entity ensures logical access that is no longer required in the event of a termination is made inaccessible in a timely manner.	No exceptions noted.
CC6.3.5	Entity's Senior Management or the Information Security Officer periodically reviews and ensures that administrative access to the critical systems is restricted to only those individuals who require such access to perform their job functions.	Inspected that the users of the critical system have been identified and their administrative access has been reviewed by the entity's Senior Management or the Information Security Officer periodically.	No exceptions noted.
CC6.3.6	Entity's Senior Management or the Information Security Officer periodically reviews and ensures that access to the critical systems is restricted to only those individuals who require such access to perform their job functions.	Inspected that the users of the critical system have been identified and their access has been reviewed by the entity's Senior Management or the Information Security Officer periodically.	No exceptions noted.
CC6.3.7	Entity ensures that access to all critical systems is restricted to only those individuals who require such access to perform their job functions.	Inspected records where the users of the critical system have been identified and their access to production database has been restricted to only those individuals who require such access to perform their job functions.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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	Entity has a documented policy that provides guidance on decommissioning of information assets that contain classified information.	Inspected the Media Disposal Policy to determine that the entity has a documented policy that provides guidance on decommissioning of information assets that contain classified information.	No exceptions noted.
CC6.6: The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
CC6.6.1	Entity requires that all staff members with access to any critical system be protected with a secure login mechanism such as Multifactor authentication.	Observed Multifactor Authentication for all critical systems to determine that the entity requires that all staff members with access to any critical system are protected with a secure login mechanism.	No exceptions noted.
CC6.6.2	Where applicable, entity ensures that endpoints with access to critical servers or data must be protected by malware-protection software.	Observed the malware-protection software to determine that the entity ensures that endpoints with access to critical servers or data must be protected by malware-protection software.	No exceptions noted.
CC6.6.3	Where applicable, entity ensures that endpoints with access to critical servers or data must be encrypted to protect from unauthorized access.	Inspected the disk encryption and the endpoint security review results of staff devices to determine that the entity ensures that endpoints with access to critical servers or data must be encrypted to protect from unauthorized access.	No exceptions noted.
CC6.6.4	Entity ensures that the production databases access and Secure Shell access to infrastructure entities are protected from public internet access.	Inspected the public access for infrastructure assets which ensures that access to infrastructure assets has been restricted from the public.	No exceptions noted.
CC6.6.5	Entity ensures that endpoints with access to critical servers or data are configured to auto-screen-lock after 15 minutes of inactivity.	Observed auto-screen lock configuration on staff devices to determine that the entity ensures that endpoints with access to critical servers or data are configured to auto-screen-lock after 15 minutes of inactivity.	No exceptions noted.
CC6.6.6	Every Production host is protected by a firewall with a deny-by-default rule. Deny by default rule set is a default on the Entity's cloud provider.	Observed the entity's firewall in the system to determine that every Production host is protected by a firewall with a deny-by-default rule.	No exceptions noted.
CC6.6.7	Entity has documented policies and procedures for endpoint security and related controls.	Inspected the Endpoint Security Policy to determine that the entity has documented policies and procedures for endpoint security and related controls.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.6.8	Entity requires that all critical endpoints are encrypted to protect them from unauthorized access.	Inspected the disk encryption and the endpoint security review results of staff devices to determine that the entity requires that all critical endpoints are encrypted to protect them from unauthorized access.	No exceptions noted.
CC6.6.9	Entity has set up measures to perform security and privacy compliance checks on the software versions and patches of remote devices prior to the establishment of the internal connection.	Observed the updated OS versions of staff devices to determine that the entity has set up measures to perform security and privacy compliance checks on the software versions and patches of remote devices prior to the establishment of the internal connection.	No exceptions noted.
CC6.6.10	Entity develops, documents, and maintains an inventory of organizational endpoint systems, including all necessary information to achieve accountability.	Observed the staff devices health monitoring checks to determine that the entity develops, documents, and maintains an inventory of organizational endpoint systems, including all necessary information to achieve accountability.	No exceptions noted.
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	Where applicable, Entity ensures that endpoints with access to critical servers or data must be encrypted to protect from unauthorized access.	Inspected the disk encryption and the endpoint security review results of staff devices to determine that the entity ensures that endpoints with access to critical servers or data must be encrypted to protect from unauthorized access.	No exceptions noted.
CC6.7.2	Entity has set up cryptographic mechanisms to encrypt all production database[s] that store customer data at rest.	Observed that the data at rest has been encrypted to determine that the entity has set up cryptographic mechanisms to encrypt all production database[s] that store customer data at rest.	No exceptions noted.
CC6.7.3	Entity has set up processes to utilize standard encryption methods, including HTTPS with the TLS algorithm, to keep transmitted data confidential.	Observed the https (TLS algorithm) and industry standard encryption to determine that the entity has set up processes to utilize standard encryption methods to keep transmitted data confidential.	No exceptions noted.
CC6.7.4	Entity develops, documents, and maintains an inventory of organizational infrastructure systems, including all necessary information to achieve accountability.	Observed the staff devices health monitoring checks to determine that the entity develops, documents, and maintains an inventory of organizational infrastructure systems, including all necessary information to achieve accountability.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.7.5	Entity ensures that customer data used in non-Production environments requires the same level of protection as the production environment.	Observed that the critical infrastructure assets have been identified to determine that the entity ensures that customer data used in non-Production environments requires the same level of protection as the production environment.	No exceptions noted.
CC6.7.6	Entity has a documented policy to manage encryption and cryptographic protection controls.	Observed the Encryption Policy to determine that the entity has a documented policy to manage encryption and cryptographic protection controls.	No exceptions noted.
CC6.7.7	Entity requires that all critical endpoints are encrypted to protect them from unauthorized access.	Inspected the disk encryption and the endpoint security review results of staff devices to determine that the entity requires that all critical endpoints are encrypted to protect them from unauthorized access.	No exceptions noted.
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	Entity has set up measures to perform security and privacy compliance checks on the software versions and patches of remote devices prior to the establishment of the internal connection.	Observed the updated OS versions of staff devices to determine that the entity has set up measures to perform security and privacy compliance checks on the software versions and patches of remote devices prior to the establishment of the internal connection.	No exceptions noted.
CC6.8.2	Every Production host is protected by a firewall with a deny-by-default rule. Deny by default rule set is a default on the Entity's cloud provider.	Observed the entity's firewall in the system to determine that every Production host is protected by a firewall with a deny-by-default rule.	No exceptions noted.
CC7.0: SYSTEM OPERATIONS			
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	Entity has set up methods to continuously monitor critical assets to generate capacity alerts to ensure optimal performance, meet future capacity requirements, and protect against denial-of-service attacks.	Observed the Production assets and their monitoring alert configurations to determine that the entity has set up methods to continuously monitor critical assets to generate capacity alerts to ensure optimal performance, meet future capacity requirements, and protect against denial-of-service attacks.	No exceptions noted.
CC7.1.2	Entity tracks all vulnerabilities and remediates them as per the policy and procedure defined to manage vulnerabilities.	Observed that the vulnerabilities have been identified and remediated as per the Vulnerability Management Policy defined to manage vulnerabilities.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.1.3	Entity identifies vulnerabilities on the Company platform through the execution of regular vulnerability scans.	Inspected records of vulnerability scans to determine that the entity identifies vulnerabilities on the Company platform.	No exceptions noted.
CC7.1.4	Entity has a documented policy and procedures to establish guidelines for managing technical vulnerabilities.	Inspected the Vulnerability Management Policy to determine that the entity has a documented policy and procedures to establish guidelines on managing technical vulnerabilities.	No exceptions noted.
CC7.1.5	Entity's infrastructure is configured to generate audit events for actions of interest related to security for all critical systems.	Observed that the audit logs exist to determine that the entity's infrastructure is configured to generate audit events for actions of interest related to security for all critical systems.	No exceptions noted.
CC7.1.6	Entity's infrastructure is configured to review and analyze audit events to detect anomalous or suspicious activity and threats.	Observed that the threat detection system has been enabled to determine that the entity's infrastructure is configured to review and analyze audit events to detect anomalous or suspicious activity and threats.	No exceptions noted.
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	Entity identifies vulnerabilities on the Company platform through the execution of regular vulnerability scans.	Inspected the records of vulnerability scans to determine that the entity identifies vulnerabilities on the Company platform.	No exceptions noted.
CC7.2.2	Entity tracks all vulnerabilities and remediates them as per the policy and procedure defined to manage vulnerabilities.	Observed that the vulnerabilities have been identified and remediated as per the Vulnerability Management Policy defined to manage vulnerabilities.	No exceptions noted.
CC7.2.3	Entity has set up methods to continuously monitor critical assets to generate capacity alerts to ensure optimal performance, meet future capacity requirements, and protect against denial-of-service attacks.	Observed the Production assets and their monitoring alert configurations to determine that the entity has set up methods to continuously monitor critical assets to generate capacity alerts to ensure optimal performance, meet future capacity requirements, and protect against denial-of-service attacks.	No exceptions noted.
CC7.2.4	Entity has a documented policy and procedures to establish guidelines for managing technical vulnerabilities.	Inspected the Vulnerability Management Policy to determine that the entity has a documented policy and procedures to establish guidelines on managing technical vulnerabilities.	No exceptions noted.
CC7.2.5	Entity's infrastructure is configured to generate audit events for actions of interest related to security for all critical systems.	Observed that the audit logs exist to determine that the entity's infrastructure is configured to generate audit events for actions of interest related to security for all critical systems.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.2.6	Entity's infrastructure is configured to review and analyze audit events to detect anomalous or suspicious activity and threats.	Observed that the threat detection system has been enabled to determine that the entity's infrastructure is configured to review and analyze audit events to detect anomalous or suspicious activity and threats.	No exceptions noted.
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	Entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.	Inspected the Internal Audit Report on Sprinto compliance automation tool to determine that the entity continuously monitors, tracks and reports the health of the information security program to the Information Security Officer and other stakeholders.	No exceptions noted.
CC7.3.2	Entity has set up measures to perform security and privacy compliance checks on the software versions and patches of remote devices prior to the establishment of the internal connection.	Observed the updated OS versions of staff devices to determine that the entity has set up measures to perform security and privacy compliance checks on the software versions and patches of remote devices prior to the establishment of the internal connection.	No exceptions noted.
CC7.3.3	Entity maintains a record of information security incidents, its investigation, and the response plan that was executed in accordance with the policy and procedure defined to report and manage incidents.	Inspected the record of information security incidents to determine that the entity maintains a record of information security incidents, its investigation and the response plan that was executed in accordance with the policy and procedure defined to report and manage incidents.	No exceptions noted.
CC7.3.4	Entity has a documented policy and procedures to establish guidelines for managing technical vulnerabilities.	Inspected the Vulnerability Management Policy to determine that the entity has a documented policy and procedures to establish guidelines on managing technical vulnerabilities.	No exceptions noted.
CC7.3.5	Entity identifies vulnerabilities on the Company platform through the execution of regular vulnerability scans.	Inspected records of vulnerability scans to determine that the entity identifies vulnerabilities on the Company platform.	No exceptions noted.
CC7.3.6	Entity tracks all vulnerabilities and remediates them as per the policy and procedure defined to manage vulnerabilities.	Observed that the vulnerabilities have been identified and remediated as per the Vulnerability Management Policy defined to manage vulnerabilities.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.3.7	Entity has set up methods to continuously monitor critical assets to generate capacity alerts to ensure optimal performance, meet future capacity requirements, and protect against denial-of-service attacks.	Observed the Production assets and their monitoring alert configurations to determine that the entity has set up methods to continuously monitor critical assets to generate capacity alerts to ensure optimal performance, meet future capacity requirements, and protect against denial-of-service attacks.	No exceptions noted.
CC7.3.8	Entity's infrastructure is configured to generate audit events for actions of interest related to security for all critical systems.	Observed that the audit logs exist to determine that the entity's infrastructure is configured to generate audit events for actions of interest related to security for all critical systems.	No exceptions noted.
CC7.3.9	Entity's infrastructure is configured to review and analyze audit events to detect anomalous or suspicious activity and threats.	Observed that the threat detection system has been enabled to determine that the entity's infrastructure is configured to review and analyze audit events to detect anomalous or suspicious activity and threats.	No exceptions noted.
CC7.3.10	Entity identifies vulnerabilities on the company platform through an annual penetration testing exercise conducted by a qualified third-party service provider.	Inspected records of the annual penetration testing exercise conducted by a qualified third-party service provider to determine that the entity identifies vulnerabilities on the company platform annually.	No exceptions noted.
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	Entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.	Inspected the Internal Audit Report on Sprinto compliance automation tool to determine that the entity continuously monitors, tracks and reports the health of the information security program to the Information Security Officer and other stakeholders.	No exceptions noted.
CC7.4.2	Entity has established a policy and procedure which includes guidelines to be undertaken in response to information security incidents.	Inspected Incident Management Policy to determine that the entity has established a policy and procedure which includes guidelines to be undertaken in response to information security incidents.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.4.3	Entity maintains a record of information security incidents, its investigation, and the response plan that was executed in accordance with the policy and procedure defined to report and manage incidents.	Inspected the record of information security incidents to determine that the entity maintains a record of information security incidents, its investigation and the response plan that was executed in accordance with the policy and procedure defined to report and manage incidents.	No exceptions noted.
CC7.5: The entity identifies, develops, and implements activities to recover from identified security incidents.			
CC7.5.1	Entity has a documented policy on managing Data Backups and makes it available for all relevant staff on the company employee portal.	Inspected the data backup for the production database to determine that the entity has a documented policy on managing Data Backups and makes it available for all relevant staff on the company employee portal.	No exceptions noted.
CC7.5.2	Entity has documented policies and procedures that establish guidelines for continuing business operations and facilitate the application of contingency planning controls.	Inspected the Business Continuity Policy and Disaster Recovery Policy to determine that the entity has documented policies and procedures that establish guidelines for continuing business operations and facilitate the application of contingency planning controls.	No exceptions noted.
CC7.5.3	Entity has documented guidelines to manage Disaster Recovery that establish guidelines and procedures for continuing business operations in case of a disruption or a security incident	Inspected the Business Continuity Policy and Disaster Recovery Policy to determine that the entity has documented guidelines to manage Disaster Recovery that establish guidelines and procedures for continuing business operations in case of a disruption or a security incident.	No exceptions noted.
CC7.5.4	Entity has documented Business Continuity & Disaster Recovery Policies, that establish guidelines and procedures on continuing business operations in case of a disruption or a security incident.	Inspected the Business Continuity Policy and Disaster Recovery Policy to determine the entity has documented Business Continuity & Disaster Recovery Policies, that establish guidelines and procedures on continuing business operations in case of a disruption or a security incident.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC8.0: CHANGE MANAGEMENT			
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	Entity develops, documents, and maintains an inventory of organizational infrastructure systems, including all necessary information to achieve accountability.	Observed that the critical infrastructure assets have been identified to determine that the entity develops, documents, and maintains an inventory of organizational infrastructure systems, including all necessary information to achieve accountability.	No exceptions noted.
CC8.1.2	Entity has documented policies and procedures to manage changes to its operating environment.	Inspected the Change Management Policy to determine that the entity has documented policies and procedures to manage changes to its operating environment.	No exceptions noted.
CC8.1.3	Entity has procedures to govern changes to its operating environment.	Inspected the Change Management source and repos to determine that the entity has procedures to govern changes to its operating environment.	No exceptions noted.
CC8.1.4	Entity has established procedures for approval when implementing changes to the operating environment.	Observed change request reviews and approval by peers to determine that the entity has established procedures for approval when implementing changes to the operating environment.	No exceptions noted.
CC9.0: RISK MITIGATION			
CC9.1: The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruption.			
CC9.1.1	Entity has documented policies and procedures that describe how to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate the Entity's service commitments and system requirements.	Inspected the Risk Management Policy to determine that the entity has documented policies and procedures that describe how to identify risks to business objectives and how those risks are assessed and mitigated incorporating the entity's service commitments and system requirements.	No exceptions noted.
CC9.1.2	Entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.	Inspected the annual formal risk assessment exercise records to determine that the entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC9.1.3	Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability, and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.	Inspected the risk assessment documentation to determine that each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability, and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.	No exceptions noted.
CC9.2: The entity assesses and manages risks associated with vendors and business partners.			
CC9.2.1	Entity has documented policies and procedures that describe how to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate Entity's service commitments and system requirements.	Inspected the Risk Management Policy to determine that the entity has documented policies and procedures that describe how to identify risks to business objectives and how those risks are assessed and mitigated incorporating the entity's service commitments and system requirements.	No exceptions noted.
CC9.2.2	Entity has a documented policy and procedures to manage Vendors/third-party suppliers and provides guidance to staff on performing a risk assessment of such vendors.	Inspected the Vendor Management Policy to determine that the entity has a documented policy and procedure to manage Vendors/third-party suppliers and provides guidance to staff on performing a risk assessment of such vendors.	No exceptions noted.
CC9.2.3	Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.	Inspected the vendor risk assessment documentation to determine that the entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.	No exceptions noted.

CONFIDENTIALITY PRINCIPLE AND CRITERIA TABLE

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
C1.0: ADDITIONAL CRITERIA FOR CONFIDENTIALITY			
C1.1: The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.			
C1.1.1	Entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.	Inspected the company policies to determine that the entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding. Observed that the policies have been reviewed and acknowledged by new staff members.	No exceptions noted.
C1.1.2	Entity has established procedures for staff to acknowledge applicable company policies periodically.	Inspected the company policies to determine that the entity has established procedures for staff to acknowledge applicable company policies periodically. Inspected records that the policies have been reviewed and acknowledged by staff members.	No exceptions noted.
C1.1.3	Entity has set up cryptographic mechanisms to encrypt all production database[s] that store customer data at rest.	Observed that the data at rest has been encrypted to determine that the entity has set up cryptographic mechanisms to encrypt all production database[s] that store customer data at rest.	No exceptions noted.
C1.1.4	Entity performs physical and/or logical labeling of information systems as per the guidelines documented policy defined for data classification.	Inspected Data Classification Policy to determine that the entity performs physical and/or logical labeling of information systems as per the guidelines documented policy defined for data classification.	No exceptions noted.
C1.1.5	Entity has a documented Information Security Policy that governs the confidentiality, integrity, and availability of information systems.	Inspected the Information Security Policy to determine that the entity has documented policies that govern the confidentiality, integrity, and availability of information systems.	No exceptions noted.
C1.1.6	Where applicable, Entity ensures that endpoints with access to critical servers or data must be encrypted to protect from unauthorized access.	Inspected the disk encryption and the endpoint security review results of staff devices to determine that the entity ensures that endpoints with access to critical servers or data must be encrypted to protect from unauthorized access.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
C1.2: The entity disposes of confidential information to meet the entity's objectives related to confidentiality.			
C1.2.1	Entity has a documented policy that provides guidance on decommissioning of information assets that contain classified information.	Inspected the Media Disposal Policy to determine that the entity has a documented policy that provides guidance on the decommissioning of information assets that contain classified information.	No exceptions noted.
C1.2.2	Entity has a documented policy outlining guidelines for the disposal and retention of information.	Inspected the Data Retention Policy to determine that the entity has a documented policy outlining guidelines for the disposal and retention of information.	No exceptions noted.

AVAILABILITY PRINCIPLE AND CRITERIA TABLE

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.0: ADDITIONAL CRITERIA FOR AVAILABILITY			
A.1.1: The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.			
A1.1.1	Entity has set up methods to continuously monitor critical assets to generate capacity alerts to ensure optimal performance, meet future capacity requirements, and protect against denial-of-service attacks.	Observed the Production assets and their monitoring alert configurations to determine that the entity has set up methods to continuously monitor critical assets to generate capacity alerts to ensure optimal performance, meet future capacity requirements, and protect against denial-of-service attacks.	No exceptions noted.
A1.2: The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.			
A1.2.1	Entity has a documented policy on managing Data Backups and makes it available for all relevant staff on the company employee portal.	Inspected the data backup for the production database to determine that the entity has a documented policy on managing Data Backups and makes it available for all relevant staff on the company employee portal.	No exceptions noted.
A1.2.2	Entity tests backup information periodically to verify media reliability and information integrity.	Observed the database backup restore exercise notes to determine that the entity tests backup information periodically to verify media reliability and information integrity.	No exceptions noted.
A1.2.3	Entity has documented guidelines to manage Disaster Recovery that establish guidelines and procedures for continuing business operations in case of a disruption or a security incident.	Inspected the Business Continuity Policy and Disaster Recovery Policy to determine that the entity has documented guidelines to manage Disaster Recovery that establish guidelines and procedures for continuing business operations in case of a disruption or a security incident.	No exceptions noted.
A1.2.4	Entity has documented policies and procedures that establish guidelines for continuing business operations and facilitate the application of contingency planning controls.	Inspected the Business Continuity Policy and Disaster Recovery Policy to determine that the entity has documented policies and procedures that establish guidelines for continuing business operations and facilitate the application of contingency planning controls.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A.1.2.5	Entity backs up relevant user and system data regularly to meet recovery time and recovery point objectives and verifies the integrity of these backups.	Inspected the Data Backup Policy to determine that relevant user and system data is backed up regularly and verified in alignment with defined recovery time and recovery point objectives.	No exceptions noted.
A1.2.6	Entity has documented Business Continuity & Disaster Recovery Policies, that establish guidelines and procedures on continuing business operations in case of a disruption or a security incident.	Inspected the Business Continuity Policy and Disaster Recovery Policy to determine the entity has documented Business Continuity & Disaster Recovery Policies, that establish guidelines and procedures on continuing business operations in case of a disruption or a security incident.	No exceptions noted.
A1.3: The entity tests recovery plan procedures supporting system recovery to meet its objectives.			
A1.3.1	Entity tests backup information periodically to verify media reliability and information integrity.	Observed the database backup restore exercise notes to determine that the entity tests backup information periodically to verify media reliability and information integrity.	No exceptions noted.
A1.3.2	Entity has procedures to conduct regular tests and exercises that determine the effectiveness and the readiness to execute the contingency plan.	Observed the disaster recovery exercise notes to determine that the entity has procedures to conduct regular tests and exercises that determine the effectiveness and the readiness to execute the contingency plan.	No exceptions noted.
A1.3.3	Entity has documented policies and procedures that establish guidelines for continuing business operations and facilitate the application of contingency planning controls.	Inspected the Business Continuity Policy and Disaster Recovery Policy to determine that the entity has documented policies and procedures that establish guidelines for continuing business operations and facilitate the application of contingency planning controls.	No exceptions noted.
A1.3.4	Entity has documented guidelines to manage Disaster Recovery that establish guidelines and procedures for continuing business operations in case of a disruption or a security incident.	Inspected the Business Continuity Policy and Disaster Recovery Policy to determine that the entity has documented guidelines to manage Disaster Recovery that establish guidelines and procedures for continuing business operations in case of a disruption or a security incident.	No exceptions noted.
A1.3.5	Entity has documented Business Continuity & Disaster Recovery Policies, that establish guidelines and procedures on continuing business operations in case of a disruption or a security incident.	Inspected the Business Continuity Policy and Disaster Recovery Policy to determine the entity has documented Business Continuity & Disaster Recovery Policies, that establish guidelines and procedures on continuing business operations in case of a disruption or a security incident.	No exceptions noted.