Noon AI

SOC 2 TYPE 2®

For the period of January 1, 2025 to August 28 2025
Report on Controls at a Service Organization Relevant to
Security, Confidentiality and Availability

AXIPRO

TABLE OF CONTENTS

SECTION I - Service Organization Management's Assertion

Assertion of Noon AI Management

We have prepared the accompanying description in Section III of Noon AI's Platform and Systems titled "Description of the Compliance Platform and the Suitability of the Design Type 2 of its Controls Relevant to Security, Confidentiality and Availability throughout the Period of January 1, 2025 to August 28 2025," (description) based on the criteria for a description of a service organization's system outlined in DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (AICPA, Description Criteria), (description criteria). The description is intended to provide users with information about Noon AI Platforms and Systems that may be useful when assessing the risks arising from interactions with Noon AI's Platforms and systems, particularly information about system controls that Noon AI has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the Trust Services Criteria outlined in TSP 100, 2017 Trust Services Criteria for Security, Confidentiality, and Availability (AICPA, Trust Services Criteria).

Noon AI uses subservice organizations to provide data center services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Noon AI, to achieve Noon AI's service commitments and system requirements based on the applicable Trust Services Criteria. The description presents Noon AI's controls, the applicable Trust Services Criteria and the types of complementary subservice organization controls assumed in the design of Noon AI's controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls are suitably designed and operating effectively and are necessary, along with controls at Noon AI, to achieve Noon AI's service commitments and system requirements based on the applicable Trust Services Criteria. The description presents the service organization's controls, the applicable Trust Services Criteria, and the complementary user entity controls assumed in the design of the service organization's controls.

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

The description presents Noon AI's Platform and systems that were designed and implemented throughout the Period of January 1, 2025 to August 28 2025, by the description criteria.
The controls stated in the description were suitably designed throughout the Period of January 1, 2025 to August 28 2025, to provide reasonable assurance that Noon AI's service commitments and system requirements would be achieved based on the applicable Trust Services Criteria, if its controls operated effectively throughout that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of Noon AI's controls throughout that period.

Noon AI
Date: 09 Sept 2025

SECTION II - Independent Service Auditor’s Report

Independent Service

Auditor's Report

To: Noon AI's Management Team

Scope

We have examined Noon AI's accompanying description of its Platforms and Systems throughout the Period of January 1, 2025 to August 28 2025 (description) based on the criteria for a description of a service system in DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (AICPA, Description Criteria), and the suitability of the design Type 2 of controls stated in the description throughout the Period of January 1, 2025 to August 28 2025, to provide reasonable assurance that Noon AI service commitments and system requirements were achieved based on the Trust Services Criteria relevant to Security, Confidentiality, and Availability (applicable Trust Services Criteria) outlined in TSP section 100, 2017 Trust Services Criteria for Security, Confidentiality & Availability (AICPA, Trust Services Criteria).

Noon AI currently uses subservice organizations. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Noon AI, to achieve Noon AI Platforms and Systems commitments and system requirements based on the applicable Trust Services Criteria. The description presents Noon AI's controls, the applicable Trust Services Criteria and the types of complementary subservice organization controls assumed in the design of Noon AI's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

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

Service Responsibilities

Noon AI is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that service commitments and system requirements were achieved. Noon AI has provided the accompanying assertion titled "Service Organization Management's Assertion" (assertion) about the description and the suitability of Design Type 2 of controls stated therein. Noon AI is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the service(s) covered by the description; selecting the applicable Trust Services Criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service commitments and system requirements.

Our responsibility is to express an opinion on the description and the suitability of Design Type 2 of controls stated in the description based on our examination. Our examination was conducted by attestation standards established by the American Institute of Certified Public Accountants.

Service Auditor's Responsibilities

Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented by the description criteria and whether the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable Trust Services Criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the Design Type 2 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 by 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 by 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 report uses and may not include every aspect of the system that individual users may consider important to meet their own informational needs. There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable Trust Services Criteria. Also, the projection to the future of any conclusions about the suitability of the Design Type 2 of controls are subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate over time.

Description of Tests of Controls

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

Opinion

In our opinion, in all material respects:

- The controls stated in the description were suitably designed throughout the Period of January 1, 2025 to August 28 2025, to provide reasonable assurance that Noon AI Platform and Services commitments and system requirements would be achieved based on the applicable Trust Services Criteria, if its controls operated effectively as of that date and if the subservice organization(s) and user entities applied the complementary controls assumed in the design of Noon AI's controls as of that date.

- The controls stated in the description operated effectively throughout the period of January 1, 2025 to August 28 2025 to provide reasonable assurance that Noon AI's Platform and Services commitments and system requirements would be achieved based on the applicable Trust Services Criteria, if its controls operated effectively as of that date, and if the subservice organization(s) and user entities applied the complementary controls assumed in the design of Noon AI's controls as of that date.

Restricted Use

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of Noon AI, user entities throughout the Period of January 1, 2025 to August 28 2025, business partners of Noon AI that are subject to risks arising from interactions with Noon AI Platforms and Systems, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

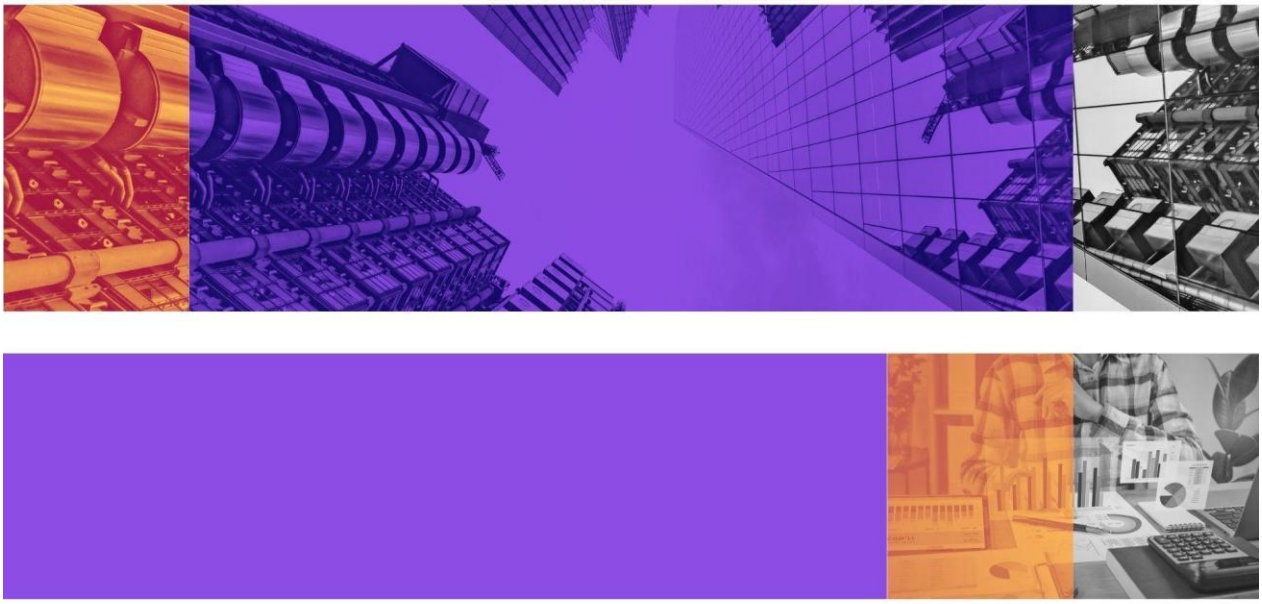
- The nature of the service provided by the service organization.
- How the service system interacts with user entities, business partners, subservice organizations, and other parties.
- Internal control and its limitations.
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
- The applicable Trust Services Criteria.
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

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

Arpitha Settipalli

Arpitha Settipalli
Montana License Number : 034303
Date : September 11, 2025

SECTION III - Description of Service Organization's System



Description of Service Organization's System

Overview of Operations

COMPANY BACKGROUND

Portal Inc. was founded in June 2021 by Stanford researchers David Witten and Raymond Guo to provide services automating recruiting. The organization is based out of New York, NY.

DESCRIPTION OF SERVICES OVERVIEW OR SERVICES PROVIDED

Portal Inc.'s core product, Noon AI is a Software as a Service (SaaS) solution that includes the following services:
Candidate sourcing: Given a Job Description, surface candidates from the web that fit the criteria, and adapt based on feedback

- Candidate outreach: Send automated emails and follow-ups to candidates
- Analytics: Share analytics on candidate outreach

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Portal Inc. designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments that Portal Inc. makes to user entities, the laws, and regulations that govern the provision of the services, and the financial, operational, and compliance requirements that Portal Inc. has established for the services. The system services are subject to the Security, Confidentiality, and Availability commitments established internally for its services.
Commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online.

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

- System features and configuration settings designed to authorize user access while restricting unauthorized users from accessing information not needed for their role; Use of intrusion detection systems to prevent and identify potential security attacks from users outside the boundaries of the system;
- 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;
- Use of encryption technologies to protect customer data both at rest and in transit;
- Use of data retention and data disposal;
- Uptime availability of production system.

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; and,
- Confidential information must be used only for the purposes explicitly stated in agreements between Portal 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 that include detailed instructions, recovery point objectives (RPOs), recovery time objectives (RTOs), roles, and responsibilities; and, Operational procedures supporting the achievement of availability commitments to user entities.

COMPONENTS OF THE SYSTEM

The System description is comprised of the following components:
Infrastructure – The collection of physical or virtual resources that supports an overall IT environment, including the physical environment and related structures, IT and hardware (for example, facilities, servers, storage, environmental monitoring equipment, data storage devices and media, mobile devices, and internal networks and connected external telecommunications networks) that the service organization used to provide the services.

Software – The application programs and IT system software that supports application programs (operating systems, middleware, and utilities), the types of databases used, the nature of external facing web applications, and the nature of applications developed in-house, including details about whether the applications in use are mobile applications or desktop or laptop applications.

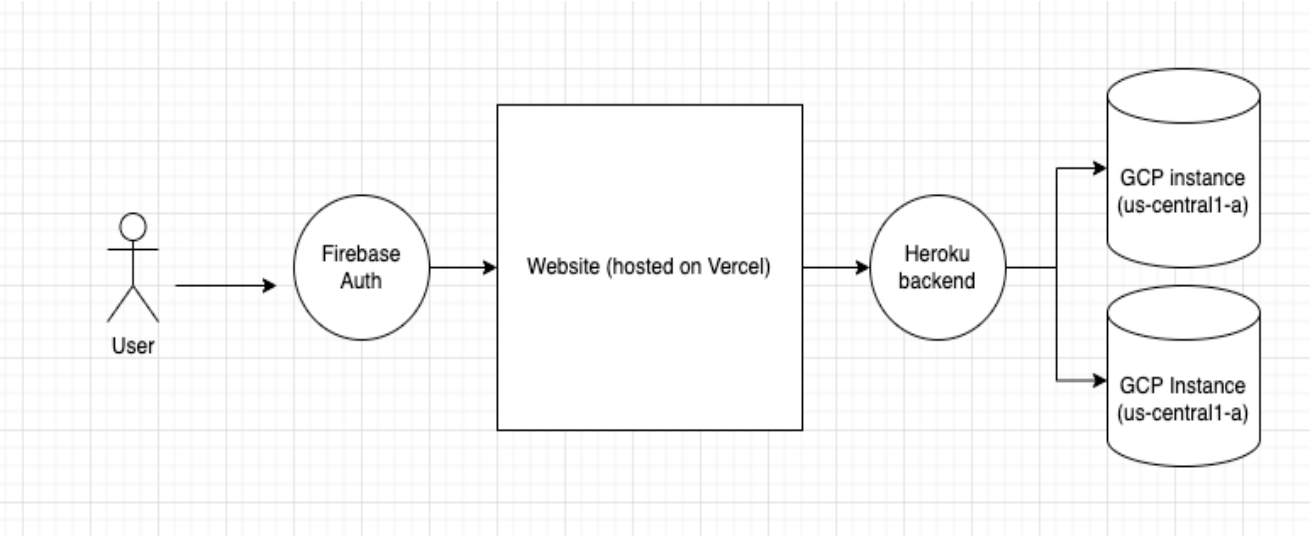
People – The personnel involved in the governance, operation, security, and use of a system (business unit personnel, developers, operators, user entity personnel, vendor personnel, and managers).

Data – The types of data used by the system, such as transaction streams, files, databases, tables, and output used or processed by the system.

Procedures – The automated and manual procedures related to the services provided, including, as appropriate, procedures by which service activities are initiated, authorized, performed, and delivered, and reports and other information prepared.

INFRASTRUCTURE

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



Hardware Type	Purpose
GCP Cloud Hosting Services	Uses Google Cloud Platform's Compute Engine to perform additional computations, including running scheduled tasks (cron-jobs) to manage and process data efficiently.
Heroku Backend Server	Handles network requests from the website the company providing backend services, running application logic, and interacting with databases.
Vercel Frontend Hosting	Deploys and hosts frontend applications, ensuring high performance and scalability with features like automatic SSL certificates, serverless functions, and seamless integration with development workflows.

SOFTWARE

System/Application	Operating System	Purpose
Firebase	Google	Stores and syncs real-time data for user applications, provides backend services like authentication, databases, and hosting
Papertrail	Part of Heroku	Aggregates, searches, and monitors log files in real-time for backend systems, aiding in debugging and performance monitoring

PEOPLE

The company employs dedicated team members to handle major product functions, including operations, and support. The IT/Engineering Team monitors the environment, as well as manages data backups and recovery.

Portal Inc. has a staff of 3 organized in the following functional areas:

- *Management* – CEO, CTO
- *Operations* – Responsible for production infrastructure availability and access/security management
- *Information Technology* – Manages laptops, software, and employee technology
- *Product Development* – Develops, tests, deploys, and maintains system source code and functionality

DATA

Portal Inc. classifies its data into four categories:

Category	Description	Examples
Public	Information not confidential, can be made public without implications	Press releases, public website
Internal	Internal information approved by management, protected from external access	Internal memos, design documents, product specs, correspondences
Customer Data	Information received from customers for processing/storage, subject to high integrity, confidentiality, and restricted availability	Customer operating data, customer PII, customers' customers' PII, confidential info
Company Data	Information collected and used by Portal Inc. to operate business, subject to high integrity/confidentiality	Legal documents, contractual agreements, employee PII, salaries

PROCESSES AND PROCEDURES

Management has developed and communicated policies and procedures to manage information security. Areas covered:

- Physical Security
- Logical Access
- Availability
- Change Control
- Data Communications
- Risk Assessment

- Data Retention
- Vendor Management

PHYSICAL SECURITY

Production servers are maintained by GCP. Google provides physical/environmental protections. Portal Inc. reviews attestations and risk analysis annually.

LOGICAL ACCESS

Role-based access control, least privilege, quarterly reviews. CTO provisions access and ensures background checks, training, and onboarding within 30 days. Access deprovisioned within 48 hours of termination.

Backups & Availability

Backups monitored by CTO in GCP, encrypted, restricted access. Incident response plan in place. Vulnerability scanning and monitoring implemented.

Change Management

SDLC policies with ticketing, approvals, QA, UAT, separate dev/test/prod environments, version control for rollback.

Data Communications

Production hosted on PaaS. Firewalls enforce HTTPS-only ingress. Automatic provisioning/deprovisioning of containers. The external firm conducts quarterly scans and annual penetration tests.

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

INTEGRITY AND ETHICAL VALUES

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

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

COMMITMENT TO COMPETENCE

Noon AI's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for jobs and how those levels translate into the requisite skills and knowledge.
Specific control activities that the service organization has implemented in this area are described below:

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

MANAGEMENT'S PHILOSOPHY AND OPERATING STYLE

The Noon AI management team must balance two competing interests: continuing to grow and develop in a cutting edge, rapidly changing technology space while remaining excellent and conservative stewards of the highly sensitive data and workflows our customers entrust to us.
The management team meets frequently to be briefed on technology changes that impact the way Noon AI can help customers build data workflows, as well as new security technologies that can help protect those workflows, and finally any regulatory changes that may require Noon AI to alter its software to maintain legal compliance. Major planned changes to the business are also reviewed by the management team to ensure they can be conducted in a way that is compatible with our core product offerings and

duties to new and existing customers.

- Specific control activities that the service organization has implemented in this area are described below:
- Executive management meetings are held to discuss major initiatives and issues that affect the business.

ORGANIZATIONAL STRUCTURE AND ASSIGNMENT OF AUTHORITY AND RESPONSIBILITY

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

Noon AI's assignment of authority and responsibility activities includes factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.
Specific control activities that the service organization has implemented in this area are described below:

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

HUMAN RESOURCE POLICIES AND PRACTICES

Noon AI's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top quality personnel who ensure the service organization operates at maximum efficiency. Noon AI's human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.
Specific control activities that the service organization has implemented in this area are described below:

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

RISK ASSESSMENT PROCESS

Noon AI's risk assessment process identifies and manages risks that could potentially affect Noon AI's ability to provide reliable and secure services to our customers. As part of this process, Noon AI maintains a risk register to track all systems and procedures that could present risks to meeting the company's

objectives. Risks are evaluated by likelihood and impact, and management creates tasks to address risks that score highly on both dimensions. The risk register is reevaluated annually, and tasks are incorporated into the regular Noon AI product development process so they can be dealt with predictably and iteratively.

INTEGRATION WITH RISK ASSESSMENT

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

INFORMATION AND COMMUNICATION SYSTEMS

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

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

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

MONITORING CONTROLS

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

ON-GOING MONITORING

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

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

REPORTING DEFICIENCIES

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

CHANGES TO THE SYSTEM

No significant changes have occurred to the services provided to user entities during the review period or since the organization's last review.

INCIDENTS

No significant incidents have occurred to the services provided to user entities during the review period or since the organization's last review.

CRITERIA NOT APPLICABLE TO THE SYSTEM

All Common Criteria/Security, Availability, and Confidentiality criteria were applicable to the Noon AI application system.

SUBSERVICE ORGANIZATIONS

This report does not include the services provided by GCP.

Complementary Subservice Organization Controls

Noon AI's services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all the trust services criteria related to Noon AI's services to be solely achieved by Noon AI control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of Noon AI.

The following subservice organization controls have been implemented by GCP and included in this report to provide additional assurance that the trust services criteria are met.

Subservice Provider – GCP		
Category	Criteria	Control
Security	CC6.4	Data center server floors, network rooms and security systems are physically isolated from public spaces and/or delivery areas.
Security	CC6.4	Access to sensitive data center zones requires approval from authorized personnel and is controlled via badge access readers, biometric identification mechanism, and/or physical locks.
Security	CC6.4	Data center perimeters are defined and secured via physical barriers.
Security	CC6.4	Access lists to high security areas in data centers are reviewed on a defined basis and inappropriate access is removed in a timely manner.
Security	CC6.4	Visitors to data center facilities must gain approval from authorized personnel, have their identity verified at the perimeter, and remain with an escort for the duration of the visit.
Security	CC6.4	Security measures utilized in data centers are assessed annually and the results are reviewed by executive management.
Security	CC6.4	Data centers are continuously staffed and monitored by security personnel using real time video surveillance and/or alerts generated by security systems.
Availability	A1.2	Critical power and telecommunications equipment in data centers is physically protected from disruption and damage.
Availability	A1.2	Redundant power is utilized to support the continued operation of critical data center equipment in the event of a loss of the primary power source(s).
Availability	A1.2	Data centers are equipped with fire detection alarms and protection equipment.
Availability	A1.2	The organization's information processing resources are distributed across distinct, geographically dispersed processing facilities to support service redundancy, and availability.
Availability	A1.2	The organization conducts disaster resiliency testing (DiRT) which covers reliability, survivability, and recovery on an ongoing basis (and at least annually).

Noon AI management, along with the subservice provider, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service

level agreements. In addition, Noon AI performs monitoring of the subservice organization controls, including the following procedures

- Reviewing and reconciling output reports.
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organization.

COMPLEMENTARY USER ENTITY CONTROLS

Noon AI's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all the Trust Services Criteria related to Noon AI's services to be solely achieved by Noon AI control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Noon AI's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

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

SECTION IV - Description of Criteria, Controls, Tests, and Results of Tests

Testing Performed and Results of Entity-Level Controls

In planning the nature, timing, and extent of testing of the controls, Axipro Technology considered the aspects of Noon AI's control environment and tested those that were considered necessary.

In addition to the tests of the design and operating effectiveness of specific controls described below, procedures included tests of the following components of the internal control environment of Noon AI application.

- Management controls and organizational structure
- Risk assessment process
- Information and communication
- Control activities
- Monitoring

Tests of the control environment included the following procedures, to the extent Noon AI considered necessary:

a) a review of Noon AI organizational structure, including the segregation of functional responsibilities, policy statements, processing manuals, and personnel controls,
b) discussions with management, operations, administrative and other personnel who are responsible for developing, ensuring adherence to and applying controls, and
c) observations of personnel in the performance of their assigned duties.

The control environment was considered in determining the nature, timing, and extent of the testing of controls and controls relevant to the achievement of the control objectives.

Procedures for Assessing Completeness and Accuracy of Information Provided by the Entity (IPE)

For tests of controls requiring the use of IPE (e.g., controls requiring system-generated populations for sample-based testing), Axipro Technology performed a combination of the following procedures where possible based on the nature of the IPE to address the completeness, accuracy, and data integrity of the data or reports used: (1) inspect the source of the IPE, (2) inspect the query, script, or parameters used to generate the IPE, (3) tie data between the IPE and the source, and/or (4) inspect the IPE for anomalous gaps in sequence or timing to determine the data is complete, accurate, and maintains its integrity. In addition to the above procedures, for tests of controls requiring management's use of IPE in the execution of the controls (e.g., periodic reviews of user access listings), Axipro Technology inspected management's procedures to assess the validity of the IPE source and the completeness, accuracy, and integrity of the data or reports.

Trust Services Criteria and Related Controls for Systems and Applications

On the pages that follow, the applicable Trust Services Criteria and the controls to meet the criteria have been specified by and are the responsibility of Noon AI. The "Tests Performed by Axipro Technology & Peer Reviewed by A.T. CPA" and the "Results of Tests" are the responsibility of the service auditor.

Information System Control Environment

The following controls apply to the services listed in Section III and their supporting technology environments.

Noon AI Controls Mapped to Security Criteria

Criteria	Supporting Noon AI's Control Activity	Criteria Description
CC1.0	**Common Criteria Related to Control Environment**	
CC1.1	• Management Updates • Acceptable Use Policy • Code of Conduct • Employee Performance	The entity demonstrates a commitment to integrity and ethical values.
CC1.2	• Board Meetings	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
CC1.3	• Organizational Chart • Acceptable Use Policy • Job Descriptions • Board Meetings	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
CC1.4	• Job Descriptions • Tech Competence • Employee Performance • Acceptable Use Policy	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
CC1.5	• Employee Performance • Internal Controls • Security Training	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives
CC2.0	**Common Criteria Related to Communication and Information**	
CC2.1	• Risk Assessment Methodology • Board Meetings • Management Updates • Deficiency Monitoring	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.

CC2.2	• Acceptable Use Policy • Employee Shared Drive • Internal Controls • Job Descriptions • Security Training • Contracts • Security Responsibility • Management Updates • Incidents External • Incident Response: Responsibility • Data Flow Diagram • Network Diagram	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
CC2.3	• Customer Onboarding • Contracts • Internal Controls • Incidents External • Pen Test	The entity communicates with external parties regarding matters affecting the functioning of internal control.
CC3.0	**Common Criteria Related to Risk Assessment**	
CC3.1	• Risk Assessment Reporting • Risk Assessment Methodology • Risk Assessment Policy • Management Updates • Annual Third-Party SOC 2 Reports Review	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
CC3.2	• Risk Assessment Reporting • Annual Third-Party SOC 2 Reports Review • Business Continuity • Risk Assessment Methodology • Asset Inventory • Data Classification Policy • Data Flow Diagram • Network Diagram	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.
CC3.3	• Risk Assessment Reporting • Risk Assessment Methodology	The entity considers the potential for fraud in assessing risks to the achievement of objectives.

CC3.4	• Board Meetings • Risk Assessment Reporting • Risk Assessment Methodology • Annual Third-Party SOC 2 Reports Review	The entity identifies and assesses changes that could significantly impact the system of internal control.
CC4.0	**Common Criteria Related to Monitoring Activities**	
CC4.1	• Firewall • Pen Test • Internal Controls • Monitoring Infrastructure • Tech Competence	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
CC4.2	• Board Meetings • Incident Response • Monitoring Infrastructure • Risk Assessment Reporting • Pen Test • Deficiency Monitoring	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management
CC5.0	**Common Criteria Related to Control Activities**	
CC5.1	• Automatic Patching • Risk Assessment Reporting • Business Continuity • Internal Controls • Data Flow Diagram • Network Diagram • Risk Assessment Methodology • Change Management: Segregation of Duties • Separation of Duties: Developers	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
CC5.2	• Automatic Patching • Firewall • Virtual Private Cloud • Business Continuity • Logical Access • User Access Review	The entity also selects and develops general control activities over technology to support the achievement of objectives.

CC5.3	• Acceptable Use Policy • Data Classification Policy • Incident Response • Logical Access • Security Training • Information Security Oversight • Internal Controls • Security Responsibility • Policy Review • Pen Test • Job Descriptions	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.
CC6.0	**Common Criteria Related to Logical and Physical Access Controls**	
CC6.1	• Password Policy • Virtual Private Cloud • Asset Inventory • Secrets Management • Critical Systems Access • Logical Access • Workstation Lockout • User Authentication • Data Flow Diagram • Data Classification Policy • Encryption at Rest • Encryption in Transit	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.
CC6.2	• Administrator Access • User Access Review • Termination of Access	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.

CC6.3	• User Access Review • Administrator Access • Logical Access • Termination of Access • Backup Schedule • Change Management: Segregation of Duties • Separation of Duties: Developers	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.
CC6.5	• Data Management Policy • Data Retention/Deletion	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.
CC6.6	• Firewall • Virtual Private Cloud • Secrets Management	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.
CC6.7	• Encryption in Transit	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.
CC6.8	• Automatic Patching • Firewall • Monitoring Infrastructure	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.
CC7.0	**Common Criteria Related to System Operations**	
CC7.1	• Firewall • Monitoring Infrastructure • Configuration Standards	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.

CC7.2	• Firewall • Monitoring Infrastructure • Pen Test	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.
CC7.3	• Incident Response • Incident Response Analysis	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.
CC7.4	• Incident Response • Incident Response Analysis • Incident Response: Responsibility	The entity responds to identified security incidents by executing a defined incident-response program to understand, contain, remediate, and communicate security incidents, as appropriate.
CC7.5	• Incident Response • Incident Response Analysis • Restore	The entity identifies, develops, and implements activities to recover from identified security incidents.
CC8.0	**Common Criteria Related to Change Management**	
CC8.1	• Change Management Process • Change Management: Release Checklist • Change Management Policy • Change Management: Infrastructure • Configuration Standards • Change Management: Emergency Process • Separation of Environments • Change Management: Pre-Approve • Change Management: Ticketing System • Automatic Patching	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.
CC9.0	**Risk Mitigation**	

CC9.1	• Contracts • Disaster Recovery Plan • Cyber Insurance	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.
CC9.2	• Contracts • Annual Third-Party SOC 2 Reports Review • Risk Assessment Methodology • Incidents External • Termination of Access • Non-Disclosure Agreement	The entity assesses and manages risks associated with vendors and business partners.

Security Criteria Mapped to Noon AI's Controls & Auditor Testing Performed and Results

Control Name	Controls Specified by Noon AI	Criteria ID	Test Performed by Axipro Technology and Results
Acceptable Use Policy	All employees are required to acknowledge the Acceptable Use Policy upon hire. The policy outlines rules for the acceptable use of information associated with information and information processing, as well as, appropriate procedures for compliance with legislative, regulatory, and contractual requirements related to proprietary software services. The policy is updated by management as needed and available to employees.	CC.1.1 CC.1.3 CC.1.4 CC.2.2 CC.5.3	Inspected the evidence provided for the Acceptable Use Policy control, noting that all employees are required to acknowledge the Acceptable Use Policy upon hire. The policy outlines rules for the acceptable use of information associated with information and information processing, as well as appropriate procedures for compliance with legislative, regulatory, and contractual requirements related to proprietary software services. The policy is updated by management as needed and available to employees. **No exceptions noted**
Administrator Access	Administrator access to in-scope applications, database, VPN, and operating system is restricted to authorized users. Administrative and privileged access, as defined by policy, is reviewed at least quarterly.	CC.6.2 CC.6.3	Inspected the evidence provided for the Control noting that administrator access to in-scope applications, database, VPN, and operating system is restricted to authorized users. Administrative and privileged access, as defined by policy, is reviewed at least quarterly. **No exceptions noted**
Annual Third-Party SOC 2 Reports Review	Third party SOC 2 reports are reviewed for impact to the organization's control environment, and the review is formally documented by management.	CC.3.1 CC.3.2 CC.3.4 CC.9.2	Inspected the evidence provided for the Control noting that third party SOC 2 reports are reviewed for impact to the organization's control environment, and the review is formally documented by management. **No exceptions noted**

Asset Inventory	An inventory of assets is maintained and updated at least annually. All assets have an assigned asset owner. All assets are classified based on the data classification convention.	CC.3.2 CC.6.1	Inspected the evidence provided for the Control noting that an inventory of assets is maintained and updated at least annually. All assets have an assigned asset owner. All assets are classified based on the data classification convention. **No exceptions noted**
Automatic Patching	Servers are configured to automatically install critical security patches.	CC.5.1 CC.5.2 CC.6.8 CC.8.1	Inspected the evidence provided for the Control noting that servers are configured to automatically install critical security patches. **No exceptions noted**
Backup Schedule	Data is backed up following a set schedule and staff is notified of back up failures; access to backups is restricted to privileged users. Backup schedules adhere to the Backup Policy.	CC.6.3	Inspected the evidence provided for the Control noting that data is backed up following a set schedule and staff is notified of back up failures; access to backups is restricted to privileged users. Backup schedules adhere to the Backup Policy. **No exceptions noted**
Board Meetings	The Board of Directors meets on a quarterly basis to provide oversight and guidance to organization management.	CC.1.2 CC.1.3 CC.2.1 CC.3.4 CC.4.2	Inspected the evidence provided for the Control noting that the Board of Directors meets on a quarterly basis to provide oversight and guidance to organization management. **No exceptions noted**
Business Continuity	A Business Continuity Plan has been developed and reviewed in the event of a catastrophic event. The plan identifies a process, roles, and milestones	CC.3.2 CC.5.1 CC.5.2	Inspected the evidence provided for the Control noting that a Business Continuity Plan has been developed and reviewed in the event of a catastrophic event. The plan identifies a process, roles, and milestones for maintaining business

	for maintaining business continuity and restoring system functionality.		continuity and restoring system functionality. **No exceptions noted**
Change Management Process	The Change Management process is documented and procedures are in place to request, document, test and approve changes. The VP of Product is the owner of the Change Management Policy and is responsible for ensuring that changes to product and engineering production environments are made in a manner appropriate to their impact on Operations.	CC.8.1	Inspected the evidence provided for the Control noting that the Change Management process is documented and procedures are in place to request, document, test and approve changes. The VP of Product is the owner of the Change Management Policy and is responsible for ensuring that changes to product and engineering production environments are made in a manner appropriate to their impact on Operations. **No exceptions noted**
Change Management: Emergency Process	Emergency changes are identified as those that if not implemented immediately would leave the company open to significant risk or application downtime. An emergency process allows these changes to be addressed immediately by the appropriate Team.	CC.8.1	Inspected the evidence provided for the Control noting that emergency changes are identified as those that if not implemented immediately would leave the company open to significant risk or application downtime. An emergency process allows these changes to be addressed immediately by the appropriate Team. **No exceptions noted**
Change Management: Infrastructure	Infrastructure changes are tested, reviewed, and approved by authorized personnel prior to implementation.	CC.8.1	Inspected the evidence provided for the Control noting that infrastructure changes are tested, reviewed, and approved by authorized personnel prior to implementation. **No exceptions noted**
Change Management: Pre-Approve	All changes are versioned, tested and approved by an	CC.8.1	Inspected the evidence provided for the Control noting that all changes are versioned, tested and

	individual separate from the developer prior to implementation. Quality assurance is measured through testing including, Integration testing or other testing, as appropriate. Testing is performed in a sandbox environment		approved by an individual separate from the developer prior to implementation. Quality assurance is measured through testing including, Integration testing or other testing, as appropriate. Testing is performed in a sandbox environment. **No exceptions noted**
Change Management: Release Checklist	Noon AI utilizes a Release Checklist to ensure that key elements of the Change Process (ex. Testing, approval to migrate) have been met.	CC.8.1	Inspected the evidence provided for the Control noting that Noon AI utilizes a Release Checklist to ensure that key elements of the Change Process (ex. Testing, approval to migrate) have been met. **No exceptions noted**
Change Management: Segregation of Duties	Segregation of duties exist during the infrastructure and application change process. Users are restricted, by role, for deploying change requests to production. Business Users do not have access to the code repository or the Development environments.	CC.5.1 CC.6.3	Inspected the evidence provided for the Control noting that segregation of duties exists during the infrastructure and application change process. Users are restricted, by role, for deploying change requests to production. Business Users do not have access to the code repository or the Development environments. **No exceptions noted**
Change Management: Ticketing System	A centralized ticketing and workflow tool tracks software change activity, including development, approvals and testing.	CC.8.1	Inspected the evidence provided for the Control noting that a centralized ticketing and workflow tool tracks software change activity, including development, approvals and testing. **No exceptions noted**
Code of Conduct	Noon AI requires all employees to acknowledge the Code of Conduct upon hire.	CC.1.1	Inspected the evidence provided for the Control noting that Noon AI requires all employees to acknowledge the Code of Conduct upon hire.

			No exceptions noted
Configuration Standards	A baseline security configuration is maintained by the information technology team and is deployed to all systems.	CC.7.1 CC.8.1	Inspected the evidence provided for the Control noting that a baseline security configuration is maintained by the information technology team and is deployed to all systems. **No exceptions noted**
Contracts	The organization utilizes a standard contractual agreement that defines relevant security commitments and requirements for both its customers as well as third party providers. Scope, responsibilities, compliance requirements, and service levels are included in the contract. The agreement template is periodically reviewed to align with business requirements.	CC.2.2 CC.9.1 CC.9.2	Inspected the evidence provided for the Control noting that the organization utilizes a standard contractual agreement that defines relevant security commitments and requirements for both its customers as well as third party providers. Scope, responsibilities, compliance requirements, and service levels are included in the contract. The agreement template is periodically reviewed to align with business requirements. **No exceptions noted**
Critical Systems Access	Permissions/groups are configured for all systems with access control list management.	CC.6.1	Inspected the evidence provided for the Control noting that Permissions/groups are configured for all systems with access control list management. **No exceptions noted**
Customer Onboarding	Customers are formally onboarded to the system and provided support via Help functions within the application.	CC.2.3	Inspected the evidence provided for the Control noting that customers are formally onboarded to the system and provided support via Help functions within the application. **No exceptions noted**
Cyber Insurance	Organization has Cyber Security	CC.9.1	Inspected the evidence provided for the

	Insurance in place.		Control noting that organization has Cyber Security Insurance in place. **No exceptions noted**
Data Classification Policy	A defined information classification scheme has been established to label and handle data. Classifications consider the legal requirements, value, criticality, and sensitivity to unauthorized disclosure or modification of the information. Data is classified into three levels: public, confidential, sensitive.	CC.3.2 CC.5.3 CC.6.1	Inspected the evidence provided for the Control noting that a defined information classification scheme has been established to label and handle data. Classifications consider the legal requirements, value, criticality, and sensitivity to unauthorized disclosure or modification of the information. Data is classified into three levels: public, confidential, sensitive. **No exceptions noted**
Data Flow Diagram	The data flow diagram is maintained, and highlights the systems that require logical access controls per data classification level.	CC.2.2 CC.3.2 CC.5.1 CC.6.1	Inspected the evidence provided for the Control noting that the data flow diagram is maintained, and highlights the systems that require logical access controls per data classification level. **No exceptions noted**
Data Management Policy	A defined Data Management Policy provides guidance on information categories, usage, storage, and transmission of data.	CC.6.5	Inspected the evidence provided for the Control noting that a defined Data Management Policy provides guidance on information categories, usage, storage, and transmission of data. **No exceptions noted**
Data Retention/Deletion	Procedures are in place to remove data from production based on retention schedules, contract requirements, and deletion rules that are applied	CC.6.5	Inspected the evidence provided for the Control noting that procedures are in place to remove data from production based on retention schedules, contract requirements, and deletion rules that are applied to specific forms of data;

	to specific forms of data; disposals are tracked; a data disposal process is in place.		disposals are tracked; a data disposal process is in place. **No exceptions noted**
Deficiency Monitoring	Control deficiencies and results of separate evaluations are communicated to, and monitored by the CTO and other senior management, as appropriate. Security and IT operational issues are tracked and monitored.	CC.2.1 CC.4.2	Inspected the evidence provided for the Control noting that control deficiencies and results of separate evaluations are communicated to, and monitored by the CTO and other senior management, as appropriate. Security and IT operational issues are tracked and monitored. **No exceptions noted**
Disaster Recovery Plan	A Disaster Recovery Plan is maintained and tested annually.	CC.9.1	Inspected the evidence provided for the Control noting that a Disaster Recovery Plan is maintained and tested annually. **No exceptions noted**
Employee Performance	A formal performance evaluation procedure is in place and employees are evaluated at least annually.	CC.1.1 CC.1.4 CC.1.5	Inspected the evidence provided for the Control noting that a formal performance evaluation procedure is in place and employees are evaluated at least annually. **No exceptions noted**
Employee Shared Drive	A centralized repository is in place for employees to access all corporate policies and procedures.	CC.2.2	Inspected the evidence provided for the Control noting that a centralized repository is in place for employees to access all corporate policies and procedures. **No exceptions noted**
Encryption at Rest	All data at rest is encrypted using industry standard algorithms.	CC.6.1	Inspected the evidence provided for the Control noting that all data at rest is encrypted using industry standard algorithms. **No exceptions noted**

Encryption in Transit	Any sensitive data that's transmitted over public networks and data in transit are encrypted.	CC.6.1 CC.6.7	Inspected the evidence provided for the Control noting that any sensitive data that's transmitted over public networks and data in transit are encrypted. **No exceptions noted**
Firewall	Web application firewalls are in place to help prevent unauthorized access threats from outside the application. Rules are configured to apply network controls within cloud service to restrict access to sensitive data to the appropriate locations and parties. Web application firewall rules are reviewed by authorized personnel on an annual basis, at minimum.	CC.4.1 CC.5.2 CC.6.6 CC.6.8 CC.7.1 CC.7.2	Inspected the evidence provided for the Control noting that web application firewalls are in place to help prevent unauthorized access threats from outside the application. Rules are configured to apply network controls within cloud service to restrict access to sensitive data to the appropriate locations and parties. Web application firewall rules are reviewed by authorized personnel on an annual basis, at minimum. **No exceptions noted**
Incident Response	Incident response guidelines are published and available to all employees and include: definition of an incident, employee responsibilities and notification procedures. Employees are responsible for reporting incidents and possible breaches of security to their supervisor who will then notifies the CPO, as appropriate.	CC.4.2 CC.5.3 CC.7.3 CC.7.4 CC.7.5	Inspected the evidence provided for the Control noting that incident response guidelines are published and available to all employees and include: definition of an incident, employee responsibilities and notification procedures. Employees are responsible for reporting incidents and possible breaches of security to their supervisor who will then notifies the CPO, as appropriate. **No exceptions noted**
Incident Response Analysis	An Incident Response captures the data necessary to analyze an incident and determine the security impact. The Security	CC.7.3 CC.7.4 CC.7.5	Inspected the evidence provided for the Control noting that an Incident Response captures the data necessary to analyze an incident and determine the security impact. The Security

	Incident Response team determines and validates the nature and severity of security incidents. The CPO then approves and delegate response activities as appropriate. Noon AI performs a root cause analysis (RCA) for incidents and information disclosures that could impact security.		Incident Response team determines and validates the nature and severity of security incidents. The CPO then approves and delegate response activities as appropriate. Noon AI performs a root cause analysis (RCA) for incidents and information disclosures that could impact security. **No exceptions noted**
Incident Response: Responsibility	The design, implementation, maintenance, execution, and periodic testing of the security incident response program and data breach response procedures are the responsibility of the Head of Engineering.	CC.2.2 CC.7.4	Inspected the evidence provided for the Control noting that the design, implementation, maintenance, execution, and periodic testing of the security incident response program and data breach response procedures are the responsibility of the Head of Engineering. **No exceptions noted**
Incidents External	External parties may report systems failures, incidents, concerns, and other complaints to appropriate personnel by submitting their issue via the organizations support webpage. The incident is documented in accordance with the Incident Response Plan, if required.	CC.2.2 CC.2.3 CC.9.2	Inspected the evidence provided for the Control noting that external parties may report systems failures, incidents, concerns, and other complaints to appropriate personnel by submitting their issue via the organizations support webpage. The incident is documented in accordance with the Incident Response Plan, if required. **No exceptions noted**
Information Security Oversight	Noon AI has formally assigned the role for oversight of information security and primary business practices. The assignee communicates the	CC.5.3	Inspected the evidence provided for the Control noting that Noon AI has formally assigned the role for oversight of information security and primary business practices. The assignee communicates the

	importance of effective information security management and of conforming to the information security management system requirements.		importance of effective information security management and of conforming to the information security management system requirements. **No exceptions noted**
Internal Controls	Internal control responsibilities are assigned to control owners who are responsible for monitoring controls for deficiencies, documenting deficiencies in a corrective action plan, and communicating them to management for review.	CC.1.5 CC.2.2 CC.2.3 CC.4.1 CC.5.1 CC.5.3	Inspected the evidence provided for the Control noting that internal control responsibilities are assigned to control owners who are responsible for monitoring controls for deficiencies, documenting deficiencies in a corrective action plan, and communicating them to management for review. **No exceptions noted**
Job Descriptions	Job descriptions are in place which define the skills and responsibilities for specific roles and are available to all employees. Job descriptions include responsibility as they relate to information security.	CC.1.3 CC.1.4 CC.2.2 CC.5.3	Inspected the evidence provided for the Control noting that job descriptions are in place which define the skills and responsibilities for specific roles and are available to all employees. Job descriptions include responsibility as they relate to information security. **No exceptions noted**
Logical Access	Logical Access Policy and Procedures are in place which define the authorization, modification, removal of access, role-based access, and the principle of least privilege. The policy is reviewed annually.	CC.5.2 CC.5.3 CC.6.1 CC.6.3	Inspected the evidence provided for the Control noting that logical Access Policy and Procedures are in place which define the authorization, modification, removal of access, role-based access, and the principle of least privilege. The policy is reviewed annually. **No exceptions noted**
Management Updates	Management presents status on	CC.1.1	Inspected the evidence provided for the Control

	corporate goals and objectives to all hands quarterly; this includes sales updates, department updates, and key operational metrics.	CC.2.1 CC.2.2 CC.3.1	noting that Management presents status on corporate goals and objectives to all hands quarterly; this includes sales updates, department updates, and key operational metrics. **No exceptions noted**
Monitoring Infrastructure	IT infrastructure monitoring tools are configured to monitor IT infrastructure security events and to generate alerts when specific predefined thresholds or event are met. Alerts are actioned as needed.	CC.4.1 CC.4.2 CC.6.8 CC.7.1 CC.7.2 C1.1	Inspected the evidence provided for the Control noting that IT infrastructure monitoring tools are configured to monitor IT infrastructure security events and to generate alerts when specific predefined thresholds or event are met. Alerts are actioned as needed. **No exceptions noted**
Network Diagram	Service boundaries are defined in the network diagram. The network diagram is reviewed annually or as business needs require.	CC.2.2 CC.3.2 CC.5.1	Inspected the evidence provided for the Control noting that service boundaries are defined in the network diagram. The network diagram is reviewed annually or as business needs require. **No exceptions noted**
Non-Disclosure Agreement	Employees and contractors are required to sign a Non-Disclosure Agreement, as are third parties that may have access to personal information. The Non-Disclosure Agreement includes the signee's and the company's responsibility with respect to information security. The template is periodically reviewed to align with business requirements.	CC.9.2	Inspected the evidence provided for the Control noting that Employees and contractors are required to sign a Non-Disclosure Agreement, as are third parties that may have access to personal information. The Non-Disclosure Agreement includes the signee's and the company's responsibility with respect to information security. The template is periodically reviewed to align with business requirements. **No exceptions noted**

Organizational Chart	The business is organized along functional areas. Within functional areas, organizational and reporting hierarchies have been defined and responsibilities have been assigned. Organizational charts are updated as needed.	CC.1.3	Inspected the evidence provided for the Control noting that the business is organized along functional areas. Within functional areas, organizational and reporting hierarchies have been defined and responsibilities have been assigned. Organizational charts are updated as needed. **No exceptions noted**
Password Policy	Password configuration settings adhere to the Logical Access Policy and Procedure document. Exceptions are approved by the CPO.	CC.6.1	Inspected the evidence provided for the Control noting that Password configuration settings adhere to the Logical Access Policy and Procedure document. Exceptions are approved by the CPO. **No exceptions noted**
Pen Test	Noon AI performs penetration tests at least annually. Test results are reviewed and tracked to satisfactory resolution.	CC.2.3 CC.4.1 CC.4.2 CC.5.3 CC.7.2	Inspected the evidence provided for the Control noting that Noon AI performs penetration tests at least annually. Test results are reviewed and tracked to satisfactory resolution. **No exceptions noted**
Policy Review	IT security related policies are reviewed and approved annually or as business needs change.	CC.5.3	Inspected the evidence provided for the Control noting that IT security related policies are reviewed and approved annually or as business needs change. **No exceptions noted**
Restore	Noon AI has documented restoration procedures for the cloud service network. Noon AI performs backup restoration testing annually, at minimum.	CC.7.5	Inspected the evidence provided for the Control noting that Noon AI has documented restoration procedures for the cloud service network. Noon AI performs backup restoration testing annually, at minimum.

			No exceptions noted
Risk Assessment Methodology	Noon AI conducts an annual Risk Assessment to identify, assess, mitigate, report and monitor security risks. Noon AI considers relevant laws and regulations when it conducts its annual Risk Assessment. The Risk Assessment scores risks based on likelihood and consequence, and high scoring risks are acted upon. Fraud risks are considered in the annual Risk Assessment.	CC.2.1 CC.3.1 CC.3.2 CC.3.3 CC.3.4 CC.5.1 CC.9.2	Inspected the evidence provided for the Control noting that Noon AI conducts an annual Risk Assessment to identify, assess, mitigate, report and monitor security risks. Noon AI considers relevant laws and regulations when it conducts its annual Risk Assessment. The Risk Assessment scores risks based on likelihood and consequence, and high scoring risks are acted upon. Fraud risks are considered in the annual Risk Assessment. **No exceptions noted**
Risk Assessment Policy	Risk assessment policy and procedures are in place and include how to identify risks, to evaluate risks, and how to address and mitigate those risks.	CC.3.1	Inspected the evidence provided for the Control noting that risk assessment policy and procedures are in place and include how to identify risks, to evaluate risks, and how to address and mitigate those risks. **No exceptions noted**
Risk Assessment Reporting	Risk Assessment results are shared with management annually.	CC.3.1 CC.3.2 CC.3.3 CC.3.4 CC.4.2 CC.5.1	Inspected the evidence provided for the Control noting that risk assessment results are shared with management annually. **No exceptions noted**
Secrets Management	Secrets Management (e.g. keys, passwords, certificates, etc.) is restricted to authorized users, limited by appropriate controls and logging within Noon AI password manager.	CC.6.1 CC.6.6	Inspected the evidence provided for the Control noting that Secrets Management (e.g. keys, passwords, certificates, etc.) is restricted to authorized users, limited by appropriate controls and logging within Noon AI password manager.

			No exceptions noted
Security Responsibility	The Information Security Policy is maintained, reviewed and annually updated by the CEO. The development of the information security program, processes and procedures are the responsibility of the CEO and CTO.	CC.2.2 CC.5.3	Inspected the evidence provided for the Control noting that the Information Security Policy is maintained, reviewed and annually updated by the CEO. The development of the information security program, processes and procedures are the responsibility of the CEO and CTO. **No exceptions noted**
Security Training	Employees and contractors complete security-related training as relevant to their duties on an annual basis. The annual security training includes information on how to report security incidents and concerns.	CC.1.5 CC.2.2 CC.5.3	Inspected the evidence provided for the Control noting that employees and contractors complete security-related training as relevant to their duties on an annual basis. The annual security training includes information on how to report security incidents and concerns. **No exceptions noted**
Separation of Duties: Developers	Access to the source code repository is restricted to authorized employees.	CC.5.1 CC.6.3	Inspected the evidence provided for the Control noting that access to the source code repository is restricted to authorized employees. **No exceptions noted**
Separation of Environments	Production, testing, and development environments are logically and physically separated.	CC.8.1	Inspected the evidence provided for the Control noting that production, testing, and development environments are logically and physically separated. **No exceptions noted**
Tech Competence	The new hire screening process includes a consideration of skills and competencies of the candidate. Each job candidate is	CC.1.4 CC.4.1	Inspected the evidence provided for the Control noting that the new hire screening process includes a consideration of skills and competencies of the candidate. Each

	interviewed by personnel within the employing department to determine if education, experience, and technical competency are appropriate for the job function. Reference checks are performed prior to hire.		job candidate is interviewed by personnel within the employing department to determine if education, experience, and technical competency are appropriate for the job function. Reference checks are performed prior to hire. **No exceptions noted**
Termination of Access	User's access to IT systems is revoked within 48 hours when employment or contract terminates. Exceptions are documented in the checklist and/or offboarding ticket.	CC.6.2 CC.6.3 CC.9.2	Inspected the evidence provided for the Control noting that user's access to IT systems is revoked within 48 hours when employment or contract terminates. Exceptions are documented in the checklist and/or offboarding ticket. **No exceptions noted**
User Access Review	Management performs a review of user access to systems based on job duties. Inactive users are removed and removal is documented.	CC.5.2 CC.6.2 CC.6.3	Inspected the evidence provided for the Control noting that management performs a review of user access to systems based on job duties. Inactive users are removed and removal is documented. **No exceptions noted**
User Authentication	Unique usernames and passwords are required to authenticate all users.	CC.6.1	Inspected the evidence provided for the Control noting that Unique usernames and passwords are required to authenticate all users. **No exceptions noted**
Virtual Private Cloud	Production systems reside within a secure VPC within cloud service.	CC.5.2 CC.6.1 CC.6.6	Inspected the evidence provided for the Control noting that production systems reside within a secure VPC within cloud service.

			No exceptions noted
Workstation Lockout	Internal users' screensavers are configured to lock after a specified period of time of inactivity and to require a password to unlock.	CC.6.1	Inspected the evidence provided for the Control noting that Internal users' screensavers are configured to lock after a specified period of time of inactivity and to require a password to unlock. **No exceptions noted**