Dart Health Technology

SOC 2 Type 1 Report

Dart Health Technology LLC

Restricted Use & Distribution

Report Issue Date: May 02, 2025

A Type 1 Independent Service Auditor's Report on Controls Relevant to Security, Confidentiality, Availability, Processing Integrity and Privacy



AUDIT AND ATTESTATION BY

PRESCIENT ASSURANCE

AICPA

Prescient Assurance LLC.
4808 Signal Forest Drive,
Signal Mountain, TN, 37377

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

Table of Contents

Management's Assertion	3
Independent Service Auditor's Report	5
System Description	9
Testing Matrices	22
Management Representation Letter	55

PRESCIENT ASSURANCE

SECTION 1

Management's Assertion



Management's Assertion

We have prepared the accompanying description of Dart Health Technology LLC's system as of April 10, 2025, based on the criteria for a description of a service organization's system set forth in DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report. The description is intended to provide report users with information about Dart Health Technology LLC's system that may be useful when assessing the risks arising from interactions with Dart Health Technology LLC's system, particularly information about system controls that Dart Health Technology LLC has designed to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Confidentiality, Availability, Processing Integrity and Privacy set forth in TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.

Dart Health Technology LLC uses a subservice organization for cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed are necessary, along with controls at Dart Health Technology LLC, to achieve Dart Health Technology LLC's service commitments and system requirements based on the applicable trust services criteria. The description presents Dart Health Technology LLC's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Dart Health Technology LLC's controls. The description does not disclose the actual controls at the subservice organization.

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

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

a. The description presents Dart Health Technology LLC's system that was designed as of April 10, 2025, in accordance with the description criteria.
b. The controls stated in the description were suitably designed as of April 10, 2025, to provide reasonable assurance that Dart Health Technology LLC's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of that date, and if the subservice organization and user entities applied the complementary controls assumed in the design of Dart Health Technology LLC's controls as of that date.

Brian Sage

Brian Sage

CEO

Dart Health Technology LLC

PRESCIENT ASSURANCE

SECTION 2

Independent Service Auditor's Report



Independent Service Auditor's Report

To: Dart Health Technology LLC

Scope

We have examined Dart Health Technology LLC's ("Dart Health Technology LLC") accompanying description of its system as of April 10, 2025, based on the criteria for a description of a service organization's system set forth in DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report, and the suitability of the design of controls stated in the description as of April 10, 2025, to provide reasonable assurance that Dart Health Technology LLC's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Confidentiality, Availability, Processing Integrity and Privacy set forth in TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.

Dart Health Technology LLC uses a subservice organization for cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed are necessary, along with controls at Dart Health Technology LLC, to achieve its service commitments and system requirements based on the applicable trust services criteria. The description presents Dart Health Technology LLC's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Dart Health Technology LLC'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 of such complementary subservice organization controls.

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

Service Organization's Responsibilities

Dart Health Technology LLC is responsible for its service commitments and system requirements and for designing effective controls within the system to provide reasonable assurance that Dart Health Technology LLC's service commitments and system requirements were achieved. In Section 1, Dart Health Technology LLC has provided the accompanying assertion titled "Management's Assertion of Dart Health Technology LLC" (assertion) about the description and the suitability of design of controls stated therein. Dart Health Technology LLC is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditors' Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of the design of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our

examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

1. Obtaining an understanding of the system and the service organization's service commitments and system requirements.
2. Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed.
3. Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
4. 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.
5. Evaluating the overall presentation of the description.

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

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

Inherent Limitations

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

Opinion

In our opinion, in all material respects:

A. The description presents Dart Health Technology LLC's system that was designed as of April 10, 2025, in accordance with the description criteria.
B. The controls stated in the description were suitably designed as of April 10, 2025, to provide reasonable assurance that Dart Health Technology LLC's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of that date and if the subservice organization and user entities applied the complementary controls assumed in the design of Dart Health Technology LLC's controls as of that date.

Restricted Use

This report is intended solely for the information and use of Dart Health Technology LLC, user entities of Dart

Health Technology LLC's system as of April 10, 2025, business partners of Dart Health Technology LLC subject to risks arising from interactions with the system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

1. The nature of the service provided by the service organization.
2. How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties.
3. Internal control and its limitations.
4. 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.
5. User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
6. The applicable trust services criteria.
7. 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.

Prescient Assurance

Prescient Assurance LLC

PRESCIENT ASSURANCE

SECTION 3

System Description



Dart Health Technology

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

Company Background

Dart Health Technology LLC (the "company") was founded on 07/06/2022 by Brian Sage and Jason Cole to provide data ETL and storage services to healthcare benefits administration entities. The organization is based out of Centennial, Colorado with additional sites in Englewood, Colorado.

Description of Services Provided

The company's core product, the Data Nexus (the "system") is a Software as a Service (SaaS) solution that includes the following services:

- Secure reception and transmission of employee benefits, eligibility, enrollment, and benefits utilization data — enables the company's customers to not have to re-invent the wheel when faced by the same challenges besetting the healthcare benefits administration industry, giving our customers their resources and time back to invest in their core business
- Several secure transmission standards, including SFTP, and web-accessible, authenticated API — enables the company's customers to utilize our highly-available service instead of having to configure and maintain the same on their own
- Configurable data output standards — enables the company's customers to receive their customers data sooner, creating shorter timelines, fewer errors, and happier customers

DC 2: The Principal Service Commitments and System Requirements

The company designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments that the company makes to user entities, the laws, and regulations that govern the provision of the services, and the financial, operational, and compliance requirements that the company has established for the services. The system services are subject to the policies established under HIPAA, SOC 2 Level 2 and the company's internal policies that include but are not limited to the following commitments established internally for its services.

- Human Resource Security Policy
- Code of Conduct
- Third-Party Management
- Risk Management
- Asset Management
- Data Management
- Cryptography
- Secure Development
- Access Control
- Business Continuity and Disaster Recovery
- Operations Security
- Physical Security
- Information Security

Commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online.

Security Commitments

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; and,
- 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

Confidentiality Commitments

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 and trainings with employees, contractors, and third parties; and,
- Confidential information must be used only for the purposes explicitly stated in agreements between the company and user entities.

Availability Commitments

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
- Operational procedures supporting the achievement of availability commitments to user entities

Privacy Commitments

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

- Adherence to relevant privacy laws and regulations, such as GDPR, to ensure that personal data is collected, processed, and stored in compliance with legal requirements.
- Implementation of data minimization practices to ensure that only the necessary personal data is collected and retained for the intended purposes.
- Obtaining explicit consent from data subjects for the collection, use, and sharing of their personal information, where applicable.
- Implementation of data subject rights management processes, including the ability to access, correct, or delete personal information upon request.
- Regular privacy impact assessments to identify and mitigate risks to personal data and ensure ongoing compliance with privacy regulations.
- Secure data transfer mechanisms and strict data-sharing agreements with third parties to protect personal information during transfers.

Processing Integrity Commitments

Processing integrity commitments include, but are not limited to, the following:

- Implementation of controls to ensure that data processing is complete, accurate, timely, and authorized, minimizing the risk of errors and unauthorized changes.
- Regular audits and reviews of data processing activities to verify the accuracy and completeness of transactions and data entries.
- Use of automated validation and verification tools to detect and correct data errors or inconsistencies during processing.
- Implementation of change management procedures to ensure that all changes to the system or processes are properly reviewed, tested, and approved before implementation.
- Continuous monitoring of system performance and processing activities to detect and address any

processing delays, failures, or irregularities.
- Implementation of backup and recovery processes to ensure that data can be restored in the evet of corruption, loss or processing failures.

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

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.

3.1 Primary Infrastructure

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

System/Application	Operating System	Purpose
AWS	Cloud Hosting Services	Virtual Private Cloud (VPC) environment that protects the network from unauthorized external access.
GitHub	Codebase	Maintain code commit discipline, ability to perform rollbacks, and CI/CD pipeline performance
Shortcut	Communication Service	Maintain operational workflow discipline
Slack	Communication Service	Maintain working communications discipline and history

3.2 Primary Software

The company is responsible for managing the development and operation of the Data Nexus platform including infrastructure components such as servers, databases, and storage systems. The company's in-scope infrastructure and software components are shown in the table below:

System/Application	Operating System	Purpose

AWS Transfer Family	AWS	Simplifies secure file transfers to and from Amazon S3 or Amazon EFS using SFTP, FTPS, and FTP
Route53	AWS	Highly available and scalable Domain Name System (DNS) web service designed to route users to internet applications by translating domain names into their corresponding IP addresses.
S3	AWS	Object storage service designed to securely encrypt, store, and retrieve any amount of cloud- accessible data
EC2	AWS	Provides resizable cloud compute capacity, including virtual servers, leased servers, static IP management and leasing, and elastic load balancers
HTTPS certificate manager	AWS	Provisioning and deployment tools to manage SSL/ TLS certificates used to secure applications and data in transit
Simple Queueing Service	AWS	fully- managed messaging queue service to send, store, and receive messages between distributed software components
Secrets Manager	AWS	Provides for the rotation, management, and retrieval of credentials, API keys, and other secrets to enhance security
CloudWatch	AWS	Monitoring and observability service that collects and tracks metrics, logs, and events from AWS resources and applications, enabling real- time insights and proactive responses to operational events
IAM	AWS	Identity and Access Management (IAM) provides secure access control for AWS resources by enabling the creation and management of users, groups, roles, and permissions
RDS	AWS	Managed service for setting up, operating, and scaling relational databases in the cloud
ECS	AWS	Container orchestration service for running our proprietary containerized applications in the cloud

3.3 People

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

The company has a staff of 4 organized in the following functional areas:

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

- CEO - Brian Sage
- CTO - Jason Cole

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

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

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

- Software Architect - Jim Kane
- Senior Software Engineer - Alex Kibler

3.4 Data

Data as defined by the company constitutes the following:

- Customer data, which may include personally identifying information related to employment, health and benefits, and medical claims history financial data

Data is categorized in four major types of data used by the company.

Category	Description	Examples
Public	Public information is not confidential and can be made public without any implications for the company	Press releases, Public website
Internal	Access to internal information is approved by management and is protected from external access.	Internal memos, Design documents, Product specifications, Correspondences
Customer data	Information received from customers for processing or storage by the company. The company must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information.	Customer operating data, Customer PII, Customers' customers' PII, Anything subject to a confidentiality agreement with a customer
Company data	Information collected and used by the company to operate the business. The company must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this	Legal documents, Contractual agreements, Employee PII, Employee salaries

	information.	

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

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

3.5 Processes, Policies and Procedures

Management has developed and communicated policies and procedures to manage the information security of the system. Changes to these procedures are performed annually and authorized by the CEO or the manager of the area in question. These procedures cover the following key security life cycle areas:

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

3.5.1 Physical Security

The company's production servers are maintained by Amazon Web Services. The physical and environmental security protections are the responsibility of Amazon Web Services. The company reviews the attestation reports and performs a risk analysis of Amazon Web Services on at least an annual basis.

3.5.2 Logical Access

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

Access to these systems are split into three levels; Administrator, User, and No Access. User access and roles are reviewed on a quarterly basis to ensure least privilege access.

Management is responsible for provisioning access to the system based on the employee's role and performing a background check. The employee is responsible for reviewing the company's policies, completing security training. These steps must be completed with 30 days of hire.

When an employee is terminated, Management is responsible for deprovisioning access to all in scope systems within 24 business hours of that employee's termination.

3.5.3 Computer Operations - Backups

Customer data is backed up and monitored by the customer's assigned engineering lead for completion and exceptions. If there is an exception, the customer's assigned engineering lead performs or assigns troubleshooting tasks to identify the root cause and either rerun the backup or as part of the next scheduled backup job.

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

3.5.4 Computer Operations - Availability

The company maintains an incident response plan to guide employees on reporting and responding to any

information security or data privacy events or incidents. Procedures are in place for identifying, reporting and acting upon breaches or other incidents.

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

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

3.5.5 Change Management

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

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

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

3.5.6 Data communications

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

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

The company engages a SaaS vulnerability scanning service to perform ongoing scans and an external security firm to perform annual vulnerability scans and penetration testing to look for unidentified vulnerabilities, and the product engineering team responds to any issues identified via the regular incident response and change management process.

3.6 Boundaries of the System

The scope of this report includes the Data Nexus system performed in AWS cloud. Any Subservice organizations carved-out of the scope of the review

This report does not include Github code repo hosting services, provided by Github in the cloud.

DC 4: Disclosures about Identified Security Incidents

No significant incidents have occurred to the services provided to user entities in the last 12 months preceding the end of the review date.

DC 5: The Applicable Trust Services Criteria and the Related Controls Designed

to Provide Reasonable Assurance that the Service Organization's Service Commitments and System Requirements were Achieved

5.1 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 the company's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of the company's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

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

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

5.2 Commitment to Competence

The company'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.

5.3 Management's Philosophy and Operating Style

The company 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 the company 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 the company to alter its software to maintain legal compliance. Major planned changes to the business are also reviewed by the management team to ensure they can be conducted in a way that is compatible with our core product offerings and duties to new and existing customers.

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

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

5.4 Organizational Structure and Assignment of Authority and Responsibility

The company'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.

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

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

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

5.5 Human Resource Policies and Practices

The company's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top quality personnel who ensures the service organization is operating at maximum efficiency. the company'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.

5.6 Risk Assessment Process

The company's risk assessment process identifies and manages risks that could potentially affect the company's ability to provide reliable and secure services to our customers. As part of this process, the company 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 company product development process so they can be dealt with predictably and iteratively.

5.7 Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of the company's system; as well as the nature of the components of the system result in risks that the criteria will not be met. The company 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, the company's management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

5.8 Information and Communications Systems

Information and communication are an integral component of the company'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.

The company uses several information and communication channels internally to share information with management, employees, contractors, and customers. The company 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, the company uses in-person and video "all hands" meetings to communicate company priorities and goals from management to all employees.

5.9 Monitoring Controls

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. The company'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.

5.9.1 On-Going Monitoring

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

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

5.10 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.

DC 6: Complementary User Entity Controls (CUECs)

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

1. User entities are responsible for understanding and complying with their contractual obligations to the company.
2. User entities are responsible for notifying the company of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of the company services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize the company services.

6. User entities are responsible for providing the company with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying the company of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.

DC 7: Complementary Subservice Organization Control

This report does not include the GitHub repository hosting services provided by GitHub.

The company'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 of the trust services criteria related to the company's services to be solely achieved by the company control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of the company.

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

Subservice Provider – AWS

Category	Criteria	Control
Security	CC6.4	Physical access to data centers is approved by an authorized individual.
Security	CC6.4	Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
Security	CC6.4	Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
Security	CC6.4	Closed circuit television camera (CCTV) are used to monitor server locations in data centers. Images are retained for 90 days, unless limited by legal or contractual obligations.
Security	CC6.4	Access to server locations is managed by electronic access control devices.

The company 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, the company performs monitoring of the subservice organization controls, including the following procedures

- Reviewing and reconciling security reports
- Holding periodic discussions with vendors and subservice organization(s)
- Testing controls performed by vendors and subservice organization(s)
- Reviewing attestation reports over services provided by vendors and subservice organization(s)

DC 8: Any Specific Criterion of the Applicable Trust Services Criteria that is Not

Relevant to the System and the Reasons it is Not Relevant

All Common Criteria/ Security, Availability, Processing Integrity, Confidentiality and Privacy criteria were applicable to the company's Data Nexus system.

DC 9: Disclosure of Significant Changes in the Last 1 Year

No significant changes have occurred to the services provided to user entities in the last 12 months preceding the end of the review date.

PRESCIENT ASSURANCE

SECTION 4

Testing Matrices



Applicable Trust Services Criteria and Related Control Activities

Trust ID	Trust Services Criteria	Control Description
A1.1	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.	The company evaluates system capacity on an ongoing basis, and system changes are implemented to help ensure that processing capacity can meet demand.
A1.1	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.	An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.	The company's data backup policy documents requirements for backup and recovery of customer data.
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.	The company has a multi-location strategy for production environments employed to permit the resumption of operations at other company data centers in the event of loss of a facility.
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.	The company performs periodic backups for production data. Data is backed up to a different location than the production system.
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.	The company's databases are replicated to a secondary data center in real-time. Alerts are configured to notify administrators if replication fails.
A1.2	The entity authorizes, designs, develops or acquires, implements, operates,	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating

	approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.	the significance of the risks associated with the identified threats, and mitigation strategies for those risks.
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.	The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	The company has Business Continuity and Disaster Recovery Plans in place that outline communication plans in order to maintain information security continuity in the event of the unavailability of key personnel.
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	The company's data backup policy documents requirements for backup and recovery of customer data.
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	The company prohibits confidential or sensitive customer data, by policy, from being used or stored in non-production systems/ environments.
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	The company requires authentication to systems and applications to use unique usernames, passwords and multi-factor authentication (MFA).
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	The company has a data classification policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel.
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	The company has written agreements in place with vendors and related third-parties. These agreements include confidentiality and privacy commitments applicable to that entity.
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	The company purges or removes customer data containing confidential information from the application environment, in accordance with best practices, when customers leave the service.
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	The company has electronic media containing confidential information purged or destroyed in accordance with best practices, and certificates of destruction are issued for each device destroyed.

CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The company performs background checks on new employees.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The company requires employees to sign a confidentiality agreement during onboarding.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The company requires contractors to sign a confidentiality agreement at the time of engagement.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The company requires contractor agreements to include a code of conduct or reference to the company code of conduct.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The company requires employees to acknowledge a code of conduct at the time of hire. Employees who violate the code of conduct are subject to disciplinary actions in accordance with a disciplinary policy.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The company managers are required to complete performance evaluations for direct reports at least annually.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The company's executive leadership is briefed by senior management at least annually on the state of the company's cybersecurity and privacy risk. The executive leadership provides feedback and direction to management as needed.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The company's executive leadership meets at least annually and maintains formal meeting minutes.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The company's board members have sufficient expertise to oversee management's ability to design, implement and operate information security controls. The board engages third-party information security experts and consultants as needed.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The responsibilities of the Executive Leadership for oversight of information security controls are defined.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	The company maintains an organizational chart that describes the organizational structure and reporting lines.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of	The responsibilities of the Executive Leadership for oversight of information security controls are defined.

	objectives.	
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	The company performs background checks on new employees.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	The company managers are required to complete performance evaluations for direct reports at least annually.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	The company requires employees to complete security awareness training within thirty days of hire and at least annually thereafter.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	The company managers are required to complete performance evaluations for direct reports at least annually.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	The company requires employees to acknowledge a code of conduct at the time of hire. Employees who violate the code of conduct are subject to disciplinary actions in accordance with a disciplinary policy.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings. If the company has committed to an SLA for a finding, the corrective action is completed within that SLA.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company provides a description of its products and services to internal and external users.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company has established a formalized whistleblower policy, and an anonymous communication channel is in place for users to report potential issues or fraud concerns.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control,	The company communicates system changes to authorized internal users.

	necessary to support the functioning of internal control.	
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company's information security policies and procedures are documented and reviewed at least annually.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company requires employees to complete security awareness training within thirty days of hire and at least annually thereafter.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company's security commitments are communicated to customers in Master Service Agreements (MSA) or Terms of Service (TOS).
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company has written agreements in place with vendors and related third-parties. These agreements include confidentiality and privacy commitments applicable to that entity.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company provides guidelines and technical support resources relating to system operations to customers.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company has an external-facing support system in place that allows users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company provides a description of its products and services to internal and external users.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company notifies customers of critical system changes that may affect their processing.
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks	The company specifies its objectives to enable the identification and assessment of risk related to the objectives.

	relating to objectives.	
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.
CC3.2	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.	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.
CC3.2	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.	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.
CC3.2	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.	The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.
CC3.2	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.	The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.

CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings. If the company has committed to an SLA for a finding, the corrective action is completed within that SLA.
CC4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.
CC4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings. If the company has committed to an SLA for a finding, the corrective action is completed within that SLA.
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	The company's information security policies and procedures are documented and reviewed at least annually.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	The company's information security policies and procedures are documented and reviewed at least annually.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology

		requirements.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company specifies its objectives to enable the identification and assessment of risk related to the objectives.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company's data backup policy documents requirements for backup and recovery of customer data.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company's information security policies and procedures are documented and reviewed at least annually.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information	The company has a data classification policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel.

	assets to protect them from security events to meet the entity's objectives.	
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.	The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.
CC6.1	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.	The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.
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.	The company requires passwords for in-scope system components to be configured according to the company's policy.
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.	The company restricts privileged access to the production network to authorized users with a business need.
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.	The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.
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.	The company restricts access to migrate changes to production to authorized personnel.
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.	The company maintains a formal inventory of production system assets.
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.	The company requires authentication to production datastores to use authorized secure authentication mechanisms, such as multi-factor authentication (MFA).
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.	The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.
CC6.1	The entity implements logical access security software, infrastructure, and	The company restricts privileged access to the firewall to authorized users with a business need.

	architectures over protected information assets to protect them from security events to meet the entity's objectives.	
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.	The company restricts privileged access to databases to authorized users with a business need.
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.	System access is restricted to authorized users only.
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.	The company restricts privileged access to encryption keys to authorized users with a business need.
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.	The company requires authentication to systems and applications to use unique usernames, passwords and multi-factor authentication (MFA).
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.	The company's network is segmented to prevent unauthorized access to customer data.
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.	The company restricts privileged access to the operating system to authorized users with a business need.
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.	The company requires authentication to the production network to use unique usernames, passwords and multi-factor authentication (MFA).
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.	The company's datastores housing sensitive customer data are encrypted at rest.
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	The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.

	removed when user access is no longer authorized.	
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.	The company requires authentication to the production network to use unique usernames, passwords and multi-factor authentication (MFA).
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.	The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.
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.	The company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.
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.	The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.
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.	The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.
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	The company requires authentication to the production network to use unique usernames, passwords and multi-factor authentication (MFA).

	changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	
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.	The company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.
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.	The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.
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.	The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	The company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.
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.	The company has electronic media containing confidential information purged or destroyed in accordance with best practices, and certificates of destruction are issued for each device destroyed.
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.	The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.
CC6.5	The entity discontinues logical and physical protections over physical assets	The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.

	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	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.	The company purges or removes customer data containing confidential information from the application environment, in accordance with best practices, when customers leave the service.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company requires authentication to the production network to use unique usernames, passwords and multi-factor authentication (MFA).
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company reviews its firewall rulesets at least annually. Required changes are tracked to completion.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company uses firewalls and configures them to prevent unauthorized access.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and	The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.

	processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	
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.	The company has a mobile device management (MDM) system in place to centrally manage mobile devices supporting the service.
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.	The company encrypts portable and removable media devices when used.
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.	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.
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.	The company deploys anti-malware technology to environments commonly susceptible to malicious attacks and configures this to be updated routinely, logged, and installed on all relevant systems.
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.	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.
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.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.
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.	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.
CC7.1	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.	The company's formal policies outline the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.
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	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.

	vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	
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.	The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.
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.	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.
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.	The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.
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.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.
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.	The company's formal policies outline the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.

	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	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.	The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.
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.	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.
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.	The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.
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.	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.
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.	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.
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.	The company tests their incident response plan at least annually.

CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	The company tests their incident response plan at least annually.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.
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.	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.
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.	The company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.
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.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.
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.	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.
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.	The company restricts access to migrate changes to production to authorized personnel.
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.	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.
CC9.1	The entity identifies, selects, and develops	The company has Business Continuity and Disaster Recovery Plans in

	risk mitigation activities for risks arising from potential business disruptions.	place that outline communication plans in order to maintain information security continuity in the event of the unavailability of key personnel.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	The company maintains cybersecurity insurance to mitigate the financial impact of business disruptions.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	The company has written agreements in place with vendors and related third-parties. These agreements include confidentiality and privacy commitments applicable to that entity.
P1.1	The entity provides notice to data subjects about its privacy practices to meet the entity's objectives related to privacy. The notice is updated and communicated to data subjects in a timely manner for changes to the entity's privacy practices, including changes in the use of personal information, to meet the entity's objectives related to privacy.	The company has a privacy policy available to customers, employees, and/or relevant third parties who need them before and/or at the time information is collected from the individual.
P1.1	The entity provides notice to data subjects about its privacy practices to meet the entity's objectives related to privacy. The notice is updated and communicated to data subjects in a timely manner for changes to the entity's privacy practices, including changes in the use of personal information, to meet the entity's objectives related to privacy.	The company provides notice when or before personal information is directly collected from the individual and/or used for a new purpose not previously identified in the privacy policies, and within a reasonable time after new information is acquired or any changes to their privacy policies or practices have been approved.
P1.1	The entity provides notice to data subjects about its privacy practices to meet the entity's objectives related to privacy. The notice is updated and communicated to data subjects in a timely manner for changes to the entity's privacy practices, including changes in the use of personal information, to meet the entity's objectives related to privacy.	The company reviews the privacy policy as needed or when changes occur and updates it accordingly to ensure it is consistent with the applicable laws, regulations, and appropriate standards.
P1.1	The entity provides notice to data	The company has established a privacy policy that uses plain and

	subjects about its privacy practices to meet the entity's objectives related to privacy. The notice is updated and communicated to data subjects in a timely manner for changes to the entity's privacy practices, including changes in the use of personal information, to meet the entity's objectives related to privacy.	simple language, is clearly dated, and provides information related to the company's practices and purposes for collecting, processing, handling, and disclosing personal information including: - organizational operating jurisdictions; - an individual's choice and consent for the collection, use, and disclosure of personal information; - an individual's right to access, update or remove personal information; - a process for individuals to exercise their rights; - requirements to only provide the essential information needed for the service; - types or categories of information collected; - purposes for the collection of information; - methods of collection (cookies or other tracking techniques, etc.); - consequences for not providing or withdrawing the essential information; - sources of information (third parties, direct collection, etc.); - types or categories of third parties (sources and disclosures); - the purpose for disclosure of information to third parties.
P1.2	The entity's privacy commitments are communicated to external users, as appropriate, and those commitments and the associated system requirements are communicated to internal users to enable them to carry out their responsibilities.	The company has a privacy policy available to customers, employees, and/or relevant third parties who need them before and/or at the time information is collected from the individual.
P1.2	The entity's privacy commitments are communicated to external users, as appropriate, and those commitments and the associated system requirements are communicated to internal users to enable them to carry out their responsibilities.	The company reviews the privacy policy as needed or when changes occur and updates it accordingly to ensure it is consistent with the applicable laws, regulations, and appropriate standards.
P1.2	The entity's privacy commitments are communicated to external users, as appropriate, and those commitments and the associated system requirements are communicated to internal users to enable them to carry out their responsibilities.	The company has a privacy policy is in place that documents and clearly communicates to individuals the extent of personal information collected, the company's obligations, the individual's rights to access, update, or erase their personal information, and an up-to-date point of contact where individuals can direct their questions, requests or concerns.
P2.1	The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice. Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons, if required. Such consent is obtained only for the intended purpose of the information to meet the entity's objectives related to privacy. The entity's basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented.	The company obtains an individual's consent and preferences at or before the time of collection, maintains documentation in electronic and/or written format, and implements the individuals selected preferences, for information collection, use, and disclosure, in a timely fashion.
P2.1	The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of	Individuals are able to opt-in and/or out of the use of non-essential cookies, and the company does not store, alter, or copy any personal or other information for which consent has not been obtained.

	personal information to the data subjects and the consequences, if any, of each choice. Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons, if required. Such consent is obtained only for the intended purpose of the information to meet the entity's objectives related to privacy. The entity's basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented.	
P2.1	The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice. Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons, if required. Such consent is obtained only for the intended purpose of the information to meet the entity's objectives related to privacy. The entity's basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented.	The company documents new purposes for previously collected information, notifies individuals of the new purpose and use of previously collected information, obtains and records an individual's consent for use or withdrawal, and ensures consented information is being used in accordance with the documented new purpose.
P2.1	The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice. Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons, if required. Such consent is obtained only for the intended purpose of the information to meet the entity's objectives related to privacy. The entity's basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented.	The company has established a privacy policy that uses plain and simple language, is clearly dated, and provides information related to the company's practices and purposes for collecting, processing, handling, and disclosing personal information including: - organizational operating jurisdictions; - an individual's choice and consent for the collection, use, and disclosure of personal information; - an individual's right to access, update or remove personal information; - a process for individuals to exercise their rights; - requirements to only provide the essential information needed for the service; - types or categories of information collected; - purposes for the collection of information; - methods of collection (cookies or other tracking techniques, etc.); - consequences for not providing or withdrawing the essential information; - sources of information (third parties, direct collection, etc.); - types or categories of third parties (sources and disclosures); - the purpose for disclosure of information to third parties.
P2.1	The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each	The company obtains, documents, and retains the explicit consent, in accordance with applicable legal and regulatory requirements, directly from an individual prior to the collection, use, or disclosure of sensitive information. Consent may be obtained through the use of either a check box, signed form.

	choice. Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons, if required. Such consent is obtained only for the intended purpose of the information to meet the entity's objectives related to privacy. The entity's basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented.	
P3.1	Personal information is collected consistent with the entity's objectives related to privacy.	The company's management reviews and approves the sources of personal information, other than the individual data subject (third-parties), to ensure that sources are reliable and that the information obtained by the third-parties has been collected in a fair and lawful manner.
P3.1	Personal information is collected consistent with the entity's objectives related to privacy.	The company reviews policies and procedures as needed or when changes occur and updates them accordingly to ensure that personal information collected is: - identified as either essential or optional; - performed with consent (implicit or explicit) in accordance with legal and regulatory requirements; and - used in alignment with and limited to the purposes identified in the privacy notice.
P3.1	Personal information is collected consistent with the entity's objectives related to privacy.	The company provides notice when or before personal information is directly collected from the individual and/or used for a new purpose not previously identified in the privacy policies, and within a reasonable time after new information is acquired or any changes to their privacy policies or practices have been approved.
P3.1	Personal information is collected consistent with the entity's objectives related to privacy.	The company's management and/or legal counsel reviews and approves the methods for the collection of personal information prior to implementation to ensure that information is obtained in a fair and lawful manner.
P3.2	For information requiring explicit consent, the entity communicates the need for such consent, as well as the consequences of a failure to provide consent for the request for personal information, and obtains the consent prior to the collection of the information to meet the entity's objectives related to privacy.	The company obtains, documents, and retains the explicit consent, in accordance with applicable legal and regulatory requirements, directly from an individual prior to the collection, use, or disclosure of sensitive information. Consent may be obtained through the use of either a check box, signed form.
P4.1	The entity limits the use of personal information to the purposes identified in the entity's objectives related to privacy.	The company reviews policies and procedures as needed or when changes occur and updates them accordingly to ensure that personal information collected is: - identified as either essential or optional; - performed with consent (implicit or explicit) in accordance with legal and regulatory requirements; and - used in alignment with and limited to the purposes identified in the privacy notice.
P4.2	The entity retains personal information consistent with the entity's objectives related to privacy.	The company's retention requirements are documented, and personal information is retained, as required, for business purposes, including to fulfill the purposes related to its collection, and/or by applicable laws or regulations.

P4.2	The entity retains personal information consistent with the entity's objectives related to privacy.	The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.
P4.3	The entity securely disposes of personal information to meet the entity's objectives related to privacy.	The company has processes and procedures in place to capture, log and verify requests, inquires, complaints, or disputes related to the individual's privacy rights of access, review, modification, and/or deletion of personal information. Access requests for personal information are logged within the company's designated tracking system for historical and audit purposes.
P4.3	The entity securely disposes of personal information to meet the entity's objectives related to privacy.	The company securely disposes of personal information in accordance with documented policies and procedures. Personal information is either anonymized, securely erased and/or destroyed when no longer required.
P5.1	The entity grants identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, provides physical or electronic copies of that information to data subjects to meet the entity's objectives related to privacy. If access is denied, data subjects are informed of the denial and reason for such denial, as required, to meet the entity's objectives related to privacy.	The company has established a privacy policy that uses plain and simple language, is clearly dated, and provides information related to the company's practices and purposes for collecting, processing, handling, and disclosing personal information including: - organizational operating jurisdictions; - an individual's choice and consent for the collection, use, and disclosure of personal information; - an individual's right to access, update or remove personal information; - a process for individuals to exercise their rights; - requirements to only provide the essential information needed for the service; - types or categories of information collected; - purposes for the collection of information; - methods of collection (cookies or other tracking techniques, etc.); - consequences for not providing or withdrawing the essential information; - sources of information (third parties, direct collection, etc.); - types or categories of third parties (sources and disclosures); - the purpose for disclosure of information to third parties.
P5.1	The entity grants identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, provides physical or electronic copies of that information to data subjects to meet the entity's objectives related to privacy. If access is denied, data subjects are informed of the denial and reason for such denial, as required, to meet the entity's objectives related to privacy.	The company, prior to granting an individual the ability to access and review personal information, authenticates the individuals or their authorized representative's identity, with an appropriate level of assurance, and verifies such access is not prohibited by law.
P5.1	The entity grants identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, provides physical or electronic copies of that information to data subjects to meet the entity's objectives related to privacy. If access is denied, data subjects are informed of the denial and reason for such denial, as required, to meet the entity's objectives related to privacy.	The company has a privacy policy is in place that documents and clearly communicates to individuals the extent of personal information collected, the company's obligations, the individual's rights to access, update, or erase their personal information, and an up-to-date point of contact where individuals can direct their questions, requests or concerns.
P5.2	The entity corrects, amends, or appends personal information based on	The company has a privacy policy is in place that documents and clearly communicates to individuals the extent of personal information

	information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity's objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and reason for such denial to meet the entity's objectives related to privacy.	collected, the company's obligations, the individual's rights to access, update, or erase their personal information, and an up-to-date point of contact where individuals can direct their questions, requests or concerns.
P5.2	The entity corrects, amends, or appends personal information based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity's objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and reason for such denial to meet the entity's objectives related to privacy.	The company communicates corrections or erasures of an individual's personal information to authorized users and relevant third parties to whom the personal information has been shared or transferred.
P6.1	The entity discloses personal information to third parties with the explicit consent of data subjects, and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy.	The company has established, maintains, and reviews documentation on the nature, extent, and purpose of personal information collected, processed, stored, and/or disclosed to third parties.
P6.1	The entity discloses personal information to third parties with the explicit consent of data subjects, and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy.	The company has written agreements in place with vendors and related third-parties. These agreements include confidentiality and privacy commitments applicable to that entity.
P6.1	The entity discloses personal information to third parties with the explicit consent of data subjects, and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy.	The company has personal information that is disclosed for legal purposes logged, tracked, and maintained in the company's designated tracking system for historical and audit purposes.
P6.1	The entity discloses personal information to third parties with the explicit consent of data subjects, and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy.	The company documents new purposes for previously collected information, notifies individuals of the new purpose and use of previously collected information, obtains and records an individual's consent for use or withdrawal, and ensures consented information is being used in accordance with the documented new purpose.
P6.1	The entity discloses personal information to third parties with the explicit consent of data subjects, and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy.	The company has established a privacy policy that uses plain and simple language, is clearly dated, and provides information related to the company's practices and purposes for collecting, processing, handling, and disclosing personal information including: - organizational operating jurisdictions; - an individual's choice and consent for the collection, use, and disclosure of personal information; - an individual's right to access, update or remove personal information; - a process for individuals to exercise their rights; - requirements to only provide the essential information needed for the service; - types or categories of information collected; - purposes for the collection of information; - methods of collection (cookies or other tracking techniques, etc.); - consequences for not providing or withdrawing the essential information; - sources of information (third parties, direct collection, etc.); - types or categories of third parties (sources and disclosures); -

		the purpose for disclosure of information to third parties.
P6.1	The entity discloses personal information to third parties with the explicit consent of data subjects, and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy.	The company obtains an individual's consent and preferences at or before the time of collection, maintains documentation in electronic and/or written format, and implements the individuals selected preferences, for information collection, use, and disclosure, in a timely fashion.
P6.1	The entity discloses personal information to third parties with the explicit consent of data subjects, and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy.	The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.
P6.2	The entity creates and retains a complete, accurate, and timely record of authorized disclosures of personal information to meet the entity's objectives related to privacy.	The company has established, maintains, and reviews documentation on the nature, extent, and purpose of personal information collected, processed, stored, and/or disclosed to third parties.
P6.3	The entity creates and retains a complete, accurate, and timely record of detected or reported unauthorized disclosures (including breaches) of personal information to meet the entity's objectives related to privacy.	The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.
P6.3	The entity creates and retains a complete, accurate, and timely record of detected or reported unauthorized disclosures (including breaches) of personal information to meet the entity's objectives related to privacy.	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.
P6.4	The entity obtains privacy commitments from vendors and other third parties who have access to personal information to meet the entity's objectives related to privacy. The entity assesses those parties' compliance on a periodic and as-needed basis and takes corrective action, if necessary.	The company has written agreements in place with vendors and related third-parties. These agreements include confidentiality and privacy commitments applicable to that entity.
P6.4	The entity obtains privacy commitments from vendors and other third parties who have access to personal information to meet the entity's objectives related to privacy. The entity assesses those parties' compliance on a periodic and as-needed basis and takes corrective action, if necessary.	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.
P6.4	The entity obtains privacy commitments from vendors and other third parties who have access to personal information to meet the entity's objectives related to privacy. The entity assesses those parties' compliance on a periodic and as-needed basis and takes corrective action,	The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.

	if necessary.	
P6.4	The entity obtains privacy commitments from vendors and other third parties who have access to personal information to meet the entity's objectives related to privacy. The entity assesses those parties' compliance on a periodic and as-needed basis and takes corrective action, if necessary.	The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.
P6.5	The entity obtains commitments from vendors and other third parties with access to personal information to notify the entity in the event of actual or suspected unauthorized disclosures of personal information. Such notifications are reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's objectives related to privacy.	The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.
P6.5	The entity obtains commitments from vendors and other third parties with access to personal information to notify the entity in the event of actual or suspected unauthorized disclosures of personal information. Such notifications are reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's objectives related to privacy.	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.
P6.5	The entity obtains commitments from vendors and other third parties with access to personal information to notify the entity in the event of actual or suspected unauthorized disclosures of personal information. Such notifications are reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's objectives related to privacy.	The company has written agreements in place with vendors and related third-parties. These agreements include confidentiality and privacy commitments applicable to that entity.
P6.6	The entity provides notification of breaches and incidents to affected data subjects, regulators, and others to meet the entity's objectives related to privacy.	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.
P6.6	The entity provides notification of breaches and incidents to affected data subjects, regulators, and others to meet the entity's objectives related to privacy.	The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.
P6.7	The entity provides data subjects with an accounting of the personal information held and disclosure of the data subjects' personal information, upon the data	The company has established, maintains, and reviews documentation on the nature, extent, and purpose of personal information collected, processed, stored, and/or disclosed to third parties.

	subjects' request, to meet the entity's objectives related to privacy.	
P6.7	The entity provides data subjects with an accounting of the personal information held and disclosure of the data subjects' personal information, upon the data subjects' request, to meet the entity's objectives related to privacy.	The company provides requested information, after verification, in a timely manner in either a portable electronic format or by mail, in accordance with applicable law.
P6.7	The entity provides data subjects with an accounting of the personal information held and disclosure of the data subjects' personal information, upon the data subjects' request, to meet the entity's objectives related to privacy.	The company has processes and procedures in place to capture, log and verify requests, inquires, complaints, or disputes related to the individual's privacy rights of access, review, modification, and/or deletion of personal information. Access requests for personal information are logged within the company's designated tracking system for historical and audit purposes.
P6.7	The entity provides data subjects with an accounting of the personal information held and disclosure of the data subjects' personal information, upon the data subjects' request, to meet the entity's objectives related to privacy.	The company, prior to granting an individual the ability to access and review personal information, authenticates the individuals or their authorized representative's identity, with an appropriate level of assurance, and verifies such access is not prohibited by law.
P7.1	The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet the entity's objectives related to privacy.	Individuals, customers, or designated account holders can update their personal information to ensure it is accurate and complete through the use of a customer web portal or by contacting the organization using the methods provided in the privacy policy.
P7.1	The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet the entity's objectives related to privacy.	The company has established, maintains, and reviews documentation on the nature, extent, and purpose of personal information collected, processed, stored, and/or disclosed to third parties.
P7.1	The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet the entity's objectives related to privacy.	The company has a privacy policy is in place that documents and clearly communicates to individuals the extent of personal information collected, the company's obligations, the individual's rights to access, update, or erase their personal information, and an up-to-date point of contact where individuals can direct their questions, requests or concerns.
P8.1	The entity implements a process for receiving, addressing, resolving, and communicating the resolution of inquiries, complaints, and disputes from data subjects and others and periodically monitors compliance to meet the entity's objectives related to privacy. Corrections and other necessary actions related to identified deficiencies are made or taken in a timely manner.	The company has established, maintains, and reviews documentation on the nature, extent, and purpose of personal information collected, processed, stored, and/or disclosed to third parties.
P8.1	The entity implements a process for receiving, addressing, resolving, and communicating the resolution of inquiries, complaints, and disputes from data subjects and others and periodically monitors compliance to meet the entity's objectives related to privacy. Corrections	The company has documented processes and procedures in place to ensure that any privacy-related complaints are addressed, and the resolution is documented in the company's designated tracking system and communicated to the individual.

	and other necessary actions related to identified deficiencies are made or taken in a timely manner.	
P8.1	The entity implements a process for receiving, addressing, resolving, and communicating the resolution of inquiries, complaints, and disputes from data subjects and others and periodically monitors compliance to meet the entity's objectives related to privacy. Corrections and other necessary actions related to identified deficiencies are made or taken in a timely manner.	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings. If the company has committed to an SLA for a finding, the corrective action is completed within that SLA.
P8.1	The entity implements a process for receiving, addressing, resolving, and communicating the resolution of inquiries, complaints, and disputes from data subjects and others and periodically monitors compliance to meet the entity's objectives related to privacy. Corrections and other necessary actions related to identified deficiencies are made or taken in a timely manner.	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.
P8.1	The entity implements a process for receiving, addressing, resolving, and communicating the resolution of inquiries, complaints, and disputes from data subjects and others and periodically monitors compliance to meet the entity's objectives related to privacy. Corrections and other necessary actions related to identified deficiencies are made or taken in a timely manner.	The company's executive leadership is briefed by senior management at least annually on the state of the company's cybersecurity and privacy risk. The executive leadership provides feedback and direction to management as needed.
P8.1	The entity implements a process for receiving, addressing, resolving, and communicating the resolution of inquiries, complaints, and disputes from data subjects and others and periodically monitors compliance to meet the entity's objectives related to privacy. Corrections and other necessary actions related to identified deficiencies are made or taken in a timely manner.	The company has a privacy policy is in place that documents and clearly communicates to individuals the extent of personal information collected, the company's obligations, the individual's rights to access, update, or erase their personal information, and an up-to-date point of contact where individuals can direct their questions, requests or concerns.
P8.1	The entity implements a process for receiving, addressing, resolving, and communicating the resolution of inquiries, complaints, and disputes from data subjects and others and periodically monitors compliance to meet the entity's objectives related to privacy. Corrections and other necessary actions related to identified deficiencies are made or taken	The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.

	in a timely manner.	
PI1.1	The entity obtains or generates, uses, and communicates relevant, quality information regarding the objectives related to processing, including definitions of data processed and product and service specifications, to support the use of products and services.	The company provides a description of its products and services to internal and external users.
PI1.1	The entity obtains or generates, uses, and communicates relevant, quality information regarding the objectives related to processing, including definitions of data processed and product and service specifications, to support the use of products and services.	The company's security commitments are communicated to customers in Master Service Agreements (MSA) or Terms of Service (TOS).
PI1.1	The entity obtains or generates, uses, and communicates relevant, quality information regarding the objectives related to processing, including definitions of data processed and product and service specifications, to support the use of products and services.	The company provides guidelines and technical support resources relating to system operations to customers.
PI1.2	The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity's objectives.	The company captures system activity, including user activity, in transaction logs.
PI1.2	The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity's objectives.	The company has established password policies with minimum system password requirements. The system validates that requirements are met or provides an error message.
PI1.2	The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity's objectives.	The company's system assesses data inputs for compliance with input requirements. On-screen alerts are generated whenever there are issues with transaction inputs or processing.
PI1.2	The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity's objectives.	The company retains customer transaction data for the life of a customer account. No historic transaction data is purged until the customer account is deleted.
PI1.2	The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity's objectives.	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.
PI1.3	The entity implements policies and procedures over system inputs, including controls over completeness and accuracy,	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and

	to result in products, services, and reporting to meet the entity's objectives.	maintenance of information systems and related technology requirements.
PI1.3	The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity's objectives.	An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.
PI1.3	The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity's objectives.	The company captures system activity, including user activity, in transaction logs.
PI1.3	The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity's objectives.	The company's system assesses data inputs for compliance with input requirements. On-screen alerts are generated whenever there are issues with transaction inputs or processing.
PI1.3	The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity's objectives.	The company has automated transactions to move files and data between different system components. Errors that occur during the creation or transmission of critical data generate an alert to system administrators.
PI1.4	The entity implements policies and procedures to make available or deliver output completely, accurately, and timely in accordance with specifications to meet the entity's objectives.	The company's datastores housing sensitive customer data are encrypted at rest.
PI1.4	The entity implements policies and procedures to make available or deliver output completely, accurately, and timely in accordance with specifications to meet the entity's objectives.	The company's system assesses data inputs for compliance with input requirements. On-screen alerts are generated whenever there are issues with transaction inputs or processing.
PI1.4	The entity implements policies and procedures to make available or deliver output completely, accurately, and timely in accordance with specifications to meet the entity's objectives.	The company has automated transactions to move files and data between different system components. Errors that occur during the creation or transmission of critical data generate an alert to system administrators.
PI1.4	The entity implements policies and procedures to make available or deliver output completely, accurately, and timely in accordance with specifications to meet the entity's objectives.	The company retains customer transaction data for the life of a customer account. No historic transaction data is purged until the customer account is deleted.
PI1.5	The entity implements policies and procedures to store inputs, items in processing, and outputs completely, accurately, and timely in accordance with system specifications to meet the entity's objectives.	The company retains customer transaction data for the life of a customer account. No historic transaction data is purged until the customer account is deleted.
PI1.5	The entity implements policies and	The company restricts privileged access to the production network to

	procedures to store inputs, items in processing, and outputs completely, accurately, and timely in accordance with system specifications to meet the entity's objectives.	authorized users with a business need.
PI1.5	The entity implements policies and procedures to store inputs, items in processing, and outputs completely, accurately, and timely in accordance with system specifications to meet the entity's objectives.	The company ensures that neither customers nor administrators have the ability to modify customer transaction data within the production application.

Signed and Accepted by

Prescient Assurance

Prescient Assurance LLC

Brian Sage

Brian Sage
CEO
Dart Health Technology LLC

Certificate of Completion

Document ID

060a3347-8032-4bb7-a2a2-9244bec96e38

Document Title

Report

Status

Completed

Name of the Company

Dart Health Technology LLC

Audit Trail

Username	Email	Action	IP Address	Date/Time
Noman Ahmed .	norman.ahmed@prescientassurance.com	Report Shared with brian@darthealth.com	10.0.21.207	2025-04-23 11:05:50
Noman Ahmed .	norman.ahmed@prescientassurance.com	Report Shared with jim@darthealth.com	10.0.21.207	2025-04-23 11:05:50
Brian Sage	brian@darthealth.com	report Signed by Client	169.197.23.68	2025-04-30 14:54:30
Noble Wilson	noble.wilson@prescientsecurity.com	report Signed by Admin	106.222.202.94	2025-05-02 05:37:52

Management Representation Letter

Dart Health Technology

PRESCIENT
ASSURANCE

Prescient Assurance LLC

May 02, 2025

Dart Health Technology LLC
7988 S Trenton St, Centennial CO 80112
+1 720-609-7491
brian@darthealth.com

In connection with your engagement to report on Dart Health Technology LLC's (service organization) System Description as of April 10, 2025 (description) based on the criteria set forth in DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (description criteria) and the suitability of the design of the controls included in the description as of April 10, 2025, to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the trust services criteria relevant to "Security, Availability, Confidentiality, Privacy and Processing Integrity", set forth in TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (applicable trust services criteria), we recognize that obtaining representations from us concerning the information contained in this letter is a significant procedure in enabling you to form an opinion about whether the description presents the system that was designed as of April 10, 2025, in accordance with the description criteria and whether the controls stated in the description were suitably designed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria, if the controls operated effectively as of April 10, 2025.

We confirm, to the best of our knowledge and belief, as of May 2, 2025, the date of your report, the following representations made to you during your examination:

1. We are responsible for the preparation and presentation of the description, including the completeness, accuracy, and method of presentation of the description, in accordance with the description criteria and the suitability of the design of the controls included in the description to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.
2. We also are responsible for our written assertion that accompanies the description of the system, both of which will be provided to you and users of the report. We are responsible for the completeness, accuracy, and method of presentation of the assertion and for having a reasonable basis for it. We reaffirm our assertion attached to the description.
3. We have evaluated the presentation of the description in accordance with the description criteria and the

suitability of the design of the controls stated therein to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria, and all relevant matters have been considered and reflected in our evaluation and in our assertion.

4. We have disclosed to you all known matters that may contradict the presentation of the description or the suitability of the design of the controls stated in the description, or our assertion.
5. We have disclosed to you any communications from regulatory agencies, user entities, or others received through the date of this letter affecting the presentation of the description or the suitability of the design of the controls included in the description.
6. We are responsible for determining the scope of your examination, including identifying the time period covered by the engagement, services that are the subject of the examination, the system providing the services (including boundaries of the system), and risks relevant to business partners who provide intellectual property or services related to the system.
7. We are responsible for selecting the trust services category(ies) and criteria to be included within the scope of our examination and determining that they are appropriate for our purposes. We are responsible for stating the applicable trust services criteria and related controls in the description. For any additional criteria specified by law, regulation, or another party, we are responsible for identifying that party in the description.
8. We are responsible for determining the effect on our service commitments and system requirements of any services provided to the service organization by other organizations and determining whether those entities are subservice organizations. We are also responsible for determining whether we will use the carve-out method or inclusive method to present information about services provided at any subservice organizations in our description.
9. We are responsible for identifying and analyzing the risks that threaten the achievement of our service commitments and system requirements based on the applicable trust services criteria.
10. We are responsible for designing and documenting controls that are suitably designed to provide reasonable assurance that our service commitments and system requirements are achieved based on the applicable trust services criteria.
11. We are responsible for specifying the principal service commitments made to user entities and the system requirements necessary to operate the system and meet commitments to our business partners.
12. We have provided you with the following:
    1. All relevant information and access, as agreed upon in the terms of the engagement, to all information such as records, documentation, service-level agreements, and internal audit or other reports, of which we are aware that is relevant to your examination and our assertion.
    2. Access to additional information you have requested from us for the purpose of the engagement.

13. We believe the effects of uncorrected misstatements (such as discrepancies in the description or deficiencies in the controls described), if any, are immaterial, individually and in the aggregate, to the presentation of the description in accordance with the description criteria or to the suitability of the design of the controls stated therein to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.
14. We have disclosed to you any known events subsequent to the date of the description of the system up to the date of this letter that would have a material effect on the presentation of the description or the suitability of the design of the controls, or our assertion.
15. We have disclosed to you any instances of noncompliance with laws and regulations, fraud, or uncorrected misstatements attributable to the service organization that are not clearly trivial and that may affect one or more user entities, and whether such incidents have been communicated appropriately to affected user entities.
16. We have disclosed to you any actual, suspected, or alleged fraud or noncompliance with laws or regulations that could adversely affect the description of the service organization's system, the suitability of the design of the controls stated therein, or achievement of its service commitments and system requirements.
17. We also have disclosed to you all instances about which we are aware of the following:
    1. Misstatements and omissions in the description.
    2. Instances in which controls have not been suitably designed as described.

18. We have disclosed to you all identified system incidents that resulted in a significant impairment of the

service organization's achievement of its service commitments and system requirements as of April 10, 2025.

19. We have disclosed to you any changes in the controls that are likely to be relevant to report users occurring through the date of this letter.
20. We have disclosed to you the effects of the COVID-19 pandemic on Dart Health Technology LLC, its operations, and technologies used in providing services.
21. We have disclosed to you any communications to customers and business partners about changes in our service level agreements or commitments as a result of the COVID-19 pandemic.
22. We have responded fully to all inquiries made to us by you during the examination.
23. We understand that your report is intended solely for the use and information of management of the service organization and others within the organization, user entities to which we provide services, and other specified parties who have sufficient knowledge and understanding to consider it, along with other information, if any. We intend to distribute your report only to those specified parties.

We understand that your examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and was designed for the purpose of expressing an opinion about whether, in all material respects, the description is presented in accordance with the description criteria and whether the controls stated therein were suitably designed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We also understand that the opinion was based on your examination and that the procedures performed in the examination were limited to those that you considered necessary.

Prescient Assurance

Prescient Assurance LLC

Brian Sage

Brian Sage
CEO
Dart Health Technology LLC