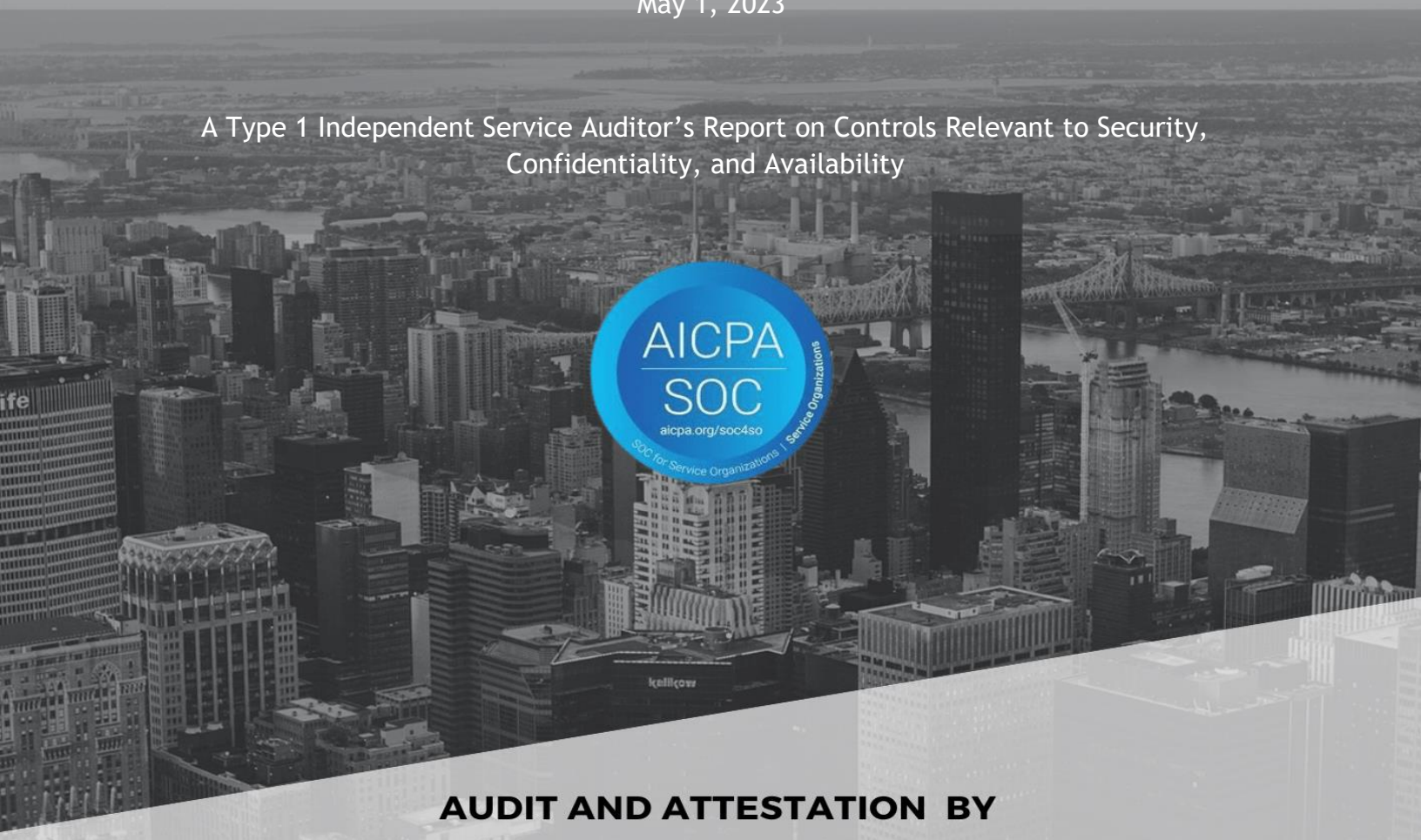
NEXELUS

SOC 2 Type 1 Report

Paradigm Software Technologies, Inc. DBA Nexelus

May 1, 2023

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



AUDIT AND ATTESTATION BY

PRESCIENT ASSURANCE

CPA™

Prescient Assurance LLC.
1100 Market Street Suite 600
Chattanooga, TN 37402

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

Table of Contents

SECTION 1

Management's Assertion

Management's Assertion

We have prepared the accompanying description of Paradigm Software Technologies, Inc. DBA Nexelus's system as of March 31, 2023, 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 Paradigm Software Technologies, Inc. DBA Nexelus's system that may be useful when assessing the risks arising from interactions with Paradigm Software Technologies, Inc. DBA Nexelus's system, particularly information about system controls that Paradigm Software Technologies, Inc. DBA Nexelus has designed and implemented to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Confidentiality and Availability set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

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

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

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

A. The description presents Paradigm Software Technologies, Inc. DBA Nexelus's system that was designed as of March 31, 2023, in accordance with the description criteria.
B. The controls stated in the description were suitably designed as of March 31, 2023, to provide reasonable assurance that Paradigm Software Technologies, Inc. DBA Nexelus'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 Paradigm Software Technologies, Inc. DBA Nexelus's controls as of that date.

DocuSigned by:
Imran Rahman
A3B8661924884F6...

Imran Rahman
EVP
Paradigm Software Technologies, Inc. DBA Nexelus

SECTION 2

Independent Service Auditor's Report

Independent Service Auditor's Report

To: Paradigm Software Technologies, Inc. DBA Nexelus

Scope

We have examined Paradigm Software Technologies, Inc. DBA Nexelus's ("Paradigm Software Technologies, Inc. DBA Nexelus") accompanying description of its system as of March 31, 2023, 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 March 31, 2023, to provide reasonable assurance that Paradigm Software Technologies, Inc. DBA Nexelus's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Confidentiality, and Availability set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

Paradigm Software Technologies, Inc. DBA Nexelus uses a subservice organization for cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Paradigm Software Technologies, Inc. DBA Nexelus, to achieve its service commitments and system requirements based on the applicable trust services criteria. The description presents Paradigm Software Technologies, Inc. DBA Nexelus's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Paradigm Software Technologies, Inc. DBA Nexelus'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 and operating effectively are necessary, along with controls at Paradigm Software Technologies, Inc. DBA Nexelus, to achieve Paradigm Software Technologies, Inc. DBA Nexelus's service commitments and system requirements based on the applicable trust services criteria. The description presents Paradigm Software Technologies, Inc. DBA Nexelus's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Paradigm Software Technologies, Inc. DBA Nexelus'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

Paradigm Software Technologies, Inc. DBA Nexelus is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Paradigm Software Technologies, Inc. DBA Nexelus's service commitments and system requirements were achieved. In Section 1, Paradigm Software Technologies, Inc. DBA Nexelus has provided the accompanying assertion titled "Management's Assertion of Paradigm Software Technologies, Inc. DBA Nexelus" (assertion) about the description and the suitability of design of controls stated therein.

Paradigm Software Technologies, Inc. DBA Nexelus is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of 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 and implemented 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 Paradigm Software Technologies, Inc. DBA Nexelus's system that was designed as of March 31, 2023, in accordance with the description criteria.
B. The controls stated in the description were suitably designed as of March 31, 2023, to provide reasonable assurance that Paradigm Software Technologies, Inc. DBA Nexelus'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 Paradigm Software Technologies, Inc. DBA Nexelus's controls as of that date.

Restricted Use

This report is intended solely for the information and use of Paradigm Software Technologies, Inc. DBA Nexelus, user entities of Paradigm Software Technologies, Inc. DBA Nexelus's system as of March 31, 2023, business partners of Paradigm Software Technologies, Inc. DBA Nexelus 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, and other parties.
3. Internal control and its limitations.
4. Complementary subservice organization controls and complementary user entity 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 LLC

DocuSigned by:
John D Wallace
F5ADFA3509EA450...

John D. Wallace, CPA
Chattanooga, TN
May 1, 2023

SECTION 3

System Description

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

Nexelus is a SaaS company that helps agencies run more efficient, transparent, and profitable operations.

Nexelus manages your project and campaign workflows with improved speed and efficiency, while our dashboards help you stay on top of estimates, costs, time, approval, billing, and profits. What's more, Nexelus is integrated with every major accounting package. Our media platform enables the placement of digital media buys on the most predominantly used Ad networks. Using a single sign-on, users can create and execute digital I/Os, reconcile campaign flights, and produce valuable KPI reports. Nexelus works at the core of agency operations to ensure that clients' advertising dollars are spent according to plan.

It is a B2B SaaS model where our clients subscribe to the product/modules, and it typically is integrated with the ERP/Financial system.

DC 2: The Principal Service Commitments and System Requirements

Paradigm Software Technologies, Inc. DBA Nexelus designs its processes and procedures to meet the objectives of Nexelus manages your project and campaign workflows with improved speed and efficiency, while our dashboards help you stay on top of estimates, costs, time, approval, billing, and profits. What's more, Nexelus is integrated with every major accounting package. Our media platform enables the placement of digital media buys on the most predominantly used Ad networks. Using a single sign-on, users can create and execute digital insertion orders, reconcile campaign flights, and produce valuable KPI reports. Nexelus works at the core of agency operations to ensure that clients' advertising dollars are spent according to plan. Those objectives are based on the service commitments that Paradigm Software Technologies, Inc. DBA Nexelus makes to user entities, the laws and regulations that govern the provision of services, and the financial, operational, and compliance requirements that Paradigm Software Technologies, Inc. DBA Nexelus has established for the services. The platform of Paradigm Software Technologies, Inc. DBA Nexelus is subject to the federal and state privacy and security laws and regulations in the jurisdictions in which Paradigm Software Technologies, Inc. DBA Nexelus operates.

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 offered online. The Privacy Policy and Terms and Conditions can be found at Paradigm Software Technologies, Inc. DBA Nexelus. Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of the platform are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role.
- Maintain commercially reasonable administrative, technical, and organizational measures that are designed to protect customer data processed.
- Encryption of data in transit.
- Maintain security procedures that are consistent with applicable industry standards.

- Document and enforce confidentiality agreements with third parties prior to sharing confidential data.
- Review documentation from third-party providers to help ensure that they are in compliance with security and confidentiality policies.
- Maintain business continuity and disaster recovery programs.
- Restrict system access to authorized personnel only.
- Regularly assess security programs and processes.
- Identification and remediation of security incidents/events.

Paradigm Software Technologies, Inc. DBA Nexelus establishes systems and operational requirements that support the achievement of service commitments, relevant laws and regulations, and other security and privacy requirements. Such requirements are communicated in Paradigm Software Technologies, Inc. DBA Nexelus' Terms and Conditions, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected.

These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the platform.

2.1 Support SLA

System Support: NEXELUS provides system technical support 24 hours per day, 7 days per week, year round. This support is to ensure System Availability and to ensure that the application website is accessible from the Internet. NEXELUS provides a dedicated telephone number to report any such system outage 24 hours per day, 7 days per week, 365 days per year.

Support: NEXELUS provides Tier II level support for COMPANY's point of contact via email (support@nexelus.net) or by telephone at 646-558-1950. The Tier II level of support provides support of up to 2 main points of contact ("POCs") at each customer, who are responsible for supporting all of the other users of the System internally in their organizations. The POCs are responsible for fielding all questions from their end users (Tier I Support). NEXELUS support is intended to provide System subject matter expertise when POCs are unable to resolve a System issue or question (Tier II). Nevertheless, it is expected that POCs have administrator-level training in order to provide adequate support to their end users.

NEXELUS adheres to the specific Acknowledgement Response Time, Resolution Estimate Response Time, and Resolution Times below during business and non-business hours and assigns resolution based on the nature and severity of the issue. Severity is assigned based on discussions between NEXELUS support personnel and the company's point of contact.

Hours	Acknowledgment Response Time
9 am to 6 pm ET Monday through Friday	Within 1-3 hours a support resource response.
Hours outside of 9 am to 6 pm ET and including weekends and holidays and days in which NEXELUS offices are either closed or operating with reduced staff.	24 hours

Resolution Estimate Response: Once the initial acknowledgment response is sent by NEXELUS to COMPANY, NEXELUS begins to look at the issue to determine the severity and the length of time it will take to resolve the issue. The Resolution Estimate Response Timetable below outlines the timeframes that NEXELUS will follow to send the Resolution Estimate Response to COMPANY. The Resolution Estimate Response will contain a severity level, an estimated resolution time frame (in accordance with below Resolution Timetable), and/or that the issue was resolved and details on the resolution. Note that the Resolution Estimate Response timeframes for Level 1 issues apply only to issues submitted to NEXELUS via phone or email. These response times do not apply to COMPANY communication that comes in from any other means.

If the NEXELUS Client Services staff requests additional information or follow-up from COMPANY to resolve the issue and does not receive any response within a reasonable time from COMPANY after three documented written attempts to the email address(es) designated by COMPANY, COMPANY will receive an email notification that the ticket has been closed and will not be further researched by Client Services. COMPANY may resubmit the issue for resolution once such additional information is provided.

Severity Levels

The following characteristics are used to identify the severity of an issue report:

- Work outage
- Number of users affected

Level 1 (High)	Level 2 (Medium)	Level 3 (Low)
Response Time		
Within four (4) business hours	Within two (2) business days	Within five (5) business days
Work Outage		
The application failure causes users to be unable to work or perform some *significant portion* of their job.	The application failure causes users to be unable to perform some *small portion* of their job, but they are still able to complete most	There is no significant work outage. This level may include questions on the application.

	other tasks. This level may include individual data issues.	
Number of Users Affected		
The application failure affects a *large* number of users.	The application failure affects a *smaller* number of users without a workaround or a large number of users with an acceptable and implemented workaround.	The number of users affected is minimal.
Workaround		
There is no acceptable workaround to the issue (i.e., the job cannot be performed in any other way).	There may or may not be an acceptable workaround to the issue.	There is an acceptable and implemented workaround to the issue.

Resolution Timing	
NEXELUS shall use its best efforts to resolve the issues within the following resolution timeframes. NEXELUS will delegate all appropriate resources to troubleshooting and resolving all issues within the estimated response time.	**Level 1 (High)** **NEXELUS shall use its best efforts to provide COMPANY with a fix, workaround, or permanent solution no later than two (2) business days.**
	Level 2 (Medium) **NEXELUS shall use its best efforts to provide COMPANY with a fix, workaround, or permanent solution no later than five (5) business days.**
	Level 3 (Low) **Any low application-related issues will be placed in the product release pipeline as long as NEXELUS deems that the issue is applicable to the core product and not a specific COMPANY request.**

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

3.1 Primary Infrastructure

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Microsoft Azure Amazon AWS	Load Balancers Virtual Network Application Gateway	Allow for the servicing, processing, and directing of network traffic and data.
Microsoft Azure Amazon AWS	IAM	Allow management of user accounts internally.
Microsoft Azure Amazon AWS	Microsoft Defender	We are using the services to monitor our resources i.e. Virtual Machine, Storage, and Network.
Microsoft Azure Amazon AWS	Azure Storage Amazon S3	Cloud-hosted storage solution with encryption capabilities used to store objects created during development and business operations i.e. artifacts, backups, and files.
Microsoft Azure Amazon AWS	Cloud Logging Audit Logs	Used for monitoring network resources, alerting based on preconfigured metric-based alarms, and application logs for all of the services.
Microsoft Azure	Virtual Machine	Cloud-hosted Virtual Machine for Web Application, Storage and AD services.
Amazon AWS	Elastic Container Service	Allows deployment, management, and scale of our docker containers running applications, service and batch processes.

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Amazon AWS	Simple Queue Service Simple Notification Service	These services are used for data processing and notifications.
Amazon AWS	Lambda	AWS Lambda allows us to run code without managing servers. It automatically executes code in response to events and scales to handle any amount of traffic.
Microsoft Azure Amazon AWS	Microsoft SQL Virtual Machine Amazon RDS Aurora MySQL	Used to store user and customer data.
Azure DevOps	Codebase & CICD/Pipeline	Codebase used for versioning, testing, and deployment of changes to the environments.
Azure DevOps	Ticketing System	Tracking issues and project management.
Drata Compliance Automation Platform	Client/Dashboard	Monitors infrastructure for common vulnerabilities and aids in ensuring compliance.

3.2 Primary Software

Primary Software		
Software	**Type**	**Purpose**
C# on Microsoft .Net/.Net Core	Server-Side Logic	Primary Development language and Runtime for Nexelus

JavaScript	Client Side Logic	Primary development language for front-end development
Microsoft SQL Server MySQL	Database	RDBMS used for development of core application
React	UI Logic	Web application framework used to power the APWorks application

3.3 People

Paradigm Software Technologies, Inc. DBA Nexelus has a staff of approximately 25 employees 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.
- Product Development: Product managers and software engineers who design and maintain the platform, including the web interface, the APIs, the databases, and the integrations with data sources. This team designs and implements new functionality, assesses, and remediates any issues or bugs found in the platform, and architects and deploys the underlying cloud infrastructure on which the platform runs. Members of the product team are responsible for peer reviews of code and infrastructure designed and authored within the team.
- Infrastructure: DevOps provides technical assistance to Paradigm Software Technologies, Inc. DBA Nexelus' developers and maintains the cloud infrastructure that the Paradigm Software Technologies, Inc. DBA Nexelus product runs on.
- Security: Employees or outsourced Individuals responsible for providing ongoing security to Paradigm Software Technologies, Inc. DBA Nexelus' assets (people, application, infrastructure, and data).
- IT and Customer Support: Individuals responsible for providing timely resolution of issues and problems.

3.4 Security Processes and Procedures

The company employs a set of procedures to obtain its objectives for network and data security. These procedures are executed by qualified and experienced team members. Procedures are in place in the following areas:

- Paradigm Software Technologies, Inc. DBA Nexelus backend application runs primarily in Azure utilizing the Web Servers (VMs), Storage, and Database services. One module utilizes some AWS services.
- Each platform instance (production, customer test, Quality Assurance "QA", Development) is contained within a separate Application development activity and should be separated from the production and test environments. The extent of separation, logical or physical, is recommended to be appropriate to the risk of the business application or be in line with customer contractual requirements. The level of separation that is necessary between production, development, and test environments should be assessed and controls established to ensure this separation. The infrastructure provides granular access control to all aspects of the

infrastructure. Access from external locations is controlled through configuration and firewall rules. Access to internal components of the platform is only possible via MFA-controlled access. Access is granted on as needed basis to relevant areas.

- User entities access their instance using standard web browsers utilizing Transport Layer Security ("TLS") 1.2 or above for encrypted communications.

- Security Policy Administration: The company's policies concerning various security, availability, processing integrity, confidentiality, and privacy matters are reviewed at least annually by the Security Team.
- Risk Assessment: At least annually the Chief Technology Officer, Development, Security, and IT Teams collaborate on an overall risk assessment for the company and the system.
- Communication: The company opportunistically and continually uses a mixture of DevOps, email, and in-person meeting opportunities for the communication of security policies and procedures. Regular confirmation of this communication is captured in annual attestations from each team member that they have read general internal policies.
- Logical Access: All team members must have unique credentials as well as established authorization to access the Company's information assets. Access to systems and information is restricted based on the responsibilities of the individual and their role.
- Change Management: The company has a Software Development Life Cycle Policy. The policy covers the planning, assignment, development, design, code review, impact considerations, infrastructure assignments, quality assurance, security testing, implementation, and maintenance of both the system software and infrastructure.

3.5 Data

There are several major types of data used by Paradigm Software Technologies, Inc. DBA Nexelus: Configuration Data, Customer Data, and Log Data. Other types of data include: Service data, Data in transit, Data at rest, and Usernames and Passwords.

Principal Data Types	
Data Types	**Protection and Breach Notification during the lifecycle of Data**
Configuration Data: Data used to configure the system	Configuration Data is stored in and includes credentials for accessing web-based software applications, including usernames and passwords; the names of databases, schema, tables, columns, custom objects, and custom fields; and models stored by customers to provide custom analysis views, and routines in the web-based software application.
Customer Data: Data owned by Paradigm Software Technologies, Inc. DBA Nexelus' customers that is	Customer Data is stored. It is encrypted both in-transit and at-rest and is protected with daily backups/versioning controls. Only authorized Paradigm Software Technologies, Inc. DBA Nexelus operators are permitted to access customer data and only for

Principal Data Types	
Data Types	**Protection and Breach Notification during the lifecycle of Data**
copied from edge compute devices to web-based software application	limited time and justifiable business use cases, such as debugging failures or other operational issues.
Log Data: Logs produced by the system.	Log Data is produced by the various services to make it easier for Paradigm Software Technologies, Inc. DBA Nexelus operators to monitor the health of the system and track down any issues. Log data may be stored by vendors that Paradigm Software Technologies, Inc. DBA Nexelus has entrusted for purposes like indexing, monitoring, and trending. Log data is retained for 90 days. More evidence needed. Could not find how long log data is retained for.
Service Data	Service Data is user and account metadata, troubleshooting, accounts receivable and billing, and related information necessary for the company to know in order to service accounts and provide the service.
Data in transit	To protect data in transit between our app and our servers, Paradigm Software Technologies, Inc. DBA Nexelus supports the latest recommended secure cipher suites to encrypt all traffic in transit, including the use of TLS 1.2 protocols, AES256 encryption, and SHA2 signatures.
Data at rest	Data at rest in Paradigm Software Technologies, Inc. DBA Nexelus' production network is encrypted using industry-standard 256-bit Advanced Encryption Standard (AES256), which applies to all types of data at rest within Paradigm Software Technologies, Inc. DBA Nexelus' systems—relational databases, file stores, database backups, etc.
Usernames and Passwords	Paradigm Software Technologies, Inc. DBA Nexelus encrypts customer passwords used to access the Paradigm Software Technologies, Inc. DBA Nexelus platform.

3.6 Third Party Access

No vendors, business partners, and others (third parties) that store, process, and transmit sensitive data or otherwise access a service organization's system.

Third Party Access	
Name of Third Party/ Vendor	**Type of Access and Connectivity to Paradigm Software Technologies, Inc. DBA Nexelus data**
N/A	N/A

3.7 System Boundaries

There are no business processes not within the boundaries of the description of the system in scope.

DC 4: Disclosures about Identified Security Incidents

No significant incidents were recorded during the observation window.

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

Paradigm Software Technologies, Inc. DBA Nexelus uses its Code of Conduct, which is read and signed by all employees as part of the onboarding process, to define and lay out our values. Paradigm Software Technologies, Inc. DBA Nexelus has also instituted a number of technical controls to prevent and disincentivize illegal and unethical actions by Paradigm Software Technologies, Inc. DBA Nexelus employees. These controls include but are not limited to:

- Logging access to resources within Paradigm Software Technologies, Inc. DBA Nexelus' network by user for full traceability.
- Limiting access to confidential information based on clearly defined roles and following the principle of least privilege.
- Rigorously upholding the standards of ethical behavior laid out in our Code of Conduct especially as they pertain to discrimination and harassment of any kind.
- Performing background checks on domestic employees as part of the hiring process.
- Protecting and valuing individuals who bring concerns to the attention of Paradigm Software Technologies, Inc. DBA Nexelus management.

Use of NDAs to prevent the disclosure of confidential information to unauthorized parties.

5.2 Commitment to Competence

Paradigm Software Technologies, Inc. DBA Nexelus' 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 have been implemented in this area are described below:

- Management has considered the competence levels for 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.
- The company periodically provides training to its new hires.

5.3 Management's Philosophy and Operating Style

Paradigm Software Technologies, Inc. DBA Nexelus management team is committed to creating a productive and encouraging work environment as well as providing a secure product to our customers and users. To accomplish this Paradigm Software Technologies, Inc. DBA Nexelus has instituted a number of processes:

- Weekly "all hands" meetings for employees to voice their blocks, successes, and concerns.
- Values conversations with the entire company, sharing the management's philosophy and operating style on as needed basis.
- A rigorous QA program ensuring that development on the Paradigm Software Technologies, Inc. DBA Nexelus application meets industry security standards.
- Meetings are held between managers on a weekly basis to prioritize objectives and tasks.
- Employees are encouraged to reach out to each other when facing obstacles.

5.4 Organizational Structure and Assignment of Authority and Responsibility

During normal operations Paradigm Software Technologies, Inc. DBA Nexelus has a simple organizational structure. Employees report directly to the More evidence needed. Could not find who employees report directly to. who ultimately provide direction, this is depicted in the org chart. Paradigm Software Technologies, Inc. DBA Nexelus has clearly defined job descriptions and as the organization grows, we have in place roles and responsibilities which will allow for the dissemination of managerial responsibilities as necessary. Paradigm Software Technologies, Inc. DBA Nexelus has taken the following steps to achieve this goal:

- Regularly updated organization chart fully accessible by employees.
- Responsibilities of roles are clearly defined in policies and job descriptions.

5.5 Human Resource Policies and Practices

Paradigm Software Technologies, Inc. DBA Nexelus consistently strives to hire and retain the most qualified individuals for the job. To meet this goal, Paradigm Software Technologies, Inc. DBA Nexelus

has in place onboarding requirements and a Human Resource Security Policy which covers employee security training, performance reviews, competency assessments, and the terms of employment.

Specifically, Paradigm Software Technologies, Inc. DBA Nexelus has the following controls in place:

- Performance reviews are conducted at least on an annual basis, and more frequently if needed for promotions, etc.
- Annual employee security training
- New employees are required to sign an employment agreement that covers non-disclosure and confidentiality.
- Clearly defined disciplinary process
- A "New Employee Checklist" which is given to new hires and is fully accessible to all Paradigm Software Technologies, Inc. DBA Nexelus employees

Lastly, Paradigm Software Technologies, Inc. DBA Nexelus recognizes that policies and procedures often need to change to serve the needs of the organization. To accomplish this, all security procedures are reviewed at least annually.

5.6 Security Management

Paradigm Software Technologies, Inc. DBA Nexelus uses an internal security team whose responsibilities fulfill the roles of full-time dedicated System Security Manager (ISSM) and full-time dedicated team members who are responsible for the management of information security throughout the organization.

The team maintains security credentials, performs the technical onboarding/off-boarding work, and updates, maintains, and annually signs to acknowledge their review of the information security policies. They are responsible for enforcing the information security policies, configuring, monitoring, and maintaining preventative, corrective, and detective controls within the Paradigm Software Technologies, Inc. DBA Nexelus environment, and ensuring user awareness training is conducted.
As the information security team maintains security, it monitors known incidents and patches as well as results from recent vulnerability assessments and addresses necessary changes to the policies and procedures. Such changes can include a reclassification of data, a reassessment of risk, changes in incident response plans, and a verification of responsibilities for authorizing and monitoring accesses. Changes are reviewed and communicated during weekly IT maintenance meetings or through system alerts.
During annual security training and awareness programs, management ensures communication of the latest security policies as well as written job descriptions for security management.
Additionally, management is responsible for ensuring business associate agreements are current for third parties and for updating the annual IT risk assessment.

5.7 Security Policies

Paradigm Software Technologies, Inc. DBA Nexelus has adopted the following Security Policies:

5.8 Personnel Security

Paradigm Software Technologies, Inc. DBA Nexelus has several personnel security procedures in place specifically during the onboarding process.

These include:

- Background checks for new domestic employees.
- Employees must read and agree to all security policies.
- Roles within the organization have been clearly defined and are reflected in the organizational chart.
- Employees are granted access/authorization based on their role and in accordance with the principle of least privilege.
- Employees are required to sign an NDA, as part of their employment agreements.
- Upon hire and annually thereafter security awareness training is completed by all Paradigm Software Technologies, Inc. DBA Nexelus employees.
- Employees are directed to report any potential security incidents to the IT Manager.

Violations of Paradigm Software Technologies, Inc. DBA Nexelus security policies have clearly defined repercussions.

5.9 Physical Security and Environmental Controls

Paradigm Software Technologies, Inc. DBA Nexelus is a hybrid between office and remote company with Because of this, physical security policy specifies procedures that are deemed unnecessary. There are specific considerations taken, however, regarding remote work and the security risks inherent specific to companies that are fully remote. These can be found in our Business Continuity and Disaster Recovery plan, and our Information Security Policy.

5.10 Change Management

Paradigm Software Technologies, Inc. DBA Nexelus' change management procedures are detailed in the Software Development Life Cycle Policy. There are five requirements for all changes to the organization, business processes, information processing facilities, and systems that affect information security in Paradigm Software Technologies, Inc. DBA Nexelus' production environment. They are as follows:

- The change must include processes for planning and testing of changes, including remediation measures.
- Documented managerial approval and authorization before proceeding with changes that may have a significant impact on information security, operations, or the production platform.
- Advance communication/warning of changes, including schedules and a description of reasonably anticipated effects, provided to all relevant internal and external stakeholders.
- Documentation of all emergency changes and subsequent review.
- A rollback process for unsuccessful deployments must be in place.

5.11 System Monitoring

Paradigm Software Technologies, Inc. DBA Nexelus uses a combination of services to monitor its network and systems. These include Microsoft Azure Log Analytics, Amazon AWS CloudWatch, the Drata Client, and Application Gateway..

- Microsoft Azure Log Analytics: It is used to collect logs from Virtual Machines, Servers, and other platforms.

- Amazon AWS CloudWatch: It is used to collect logs for the Amazon AWS services such as S3 buckets, RDS, SNS, Lambda, SQS, ECS, and VPC.
- Compliance Automation Platform Client: Compliance Automation Platform allows us to monitor multiple aspects of our attack surface including employee devices (ensuring anti-malware, HDD encryption, etc. are in place), monitoring Azure and AWS resources for potential configuration vulnerabilities, and tracking necessary patches/updates.
- Application Gateway: Provide firewall functionality and redundancy.

Paradigm Software Technologies, Inc. DBA Nexelus is constantly striving to improve our security monitoring capabilities and uses Microsoft Azure and Amazon AWS documentation on best practices to inform the alarming and logging measures we take.

5.12 Incident Management

Paradigm Software Technologies, Inc. DBA Nexelus' incident response procedures are detailed in its Incident Response Plan. Our primary goals will be to investigate, contain any exploitations, eradicate any threats, recover Paradigm Software Technologies, Inc. DBA Nexelus systems, and remediate any vulnerabilities. Throughout this process, thorough documentation will be required as well as a Root cause Analysis report.
Specific steps that Paradigm Software Technologies, Inc. DBA Nexelus will take are:

- The Security Manager will manage the incident response effort.
- All correspondence will take place within the "Incident Management" Paradigm Software Technologies, Inc. DBA Nexelus - Dev Ops platform.
- A recurring Incident Response Meeting will be held at regular intervals until the incident is resolved.
- Paradigm Software Technologies, Inc. DBA Nexelus will inform all necessary parties of the incident without undue delay.

5.13 Data Backup and Recovery

Paradigm Software Technologies, Inc. DBA Nexelus uses to ensure full backup recovery of its database. Paradigm Software Technologies, Inc. DBA Backup and Recovery is specified in relevant policy. Access to Paradigm Software Technologies, Inc. DBA Nexelus databases is heavily restricted using role-based authorization controls.

5.14 System Account Management

Paradigm Software Technologies, Inc. DBA Nexelus' access management procedures are documented in its System Access Control Policy. Paradigm Software Technologies, Inc. DBA Nexelus uses Role-based authorization to control access to its network infrastructure. Paradigm Software Technologies, Inc. DBA Nexelus uses the principle of least privilege to determine the type and level of access to grant users. A number of standards are in place that Paradigm Software Technologies, Inc. DBA Nexelus uses when

granting access to its systems:

- Technical access to Paradigm Software Technologies, Inc. DBA Nexelus networks must be formally documented.

- Background checks will be performed on all employees granted access to Paradigm Software Technologies, Inc. DBA Nexelus networks.
- Only authorized Paradigm Software Technologies, Inc. DBA Nexelus employees and third parties working off a signed contract or statement of work, with a business need, shall be granted access to the Paradigm Software Technologies, Inc. DBA Nexelus production network.

With regards to access provisioning, Paradigm Software Technologies, Inc. DBA Nexelus uses the following controls:

- New employees and/or contractors are not to be granted access to any Paradigm Software Technologies, Inc. DBA Nexelus production systems until after they have completed all HR onboarding tasks, which includes receiving and passing a background check (as applicable), review and signing of all company policies, signing of Paradigm Software Technologies, Inc. DBA Nexelus' NDA, and completion of cybersecurity awareness training.
- Access is restricted to only what is necessary to perform job duties.
- No access may be granted earlier than the official employee start date.
- Access requests and rights modifications shall be documented in an access request ticket or email. No permissions shall be granted without approval from the system/data owner or management.
- Records of all permission and privilege changes shall be maintained for no less than one year.
- Access rights of users must be removed promptly within 48 hours of notification being given to the IT Manager.
- If current access rights are no longer needed due to transfer or change of role, termination of those rights must be performed promptly within 48 hours of notification being given to the IT Manager.

5.15 Risk Management Program

5.15.1 Data Classification

Paradigm Software Technologies, Inc. DBA Nexelus has four classifications for the data it uses, processes, and produces. The classifications are:

- Restricted
- Confidential
- Internal Use
- Public

Restricted Data

- Highly sensitive information

- Level of protection is dictated externally by legal and/or contractual requirements.
- Must be limited to only authorized employees, contractors, and business partners with a specific business need

Confidential Data

- Sensitive information
- Level of protection is dictated internally by Nexelus.
- Must be limited to only authorized employees, contractors, and business partners with a specific business need

Internal Use Data

- Non-sensitive Information
- Originating within or owned by Nexelus or entrusted to it by others.
- May be shared with authorized employees, contractors, and business partners who have a business need, but may not be released to the public, due to the negative impact it might have on the company's business interests

Public

- Information that has been approved for release to the general public

5.15.2 Risk Management Responsibilities

Paradigm Software Technologies, Inc. DBA Nexelus' Risk Assessment Policy details the primary responsibilities.

Role	Responsibility
CTO	Ultimately responsible party for the acceptance and/or treatment of any risks to the organization.
Head of Development/Engineering	Can approve the avoidance, remediation, transference, or acceptance of any risk cited in the Risk Register. This person shall be responsible for communicating risks to top management and the board and adopting risk treatments in accordance with executive direction.
Security Officer	Shall be responsible for adherence to the Risk Management Policy.

- Identification of risks
- Assessment of their potential impact
- Paradigm Software Technologies, Inc. DBA Nexelus' risk treatment towards the risk

Identification of risks involves categorization and investigation. Examples of categories used are

- Technical
- Legal
- Human Resources
- Information Security
- Finance
- Sales

The risk assessment focuses on the likelihood and potential impact of risks to Paradigm Software Technologies, Inc. DBA Nexelus. Likelihood can be assessed as not likely, somewhat likely, or very likely. The impact can be assessed as not impactful, somewhat impactful, and very impactful. These factors together will give an overall risk ranking.

Paradigm Software Technologies, Inc. DBA Nexelus' stance towards any given risk is based on the assessment described above. Where Paradigm Software Technologies, Inc. DBA Nexelus chooses a risk response other than "Accept," it shall develop a Risk Treatment Plan. Paradigm Software Technologies, Inc. DBA Nexelus' stance will fall into one of the following categories:

- Mitigate: Paradigm Software Technologies, Inc. DBA Nexelus may take actions or employ strategies to reduce the risk.
- Accept: Paradigm Software Technologies, Inc. DBA Nexelus may decide to accept and monitor the risk at the present time. This may be necessary for some risks that arise from external events.
- Transfer: Paradigm Software Technologies, Inc. DBA Nexelus may decide to pass the risk on to another party. For example, contractual terms may be agreed to ensure that the risk is not borne by Paradigm Software Technologies, Inc. DBA Nexelus, or insurance may be appropriate for protection against financial loss.
- Eliminate: The risk may be such that Paradigm Software Technologies, Inc. DBA Nexelus could decide to cease the activity or to change it in such a way as to end the risk.

Paradigm Software Technologies, Inc. DBA Nexelus details our key business processes and critical services.

Risk Assessment

Paradigm Software Technologies, Inc. DBA Nexelus' Risk Assessment process takes into account a number of factors each of which contributes to both the likelihood and potential impact of a given risk. These include:

- The criticality of potentially impacted business processes as laid out in the Business Continuity and Disaster Recovery Plan.
- Whether a risk could potentially impact the confidentiality, availability, integrity, or privacy of customer data or PII.
- Potential monetary loss.
- The ability of the risk to impact Paradigm Software Technologies, Inc. DBA Nexelus' business objectives.
- Potential impact to Paradigm Software Technologies, Inc. DBA Nexelus customers or vendors.

Paradigm Software Technologies, Inc. DBA Nexelus uses Risk Treatment Plans for any response to risks other than "Accept."

Risk Analysis

Paradigm Software Technologies, Inc. DBA Nexelus' Risk Analysis Method is as follows:

Service Weightage

Service Weightage	Value
Critical	3
Medium	2
Low	1

Risk Value: Risk value defines probability of occurrence of a risk.

Risk Values		
Probability	**Risk**	**Value**
If occurs once or more in a week	Certain	5
if occurs in 2 to 4 months	Likely	4
If occurs in 4 to 6 months	Possible	3
If occurs once or more in six months	Unlikely	4
If occurs once or more in a year	Rare	1

Risk Impact Value: Risk Impact Value defines how much a risk will impact business if it occurs.

Risk Impact		
Impact Value	**Risk**	**Value**
Business Operations are affected for more than client SLA	Critical	4
Business Operations are affected within limits defined with client SLA	High	3
Disruption in operational or business operations within accepted limits of SLA	Medium	2
Disruption in service(s) but have no impact in SLA	Low	1

Risk Level: Risk level is a cross product of Service Weightage, Risk Value, and Risk Impact Value. A Risk with Critical and High level will be treated.

Risk Level = **SERVICE VALUE x PROBABILITY x IMPACT**

Risk Level		
Risk Level	**Risk**	**Value**
Greater than 16.0	Critical	4
Greater than 9.0 but less than or equal to 16.0	High	3

Risk Response

In accordance with Paradigm Software Technologies, Inc. DBA Nexelus', risks will be prioritized and mapped according to the descriptions listed above. The following responses to risk should be employed. Where Paradigm Software Technologies, Inc. DBA Nexelus chooses a risk response other than "Accept,"

it shall develop a risk treatment plan.

- Mitigate: Paradigm Software Technologies, Inc. DBA Nexelus may take actions or employ strategies to reduce the risk.
- Accept: Paradigm Software Technologies, Inc. DBA Nexelus may decide to accept and monitor the risk at the present time. This may be necessary for some risks that arise from external events.
- Transfer: Paradigm Software Technologies, Inc. DBA Nexelus may decide to pass the risk on to another party. For example, contractual terms may be agreed to ensure that the risk is not borne by Paradigm Software Technologies, Inc. DBA Nexelus, or insurance may be appropriate for protection against financial loss.
- Eliminate: The risk may be such that Paradigm Software Technologies, Inc. DBA Nexelus could decide to cease the activity or to change it in such a way as to end the risk.

5.15.4 Integration with Risk Assessment

Paradigm Software Technologies, Inc. DBA Nexelus is committed to handling and remediating risks inherent in any commitments, agreements, or responsibilities it may enter into or take on during the operation of the company. Due to the nature of these risks it may be necessary for Paradigm Software Technologies, Inc. DBA Nexelus to develop specialized controls. Paradigm Software Technologies, Inc. DBA Nexelus takes into account all relevant factors; contractual, legal, and regulatory when designing these controls. Paradigm Software Technologies, Inc. DBA Nexelus' Head of Engineering has the final say on the design and implementation of these controls.

In general, Paradigm Software Technologies, Inc. DBA Nexelus' Risk Assessment procedure is still applicable to risks inherent in Paradigm Software Technologies, Inc. DBA Nexelus' commitments and contractual responsibilities should be applied to determining the severity of risks.

5.16 Information and Communications Systems

Paradigm Software Technologies, Inc. DBA Nexelus uses Teams and Dev Ops for restricted internal communications. Paradigm Software Technologies, Inc. DBA Nexelus also uses Teams video conferencing and Office 365 for both internal and external communications.

For workflow, project management, and sharing of internal documents Paradigm Software Technologies, Inc. DBA Nexelus uses MS Project and Dev Ops components.

5.17 Data Communication

All traffic within the network is redirected from HTTP to HTTPS.
Access Control to the production code base is limited via the following controls:

- The production code branch is protected, requiring a merge request and approval before any changes can be made. This also protects the branch from being deleted.
- RBAC approach is used for accessing the application code repository.
- All default regular-user accounts have been removed.

5.18 Monitoring Controls

Paradigm Software Technologies, Inc. DBA Nexelus takes a dual approach to continuous monitoring using both internal monitoring and relying on third parties.

5.18.1 Internal Monitoring

Paradigm Software Technologies, Inc. DBA Nexelus has a highly interconnected business process allowing for visibility and insight by management into the operations of each department. Corrective action is initiated through communication such as email or phone calls. Within departments, code reviews and Paradigm Software Technologies, Inc. DBA Nexelus' quality assurance program help ensure internal controls are being followed and implemented.

5.18.2 Third Party Monitoring

Paradigm Software Technologies, Inc. DBA Nexelus contracts a third party to perform annual penetration tests and uses the Drata client to monitor for new vulnerabilities. The process for reporting any deficiencies with regards to Paradigm Software Technologies, Inc. DBA Nexelus policies, and procedures are clearly spelled out in each relevant policy.

DC 6: Complementary User Entity Controls (CUECs)

Paradigm Software Technologies, Inc. DBA Nexelus' 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 Paradigm Software Technologies, Inc. DBA Nexelus' services to be solely achieved by Paradigm Software Technologies, Inc. DBA Nexelus' control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Paradigm Software Technologies, Inc. DBA Nexelus.

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

- User entities are responsible for understanding and complying with their contractual obligations to Paradigm Software Technologies, Inc. DBA Nexelus.
- User entities are responsible for notifying Paradigm Software Technologies, Inc. DBA Nexelus of changes made to technical or administrative contact information.
- User entities are responsible for maintaining their own system(s) of record.
- User entities are responsible for ensuring the supervision, management, and control of the use of Paradigm Software Technologies, Inc. DBA Nexelus services by their personnel.
- User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Paradigm Software Technologies, Inc. DBA Nexelus services.

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

Trust Services Criteria	Complementary User Entity Controls
CC2.1	User entities are responsible for the security and integrity of data housed under user entity control, particularly the data utilized by Paradigm Software Technologies, Inc. DBA Nexelus systems and services.
CC6.2	Determination of personnel who need specific functionality and the granting of such functionality is the responsibility of authorized personnel at the user entity. This includes allowing access to Paradigm Software Technologies, Inc. DBA Nexelus' application keys and API keys for access to the web service API.
CC6.3	Authorized users and their associated access are reviewed periodically.
CC6.6	User entities will ensure protective measures are in place for their data as it traverses from user entity to Paradigm Software Technologies, Inc. DBA Nexelus.
CC6.6	User entities should establish adequate physical security and environmental controls of all devices and access points residing at their operational facilities, including remote employees or at-home agents for which the user entity allows connectivity in order to provide authorized information to Paradigm Software Technologies, Inc. DBA Nexelus.
C1.1	User entities assign responsibility to personnel, and those personnel identify which data used by Paradigm Software Technologies, Inc. DBA Nexelus is to be considered "sensitive".

DC 7: Complementary Subservice Organization Controls (CSOCs)

Paradigm Software Technologies, Inc. DBA Nexelus uses AWS, Azure as a subservice organization for data center colocation services. Paradigm Software Technologies, Inc. DBA Nexelus' controls related to their system cover only a portion of the overall internal control for each user entity of the System. The description does not extend to the services provided by the subservice organization that provides colocation services for IT infrastructure. Section 4 of this report and the description of the system only cover the Trust Services Criteria and related controls of the Company and exclude the related controls of AWS, Azure.

Although the subservice organization has been "carved out" for the purposes of this report, certain Trust Services Criteria are intended to be met by controls at the subservice organization.

Complementary Subservice Organization Controls (CSOCs) are expected to be in place at AWS, Azure related to physical security and environmental protection, as well as backup, recovery, and redundancy controls related to availability. AWS, Azure physical security controls mitigate the risk of fires, power loss, climate, and temperature variabilities. Management of Paradigm Software Technologies, Inc. DBA Nexelus receives and reviews the AWS, Azure SOC 2 report annually. In addition, through its operational activities, Paradigm Software Technologies, Inc. DBA Nexelus management monitors the services performed by AWS, Azure to determine whether operations and controls expected to be implemented at the subservice organization are functioning effectively. Management also has communication with the subservice organization to monitor compliance with the service agreement, stay abreast of changes planned at the hosting facility, and relay any issues or concerns to AWS, Azure management.

It is not feasible for the criteria related to the System to be achieved solely by Paradigm Software Technologies, Inc. DBA Nexelus. Therefore, each user entity's internal control must be evaluated in conjunction with Paradigm Software Technologies, Inc. DBA Nexelus' controls and related tests, and results described in Section 4 of this report, considering the related CSOCs expected to be implemented at the subservice organization as described below.

Criteria	Complementary Subservice Organization Controls
CC6.4	AWS, Azure is responsible for restricting data center access to authorized personnel.
CC6.4	AWS, Azure is responsible for the 24/7 monitoring of data centers by closed circuit cameras and security personnel.
CC7.2 A1.2	AWS, Azure is responsible for the installation of fire suppression and detection, and environmental monitoring systems at the data centers.
CC7.2 A1.2	AWS, Azure is responsible for protecting data centers against disruption in power supply to the processing environment by an uninterruptible power supply.
CC7.2 A1.2	AWS, Azure is responsible for overseeing the regular maintenance of environmental protections at data centers.

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

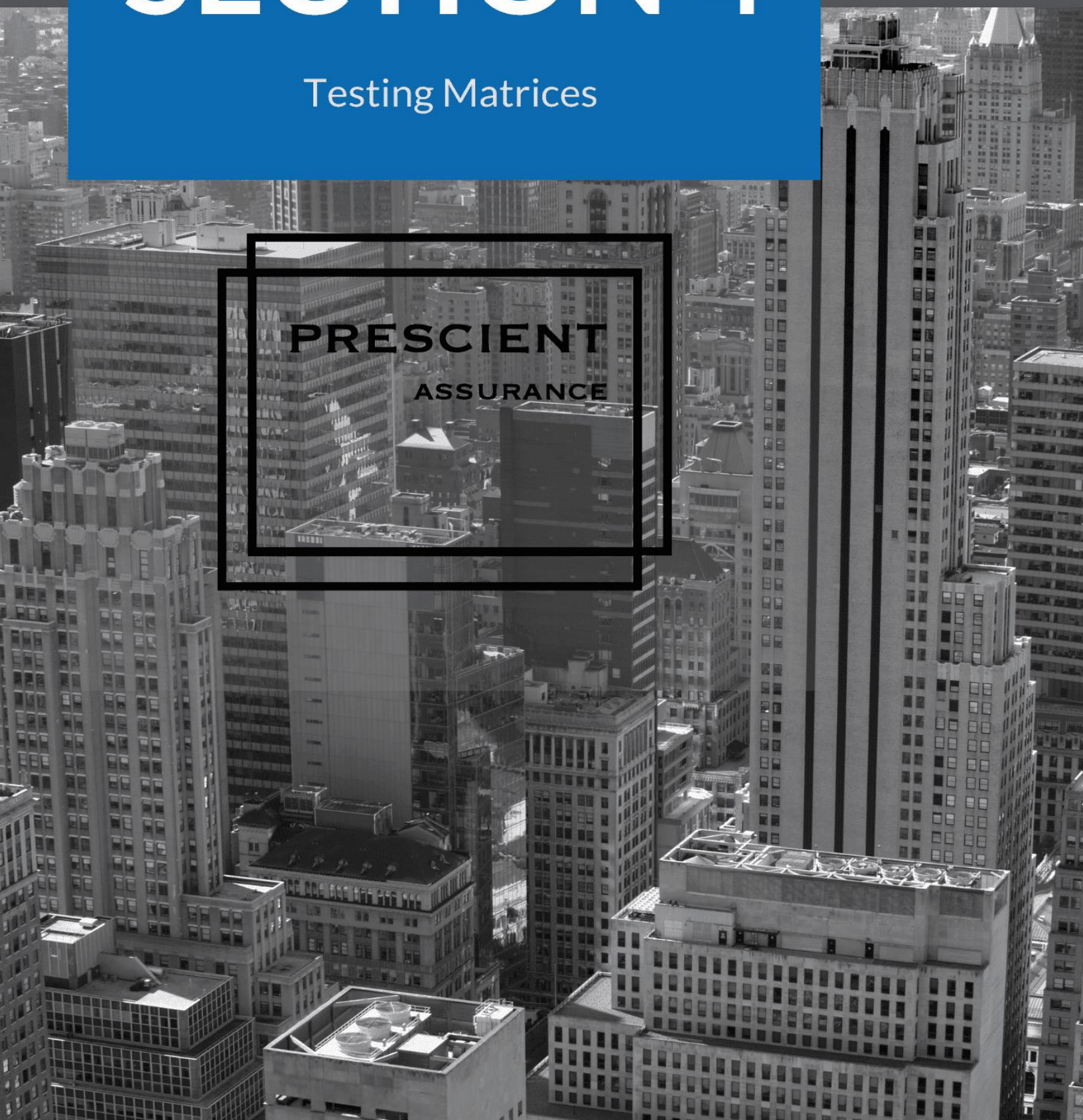
There are no trust services criteria that are not relevant to the system in scope.

DC 9: Disclosures of Significant Changes In Last 1 Year

No significant changes have occurred in the last 1 year.

SECTION 4

Testing Matrices



Tests of Design of Controls and Results of Tests

Scope of Testing

This report on the controls relates to Nexelus provided by Paradigm Software Technologies, Inc. DBA Nexelus. The scope of the testing was restricted to Nexelus, and its boundaries as defined in Section 3.

Prescient Assurance LLC conducted the examination testing as of March 31, 2023.

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

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

Types of Tests Generally Performed

The table below describes the nature of our audit procedures and tests performed to evaluate the design of the controls detailed in the matrices that follow:

Test Types	Description of Tests
Inquiry	Inquired of relevant personnel with the requisite knowledge and experience regarding the performance and application of the related control activity. This included in-person interviews, telephone calls, e-mails, web-based conferences, or a combination of the preceding.
Inspection	Inspected documents and records indicating the performance of the control. This includes, but is not limited to, the following: • Examination / Inspection of source documentation and authorizations to verify transactions processed. • Examination / Inspection of documents or records for evidence of performance, such as the existence of initials or signatures. • Examination / Inspection of systems documentation, configurations, and settings; and • Examination / Inspection of procedural documentation such as operations manuals, flow charts, and job descriptions.

Observation	Observed the implementation, application, or existence of specific controls as represented. Observed the relevant processes or procedures during fieldwork. This included, but was not limited to, witnessing the performance of controls or evidence of control performance with relevant personnel, systems, or locations relevant to the performance of control policies and procedures.
Re-performance	Re-performed the control to verify the design and/or operation of the control activity as performed if applicable.

Reliability of Information Provided by the Service Organization

Observation and inspection procedures were performed related to certain system-generated reports, listings, and queries to assess the accuracy and completeness (reliability) of the information used in the performance of our testing of the controls.

Test Results

The results of each test applied are listed alongside each respective test applied within the Testing Matrices. Test results not deemed as control deviations are noted by the phrase "No exceptions noted." in the test result column of the Testing Matrices.

Any phrase other than this constitutes either a test result that is the result of non-occurrence, a change in the application of the control activity, or a deficiency in the design of the control activity.

Testing deviations identified within the Testing Matrices are not necessarily weaknesses in the total system of controls, as this determination can only be made after consideration of controls in place at user entities and subservice organizations, if applicable, and other factors.

Trust ID	COSO Principle	Control Description	Test Applied by the Service Auditor	Test Results
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.	Paradigm Software Technologies, Inc. DBA Nexelus has implemented tools to monitor Paradigm Software Technologies, Inc. DBA Nexelus's servers and notify appropriate personnel of any events or incidents based on predetermined criteria. Incidents are escalated per policy.	Observed that the CPU server is monitored through AWS and Azure with alerts configured to notify the relevant personnel about any performance issues.	No exceptions noted.
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.	Paradigm Software Technologies, Inc. DBA Nexelus has implemented tools to monitor Paradigm Software Technologies, Inc. DBA Nexelus's databases and notify appropriate personnel of any events or incidents based on predetermined criteria. Incidents are escalated per policy.	Inspected the Data Protection Policy to determine that Nexelus uses Microsoft Azure Monitor to monitor the entire cloud service operation and in case of system failure, the alarm is triggered and key personnel are notified by text, chat, and/or email message in order to take appropriate corrective action.	No exceptions noted.
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.	Paradigm Software Technologies, Inc. DBA Nexelus authorizes designated member(s) with the autonomy to validate, change, and release critical security patches and bug fixes, outside of the standard change management process, when absolutely necessary to ensure security standards and availability of the systems.	Inspected the Software Development Life Cycle Policy, which states that overrides of edit checks, approvals, and changes to confirmed transactions should be appropriately authorized, documented, and reviewed to determine that the company has a documented critical change management procedure.	No exceptions noted.
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.	Paradigm Software Technologies, Inc. DBA Nexelus has implemented tools to monitor Paradigm Software Technologies, Inc. DBA Nexelus's SQL databases and notify appropriate personnel of any events or incidents based on	Inspected the Data Protection Policy which states that the company uses Microsoft Azure Monitor to monitor the entire cloud service operation and if a system failure and alarm is triggered, key personnel are notified in order to take appropriate corrective action.	No exceptions noted.

		predetermined criteria. Incidents are escalated per policy.		
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.	Paradigm Software Technologies, Inc. DBA Nexelus routinely evaluates and provisions new server instances or additional when predefined capacity thresholds are met.	Inspected the Backup Policy to determine that Nexelus stores customer data in a secure production account in Microsoft Azure, using a combination of Microsoft SQL Server databases. By default, Microsoft Azure Cloud Storage provides durable infrastructure to store important data and is designed for the high durability of objects.	No exceptions noted.
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.	Paradigm Software Technologies, Inc. DBA Nexelus has implemented tools to monitor Paradigm Software Technologies, Inc. DBA Nexelus's messaging queues and notify appropriate personnel of any events or incidents based on predetermined criteria. Incidents are escalated per policy.	Inspected the Data Protection Policy to determine that the company uses Microsoft Azure Monitor to monitor the entire cloud service operation and if a system failure or alarm is triggered, key personnel are notified by text, chat, and/or email message to take appropriate corrective action.	No exceptions noted.
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.	Paradigm Software Technologies, Inc. DBA Nexelus uses a load balancer to automatically distribute incoming application traffic across multiple instances and availability zones.	Inspected the AWS resources to determine that the company uses load balancers in AWS to distribute traffic across multiple zones.	No exceptions noted.
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.	Paradigm Software Technologies, Inc. DBA Nexelus monitors its processing capacity and usage on a quarterly basis in order to appropriately manage capacity demand and to enable the implementation of additional capacity to meet availability commitments.	Inspected the Data Protection Policy to determine that the company uses Microsoft Azure Monitor to monitor the entire cloud service operation and if a system failure or alarm is triggered, key personnel are notified by text, chat, and/or email message to take appropriate corrective action.	No exceptions noted.

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.	Paradigm Software Technologies, Inc. DBA Nexelus's cloud infrastructure is monitored through an operational audit system that sends alerts to appropriate personnel	Inspected the Vulnerability Management Policy to determine that the company is required to run technical audit tests as part of the company's operational audit.	No exceptions noted.
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.	Paradigm Software Technologies, Inc. DBA Nexelus has an automated email sent to appropriate personnel when the backup process fails. Failed backups are resolved in a timely manner.	Inspected the Backup Policy to determine that Nexelus has configured Microsoft Azure to perform automatic backups of all customer and system data and any failures trigger an incident by alerting the administrator.	No exceptions noted.
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.	Paradigm Software Technologies, Inc. DBA Nexelus has a defined backup policy that establishes the requirements for backup information, software, and systems.	Inspected the Backup Policy to determine that the company has documented the requirements for establishing backup of data and systems.	No exceptions noted.
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.	Paradigm Software Technologies, Inc. DBA Nexelus utilizes multiple availability zones to replicate production data across different zones.	Inspected the Backup Policy to determine that the company is required to implement an automated process that backs up all data to a separate region in the same country.	No exceptions noted.
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.	Paradigm Software Technologies, Inc. DBA Nexelus has an established Disaster Recovery Plan that outlines roles and responsibilities and detailed procedures for recovery of systems.	Inspected the Disaster Recovery Plan to determine that the disaster recovery procedure and the roles and responsibilities of the CTO for the implementation of recovery procedures have been defined by the company.	No exceptions noted.
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes,	Paradigm Software Technologies, Inc. DBA Nexelus monitors the status of backups on a daily basis and action is taken when the backup process fails.	Inspected the Backup Policy to determine that, by default, data is backed up daily and is monitored and alerted by Microsoft Azure Monitor. Backup failures trigger an incident by alerting the Administrator.	No exceptions noted.

	and recovery infrastructure to meet its 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.	Paradigm Software Technologies, Inc. DBA Nexelus performs backups daily and retains them in accordance with a predefined schedule in the Backup Policy.	Inspected the Backup Policy to determine that the company is required to perform daily data backups using an automated process that backs up all data to a separate region in the same country.	No exceptions noted.
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.	Paradigm Software Technologies, Inc. DBA Nexelus conducts annual BCP/DR tests and documents according to the BCDR Plan.	Inspected the Business Continuity Plan to determine that the company is required to simulate and test the Business Continuity Plan at least once a year. Inspected the Disaster Recovery Plan to determine that the company is required to test the Disaster Recovery Plan at least annually.	No exceptions noted.
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	Paradigm Software Technologies, Inc. DBA Nexelus performs backups daily and retains them in accordance with a predefined schedule in the Backup Policy.	Inspected the Backup Policy to determine that the company is required to perform daily data backups using an automated process that backs up all data to a separate region in the same country.	No exceptions noted.
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	Paradigm Software Technologies, Inc. DBA Nexelus authorizes designated member(s) with the autonomy to validate, change, and release critical security patches and bug fixes, outside of the standard change management process, when absolutely necessary to ensure security standards and availability of the systems.	Inspected the Software Development Life Cycle Policy, which states that overrides of edit checks, approvals, and changes to confirmed transactions should be appropriately authorized, documented, and reviewed to determine that the company has a documented critical change management procedure.	No exceptions noted.
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	Paradigm Software Technologies, Inc. DBA Nexelus conducts annual BCP/DR tests and documents according to the BCDR Plan.	Inspected the Business Continuity Plan to determine that the company is required to simulate and test the Business Continuity Plan at least once a year. Inspected the Disaster Recovery Plan to	No exceptions noted.

			determine that the company is required to test the Disaster Recovery Plan at least annually.	
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	Paradigm Software Technologies, Inc. DBA Nexelus tests the integrity and completeness of back-up information on an annual basis.	Inspected the Backup Policy to determine that Nexelus stores customer data in a secure production account in Microsoft Azure, using a combination of Microsoft SQL Server databases. By default, Microsoft Azure Cloud Storage provides durable infrastructure to store important data and is designed for the high durability of objects.	No exceptions noted.
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	Paradigm Software Technologies, Inc. DBA Nexelus has an established Disaster Recovery Plan that outlines roles and responsibilities and detailed procedures for recovery of systems.	Inspected the Disaster Recovery Plan to determine that the disaster recovery procedure and the roles and responsibilities of the CTO for the implementation of recovery procedures have been defined by the company.	No exceptions noted.
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	Paradigm Software Technologies, Inc. DBA Nexelus has a clean desk policy in place to ensure that documents containing sensitive data are not in public areas or laying on unattended employee work areas	Inspected the Information Security Policy to determine that the company requires users to lock all sensitive data securely at the end of the workday, lock their computers when not in use, secure all computing devices, avoid leaving keys unattended, avoid leaving sensitive documents on their desks, and shred all sensitive documents before disposal.	No exceptions noted.
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	Storage buckets that contain customer data are versioned.	Observed that the storage buckets are versioned on AWS and Azure.	No exceptions noted.
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	Username and password (password standard implemented) or SSO required to authenticate into application, MFA optional for external users, and MFA required for employee users.	Inspected the Password Policy to determine that the company requires users to grant access to an application through a single-sign-on (SSO) provider, and requires MFA to be enabled for all systems.	No exceptions noted.
C1.1	The entity identifies and maintains confidential information to meet the entity's	Paradigm Software Technologies, Inc. DBA Nexelus ensures that all connections to its web	Inspected the Data Protection Policy to determine that the company requires all Internet and intranet connections to be encrypted and authenticated using a	No exceptions noted.

	objectives related to confidentiality.	application from its users are encrypted.	strong protocol, key exchange, and cipher.	
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	Appropriate levels of access to infrastructure and code review tools are granted to new employees within one week of their start date.	Inspected the System Access Control Policy to determine that the company requires the Security Officer to grant access to the infrastructure and code review tools upon satisfaction that the access privileges requested are in line with the user's job requirements.	No exceptions noted.
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	Paradigm Software Technologies, Inc. DBA Nexelus has established formal guidelines for passwords to govern the management and use of authentication mechanisms.	Inspected the Password Policy to determine that formal guidelines and requirements regarding password length and complexity have been established by the management.	No exceptions noted.
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	Paradigm Software Technologies, Inc. DBA Nexelus's new hire contracts include a non-disclosure agreement (NDA)	Inspected the Data Protection Policy to determine that Nexelus uses confidentiality or non-disclosure agreements to protect confidential information using legally enforceable terms and these agreements are applicable to both internal and external parties.	No exceptions noted.
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	Paradigm Software Technologies, Inc. DBA Nexelus maintains an accurate network diagram that is accessible to the engineering team and is reviewed by management on an annual basis.	Inspected the Asset Management Policy to determine that the company is required to maintain a network diagram and provide it to all appropriate service personnel.	No exceptions noted.
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	Paradigm Software Technologies, Inc. DBA Nexelus's customer data is segregated from the data of other customers	Inspected the Data Protection Policy to determine that the company requires customer data to be logically separated at the database level using a unique identifier for the customer.	No exceptions noted.
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	Paradigm Software Technologies, Inc. DBA Nexelus requires two-factor authentication to access sensitive systems and applications in the form of user ID, password, OTP and/or certificate.	Inspected the Password Policy to determine that MFA is required to be enabled for all systems that provide the option for Multi-Factor Authentication (MFA).	No exceptions noted.

C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	Paradigm Software Technologies, Inc. DBA Nexelus allows for external users to implement multi-factor authentication on their accounts in order to require two forms of authentication prior to authentication	Inspected the Password Policy to determine that the company requires MFA to be enabled for any and all systems that provide the option for Multi-Factor Authentication (MFA).	No exceptions noted.
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	Paradigm Software Technologies, Inc. DBA Nexelus has established a data classification policy in order to identify the types of confidential information possessed by the entity and types of protection that are required.	Inspected the Data Classification Policy, which classifies data as restricted, internal, and public to determine that a data classification policy is in place to identify the types of confidential information possessed by the entity and the types of protection required.	No exceptions noted.
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	Role-based security is in place for internal and external users, including super admin users.	Inspected the System Access Control Policy to determine that the company requires users to be granted access to company systems and applications based on the principle of least privilege and Role-Based Access Control (RBAC).	No exceptions noted.
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	Users can only access the production system remotely through the use of encrypted communication systems.	Inspected the Data Classification Policy to determine that the company allows remote access to restricted data on its production systems through VPN and 2FA only.	No exceptions noted.
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	Paradigm Software Technologies, Inc. DBA Nexelus establishes written policies related to retention periods for the confidential information it maintains.	Inspected the Data Retention Policy to determine that customer data is required to be retained for as long as the account is in an active state and expired account data will be retained for 30 Days.	No exceptions noted.
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	Paradigm Software Technologies, Inc. DBA Nexelus uses test data within test environments.	Inspected the Software Development Life Cycle Policy to determine that the company prohibits production data from being used in the testing environment.	No exceptions noted.
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	Storage buckets that contain customer data are versioned.	Observed that the storage buckets are versioned on AWS and Azure.	No exceptions noted.
C1.2	The entity disposes of confidential information to meet	Paradigm Software Technologies, Inc. DBA Nexelus has formal policies	Inspected the Information Security Policy to determine that procedures for disposal of sensitive data on paper have	No exceptions noted.

	the entity's objectives related to confidentiality.	and procedures in place to guide personnel in the disposal of paper documents containing sensitive data.	been described stating that any sensitive documents must be disposed of in the official shredder bins.	
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	Paradigm Software Technologies, Inc. DBA Nexelus has formal policies and procedures in place to guide personnel in the disposal of hardware containing sensitive data.	Inspected the Data Retention Policy to determine that the requirements and controls/procedures to manage the deletion of customer data have been described. Inspected the Information Security Policy to determine that procedures for the disposal of sensitive data have been described stating that whiteboards containing restricted and/or sensitive information should be erased and the company requires to destroy, delete, erase, or conceal company data, or otherwise making such files or data unavailable or inaccessible to other authorized users.	No exceptions noted.
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	Paradigm Software Technologies, Inc. DBA Nexelus uses a termination checklist to ensure that an employee's system access, including physical access, is removed within a specified timeframe and all organization assets (physical or electronic) are properly returned.	Inspected the System Access Control Policy to determine that the HR Department users and their supervisors are required to notify the Security Officer upon completion or termination of access needs and facilitate completion of the termination checklist.	No exceptions noted.
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	Paradigm Software Technologies, Inc. DBA Nexelus deletes customer data within 30 days of the customer terminating its contract.	Inspected the Data Retention Policy to determine that the company is required to retain expired customer account data for 30 days. After this period, the account and related data will be removed.	No exceptions noted.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	Paradigm Software Technologies, Inc. DBA Nexelus's new hires are required to pass a background check as a condition of their employment.	Inspected the Acceptable Use Policy to determine that the company is required to conduct background verification checks for all employees in accordance with the relevant laws, regulations, and ethics.	No exceptions noted.

CC1.1	The entity demonstrates a commitment to integrity and ethical values.	Paradigm Software Technologies, Inc. DBA Nexelus Management has approved security policies, and all employees accept these procedures when hired. Management also ensures that security policies are accessible to all employees and contractors.	Inspected the Information Security Policy to determine that all ISP policies are required to be reviewed, modified, or edited by management annually and accessible to employees. Employees are required to accept the policies upon hire.	No exceptions noted.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	Paradigm Software Technologies, Inc. DBA Nexelus has established a Data Protection Policy and requires all employees to accept it upon hire. Management monitors employees' acceptance of the policy.	Inspected the Data Protection Policy to determine that the data protection processes and implementation guidelines have been documented. Inspected the Information Security Policy to determine that the security policies must be reviewed and signed upon hire and on an annual basis by all employees.	No exceptions noted.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	Paradigm Software Technologies, Inc. DBA Nexelus requires its contractors to read and accept the Code of Conduct, read and accept the Acceptable Use Policy, and pass a background check.	Inspected the Code of Conduct and Acceptable Use Policy to determine that the company requires all contractors to read and accept these policies. Inspected the Acceptable Use Policy to determine that the company requires all contractors to pass a background verification check.	No exceptions noted.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	Paradigm Software Technologies, Inc. DBA Nexelus has a formal Code of Conduct approved by management and accessible to all employees. All employees must accept the Code of Conduct upon hire.	Inspected the Code of Conduct to determine that the company requires new employees to sign their acknowledgment of the Code at the time of hiring.	No exceptions noted.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	Paradigm Software Technologies, Inc. DBA Nexelus has policies and procedures in place to establish acceptable use of information assets approved by management, posted on the company wiki, and accessible to all employees.	Inspected the Acceptable Use Policy to determine that the company has outlined the requirements for background checks, agreement signing, adherence to the acceptable use of assets, onboarding and offboarding processes, and safety of computing assets.	No exceptions noted.

		All employees must accept the Acceptable Use Policy upon hire.		
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 of directors or a relevant subcommittee is briefed by senior management at least annually on the state of the company's cybersecurity and privacy risk. The board provides feedback and direction to management as needed.	Observed meeting minutes to determine that the company's board of directors or a relevant subcommittee is briefed by senior management at least annually on the state of the company's cybersecurity and privacy risk. The board provides feedback and direction to management as needed.	No exceptions noted.
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 of directors meets at least annually and maintains formal meeting minutes. The board includes directors that are independent of the company.	Observed meeting minutes to determine that the company's board of directors meets at least annually and maintains formal meeting minutes. The board includes directors that are independent of the company.	No exceptions noted.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Paradigm Software Technologies, Inc. DBA Nexelus conducts a Risk Assessment at least annually.	Inspected the Risk Assessment Policy to determine that the company is required to update the risk assessment report when newly identified risks are identified and reviewed at least annually.	No exceptions noted.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Paradigm Software Technologies, Inc. DBA Nexelus has an assigned security team that is responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines.	Inspected the Information Security Policy to determine that the Network Manager and General Manager are responsible for the development, dissemination, and enforcement of the information security policies. Additionally, the policies are required to be reviewed by a security or compliance committee.	No exceptions noted.
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.	Observed Linkedin profiles to determine that 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.	No exceptions noted.

CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Management reviews security policies on an annual basis.	Inspected the Information Security Policy to determine that senior management and key personnel are required to review the security policies annually.	No exceptions noted.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Paradigm Software Technologies, Inc. DBA Nexelus engages with third-party to conduct vulnerability scans of the production environment at least quarterly. Results are reviewed by management and high-priority findings are tracked to resolution.	Inspected the Vulnerability Management Policy to determine that the company is required to perform vulnerability scans on all production systems at least annually.	No exceptions noted.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Management has established defined roles and responsibilities to oversee implementation of the information security policy across the organization.	Inspected the Information Security Policy to determine that the company has assigned the responsibility of managing and enforcing the information security policies to the Network Manager and General Manager.	No exceptions noted.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Paradigm Software Technologies, Inc. DBA Nexelus engages with third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and high-priority findings are tracked to resolution.	Inspected the Vulnerability Management Policy to determine that the company is required to perform penetration testing is performed regularly by either a certified penetration tester on Nexelus' security team or an independent third party.	No exceptions noted.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Paradigm Software Technologies, Inc. DBA Nexelus has an assigned security team that is responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines.	Inspected the Information Security Policy to determine that the Network Manager and General Manager are responsible for the development, dissemination, and enforcement of the information security policies. Additionally, the policies are required to be reviewed by a security or compliance committee.	No exceptions noted.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate	Paradigm Software Technologies, Inc. DBA Nexelus reviews its organizational structure,	Observed the company's automated compliance platform to determine that Paradigm Software Technologies, Inc. DBA Nexelus reviews its organizational	No exceptions noted.

	authorities and responsibilities in the pursuit of objectives.	reporting lines, authorities, and responsibilities in terms of information security on an annual basis.	structure, reporting lines, authorities, and responsibilities in terms of information security on an annual basis.	
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	All Paradigm Software Technologies, Inc. DBA Nexelus positions have a detailed job description that lists qualifications, such as requisite skills and experience, which candidates must meet in order to be hired by Paradigm Software Technologies, Inc. DBA Nexelus.	Observed Job descriptions to determine that all Paradigm Software Technologies, Inc. DBA Nexelus positions have a detailed job description that lists qualifications, such as requisite skills and experience, which candidates must meet in order to be hired by Paradigm Software Technologies, Inc. DBA Nexelus.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Paradigm Software Technologies, Inc. DBA Nexelus has a defined vendor management policy that establishes requirements of ensuring third-party entities meet the organization's data preservation and protection requirements.	Inspected the Vendor Management Policy to determine that the company requires its vendors to maintain the integrity, security, and privacy of the company's data.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Paradigm Software Technologies, Inc. DBA Nexelus evaluates the performance of all employees through a formal, annual performance evaluation.	Observed performance evaluations to determine that Paradigm Software Technologies, Inc. DBA Nexelus evaluates the performance of all employees through a formal, annual performance evaluation.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Paradigm Software Technologies, Inc. DBA Nexelus has established training programs for privacy and information security to help employees understand their obligations and responsibilities to comply with Paradigm Software Technologies, Inc. DBA Nexelus's security policies and procedures, including the identification and reporting of incidents. All full-time employees are	Inspected the Information Security Policy to determine that the company requires new employees to complete information security awareness training upon hire and annually after that.	No exceptions noted.

		required to complete the training upon hire and annually thereafter.		
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Paradigm Software Technologies, Inc. DBA Nexelus's new hires are required to pass a background check as a condition of their employment.	Inspected the Acceptable Use Policy to determine that the company is required to conduct background verification checks for all employees in accordance with the relevant laws, regulations, and ethics.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Paradigm Software Technologies, Inc. DBA Nexelus requires its contractors to read and accept the Code of Conduct, read and accept the Acceptable Use Policy, and pass a background check.	Inspected the Code of Conduct and Acceptable Use Policy to determine that the company requires all contractors to read and accept these policies. Inspected the Acceptable Use Policy to determine that the company requires all contractors to pass a background verification check.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Paradigm Software Technologies, Inc. DBA Nexelus's new hires and/or internal transfers are required to go through an official recruiting process during which their qualifications and experience are screened to ensure that they are competent and capable of fulfilling their responsibilities.	Observed the recruitment process to determine that Paradigm Software Technologies, Inc. DBA Nexelus's new hires and/or internal transfers are required to go through an official recruiting process during which their qualifications and experience are screened to ensure that they are competent and capable of fulfilling their responsibilities.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Paradigm Software Technologies, Inc. DBA Nexelus has a formal Code of Conduct approved by management and accessible to all employees. All employees must accept the Code of Conduct upon hire.	Inspected the Code of Conduct to determine that the company requires new employees to sign their acknowledgment of the Code at the time of hiring.	No exceptions noted.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Paradigm Software Technologies, Inc. DBA Nexelus has policies and procedures in place to establish acceptable use of information assets approved by management, posted on	Inspected the Acceptable Use Policy to determine that the company has outlined the requirements for background checks, agreement signing, adherence to the acceptable use of assets, onboarding and offboarding	No exceptions noted.

		the company wiki, and accessible to all employees. All employees must accept the Acceptable Use Policy upon hire.	processes, and safety of computing assets.	
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Paradigm Software Technologies, Inc. DBA Nexelus has established training programs for privacy and information security to help employees understand their obligations and responsibilities to comply with Paradigm Software Technologies, Inc. DBA Nexelus's security policies and procedures, including the identification and reporting of incidents. All full-time employees are required to complete the training upon hire and annually thereafter.	Inspected the Information Security Policy to determine that the company requires new employees to complete information security awareness training upon hire and annually after that.	No exceptions noted.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Paradigm Software Technologies, Inc. DBA Nexelus has a formal Code of Conduct approved by management and accessible to all employees. All employees must accept the Code of Conduct upon hire.	Inspected the Code of Conduct to determine that the company requires new employees to sign their acknowledgment of the Code at the time of hiring.	No exceptions noted.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Paradigm Software Technologies, Inc. DBA Nexelus evaluates the performance of all employees through a formal, annual performance evaluation.	Observed performance evaluations to determine that Paradigm Software Technologies, Inc. DBA Nexelus evaluates the performance of all employees through a formal, annual performance evaluation.	No exceptions noted.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Paradigm Software Technologies, Inc. DBA Nexelus conducts continuous monitoring of security controls using Drata, and addresses issues in a timely manner.	Inspected the Information Security Policy, which states that monitoring activities may be conducted on an ongoing basis or whenever deemed necessary to determine that the company conducts continuous monitoring of security controls using Drata, and addresses issues in a timely manner.	No exceptions noted.

CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Paradigm Software Technologies, Inc. DBA Nexelus has a defined policy that establishes requirements for the proper management and tracking of organizational assets.	Inspected the Asset Management Policy to determine that the company has outlined the procedures for properly managing its physical and digital assets according to the best practices and hardening standards.	No exceptions noted.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Paradigm Software Technologies, Inc. DBA Nexelus identifies, inventories, classifies, and assigns owners to IT assets.	Inspected the Asset Management Policy to determine that the company has documented the standards for maintaining an asset inventory for physical and virtual assets.	No exceptions noted.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Paradigm Software Technologies, Inc. DBA Nexelus maintains an accurate architectural diagram to document system boundaries to support the functioning of internal control.	Inspected the Asset Management Policy to determine that the company maintains an updated network diagram that is accessible to all relevant personnel.	No exceptions noted.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Paradigm Software Technologies, Inc. DBA Nexelus Management has approved all policies that detail how customer data may be made accessible and should be handled. These policies are accessible to all employees and contractors.	Inspected the System Access Control Policy, Asset Management Policy, Data Classification Policy, Data Protection Policy, and Vendor Management Policy to determine that these policies provide guidance on accessing, handling, processing, and securing customer data and are accessible to all employees and contractors.	No exceptions noted.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Paradigm Software Technologies, Inc. DBA Nexelus authorizes access to information resources, including data and the systems that store or process customer data, based on the principle of least privilege.	Inspected the System Access Control Policy to determine that the company requires all access to be regulated by the role-based access control (RBAC) method, based on the principle of least privilege.	No exceptions noted.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Paradigm Software Technologies, Inc. DBA Nexelus conducts a Risk Assessment at least annually.	Inspected the Risk Assessment Policy to determine that the company is required to update the risk assessment report when newly identified risks are identified and reviewed at least annually.	No exceptions noted.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Paradigm Software Technologies, Inc. DBA Nexelus has an established policy and procedures that	Inspected the Encryption Policy to determine that the company has established the cryptographic controls	No exceptions noted.

		governs the use of cryptographic controls.	and procedures for cryptographic key management and protection.	
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Paradigm Software Technologies, Inc. DBA Nexelus ensures that file integrity monitoring (FIM) software is in place to detect whether operating system and application software files have been tampered with.	Inspected the Data Protection Policy to determine that the company must have security monitoring enabled for all production systems including activity and file integrity monitoring, vulnerability scanning, and malware detection, as applicable.	No exceptions noted.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Paradigm Software Technologies, Inc. DBA Nexelus has a defined Information Security Policy that covers policies and procedures to support the functioning of internal control.	Inspected the Information Security Policy to determine that the company has described the procedures for all essential internal control activities, including the responsibilities of the CTO, staff training requirements, use of the Internet, workspace, remote access privileges, teleworking, mobile devices, and a disciplinary process to be followed when any of these procedures are not followed.	No exceptions noted.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Paradigm Software Technologies, Inc. DBA Nexelus 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.	Observed that the company uses Drata to perform self-assessments of internal controls.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Paradigm Software Technologies, Inc. DBA Nexelus has an established Incident Response Plan that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents and annual testing.	Inspected the Incident Response Plan to determine that the process of establishing and executing the incident response plan along with the roles and responsibilities of the ISM and other key personnel has been described for responding to incidents.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal	Paradigm Software Technologies, Inc. DBA Nexelus has established training programs for privacy and information security to	Inspected the Information Security Policy to determine that the company requires new employees to complete information security awareness training upon hire and annually after that.	No exceptions noted.

	control, necessary to support the functioning of internal control.	help employees understand their obligations and responsibilities to comply with Paradigm Software Technologies, Inc. DBA Nexelus's security policies and procedures, including the identification and reporting of incidents. All full-time employees are required to complete the training upon hire and annually thereafter.		
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Paradigm Software Technologies, Inc. DBA Nexelus has policies and procedures in place to establish acceptable use of information assets approved by management, posted on the company wiki, and accessible to all employees. All employees must accept the Acceptable Use Policy upon hire.	Inspected the Acceptable Use Policy to determine that the company has outlined the requirements for background checks, agreement signing, adherence to the acceptable use of assets, onboarding and offboarding processes, and safety of computing assets.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Paradigm Software Technologies, Inc. DBA Nexelus has established a Data Protection Policy and requires all employees to accept it upon hire. Management monitors employees' acceptance of the policy.	Inspected the Data Protection Policy to determine that the data protection processes and implementation guidelines have been documented. Inspected the Information Security Policy to determine that the security policies must be reviewed and signed upon hire and on an annual basis by all employees.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Paradigm Software Technologies, Inc. DBA Nexelus has implemented an Incident Response Plan that includes creating, prioritizing, assigning, and tracking follow-ups to completion and lend support to Business Continuity/Disaster Recovery.	Inspected the Incident Response Plan to determine that the company has defined the incident response process, which requires conducting a post-mortem that includes root cause analysis and documentation of any lessons learned.	No exceptions noted.

CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Paradigm Software Technologies, Inc. DBA Nexelus provides a process to employees for reporting security, confidentiality, integrity, and availability features, incidents, and concerns, and other complaints to company management.	Inspected the Responsible Disclosure Policy to determine that an email address (vulnerability@nexelus.net) has been provided to employees to report vulnerabilities to Nexelus' Product Security Team.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Paradigm Software Technologies, Inc. DBA Nexelus has a formal Code of Conduct approved by management and accessible to all employees. All employees must accept the Code of Conduct upon hire.	Inspected the Code of Conduct to determine that the company requires new employees to sign their acknowledgment of the Code at the time of hiring.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Paradigm Software Technologies, Inc. DBA Nexelus has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company.	Inspected the Incident Response Plan to determine that the company requires the DevOps, HR & Facilities, and Security teams to coordinate in executing a response to identified security threats.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Paradigm Software Technologies, Inc. DBA Nexelus has implemented an Incident Response Plan that includes documenting "Lessons Learned" and "Root Cause Analysis" after incidents and sharing them with the broader engineering team to support Business Continuity/Disaster Recovery.	Inspected the Incident Response Plan to determine that the company requires the Information Security Manager to prepare a root cause report and a "lessons learned" document as part of the incident post-mortem analysis.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The security team communicates important information security events to company management in a timely manner.	Inspected the Incident Response Plan to determine that the company requires users to report any incidents to their immediate managers within 24 hours, and the managers are required to notify the Information Security Manager immediately.	No exceptions noted.

CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Paradigm Software Technologies, Inc. DBA Nexelus conducts continuous monitoring of security controls using Drata, and addresses issues in a timely manner.	Inspected the Information Security Policy, which states that monitoring activities may be conducted on an ongoing basis or whenever deemed necessary to determine that the company conducts continuous monitoring of security controls using Drata, and addresses issues in a timely manner.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Paradigm Software Technologies, Inc. DBA Nexelus Management has approved security policies, and all employees accept these procedures when hired. Management also ensures that security policies are accessible to all employees and contractors.	Inspected the Information Security Policy to determine that all ISP policies are required to be reviewed, modified, or edited by management annually and accessible to employees. Employees are required to accept the policies upon hire.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	Paradigm Software Technologies, Inc. DBA Nexelus has implemented an Incident Response Plan that includes documenting "Lessons Learned" and "Root Cause Analysis" after incidents and sharing them with the broader engineering team to support Business Continuity/Disaster Recovery.	Inspected the Incident Response Plan to determine that the company requires the Information Security Manager to prepare a root cause report and a "lessons learned" document as part of the incident post-mortem analysis.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	Paradigm Software Technologies, Inc. DBA Nexelus has an established Incident Response Plan that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents and annual testing.	Inspected the Incident Response Plan to determine that the process of establishing and executing the incident response plan along with the roles and responsibilities of the ISM and other key personnel has been described for responding to incidents.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	Paradigm Software Technologies, Inc. DBA Nexelus maintains a Terms of Service that is available to all external users and	Observed the SaaS agreement to determine that Paradigm Software Technologies, Inc. DBA Nexelus maintains a Terms of Service that is available to all external users and	No exceptions noted.

		internal employees, and the terms detail the company's security and availability commitments regarding the systems. Client Agreements or Master Service Agreements are in place for when the Terms of Service may not apply.	internal employees, and the terms detail the company's security and availability commitments regarding the systems. Client Agreements or Master Service Agreements are in place for when the Terms of Service may not apply.	
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	Paradigm Software Technologies, Inc. DBA Nexelus has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company.	Inspected the Incident Response Plan to determine that the company requires the DevOps, HR & Facilities, and Security teams to coordinate in executing a response to identified security threats.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	Paradigm Software Technologies, Inc. DBA Nexelus provides a process to external users for reporting security, confidentiality, integrity, and availability failures, incidents, concerns, and other complaints.	Inspected the company's website to determine that Nexelus provides an email address (hello@nexelus.net) and a phone number (646-558-1950 ext.128) for external users to report complaints and other concerns.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	Paradigm Software Technologies, Inc. DBA Nexelus has implemented an Incident Response Plan that includes creating, prioritizing, assigning, and tracking follow-ups to completion and lend support to Business Continuity/Disaster Recovery.	Inspected the Incident Response Plan to determine that the company has defined the incident response process, which requires conducting a post-mortem that includes root cause analysis and documentation of any lessons learned.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	Paradigm Software Technologies, Inc. DBA Nexelus maintains a Privacy Policy that is available to all external users and internal employees, and it details the company's confidentiality and privacy commitments.	Observed the SaaS agreement to determine that Paradigm Software Technologies, Inc. DBA Nexelus maintains a Privacy Policy that is available to all external users and internal employees, and it details the company's confidentiality and privacy commitments.	No exceptions noted.

CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	Paradigm Software Technologies, Inc. DBA Nexelus maintains a directory of its key vendors, including their compliance reports. Critical vendor compliance reports are reviewed annually.	Inspected the Vendor Management Policy to determine that the company may choose to audit IT vendors and partners to ensure compliance with applicable security policies, as well as legal, regulatory, and contractual obligations.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	Paradigm Software Technologies, Inc. DBA Nexelus maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.	Inspected the Vendor Management Policy to determine that the company is required to maintain vendor inventory and vendor contracts that must include confidentiality and privacy commitments.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	Paradigm Software Technologies, Inc. DBA Nexelus's security commitments are communicated to external users, as appropriate.	Observed the SaaS agreement to determine that Paradigm Software Technologies, Inc. DBA Nexelus's security commitments are communicated to external users, as appropriate.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	Paradigm Software Technologies, Inc. DBA Nexelus communicates system changes to customers that may affect security, availability, processing integrity, or confidentiality.	Observed release notes to determine that Paradigm Software Technologies, Inc. DBA Nexelus communicates system changes to customers that may affect security, availability, processing integrity, or confidentiality.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	Paradigm Software Technologies, Inc. DBA Nexelus has a defined vendor management policy that establishes requirements of ensuring third-party entities meet the organization's data preservation and protection requirements.	Inspected the Vendor Management Policy to determine that the company requires its vendors to maintain the integrity, security, and privacy of the company's data.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	Paradigm Software Technologies, Inc. DBA Nexelus tracks security deficiencies through internal tools and closes them within an SLA that management has pre-specified.	Inspected the Vulnerability Management Policy to determine that the company is required to raise a Microsoft DevOps ticket for each incident and use it to track security incidents to remediation within an SLA based on their severity levels.	No exceptions noted.
CC3.1	The entity specifies objectives with sufficient clarity to enable	Paradigm Software Technologies, Inc. DBA	Inspected the Risk Assessment Policy to determine that the company is required to update the risk assessment	No exceptions noted.

	the identification and assessment of risks relating to objectives.	Nexelus conducts a Risk Assessment at least annually.	report when newly identified risks are identified and reviewed at least annually.	
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	Paradigm Software Technologies, Inc. DBA Nexelus has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	Inspected the Risk Assessment Policy to determine that the company has defined risk assessment processes and remediation strategies for identified risks based on their risk levels.	No exceptions noted.
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	Paradigm Software Technologies, Inc. DBA Nexelus engages with third-party to conduct vulnerability scans of the production environment at least quarterly. Results are reviewed by management and high priority findings are tracked to resolution.	Inspected the Vulnerability Management Policy to determine that the company is required to perform vulnerability scans on all production systems at least annually.	No exceptions noted.
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	Paradigm Software Technologies, Inc. DBA Nexelus engages with third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution.	Inspected the Vulnerability Management Policy to determine that the company is required to perform penetration testing is performed regularly by either a certified penetration tester on Nexelus' security team or an independent third party.	No exceptions noted.
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.	Paradigm Software Technologies, Inc. DBA Nexelus engages with third-party to conduct vulnerability scans of the production environment at least quarterly. Results are reviewed by management and high priority findings are tracked to resolution.	Inspected the Vulnerability Management Policy to determine that the company is required to perform vulnerability scans on all production systems at least annually.	No exceptions noted.
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.	Paradigm Software Technologies, Inc. DBA Nexelus conducts a Risk Assessment at least annually.	Inspected the Risk Assessment Policy to determine that the company is required to update the risk assessment report when newly identified risks are	No exceptions noted.

			identified and reviewed 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.	Paradigm Software Technologies, Inc. DBA Nexelus's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	Inspected the Risk Assessment Policy to determine that the requirements for a risk remediation and treatment process have been documented.	No exceptions noted.
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.	Paradigm Software Technologies, Inc. DBA Nexelus has a defined vendor management policy that establishes requirements of ensuring third-party entities meet the organization's data preservation and protection requirements.	Inspected the Vendor Management Policy to determine that the company requires its vendors to maintain the integrity, security, and privacy of the company's data.	No exceptions noted.
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.	Paradigm Software Technologies, Inc. DBA Nexelus has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	Inspected the Risk Assessment Policy to determine that the company has defined risk assessment processes and remediation strategies for identified risks based on their risk levels.	No exceptions noted.
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.	Paradigm Software Technologies, Inc. DBA Nexelus maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.	Inspected the Vendor Management Policy to determine that the company is required to maintain vendor inventory and vendor contracts that must include confidentiality and privacy commitments.	No exceptions noted.
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.	Paradigm Software Technologies, Inc. DBA Nexelus maintains a directory of its key vendors, including their compliance reports. Critical vendor compliance reports are reviewed annually.	Inspected the Vendor Management Policy to determine that the company may choose to audit IT vendors and partners to ensure compliance with applicable security policies, as well as legal, regulatory, and contractual obligations.	No exceptions noted.
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	Paradigm Software Technologies, Inc. DBA Nexelus conducts a Risk Assessment at least annually.	Inspected the Risk Assessment Policy to determine that the company is required to update the risk assessment report when newly identified risks are	No exceptions noted.

			identified and reviewed at least annually.	
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	Paradigm Software Technologies, Inc. DBA Nexelus's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	Inspected the Risk Assessment Policy to determine that the requirements for a risk remediation and treatment process have been documented.	No exceptions noted.
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	Paradigm Software Technologies, Inc. DBA Nexelus has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	Inspected the Risk Assessment Policy to determine that the company has defined risk assessment processes and remediation strategies for identified risks based on their risk levels.	No exceptions noted.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	Paradigm Software Technologies, Inc. DBA Nexelus maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.	Inspected the Vendor Management Policy to determine that the company is required to maintain vendor inventory and vendor contracts that must include confidentiality and privacy commitments.	No exceptions noted.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	Paradigm Software Technologies, Inc. DBA Nexelus conducts a Risk Assessment at least annually.	Inspected the Risk Assessment Policy to determine that the company is required to update the risk assessment report when newly identified risks are identified and reviewed at least annually.	No exceptions noted.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	Paradigm Software Technologies, Inc. DBA Nexelus engages with third-party to conduct vulnerability scans of the production environment at least quarterly. Results are reviewed by management and high-priority findings are tracked to resolution.	Inspected the Vulnerability Management Policy to determine that the company is required to perform vulnerability scans on all production systems at least annually.	No exceptions noted.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	Paradigm Software Technologies, Inc. DBA Nexelus reviews its organizational structure, reporting lines, authorities,	Observed the company's automated compliance platform to determine that Paradigm Software Technologies, Inc. DBA Nexelus reviews its organizational structure, reporting lines, authorities,	No exceptions noted.

		and responsibilities in terms of information security on an annual basis.	and responsibilities in terms of information security on an annual basis.	
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	Paradigm Software Technologies, Inc. DBA Nexelus engages with third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and high-priority findings are tracked to resolution.	Inspected the Vulnerability Management Policy to determine that the company is required to perform penetration testing is performed regularly by either a certified penetration tester on Nexelus' security team or an independent third party.	No exceptions noted.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	Paradigm Software Technologies, Inc. DBA Nexelus has a defined vendor management policy that establishes requirements of ensuring third-party entities meet the organization's data preservation and protection requirements.	Inspected the Vendor Management Policy to determine that the company requires its vendors to maintain the integrity, security, and privacy of the company's data.	No exceptions noted.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	Paradigm Software Technologies, Inc. DBA Nexelus has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	Inspected the Risk Assessment Policy to determine that the company has defined risk assessment processes and remediation strategies for identified risks based on their risk levels.	No exceptions noted.
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.	Paradigm Software Technologies, Inc. DBA Nexelus conducts a Risk Assessment at least annually.	Inspected the Risk Assessment Policy to determine that the company is required to update the risk assessment report when newly identified risks are identified and reviewed at least annually.	No exceptions noted.
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.	Paradigm Software Technologies, Inc. DBA Nexelus has a defined System Access Control Policy that requires annual access control reviews to be conducted and access	Inspected the System Access Control Policy to determine that the company requires the Security Officer to conduct annual user access reviews. Additionally, access requests are required to be raised through the company's ticketing system.	No exceptions noted.

		request forms be filled out for new hires and employee transfers.		
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.	Paradigm Software Technologies, Inc. DBA Nexelus engages with third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and high-priority findings are tracked to resolution.	Inspected the Vulnerability Management Policy to determine that the company is required to perform penetration testing is performed regularly by either a certified penetration tester on Nexelus' security team or an independent third party.	No exceptions noted.
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.	Paradigm Software Technologies, Inc. DBA Nexelus performs annual access control reviews.	Inspected the System Access Control Policy to determine that the company is required to review and update all access privileges on an annual basis.	No exceptions noted.
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.	Paradigm Software Technologies, Inc. DBA Nexelus maintains a directory of its key vendors, including its agreements that specify terms, conditions, and responsibilities.	Inspected the Vendor Management Policy to determine that the company is required to maintain vendor inventory and vendor contracts that must include confidentiality and privacy commitments.	No exceptions noted.
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.	Paradigm Software Technologies, Inc. DBA Nexelus engages with third-party to conduct vulnerability scans of the production environment at least quarterly. Results are reviewed by management and high-priority findings are tracked to resolution.	Inspected the Vulnerability Management Policy to determine that the company is required to perform vulnerability scans on all production systems at least annually.	No exceptions noted.
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.	Paradigm Software Technologies, Inc. DBA Nexelus has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	Inspected the Risk Assessment Policy to determine that the company has defined risk assessment processes and remediation strategies for identified risks based on their risk levels.	No exceptions noted.

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.	Paradigm Software Technologies, Inc. DBA Nexelus maintains a directory of its key vendors, including its agreements that specify terms, conditions, and responsibilities.	Inspected the Vendor Management Policy to determine that the company is required to maintain vendor inventory and vendor contracts that must include confidentiality and privacy commitments.	No exceptions noted.
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.	Paradigm Software Technologies, Inc. DBA Nexelus engages with third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and high-priority findings are tracked to resolution.	Inspected the Vulnerability Management Policy to determine that the company is required to perform penetration testing is performed regularly by either a certified penetration tester on Nexelus' security team or an independent third party.	No exceptions noted.
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.	Paradigm Software Technologies, Inc. DBA Nexelus has implemented an Incident Response Plan that includes documenting "Lessons Learned" and "Root Cause Analysis" after incidents and sharing them with the broader engineering team to support Business Continuity/Disaster Recovery.	Inspected the Incident Response Plan to determine that the company requires the Information Security Manager to prepare a root cause report and a "lessons learned" document as part of the incident post-mortem analysis.	No exceptions noted.
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.	Paradigm Software Technologies, Inc. DBA Nexelus has an established Incident Response Plan that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents and annual testing.	Inspected the Incident Response Plan to determine that the process of establishing and executing the incident response plan along with the roles and responsibilities of the ISM and other key personnel has been described for responding to incidents.	No exceptions noted.
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	Paradigm Software Technologies, Inc. DBA Nexelus has identified an incident response team that quantifies and monitors incidents involving security,	Inspected the Incident Response Plan to determine that the company requires the DevOps, HR & Facilities, and Security teams to coordinate in executing a response to identified security threats.	No exceptions noted.

	the board of directors, as appropriate.	availability, processing integrity, and confidentiality at the company.		
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.	Paradigm Software Technologies, Inc. DBA Nexelus's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	Inspected the Risk Assessment Policy to determine that the requirements for a risk remediation and treatment process have been documented.	No exceptions noted.
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.	Paradigm Software Technologies, Inc. DBA Nexelus has implemented an Incident Response Plan that includes creating, prioritizing, assigning, and tracking follow-ups to completion and lend support to Business Continuity/Disaster Recovery.	Inspected the Incident Response Plan to determine that the company has defined the incident response process, which requires conducting a post-mortem that includes root cause analysis and documentation of any lessons learned.	No exceptions noted.
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.	Paradigm Software Technologies, Inc. DBA Nexelus engages with third-party to conduct vulnerability scans of the production environment at least quarterly. Results are reviewed by management and high-priority findings are tracked to resolution.	Inspected the Vulnerability Management Policy to determine that the company is required to perform vulnerability scans on all production systems at least annually.	No exceptions noted.
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.	Paradigm Software Technologies, Inc. DBA Nexelus has an assigned security team that is responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines.	Inspected the Information Security Policy to determine that the Network Manager and General Manager are responsible for the development, dissemination, and enforcement of the information security policies. Additionally, the policies are required to be reviewed by a security or compliance committee.	No exceptions noted.
CC4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for	Paradigm Software Technologies, Inc. DBA Nexelus conducts a Risk Assessment at least annually.	Inspected the Risk Assessment Policy to determine that the company is required to update the risk assessment report when newly identified risks are	No exceptions noted.

	taking corrective action, including senior management and the board of directors, as appropriate.		identified and reviewed 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.	Paradigm Software Technologies, Inc. DBA Nexelus has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	Inspected the Risk Assessment Policy to determine that the company has defined risk assessment processes and remediation strategies for identified risks based on their risk levels.	No exceptions noted.
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Paradigm Software Technologies, Inc. DBA Nexelus engages with third-party to conduct vulnerability scans of the production environment at least quarterly. Results are reviewed by management and high-priority findings are tracked to resolution.	Inspected the Vulnerability Management Policy to determine that the company is required to perform vulnerability scans on all production systems at least annually.	No exceptions noted.
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Paradigm Software Technologies, Inc. DBA Nexelus engages with third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and high-priority findings are tracked to resolution.	Inspected the Vulnerability Management Policy to determine that the company is required to perform penetration testing is performed regularly by either a certified penetration tester on Nexelus' security team or an independent third party.	No exceptions noted.
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Paradigm Software Technologies, Inc. DBA Nexelus conducts a Risk Assessment at least annually.	Inspected the Risk Assessment Policy to determine that the company is required to update the risk assessment report when newly identified risks are identified and reviewed at least annually.	No exceptions noted.
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Paradigm Software Technologies, Inc. DBA Nexelus reviews its organizational structure, reporting lines, authorities, and responsibilities in terms of information security on an annual basis.	Observed the company's automated compliance platform to determine that Paradigm Software Technologies, Inc. DBA Nexelus reviews its organizational structure, reporting lines, authorities, and responsibilities in terms of information security on an annual basis.	No exceptions noted.

CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Paradigm Software Technologies, Inc. DBA Nexelus conducts continuous monitoring of security controls using Drata, and addresses issues in a timely manner.	Inspected the Information Security Policy, which states that monitoring activities may be conducted on an ongoing basis or whenever deemed necessary to determine that the company conducts continuous monitoring of security controls using Drata, and addresses issues in a timely manner.	No exceptions noted.
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Paradigm Software Technologies, Inc. DBA Nexelus's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	Inspected the Risk Assessment Policy to determine that the requirements for a risk remediation and treatment process have been documented.	No exceptions noted.
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Paradigm Software Technologies, Inc. DBA Nexelus has an assigned security team that is responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines.	Inspected the Information Security Policy to determine that the Network Manager and General Manager are responsible for the development, dissemination, and enforcement of the information security policies. Additionally, the policies are required to be reviewed by a security or compliance committee.	No exceptions noted.
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Paradigm Software Technologies, Inc. DBA Nexelus has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	Inspected the Risk Assessment Policy to determine that the company has defined risk assessment processes and remediation strategies for identified risks based on their risk levels.	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	Paradigm Software Technologies, Inc. DBA Nexelus engages with third-party to conduct vulnerability scans of the production environment at least quarterly. Results are reviewed by management and high priority findings are tracked to resolution.	Inspected the Vulnerability Management Policy to determine that the company is required to perform vulnerability scans on all production systems at least annually.	No exceptions noted.

CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	Paradigm Software Technologies, Inc. DBA Nexelus has an assigned security team that is responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines.	Inspected the Information Security Policy to determine that the Network Manager and General Manager are responsible for the development, dissemination, and enforcement of the information security policies. Additionally, the policies are required to be reviewed by a security or compliance committee.	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	Paradigm Software Technologies, Inc. DBA Nexelus's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	Inspected the Risk Assessment Policy to determine that the requirements for a risk remediation and treatment process have been documented.	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	Paradigm Software Technologies, Inc. DBA Nexelus Management has approved security policies, and all employees accept these procedures when hired. Management also ensures that security policies are accessible to all employees and contractors.	Inspected the Information Security Policy to determine that all ISP policies are required to be reviewed, modified, or edited by management annually and accessible to employees. Employees are required to accept the policies upon hire.	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	Paradigm Software Technologies, Inc. DBA Nexelus has established training programs for privacy and information security to help employees understand their obligations and responsibilities to comply with Paradigm Software Technologies, Inc. DBA Nexelus's security policies and procedures, including the identification and reporting of incidents. All full-time employees are required to complete the training upon hire and annually thereafter.	Inspected the Information Security Policy to determine that the company requires new employees to complete information security awareness training upon hire and annually after that.	No exceptions noted.

CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	Paradigm Software Technologies, Inc. DBA Nexelus authorizes access to information resources, including data and the systems that store or process customer data, based on the principle of least privilege.	Inspected the System Access Control Policy to determine that the company requires all access to be regulated by the role-based access control (RBAC) method, based on the principle of least privilege.	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	Paradigm Software Technologies, Inc. DBA Nexelus Management has approved all policies that detail how customer data may be made accessible and should be handled. These policies are accessible to all employees and contractors.	Inspected the System Access Control Policy, Asset Management Policy, Data Classification Policy, Data Protection Policy, and Vendor Management Policy to determine that these policies provide guidance on accessing, handling, processing, and securing customer data and are accessible to all employees and contractors.	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	Paradigm Software Technologies, Inc. DBA Nexelus has an established policy and procedures that governs the use of cryptographic controls.	Inspected the Encryption Policy to determine that the company has established the cryptographic controls and procedures for cryptographic key management and protection.	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	Paradigm Software Technologies, Inc. DBA Nexelus conducts continuous monitoring of security controls using Drata, and addresses issues in a timely manner.	Inspected the Information Security Policy, which states that monitoring activities may be conducted on an ongoing basis or whenever deemed necessary to determine that the company conducts continuous monitoring of security controls using Drata, and addresses issues in a timely manner.	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	Paradigm Software Technologies, Inc. DBA Nexelus engages with third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and high-priority findings are tracked to resolution.	Inspected the Vulnerability Management Policy to determine that the company is required to perform penetration testing is performed regularly by either a certified penetration tester on Nexelus' security team or an independent third party.	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	Paradigm Software Technologies, Inc. DBA Nexelus conducts a Risk Assessment at least annually.	Inspected the Risk Assessment Policy to determine that the company is required to update the risk assessment report when newly identified risks are	No exceptions noted.

			identified and reviewed 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.	Paradigm Software Technologies, Inc. DBA Nexelus conducts annual BCP/DR tests and documents according to the BCDR Plan.	Inspected the Business Continuity Plan to determine that the company is required to simulate and test the Business Continuity Plan at least once a year. Inspected the Disaster Recovery Plan to determine that the company is required to test the Disaster Recovery Plan at least annually.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Paradigm Software Technologies, Inc. DBA Nexelus has an established Disaster Recovery Plan that outlines roles and responsibilities and detailed procedures for recovery of systems.	Inspected the Disaster Recovery Plan to determine that the disaster recovery procedure and the roles and responsibilities of the CTO for the implementation of recovery procedures have been defined by the company.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Paradigm Software Technologies, Inc. DBA Nexelus Management has approved security policies, and all employees accept these procedures when hired. Management also ensures that security policies are accessible to all employees and contractors.	Inspected the Information Security Policy to determine that all ISP policies are required to be reviewed, modified, or edited by management annually and accessible to employees. Employees are required to accept the policies upon hire.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Paradigm Software Technologies, Inc. DBA Nexelus provides a process to employees for reporting security, confidentiality, integrity, and availability features, incidents, and concerns, and other complaints to company management.	Inspected the Responsible Disclosure Policy to determine that an email address (vulnerability@nexelus.net) has been provided to employees to report vulnerabilities to Nexelus' Product Security Team.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Paradigm Software Technologies, Inc. DBA Nexelus has a formal Code of Conduct approved by management and accessible to all employees. All	Inspected the Code of Conduct to determine that the company requires new employees to sign their acknowledgment of the Code at the time of hiring.	No exceptions noted.

		employees must accept the Code of Conduct upon hire.		
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Paradigm Software Technologies, Inc. DBA Nexelus has a defined Business Continuity Plan that outlines the proper procedures to respond, recover, resume, and restore operations following a disruption.	Inspected the Business Continuity Plan to determine that the company has established a Business Continuity Plan that defines the procedures to recover the company's data and operations following a disruption in conjunction with the Disaster Recovery Plan.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Management reviews security policies on an annual basis.	Inspected the Information Security Policy to determine that senior management and key personnel are required to review the security policies annually.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Paradigm Software Technologies, Inc. DBA Nexelus has a defined Information Security Policy that covers policies and procedures to support the functioning of internal control.	Inspected the Information Security Policy to determine that the company has described the procedures for all essential internal control activities, including the responsibilities of the CTO, staff training requirements, use of the Internet, workspace, remote access privileges, teleworking, mobile devices, and a disciplinary process to be followed when any of these procedures are not followed.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Paradigm Software Technologies, Inc. DBA Nexelus has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	Inspected the Risk Assessment Policy to determine that the company has defined risk assessment processes and remediation strategies for identified risks based on their risk levels.	No exceptions noted.
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.	Paradigm Software Technologies, Inc. DBA Nexelus has a defined policy that establishes requirements for the proper management and tracking of organizational assets.	Inspected the Asset Management Policy to determine that the company has outlined the procedures for properly managing its physical and digital assets according to the best practices and hardening standards.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets	Users can only access the production system remotely through the use of encrypted communication systems.	Inspected the Data Classification Policy to determine that the company allows remote access to restricted data on its	No exceptions noted.

	to protect them from security events to meet the entity's objectives.		production systems through VPN and 2FA 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.	Paradigm Software Technologies, Inc. DBA Nexelus uses a version control system to manage source code, documentation, release labeling, and other change management tasks. Access to the system must be approved by a system admin.	Observed that the company uses Azure DevOps as its version control system. Inspected the Software Development Life Cycle to determine that the company is required to use a configuration control system.	No exceptions noted.
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.	Paradigm Software Technologies, Inc. DBA Nexelus stores customer data in databases that is encrypted at rest.	Inspected the Data Protection Policy to determine that the company is required to encrypt all databases, datastores, and file systems according to the Encryption Policy.	No exceptions noted.
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.	Paradigm Software Technologies, Inc. DBA Nexelus has an established key management process in place to support the organization's use of cryptographic techniques.	Inspected the Encryption Policy to determine that the company has described a key management system to guide the workforce in the use of public and private encryption keys.	No exceptions noted.
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.	Paradigm Software Technologies, Inc. DBA Nexelus has a defined policy that establishes requirements for the use of cryptographic controls.	Inspected the Encryption Policy to determine that cryptographic controls to protect individual systems or information and key management procedures have been described.	No exceptions noted.
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.	Paradigm Software Technologies, Inc. DBA Nexelus identifies, inventories, classifies, and assigns owners to IT assets.	Inspected the Asset Management Policy to determine that the company has documented the standards for maintaining an asset inventory for physical and virtual assets.	No exceptions noted.
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.	Paradigm Software Technologies, Inc. DBA Nexelus ensures that company-issued laptops have encrypted hard-disks.	Inspected the Acceptable Use Policy to determine that device encryption must be enabled for all mobile devices accessing company data, such as whole-disk encryption for all laptops. Inspected the System Access Control	No exceptions noted.

			Policy to determine that the company requires the workstation hard drives to be encrypted.	
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.	Hardening standards are in place to ensure that newly deployed server instances are appropriately secured.	Inspected the Asset Management Policy to determine that system hardening standards have been defined.	No exceptions noted.
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.	Appropriate levels of access to infrastructure and code review tools are granted to new employees within one week of their start date.	Inspected the System Access Control Policy to determine that the company requires the Security Officer to grant access to the infrastructure and code review tools upon satisfaction that the access privileges requested are in line with the user's job requirements.	No exceptions noted.
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.	Role-based security is in place for internal and external users, including super admin users.	Inspected the System Access Control Policy to determine that the company requires users to be granted access to company systems and applications based on the principle of least privilege and Role-Based Access Control (RBAC).	No exceptions noted.
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.	Paradigm Software Technologies, Inc. DBA Nexelus has established formal guidelines for passwords to govern the management and use of authentication mechanisms.	Inspected the Password Policy to determine that formal guidelines and requirements regarding password length and complexity have been established by the management.	No exceptions noted.
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.	Paradigm Software Technologies, Inc. DBA Nexelus has established a Data Protection Policy and requires all employees to accept it upon hire. Management monitors employees' acceptance of the policy.	Inspected the Data Protection Policy to determine that the data protection processes and implementation guidelines have been documented. Inspected the Information Security Policy to determine that the security policies must be reviewed and signed upon hire and on an annual basis by all employees.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security	Username and password (password standard implemented) or SSO required to authenticate into application, MFA optional for	Inspected the Password Policy to determine that the company requires users to grant access to an application through a single-sign-on (SSO) provider, and requires MFA to be enabled for all systems.	No exceptions noted.

	events to meet the entity's objectives.	external users, and MFA required for employee users.		
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.	Paradigm Software Technologies, Inc. DBA Nexelus maintains an accurate network diagram that is accessible to the engineering team and is reviewed by management on an annual basis.	Inspected the Asset Management Policy to determine that the company is required to maintain a network diagram and provide it to all appropriate service personnel.	No exceptions noted.
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.	Paradigm Software Technologies, Inc. DBA Nexelus requires two-factor authentication to access sensitive systems and applications in the form of user ID, password, OTP and/or certificate.	Inspected the Password Policy to determine that MFA is required to be enabled for all systems that provide the option for Multi-Factor Authentication (MFA).	No exceptions noted.
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.	Paradigm Software Technologies, Inc. DBA Nexelus ensures that a password manager is installed on all company-issued laptops.	Inspected the Password Policy to determine that the company-approved password manager is required to be installed on all company-issued laptops.	No exceptions noted.
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.	Access to corporate network, production machines, network devices, and support tools requires a unique ID.	Inspected the System Access Control Policy to determine that users are required to use unique user IDs and passwords to access systems and applications.	No exceptions noted.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	Paradigm Software Technologies, Inc. DBA Nexelus uses a termination checklist to ensure that an employee's system access, including physical access, is removed within a specified timeframe and all organization assets (physical or electronic) are properly returned.	Inspected the System Access Control Policy to determine that the HR Department users and their supervisors are required to notify the Security Officer upon completion or termination of access needs and facilitate completion of the termination checklist.	No exceptions noted.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users	Paradigm Software Technologies, Inc. DBA Nexelus performs annual access control reviews.	Inspected the System Access Control Policy to determine that the company is required to review and update all access privileges on an annual basis.	No exceptions noted.

	whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.			
CC6.2	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.	Paradigm Software Technologies, Inc. DBA Nexelus has a defined System Access Control Policy that requires annual access control reviews to be conducted and access request forms be filled out for new hires and employee transfers.	Inspected the System Access Control Policy to determine that the company requires the Security Officer to conduct annual user access reviews. Additionally, access requests are required to be raised through the company's ticketing system.	No exceptions noted.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	Access to corporate network, production machines, network devices, and support tools requires a unique ID.	Inspected the System Access Control Policy to determine that users are required to use unique user IDs and passwords to access systems and applications.	No exceptions noted.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	Appropriate levels of access to infrastructure and code review tools are granted to new employees within one week of their start date.	Inspected the System Access Control Policy to determine that the company requires the Security Officer to grant access to the infrastructure and code review tools upon satisfaction that the access privileges requested are in line with the user's job requirements.	No exceptions noted.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	Access to infrastructure and code review tools is removed from terminated employees within one business day.	Inspected the System Access Control Policy to determine that the Security Officer is required to revoke access of terminated employees immediately or as soon as possible.	No exceptions noted.

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.	Paradigm Software Technologies, Inc. DBA Nexelus has a defined System Access Control Policy that requires annual access control reviews to be conducted and access request forms be filled out for new hires and employee transfers.	Inspected the System Access Control Policy to determine that the company requires the Security Officer to conduct annual user access reviews. Additionally, access requests are required to be raised through the company's ticketing system.	No exceptions noted.
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.	Appropriate levels of access to infrastructure and code review tools are granted to new employees within one week of their start date.	Inspected the System Access Control Policy to determine that the company requires the Security Officer to grant access to the infrastructure and code review tools upon satisfaction that the access privileges requested are in line with the user's job requirements.	No exceptions noted.
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.	Role-based security is in place for internal and external users, including super admin users.	Inspected the System Access Control Policy to determine that the company requires users to be granted access to company systems and applications based on the principle of least privilege and Role-Based Access Control (RBAC).	No exceptions noted.
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.	Access to infrastructure and code review tools is removed from terminated employees within one business day.	Inspected the System Access Control Policy to determine that the Security Officer is required to revoke access of terminated employees immediately or as soon as possible.	No exceptions noted.
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	Paradigm Software Technologies, Inc. DBA Nexelus uses a termination checklist to ensure that an employee's system access, including physical access, is removed within a specified	Inspected the System Access Control Policy to determine that the HR Department users and their supervisors are required to notify the Security Officer upon completion or termination of access needs and facilitate	No exceptions noted.

	the concepts of least privilege and segregation of duties, to meet the entity's objectives.	timeframe and all organization assets (physical or electronic) are properly returned.	completion of the termination checklist.	
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.	Paradigm Software Technologies, Inc. DBA Nexelus performs annual access control reviews.	Inspected the System Access Control Policy to determine that the company is required to review and update all access privileges on an annual basis.	No exceptions noted.
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.	Access to corporate networks, production machines, network devices, and support tools requires a unique ID.	Inspected the System Access Control Policy to determine that users are required to use unique user IDs and passwords to access systems and applications.	No exceptions noted.
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.	Paradigm Software Technologies, Inc. DBA Nexelus maintains a directory of its key vendors, including its agreements that specify terms, conditions, and responsibilities.	Inspected the Vendor Management Policy to determine that the company is required to maintain vendor inventory and vendor contracts that must include confidentiality and privacy commitments.	No exceptions noted.
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.	Paradigm Software Technologies, Inc. DBA Nexelus maintains a directory of its key vendors, including their compliance reports. Critical vendor compliance reports are reviewed annually.	Inspected the Vendor Management Policy to determine that the company may choose to audit IT vendors and partners to ensure compliance with applicable security policies, as well as legal, regulatory, and contractual obligations.	No exceptions noted.
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	Paradigm Software Technologies, Inc. DBA Nexelus uses a termination checklist to ensure that an employee's system access, including physical access, is removed within a specified	Inspected the System Access Control Policy to determine that the HR Department users and their supervisors are required to notify the Security Officer upon completion or termination of access needs and facilitate	No exceptions noted.

	personnel to meet the entity's objectives.	timeframe and all organization assets (physical or electronic) are properly returned.	completion of the termination checklist.	
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.	Paradigm Software Technologies, Inc. DBA Nexelus has security policies that have been approved by management and detail how physical security for the company's headquarters is maintained. These policies are accessible to all employees and contractors.	Inspected the Physical Security Policy stating the access requirements and roles and responsibilities for physical security to determine that a Physical Security Policy is in place and is accessible to all employees and contractors.	No exceptions noted.
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.	Paradigm Software Technologies, Inc. DBA Nexelus has security policies that have been approved by management and detail how physical access to the company's headquarters is maintained. These policies are accessible to all employees and contractors.	Inspected the Physical Security Policy stating the access requirements and roles and responsibilities for physical security to determine that Physical Security Policy is in place and is accessible to employees and contractors.	No exceptions noted.
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.	Paradigm Software Technologies, Inc. DBA Nexelus performs annual access control reviews.	Inspected the System Access Control Policy to determine that the company is required to review and update all access privileges on an annual basis.	No exceptions noted.
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.	Paradigm Software Technologies, Inc. DBA Nexelus uses a termination checklist to ensure that an employee's system access, including physical access, is removed within a specified timeframe and all organization assets (physical or electronic) are properly returned.	Inspected the System Access Control Policy to determine that the HR Department users and their supervisors are required to notify the Security Officer upon completion or termination of access needs and facilitate completion of the termination checklist.	No exceptions noted.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data	Paradigm Software Technologies, Inc. DBA Nexelus has formal policies and procedures in place to	Inspected the Data Retention Policy to determine that the requirements and controls/procedures to manage the deletion of customer data have been	No exceptions noted.

	and software from those assets has been diminished and is no longer required to meet the entity's objectives.	guide personnel in the disposal of hardware containing sensitive data.	described. Inspected the Information Security Policy to determine that procedures for the disposal of sensitive data have been described stating that whiteboards containing restricted and/or sensitive information should be erased and the company requires to destroy, delete, erase, or conceal company data, or otherwise making such files or data unavailable or inaccessible to other authorized users.	
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Username and password (password standard implemented) or SSO required to authenticate into application, MFA optional for external users, and MFA required for employee users.	Inspected the Password Policy to determine that the company requires users to grant access to an application through a single-sign-on (SSO) provider, and requires MFA to be enabled for all systems.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Paradigm Software Technologies, Inc. DBA Nexelus ensures that all company-issued computers use a screensaver lock with a timeout of no more than 15 minutes.	Inspected the System Access Control Policy to determine that the company requires users to make information systems inaccessible by any other individual by using a password-protected screen saver or logging off when left unattended.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Paradigm Software Technologies, Inc. DBA Nexelus ensures that all connections to its web application from its users are encrypted.	Inspected the Data Protection Policy to determine that the company requires all Internet and intranet connections to be encrypted and authenticated using a strong protocol, key exchange, and cipher.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Read/Write access to cloud data storage is configured to restrict public access.	Inspected the System Access Control Policy which states that the level of security assigned to a user to the organization's information systems is based on the minimum necessary amount of data access required to carry out legitimate job responsibilities assigned to a user's job classification, to determine that cloud data storage is restricted at the company.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from	Application Gateway in place to protect Paradigm Software Technologies, Inc. DBA	Observed that the company uses AWS's firewalls to protect the company's application from outside threats.	No exceptions noted.

	sources outside its system boundaries.	Nexelus's application from outside threats.		
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	No public SSH is allowed.	Observed that public SSH is denied on AWS.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Paradigm Software Technologies, Inc. DBA Nexelus uses configurations that ensure only approved networking ports and protocols are implemented, including firewalls.	Observed that the built-in firewall feature of AWS has been used by Nexelus to deny all traffic that is not explicitly allowed.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Paradigm Software Technologies, Inc. DBA Nexelus automatically logs users out after a predefined inactivity interval and requires users to reauthenticate	Inspected the System Access Control Policy to determine that the company requires users to make information systems inaccessible by using a password-protected screen saver or logging off the system.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Users can only access the production system remotely through the use of encrypted communication systems.	Inspected the Data Classification Policy to determine that the company allows remote access to restricted data on its production systems through VPN and 2FA only.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Paradigm Software Technologies, Inc. DBA Nexelus requires two-factor authentication to access sensitive systems and applications in the form of user ID, password, OTP and/or certificate.	Inspected the Password Policy to determine that MFA is required to be enabled for all systems that provide the option for Multi-Factor Authentication (MFA).	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Paradigm Software Technologies, Inc. DBA Nexelus has established formal guidelines for passwords to govern the management and use of authentication mechanisms.	Inspected the Password Policy to determine that formal guidelines and requirements regarding password length and complexity have been established by the management.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	An intrusion detection system (IDS) is in place to detect potential intrusions, alert personnel when a potential intrusion is detected	Inspected the Data Protection Policy to determine that the company uses Microsoft Azure Monitor to monitor the entire cloud service operation.	No exceptions noted.

CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Paradigm Software Technologies, Inc. DBA Nexelus maintains an accurate network diagram that is accessible to the engineering team and is reviewed by management on an annual basis.	Inspected the Asset Management Policy to determine that the company is required to maintain a network diagram and provide it to all appropriate service personnel.	No exceptions noted.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	Paradigm Software Technologies, Inc. DBA Nexelus has established a Data Protection Policy and requires all employees to accept it upon hire. Management monitors employees' acceptance of the policy.	Inspected the Data Protection Policy to determine that the data protection processes and implementation guidelines have been documented. Inspected the Information Security Policy to determine that the security policies must be reviewed and signed upon hire and on an annual basis by all employees.	No exceptions noted.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	Paradigm Software Technologies, Inc. DBA Nexelus ensures that company-issued laptops have encrypted hard-disks.	Inspected the Acceptable Use Policy to determine that device encryption must be enabled for all mobile devices accessing company data, such as whole-disk encryption for all laptops. Inspected the System Access Control Policy to determine that the company requires the workstation hard drives to be encrypted.	No exceptions noted.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	Paradigm Software Technologies, Inc. DBA Nexelus ensures that company-issued removable media devices (USB drives) are encrypted.	Inspected the Information Security Policy to determine that the company requires all mass storage devices, including USB drives, to be secured through encryption.	No exceptions noted.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	Paradigm Software Technologies, Inc. DBA Nexelus uses encryption to protect user authentication and admin sessions of the internal admin tool transmitted over the Internet.	Inspected the Data Protection Policy to determine that all Internet and intranet connections are to be encrypted and authenticated using a strong protocol, a strong key exchange, and a strong cipher.	No exceptions noted.
CC6.7	The entity restricts the transmission, movement, and removal of information to	Paradigm Software Technologies, Inc. DBA Nexelus uses DLP (Data Loss	Inspected the Information Security Policy to determine that the company requires a data loss prevention tool to	No exceptions noted.

	authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	Prevention) software to prevent unencrypted sensitive information from being transmitted over email	be used and prohibits users from disabling or circumventing it.	
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.	Paradigm Software Technologies, Inc. DBA Nexelus stores customer data in databases that is encrypted at rest.	Inspected the Data Protection Policy to determine that the company is required to encrypt all databases, datastores, and file systems according to the Encryption Policy.	No exceptions noted.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	Paradigm Software Technologies, Inc. DBA Nexelus's customer data is segregated from the data of other customers	Inspected the Data Protection Policy to determine that the company requires customer data to be logically separated at the database level using a unique identifier for the customer.	No exceptions noted.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	No public SSH is allowed.	Observed that public SSH is denied on AWS.	No exceptions noted.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	Paradigm Software Technologies, Inc. DBA Nexelus ensures that all connections to its web application from its users are encrypted.	Inspected the Data Protection Policy to determine that the company requires all Internet and intranet connections to be encrypted and authenticated using a strong protocol, key exchange, and cipher.	No exceptions noted.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	Paradigm Software Technologies, Inc. DBA Nexelus has infrastructure logging configured to monitor web traffic and suspicious activity. When anomalous traffic activity is identified, alerts are automatically created, sent to appropriate	Inspected the Data Protection Policy to determine that the company uses Microsoft Azure Monitor to monitor the entire cloud service operation and if a system failure or alarm is triggered, key personnel are notified by text, chat, and/or email message to take appropriate corrective action.	No exceptions noted.

		personnel and resolved, as necessary.		
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.	Paradigm Software Technologies, Inc. DBA Nexelus's workstations operating system (OS) security patches are applied.	Inspected the Asset Management Policy to determine that OS patches are required to be evaluated periodically and installed during off-peak hours. Disclosure: Patching is handled manually during maintenance to ensure that there is no interruption to the system.	No exceptions noted.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	Paradigm Software Technologies, Inc. DBA Nexelus requires antivirus software to be installed on workstations to protect the network against malware.	Inspected the Asset Management Policy to determine that the company requires updated antivirus and anti-malware tools to be installed on all workstations.	No exceptions noted.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	Paradigm Software Technologies, Inc. DBA Nexelus ensures that virtual machine OS patches are applied monthly.	Inspected the Asset Management Policy to determine that the company is required to evaluate and install OS patches periodically.	No exceptions noted.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	Paradigm Software Technologies, Inc. DBA Nexelus ensures that file integrity monitoring (FIM) software is in place to detect whether operating system and application software files have been tampered with.	Inspected the Data Protection Policy to determine that the company must have security monitoring enabled for all production systems including activity and file integrity monitoring, vulnerability scanning, and malware detection, as applicable.	No exceptions noted.
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.	An intrusion detection system (IDS) is in place to detect potential intrusions, alert personnel when a potential intrusion is detected	Inspected the Data Protection Policy to determine that the company uses Microsoft Azure Monitor to monitor the entire cloud service operation.	No exceptions noted.
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.	Paradigm Software Technologies, Inc. DBA Nexelus engages with third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management	Inspected the Vulnerability Management Policy to determine that the company is required to perform penetration testing is performed regularly by either a certified penetration tester on Nexelus' security team or an independent third party.	No exceptions noted.

		and high priority findings are tracked to resolution.		
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.	Paradigm Software Technologies, Inc. DBA Nexelus uses a version control system to manage source code, documentation, release labeling, and other change management tasks. Access to the system must be approved by a system admin.	Observed that the company uses Azure DevOps as its version control system. Inspected the Software Development Life Cycle to determine that the company is required to use a configuration control system.	No exceptions noted.
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.	Paradigm Software Technologies, Inc. DBA Nexelus engages with third-party to conduct vulnerability scans of the production environment at least quarterly. Results are reviewed by management and high-priority findings are tracked to resolution.	Inspected the Vulnerability Management Policy to determine that the company is required to perform vulnerability scans on all production systems at least annually.	No exceptions noted.
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.	Paradigm Software Technologies, Inc. DBA Nexelus has infrastructure logging configured to monitor web traffic and suspicious activity. When anomalous traffic activity is identified, alerts are automatically created, sent to appropriate personnel, and resolved, as necessary.	Inspected the Data Protection Policy to determine that the company uses Microsoft Azure Monitor to monitor the entire cloud service operation and if a system failure or alarm is triggered, key personnel are notified by text, chat, and/or email message to take appropriate corrective action.	No exceptions noted.
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.	When Paradigm Software Technologies, Inc. DBA Nexelus's application code changes, code reviews, and tests are performed by someone other than the person who made the code change.	Inspected the Software Development Life Cycle Policy to determine that code changes are required to be reviewed by individuals other than the originating code author.	No exceptions noted.
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)	Paradigm Software Technologies, Inc. DBA Nexelus conducts continuous monitoring of security controls using Drata, and addresses issues in a timely manner.	Inspected the Information Security Policy, which states that monitoring activities may be conducted on an ongoing basis or whenever deemed necessary to determine that the company conducts continuous monitoring of security controls using	No exceptions noted.

	susceptibilities to newly discovered vulnerabilities.		Drata, and addresses issues in a timely manner.	
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.	Paradigm Software Technologies, Inc. DBA Nexelus tracks and prioritizes security deficiencies through internal tools according to their severity by an independent technical resource.	Inspected the Vulnerability Management Policy to determine that the company is required to assign a priority level critical, high, medium, or low to all identified vulnerabilities.	No exceptions noted.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	Paradigm Software Technologies, Inc. DBA Nexelus uses logging software that sends alerts to appropriate personnel. Corrective actions are performed, as necessary, in a timely manner.	Inspected the Asset Management Policy to determine that the company is required to enable logging as part of its system hardening standards.	No exceptions noted.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	Paradigm Software Technologies, Inc. DBA Nexelus's cloud infrastructure is monitored through an operational audit system that sends alerts to appropriate personnel	Inspected the Vulnerability Management Policy to determine that the company is required to run technical audit tests as part of the company's operational audit.	No exceptions noted.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	Paradigm Software Technologies, Inc. DBA Nexelus is using Drata to monitor the security and compliance of its cloud infrastructure configuration	Inspected the Vulnerability Management Policy to determine that an automated Drata security agent is installed on all employees' machines for scanning and identification of system vulnerabilities.	No exceptions noted.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors	Paradigm Software Technologies, Inc. DBA Nexelus engages with third-party to conduct vulnerability scans of the	Inspected the Vulnerability Management Policy to determine that the company is required to perform vulnerability scans on all production systems at least annually.	No exceptions noted.

	affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	production environment at least quarterly. Results are reviewed by management and high-priority findings are tracked to resolution.		
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.	Paradigm Software Technologies, Inc. DBA Nexelus has infrastructure logging configured to monitor web traffic and suspicious activity. When anomalous traffic activity is identified, alerts are automatically created, sent to appropriate personnel, and resolved, as necessary.	Inspected the Data Protection Policy to determine that the company uses Microsoft Azure Monitor to monitor the entire cloud service operation and if a system failure or alarm is triggered, key personnel are notified by text, chat, and/or email message to take appropriate corrective action.	No exceptions noted.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	An intrusion detection system (IDS) is in place to detect potential intrusions, alert personnel when a potential intrusion is detected	Inspected the Data Protection Policy to determine that the company uses Microsoft Azure Monitor to monitor the entire cloud service operation.	No exceptions noted.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	Paradigm Software Technologies, Inc. DBA Nexelus uses a system that collects and stores server logs in a central location. The system can be queried in an ad hoc fashion by authorized users.	Inspected the Asset Management Policy to determine that the company uses Drata's automated system to query across the cloud-based infrastructure to obtain detailed records of all digital assets.	No exceptions noted.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	Paradigm Software Technologies, Inc. DBA Nexelus does not use Root Account on Infrastructure provider	Inspected the System Access Control Policy to determine that the root account is to be disabled.	No exceptions noted.

CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Paradigm Software Technologies, Inc. DBA Nexelus has an established Incident Response Plan that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents and annual testing.	Inspected the Incident Response Plan to determine that the process of establishing and executing the incident response plan along with the roles and responsibilities of the ISM and other key personnel has been described for responding to incidents.	No exceptions noted.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Paradigm Software Technologies, Inc. DBA Nexelus has implemented an Incident Response Plan that includes documenting "Lessons Learned" and "Root Cause Analysis" after incidents and sharing them with the broader engineering team to support Business Continuity/Disaster Recovery.	Inspected the Incident Response Plan to determine that the company requires the Information Security Manager to prepare a root cause report and a "lessons learned" document as part of the incident post-mortem analysis.	No exceptions noted.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Paradigm Software Technologies, Inc. DBA Nexelus has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company.	Inspected the Incident Response Plan to determine that the company requires the DevOps, HR & Facilities, and Security teams to coordinate in executing a response to identified security threats.	No exceptions noted.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Paradigm Software Technologies, Inc. DBA Nexelus tracks and prioritizes security deficiencies through internal tools according to their severity by an independent technical resource.	Inspected the Vulnerability Management Policy to determine that the company is required to assign a priority level critical, high, medium, or low to all identified vulnerabilities.	No exceptions noted.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Paradigm Software Technologies, Inc. DBA Nexelus has implemented an Incident Response Plan that includes creating, prioritizing, assigning, and tracking follow-ups to	Inspected the Incident Response Plan to determine that the company has defined the incident response process, which requires conducting a post-mortem that includes root cause analysis and documentation of any lessons learned.	No exceptions noted.

		completion and lend support to Business Continuity/Disaster Recovery.		
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 security team communicates important information security events to company management in a timely manner.	Inspected the Incident Response Plan to determine that the company requires users to report any incidents to their immediate managers within 24 hours, and the managers are required to notify the Information Security Manager immediately.	No exceptions noted.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Paradigm Software Technologies, Inc. DBA Nexelus has implemented an Incident Response Plan that includes documenting "Lessons Learned" and "Root Cause Analysis" after incidents and sharing them with the broader engineering team to support Business Continuity/Disaster Recovery.	Inspected the Incident Response Plan to determine that the company requires the Information Security Manager to prepare a root cause report and a "lessons learned" document as part of the incident post-mortem analysis.	No exceptions noted.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Paradigm Software Technologies, Inc. DBA Nexelus tracks and prioritizes security deficiencies through internal tools according to their severity by an independent technical resource.	Inspected the Vulnerability Management Policy to determine that the company is required to assign a priority level critical, high, medium, or low to all identified vulnerabilities.	No exceptions noted.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Paradigm Software Technologies, Inc. DBA Nexelus has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company.	Inspected the Incident Response Plan to determine that the company requires the DevOps, HR & Facilities, and Security teams to coordinate in executing a response to identified security threats.	No exceptions noted.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Paradigm Software Technologies, Inc. DBA Nexelus has implemented an Incident Response Plan that includes creating, prioritizing, assigning, and tracking follow-ups to	Inspected the Incident Response Plan to determine that the company has defined the incident response process, which requires conducting a post-mortem that includes root cause analysis and documentation of any lessons learned.	No exceptions noted.

		completion and lend support to Business Continuity/Disaster Recovery.		
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.	Paradigm Software Technologies, Inc. DBA Nexelus has an established Incident Response Plan that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents and annual testing.	Inspected the Incident Response Plan to determine that the process of establishing and executing the incident response plan along with the roles and responsibilities of the ISM and other key personnel has been described for responding to incidents.	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Paradigm Software Technologies, Inc. DBA Nexelus has an established Disaster Recovery Plan that outlines roles and responsibilities and detailed procedures for recovery of systems.	Inspected the Disaster Recovery Plan to determine that the disaster recovery procedure and the roles and responsibilities of the CTO for the implementation of recovery procedures have been defined by the company.	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Paradigm Software Technologies, Inc. DBA Nexelus tracks and prioritizes security deficiencies through internal tools according to their severity by an independent technical resource.	Inspected the Vulnerability Management Policy to determine that the company is required to assign a priority level critical, high, medium, or low to all identified vulnerabilities.	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Paradigm Software Technologies, Inc. DBA Nexelus has a defined Business Continuity Plan that outlines the proper procedures to respond, recover, resume, and restore operations following a disruption.	Inspected the Business Continuity Plan to determine that the company has established a Business Continuity Plan that defines the procedures to recover the company's data and operations following a disruption in conjunction with the Disaster Recovery Plan.	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Paradigm Software Technologies, Inc. DBA Nexelus performs backups daily and retains them in accordance with a predefined schedule in the Backup Policy.	Inspected the Backup Policy to determine that the company is required to perform daily data backups using an automated process that backs up all data to a separate region in the same country.	No exceptions noted.

CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Paradigm Software Technologies, Inc. DBA Nexelus has implemented an Incident Response Plan that includes documenting "Lessons Learned" and "Root Cause Analysis" after incidents and sharing them with the broader engineering team to support Business Continuity/Disaster Recovery.	Inspected the Incident Response Plan to determine that the company requires the Information Security Manager to prepare a root cause report and a "lessons learned" document as part of the incident post-mortem analysis.	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Paradigm Software Technologies, Inc. DBA Nexelus ensures that incident response plan testing is performed on an annual basis.	Inspected the Incident Response Plan to determine that the incident response plan is required to be tested annually.	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Paradigm Software Technologies, Inc. DBA Nexelus has an established Incident Response Plan that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents and annual testing.	Inspected the Incident Response Plan to determine that the process of establishing and executing the incident response plan along with the roles and responsibilities of the ISM and other key personnel has been described for responding to incidents.	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Paradigm Software Technologies, Inc. DBA Nexelus has implemented an Incident Response Plan that includes creating, prioritizing, assigning, and tracking follow-ups to completion and lend support to Business Continuity/Disaster Recovery.	Inspected the Incident Response Plan to determine that the company has defined the incident response process, which requires conducting a post-mortem that includes root cause analysis and documentation of any lessons learned.	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Paradigm Software Technologies, Inc. DBA Nexelus has identified an incident response team that quantifies and monitors incidents involving security, availability, processing	Inspected the Incident Response Plan to determine that the company requires the DevOps, HR & Facilities, and Security teams to coordinate in executing a response to identified security threats.	No exceptions noted.

		integrity, and confidentiality at the company.		
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.	When Paradigm Software Technologies, Inc. DBA Nexelus's application code changes, code reviews and tests are performed by someone other than the person who made the code change.	Inspected the Software Development Life Cycle Policy to determine that code changes are required to be reviewed by individuals other than the originating code author.	No exceptions noted.
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.	Paradigm Software Technologies, Inc. DBA Nexelus ensures that releases are approved by appropriate members of management prior to production release.	Inspected the Software Development Life Cycle to determine that the company requires all changes to the production code to be approved by an authorized owner of that environment.	No exceptions noted.
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.	Separate environments are used for testing and production for Paradigm Software Technologies, Inc. DBA Nexelus's application	Inspected the Software Development Life Cycle Policy to determine that the company requires application development activity to be separated from the production and test environments.	No exceptions noted.
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.	Only authorized Paradigm Software Technologies, Inc. DBA Nexelus personnel can push or make changes to production code.	Inspected the Software Development Life Cycle Policy to determine that all changes to production environments are required to follow change control procedures, including human approval of all changes granted by an authorized owner of that environment.	No exceptions noted.
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.	Paradigm Software Technologies, Inc. DBA Nexelus has developed policies and procedures governing the system development life cycle, including documented policies for tracking, testing, approving, and validating changes.	Inspected the Software Development Life Cycle Policy to determine that the company has described the software development phases, and security control guidelines including the change control procedures to be followed for planning, testing, approving, implementing, and tracking changes.	No exceptions noted.
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software,	Paradigm Software Technologies, Inc. DBA Nexelus ensures that code changes are tested prior to implementation to ensure quality and security.	Inspected the Software Development Life Cycle Policy to determine that code changes are required to be reviewed by individuals other than the originating code author and by individuals knowledgeable in code	No exceptions noted.

	and procedures to meet its objectives.		review techniques and secure coding practices.	
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.	Paradigm Software Technologies, Inc. DBA Nexelus uses a version control system to manage source code, documentation, release labeling, and other change management tasks. Access to the system must be approved by a system admin.	Observed that the company uses Azure DevOps as its version control system. Inspected the Software Development Life Cycle to determine that the company is required to use a configuration control system.	No exceptions noted.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Paradigm Software Technologies, Inc. DBA Nexelus has implemented an Incident Response Plan that includes documenting "Lessons Learned" and "Root Cause Analysis" after incidents and sharing them with the broader engineering team to support Business Continuity/Disaster Recovery.	Inspected the Incident Response Plan to determine that the company requires the Information Security Manager to prepare a root cause report and a "lessons learned" document as part of the incident post-mortem analysis.	No exceptions noted.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Paradigm Software Technologies, Inc. DBA Nexelus has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company.	Inspected the Incident Response Plan to determine that the company requires the DevOps, HR & Facilities, and Security teams to coordinate in executing a response to identified security threats.	No exceptions noted.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Paradigm Software Technologies, Inc. DBA Nexelus performs backups daily and retains them in accordance with a predefined schedule in the Backup Policy.	Inspected the Backup Policy to determine that the company is required to perform daily data backups using an automated process that backs up all data to a separate region in the same country.	No exceptions noted.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Paradigm Software Technologies, Inc. DBA Nexelus utilizes multiple availability zones to replicate production data across different zones.	Inspected the Backup Policy to determine that the company is required to implement an automated process that backs up all data to a separate region in the same country.	No exceptions noted.

CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Paradigm Software Technologies, Inc. DBA Nexelus has a defined backup policy that establishes the requirements for backup information, software, and systems.	Inspected the Backup Policy to determine that the company has documented the requirements for establishing backup of data and systems.	No exceptions noted.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Paradigm Software Technologies, Inc. DBA Nexelus has an established Incident Response Plan that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents and annual testing.	Inspected the Incident Response Plan to determine that the process of establishing and executing the incident response plan along with the roles and responsibilities of the ISM and other key personnel has been described for responding to incidents.	No exceptions noted.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Paradigm Software Technologies, Inc. DBA Nexelus has an established Disaster Recovery Plan that outlines roles and responsibilities and detailed procedures for recovery of systems.	Inspected the Disaster Recovery Plan to determine that the disaster recovery procedure and the roles and responsibilities of the CTO for the implementation of recovery procedures have been defined by the company.	No exceptions noted.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Paradigm Software Technologies, Inc. DBA Nexelus has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	Inspected the Risk Assessment Policy to determine that the company has defined risk assessment processes and remediation strategies for identified risks based on their risk levels.	No exceptions noted.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Paradigm Software Technologies, Inc. DBA Nexelus has implemented an Incident Response Plan that includes creating, prioritizing, assigning, and tracking follow-ups to completion and lend support to Business Continuity/Disaster Recovery.	Inspected the Incident Response Plan to determine that the company has defined the incident response process, which requires conducting a post-mortem that includes root cause analysis and documentation of any lessons learned.	No exceptions noted.

CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Paradigm Software Technologies, Inc. DBA Nexelus has a defined Business Continuity Plan that outlines the proper procedures to respond, recover, resume, and restore operations following a disruption.	Inspected the Business Continuity Plan to determine that the company has established a Business Continuity Plan that defines the procedures to recover the company's data and operations following a disruption in conjunction with the Disaster Recovery Plan.	No exceptions noted.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Paradigm Software Technologies, Inc. DBA Nexelus conducts annual BCP/DR tests and documents according to the BCDR Plan.	Inspected the Business Continuity Plan to determine that the company is required to simulate and test the Business Continuity Plan at least once a year. Inspected the Disaster Recovery Plan to determine that the company is required to test the Disaster Recovery Plan at least annually.	No exceptions noted.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	Paradigm Software Technologies, Inc. DBA Nexelus maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.	Inspected the Vendor Management Policy to determine that the company is required to maintain vendor inventory and vendor contracts that must include confidentiality and privacy commitments.	No exceptions noted.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	Paradigm Software Technologies, Inc. DBA Nexelus has a defined vendor management policy that establishes requirements of ensuring third-party entities meet the organization's data preservation and protection requirements.	Inspected the Vendor Management Policy to determine that the company requires its vendors to maintain the integrity, security, and privacy of the company's data.	No exceptions noted.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	Paradigm Software Technologies, Inc. DBA Nexelus maintains a directory of its key vendors, including their compliance reports. Critical vendor compliance reports are reviewed annually.	Inspected the Vendor Management Policy to determine that the company may choose to audit IT vendors and partners to ensure compliance with applicable security policies, as well as legal, regulatory, and contractual obligations.	No exceptions noted.