SOC 2 Type 1 Report

Upollo Pty Ltd.

November 8, 2023

A Type 1 Independent Service Auditor's Report on Controls Relevant to Security

AICPA
SOC
aicpa.org/soc4so
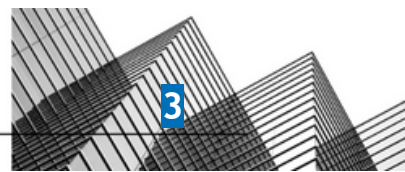SOC for Service Organizations | Service Organizations

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

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

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

2

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

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

PRESCIENT
ASSURANCE

3

SECTION 1

Management's Assertion

Management's Assertion

We have prepared the accompanying description of Upollo Pty Ltd.'s system as of October 1, 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 Upollo Pty Ltd.'s system that may be useful when assessing the risks arising from interactions with Upollo Pty Ltd.'s system, particularly information about system controls that Upollo Pty Ltd. 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 set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

Upollo Pty Ltd. 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 Upollo Pty Ltd., to achieve Upollo Pty Ltd.'s service commitments and system requirements based on the applicable trust services criteria. The description presents Upollo Pty Ltd.'s controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Upollo Pty Ltd.'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 Upollo Pty Ltd., to achieve Upollo Pty Ltd.'s service commitments and system requirements based on the applicable trust services criteria. The description presents Upollo Pty Ltd.'s controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Upollo Pty Ltd.'s controls.

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

A. The description presents Upollo Pty Ltd.'s system that was designed as of October 1, 2023, in accordance with the description criteria.
B. The controls stated in the description were suitably designed as of October 1, 2023, to provide reasonable assurance that Upollo Pty Ltd.'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 Upollo Pty Ltd.'s controls as of that date.

DocuSigned by:

Cayden Meyer

7FEE69A42D974CB...

Cayden Meyer
Founder and CEO of Upollo Pty Ltd.

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

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

PRESCIENT
ASSURANCE

5
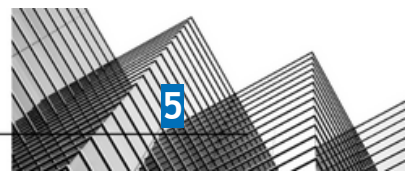
SECTION 2

Independent Service Auditor's Report

PRESCIENT

ASSURANCE
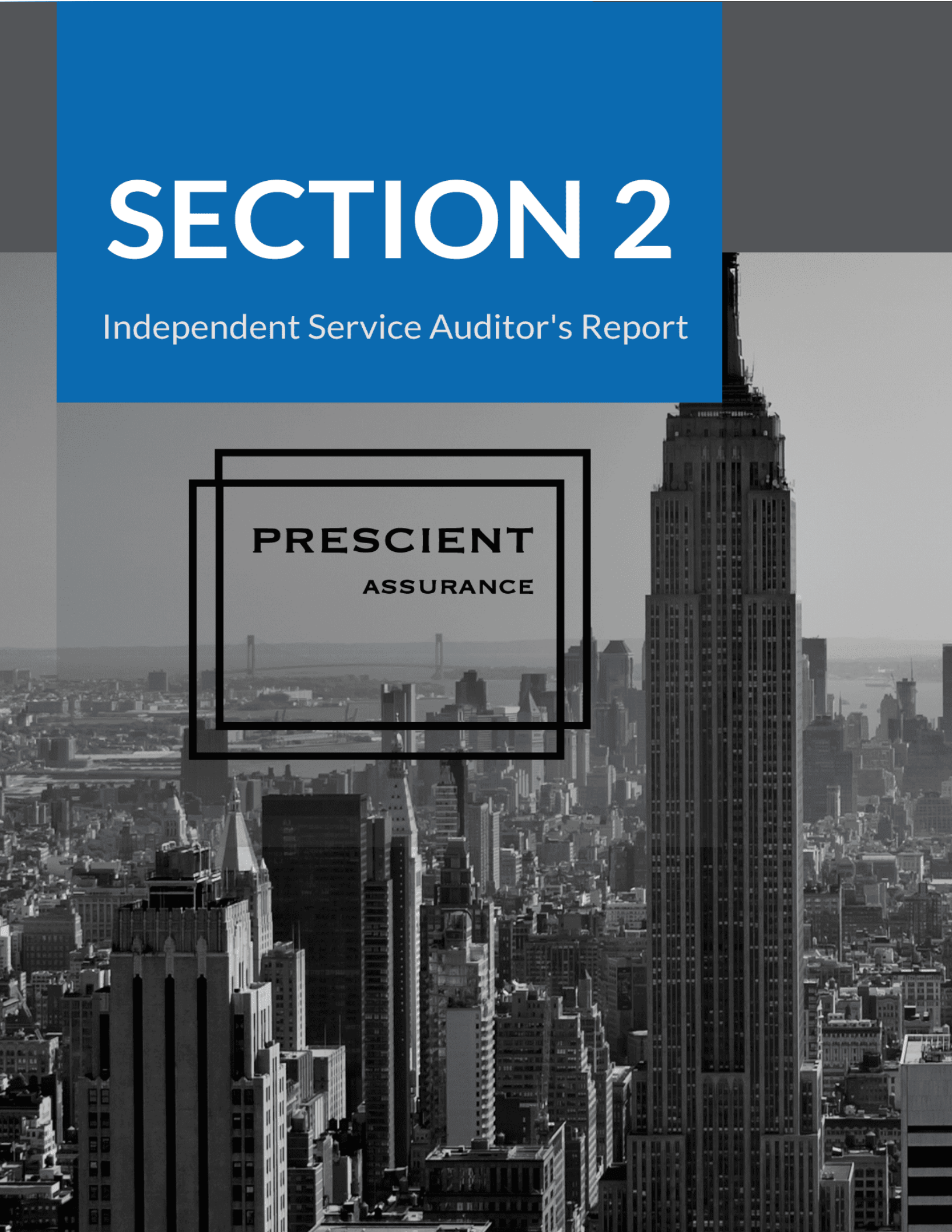
Independent Service Auditor's Report

To: Upollo Pty Ltd.

Scope

We have examined Upollo Pty Ltd.'s ("Upollo Pty Ltd.") accompanying description of its system as of October 1, 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 October 1, 2023, to provide reasonable assurance that Upollo Pty Ltd.'s service commitments and system requirements were achieved based on the trust services criteria relevant to Security set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.*

Upollo Pty Ltd. 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 Upollo Pty Ltd., to achieve its service commitments and system requirements based on the applicable trust services criteria. The description presents Upollo Pty Ltd.'s controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Upollo Pty Ltd.'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 Upollo Pty Ltd., to achieve Upollo Pty Ltd.'s service commitments and system requirements based on the applicable trust services criteria. The description presents Upollo Pty Ltd.'s controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Upollo Pty Ltd.'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

Upollo Pty Ltd. 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 Upollo Pty Ltd.'s service commitments and system requirements were achieved. In Section 1, Upollo Pty Ltd. has provided the accompanying assertion titled "Management's Assertion of Upollo Pty Ltd." (assertion) about the description and the suitability of design of controls stated therein. Upollo Pty Ltd. 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.

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

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

PRESCIENT
ASSURANCE

7

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.

PRESCIENT
ASSURANCE

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

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

8

Opinion

In our opinion, in all material respects:

A. The description presents Upollo Pty Ltd.'s system that was designed as of October 1, 2023 in accordance with the description criteria.
B. The controls stated in the description were suitably designed as of October 1, 2023, to provide reasonable assurance that Upollo Pty Ltd.'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 Upollo Pty Ltd.'s controls as of that date.

Restricted Use

This report is intended solely for the information and use of Upollo Pty Ltd., user entities of Upollo Pty Ltd.'s system as of October 1, 2023, business partners of Upollo Pty Ltd. 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.

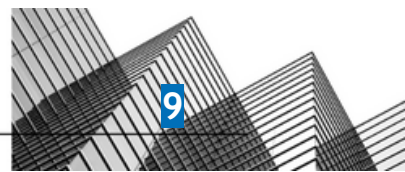Prescient Assurance LLC

DocuSigned by:

John D Wallace

F5ADFA3569EA450

John D. Wallace, CPA
Chattanooga, TN
November 8, 2023

PRESCIENT
ASSURANCE

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

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

9

SECTION 3

System Description

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

Upollo is on a mission to help subscription businesses grow. They convert, retain and expand users for subscription businesses by understanding who is ready, why they are ready and how to convert that into a successful outcome.

They have customers across the globe and add millions in additional revenue each year to their customers.

Their growth platforms offer AI based opportunity scoring, opportunity enrichment, account sharing, multi-accounting detection and more.

DC 2: The Principal Service Commitments and System Requirements

Upollo Pty Ltd. designs its processes and procedures to meet the objectives of the Upollo platform. Those objectives are based on the service commitments that Upollo Pty Ltd. makes to user entities, the laws and regulations that govern the provision of services, and the financial, operational, and compliance requirements that Upollo Pty Ltd. has established for the services. The platform of Upollo Pty Ltd. is subject to the federal and state privacy and security laws and regulations in the jurisdictions in which Upollo Pty Ltd. 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 offering provided online. The Privacy Policy and Terms and Conditions can be found at Upollo Pty Ltd.. Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of the platform that 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 at rest and 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.

Upollo Pty Ltd. establishes systems and operational requirements that support the achievement of service commitments, relevant laws and regulations, and other security and privacy requirements. Such

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

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

11

requirements are communicated in Upollo Pty Ltd.'s Terms and Conditions (https://upollo.ai/terms) 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 Sample Support SLA

Severity	Response Time
Severity 1, Critical: 1. Access to Upollo Pty Ltd. platform in production is down. 2. Production APIs/microservice is down or severely impacted such that routine operation is impossible. More than 50% of containers and hosts in the application are in an unhealthy state.	Within 1 Hour during business hours
Severity 2, High: 1. Production issue where the system is functioning but in degraded or restricted capacity. 2. At least 25% of containers and hosts in the application are in an unhealthy state.	Within 2 Hours during business hours
Severity 3, Medium: Production issue where minor functionality is impacted or a development issue.	Within 2 business days
Severity 4, Low: Request for information with no impact to business operations	Within 5 business days

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

PRESCIENT
ASSURANCE

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

12

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

3.1 Primary Infrastructure

Primary Infrastructure		
Managed Infrastructure Provider	**Type**	**Purpose**
GCP	Load Balancers Cloud Run API Gateway	Allow for the servicing, processing, and directing of network traffic and data.
GCP	IAM	Allow management of user accounts internally.
GCP	WAF Cloud Armor	Protects the network traffic against denial of service and web attacks.
GCP	Cloud Storage Buckets	Cloud-hosted storage solution with encryption capabilities used to store objects created during development and business operations i.e. artifacts, backups, and authentication files.
GCP	Cloud Logging Audit Logs	Used for monitoring network resources, alerting based on preconfigured metric-based alarms, and application logs for all of the services.
GCP	Firebase Authentication	User for user management and access control
GCP	Artifact Registry	Repository for all product containers
Google Workspace	User Authentication	Used for Upollo user management and access control
Github	Codebase & CICD/Pipeline	Codebase used for versioning, testing, and deployment of changes to the environments.
Linear	Issue Tracking	Linear is an issue tracking tool that streamlines software projects, sprints, tasks, and bug tracking.
Drata Compliance Automation Platform	Client/Dashboard	Monitors infrastructure for common vulnerabilities and aids in ensuring compliance.
GCP	Bigtable	Transactional database for customer data
GCP	BigQuery	Analytics

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

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

13

Primary Infrastructure		
Managed Infrastructure Provider	**Type**	**Purpose**
GCP	CloudSQL	Transactional database for customer data
GCP	Cloud Pub/Sub	Cross service communication
GCP	Cloud Tasks	Task Queues

3.2 Primary Software

Primary Software		
Software	**Type**	**Purpose**
React	UI Logic	Web application framework used to power the web application/sync configuration tool

3.3 People

Upollo Pty Ltd. has a staff of approximately 9 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 Upollo Pty Ltd.'s developers and maintains the cloud infrastructure that the Upollo Pty Ltd. product runs on.
- **Security:** Employees or outsourced Individuals responsible for providing ongoing security to Upollo Pty Ltd.'s assets (people, application, infrastructure and data).
- **IT and Customer Support:** Individuals responsible for providing timely resolution of issues and problems.

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

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

14

3.4 Security Processes and Procedures

The company employs a set of procedures in order 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:

- Upollo Pty Ltd. backend application runs in GCP utilizing the Storage and Database services.
- Each platform instance (production, customer test, Quality Assurance "QA") is contained within a separate Google Cloud Project. The project 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 utilizing Secure Shell ("SSH") protocol. Access is granted on a project and component within each project (e.g., pods, storage, and database) basis.
- Data is persisted in Bigtable, Postgres and BigQuery. These systems utilize Advanced Encryption Standard ("AES") 256 encrypted disks for all data stored at rest.
- 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 Executive, 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 intranet services, 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 three major types of data used by Upollo Pty Ltd.: Configuration Data, Customer Data, and Log Data. Other types of data include: Service data, Data in transit, Data at rest, and Usernames and Passwords.

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

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

15

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 a combination of Google Cloud Secrets Manager, Terraform and Github, according to relevant access restrictions, 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.
Customer Data: Data owned by Upollo Pty Ltd.'s customers that is copied from edge compute devices to web-based software application	Customer Data is stored in GCP, specifically Bigtable, Postgres and BigQuery. It is encrypted both in-transit and at-rest and is protected with daily backups/versioning controls. Only authorized Upollo Pty Ltd. operators are permitted to access customer data and only for 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 Upollo Pty Ltd. operators to monitor the health of the system and track down any issues. Log data may be stored by vendors that Upollo Pty Ltd. has entrusted for purposes like indexing, monitoring, and trending. Log data is retained for 365 days.
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, Upollo Pty Ltd. 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, whenever supported by the clients.
Data at rest	Data at rest in Upollo Pty Ltd.'s production network is encrypted using industry-standard 256-bit Advanced Encryption Standard (AES256), which applies to all types of data at rest within Upollo Pty Ltd.'s systems— relational databases, file stores, database backups, etc.
Usernames and passwords	Upollo Pty Ltd. encrypts customer usernames and passwords used to access the Upollo Pty Ltd. platform using cryptographic hash functions.

3.6 Third Party Access

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

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

PRESCIENT
ASSURANCE

16

Vendors, business partners, and others (third parties) often store, process, and transmit sensitive data or otherwise access a service organization's system. These third parties may provide components of the system. Service organization management may need to describe the components of the system provided by such third parties. Such disclosures may include, for example, the nature of the third parties' access and connectivity to the service organization's system.

Third Party Access	
Name of Third Party/ Vendor	Type of Access and Connectivity to Upollo Pty Ltd. 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

Upollo Pty Ltd. 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. Upollo Pty Ltd. has also instituted a number of technical controls to prevent and disincentivize illegal and unethical actions by Upollo Pty Ltd. employees. These controls include but are not limited to:

- Logging all traffic within Upollo Pty Ltd. 's 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 Upollo Pty Ltd. management.

PRESCIENT
ASSURANCE

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

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

17

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

5.2 Commitment to Competence

Upollo Pty Ltd.'s management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for jobs and how those levels translate into the requisite skills and knowledge.

Specific control activities that 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

Upollo Pty Ltd.'s 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 Upollo Pty Ltd. has instituted a number of processes:

- Weekly "all hands" meetings for employees to voice their blocks, successes, and concerns.
- A rigorous QA program ensures that development on the Upollo Pty Ltd. 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 Upollo Pty Ltd. has a simple organizational structure. Employees report directly to the CEO who ultimately provides direction. Upollo Pty Ltd. has clearly defined job descriptions and as the organization grows, we have in place roles and responsibilities which will allow for dissemination of managerial responsibilities as necessary. Upollo Pty Ltd. 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

Upollo Pty Ltd. consistently strives to hire and retain the most qualified individuals for the job. To meet this goal, Upollo Pty Ltd. has in place onboarding requirements and a Human Resource Security Policy which cover employee security training, performance reviews, competency assessments, and the terms of employment.

Specifically, Upollo Pty Ltd. has the following controls in place:

- Annual Performance Reviews

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

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

18

- Annual employee security training
- New employees are required to sign a non-disclosure or confidentiality agreement.
- Clearly defined disciplinary process
- A "New Employee Checklist" which is given to new hires and is fully accessible to all Upollo Pty Ltd. employees

Lastly, Upollo Pty Ltd. 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

Upollo Pty Ltd. uses an internal security team whose responsibilities fulfill the roles of full-time dedicated System Security Manager (ISSM) and full-time dedicated Information System Security Officer (ISSO) who are responsible for 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 Upollo Pty Ltd. 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

Upollo Pty Ltd. has adopted the following Security Policies:

1. Acceptable Use Policy
2. Asset Management Policy
3. Data Classification Policy
4. Data Protection Policy
5. Data Retention Policy
6. Encryption Policy
7. Incident Response Plan
8. Information Security Policy
9. Password Policy
10. Physical Security Policy
11. Responsible Disclosure Policy

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

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

19

12. Risk Assessment Policy
13. Software Development Life Cycle Policy
14. System Access Control Policy
15. Vendor Management Policy
16. Vulnerability Management Policy

5.8 Personnel Security

Upollo Pty Ltd. 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.
- Upon hire and annually thereafter security awareness training is completed by all Upollo Pty Ltd. employees.
- Employees are directed to report any potential security incidents to the IT Manager.

Violations of Upollo Pty Ltd. security policies have clearly defined repercussions.

5.9 Physical Security and Environmental Controls

Upollo Pty Ltd. is a fully remote company with no centralized headquarters or physical network. Because of this, physical and environmental security procedures have been 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 BYOD policy, our Business Continuity and Disaster Recovery plan, and our Information Security Policy.

5.10 Change Management

Upollo Pty Ltd.'s 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 Upollo Pty Ltd.'s 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.

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

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

20

- Documentation of all emergency changes and subsequent review.
- A rollback process for unsuccessful deployments must be in place.

5.11 System Monitoring

Upollo Pty Ltd. uses a combination of services to monitor its network and systems. These include GCP Cloud Logging, GCP Monitoring, GCP Tracing, the Drata Client, Web Application Firewall (WAF), and GCP Audit Logs.

- GCP Cloud Logging: Used for monitoring of network usage, availability, and overall performance and health of network resources. Also logs metrics for fine-tuning alarms and alerts as usage data is received. GCP Cloud Logging is used in conjunction with GCP Audit Logs to monitor for failed and successful authorization attempts.
- GCP Monitoring: Used for monitoring and alerting of key resources
- GCP Tracing: Used for monitoring latency and performance
- 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 GCP resources for potential configuration vulnerabilities, and tracking necessary patches/updates.
- GCP Audit Logs: Used to log actions taken by users and services within our GCP account.
- WAF: Provide metrics regarding attempted and successful requests to the application.

Upollo Pty Ltd. is constantly striving to improve our security monitoring capabilities and uses GCP's documentation on best practices to inform the alarming and logging measures we take.

5.12 Incident Management

Upollo Pty Ltd.'s incident response procedures are detailed in its Incident Response Plan. Our primary goals will be to investigate, contain any exploitations, eradicate any threats, recover Upollo Pty Ltd. systems, and remediate any vulnerabilities. Throughout this process thorough documentation will be required as well as a post-mortem report.

Specific steps that Upollo Pty Ltd. will take are:

- The Security Manager will manage the incident response effort.
- All correspondence will take place within the "Incident Management" Upollo Pty Ltd. Google Chat channel.
- A recurring Incident Response Meeting will be held at regular intervals until the incident is resolved.
- Upollo Pty Ltd. will inform all necessary parties of the incident without undue delay.

5.13 Data Backup and Recovery

Upollo Pty Ltd. uses automated systems to ensure full backup recovery of its database. Access to Upollo Pty Ltd. databases is heavily restricted using role-based authorization controls.

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

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

21

5.14 System Account Management

Upollo Pty Ltd. 's access management procedures are documented in its System Access Control Policy. Upollo Pty Ltd. uses Role-based authorization to control access to its network infrastructure. Upollo Pty Ltd. uses the principle of least privilege to determine the type and level of access to grant users. A number of standards are in place which Upollo Pty Ltd. uses when granting access to its systems:

- Technical access to Upollo Pty Ltd. networks must be formally documented.
- Background checks will be performed on domestic persons granted access to Upollo Pty Ltd. networks.
- Only authorized Upollo Pty Ltd. employees and third parties working off a signed contract or statement of work, with a business need, shall be granted access to the Upollo Pty Ltd. production network

With regards to access provisioning, Upollo Pty Ltd. uses the following controls:

- New employees and/or contractors are not to be granted access to any Upollo Pty Ltd. production systems until after they have completed all HR on-boarding tasks, which includes issuing a background check (as applicable, results to be received within 30 days), review and signing of all company policies, signing of Upollo Pty Ltd.'s 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 72 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 72 hours of notification being given to the IT Manager.

5.15 Risk Management Program

5.15.1 Data Classification

Upollo Pty Ltd. has four classifications for the data it uses, processes, and produces. The classifications are:

- Confidential
- Restricted
- Public
- Internal Use

Confidential data is sensitive business information and the level of protection is dictated internally by Upollo Pty Ltd. Examples include:

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

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

22

- PII
- Customer Data
- Upollo Pty Ltd. financial and banking data
- Incident Reports
- Risk Assessment Reports
- Technical Vulnerability Reports
- Secret and Private Keys
- Source Code

Restricted data is defined as proprietary information requiring thorough protection. Access to this data is restricted to employees on a "need-to-know" basis. Approval is required for distribution. Examples include:

- Internal Policies
- Legal Documents
- Internal Reports
- Slack Messages
- Emails
- Contracts
- Bug Reports and Maintenance

Public data is defined as: Documents intended for public consumption which can be freely distributed outside of Upollo Pty Ltd. Examples include:

- Marketing Materials
- Product Descriptions
- Release Notes
- External Facing Policies

Internal Use data is information originating within or owned by Upollo Pty Ltd. or entrusted to it by others. Internal Use information may be shared with authorized employees, contractors, and business partners who have a business need, but may not be released to the general public, due to the negative impact it might have on the company's business interests. By default, all data that is not explicitly classified as Restricted, Confidential, or Public data should be treated as Internal Use data.

5.15.2 Risk Management Responsibilities

Upollo Pty Ltd.'s Risk Assessment Policy details the primary responsibilities.

Role	Responsibility
CEO	Ultimately responsible party for the acceptance and/or treatment of any risks to the organization.

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

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

23

Engineering Lead	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.

5.15.3 Risk Management Program Activities

On a practical level, Upollo Pty Ltd.'s Risk Management process involves 3 stages:

- Identification of risks
- Assessment of their potential impact
- Upollo Pty Ltd.'s 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 Upollo Pty Ltd.. Likelihood can be assessed as not likely, somewhat likely, or very likely. Impact can be assessed as not impactful, somewhat impactful, and very impactful. These factors together will give an overall risk ranking.

Upollo Pty Ltd.'s stance towards any given risk is based on the assessment described above. Where Upollo Pty Ltd. chooses a risk response other than "Accept," it shall develop a Risk Treatment Plan. Upollo Pty Ltd.'s stance will fall into one of the following categories:

- Mitigate: Upollo Pty Ltd. may take actions or employ strategies to reduce the risk.
- Accept: Upollo Pty Ltd. 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: Upollo Pty Ltd. 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 Upollo Pty Ltd., or insurance may be appropriate for protection against financial loss.
- Eliminate: The risk may be such that Upollo Pty Ltd. could decide to cease the activity or to change it in such a way as to end the risk.

Upollo Pty Ltd.'s details our key business processes and critical services.

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

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

PRESCIENT
ASSURANCE

24

5.16 Risk Assessment

Upollo Pty Ltd.'s 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 Upollo Pty Ltd.'s business objectives.
- Potential impact to Upollo Pty Ltd. customers or vendors.

Upollo Pty Ltd. uses Risk Treatment Plans for any response to risks other than "Accept."

5.17 Risk Analysis

Upollo Pty Ltd.'s Risk Analysis Method is as follows:

	Risk = Likelihood * Impact	Likelihood		
		Very likely: 3	Somewhat likely: 2	Not likely: 1
Impact	Very impactful: 3	9	6	3
	Somewhat impactful: 2	6	4	2
	Not impactful: 1	3	2	1

Risk Level	Risk Description
Low (1–2)	A threat event could be expected to have a limited adverse effect on organizational operations, mission capabilities, assets, individuals, customers or other organizations.
Moderate (3–6)	A threat event could be expected to have a serious adverse effect on organizational operations, mission capabilities, assets, individuals, customers or other organizations
High (7–9)	A threat event could be expected to have a severe adverse effect on organizational operations, mission capabilities, assets, individuals, customers or other organizations.

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

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

25

Impact Level	Impact Description
Not impactful (1)	A threat event could be expected to have a limited adverse effect, meaning: degradation of mission capability yet primary functions can still be performed; minor damage; minor financial loss; or range of effects is limited to some cyber resources but no critical resources.
Somewhat impactful (2)	A threat event could be expected to have a serious adverse effect, meaning: significant degradation of mission capability yet primary functions can still be performed at a reduced capacity; minor damage; minor financial loss; or range of effects is significant to some cyber resources and some critical resources.
Very impactful (3)	A threat event could be expected to have a severe or catastrophic adverse effect, meaning: severe degradation or loss of mission capability and one or more primary functions cannot be performed; major damage; major financial loss; or range of effects is extensive to most cyber resources and most critical resources.

Likelihood Level	Likelihood Description
Not likely (1)	Adversary is unlikely to initiate a threat event; non-adversarial threat event (e.g., nature, error, accident) is unlikely to occur; or threat is unlikely to have adverse impacts.
Somewhat likely (2)	Adversary is somewhat unlikely to initiate a threat event; non-adversarial threat event (e.g., nature, error, accident) is somewhat unlikely to occur; or threat is somewhat unlikely to have adverse impacts.
Very likely (3)	Adversary is highly likely to initiate a threat event; non-adversarial threat event (e.g., nature, error, accident) is highly likely to occur; or threat is highly likely to have adverse impacts.

5.18 Risk Response

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

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

PRESCIENT
ASSURANCE

26

In accordance with Upollo Pty Ltd.'s , risks will be prioritized and mapped according to the descriptions listed above. The following responses to risk should be employed. Where Upollo Pty Ltd. chooses a risk response other than "Accept," it shall develop a risk treatment plan.

- **Mitigate:** Upollo Pty Ltd. may take actions or employ strategies to reduce the risk.
- **Accept:** Upollo Pty Ltd. 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:** Upollo Pty Ltd. 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 Upollo Pty Ltd., or insurance may be appropriate for protection against financial loss.
- **Eliminate:** The risk may be such that Upollo Pty Ltd. could decide to cease the activity or to change it in such a way as to end the risk.

5.19 Integration with Risk Assessment

Upollo Pty Ltd. 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 Upollo Pty Ltd. to develop specialized controls. Upollo Pty Ltd. takes into account all relevant factors; contractual, legal, and regulatory when designing these controls. Upollo Pty Ltd.'s Head of Engineering has the final say on the design and implementation of these controls.

In general, Upollo Pty Ltd.'s Risk Assessment procedure is still applicable to risks inherent in Upollo Pty Ltd.'s commitments and contractual responsibilities and should be applied to determining the severity of risks.

5.20 Information and Communications Systems

Upollo Pty Ltd. uses Google Chat for restricted internal communications. Upollo Pty Ltd. also uses video conferencing tools and a company gmail for both internal and external communications.

For workflow, project management, and sharing of internal documents Upollo Pty Ltd. uses Linear and Google Workspace.

5.20.1 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.

5.21 Monitoring Controls

Upollo Pty Ltd. takes a dual approach to continuous monitoring using both internal monitoring and relying on third parties.

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

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

27

5.21.1 Internal Monitoring

Upollo Pty Ltd. has a highly interconnected business process allowing for visibility and insight by management into the operations of each department. Corrective action is initiated through direct conference calls. Within departments, code reviews and Upollo Pty Ltd.'s quality assurance program help ensure internal controls are being followed and implemented.

5.21.2 Third Party Monitoring

Upollo Pty Ltd. contracts a third party to perform annual penetration tests and uses the Drata client to monitor for new vulnerabilities. The process for reporting of any deficiencies with regards to Upollo Pty Ltd. policies and procedures is clearly spelled out in each relevant policy.

DC 6: Complementary User Entity Controls (CUECs)

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

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 Upollo Pty Ltd.
- User entities are responsible for notifying Upollo Pty Ltd. 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 Upollo Pty Ltd. 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 Upollo Pty Ltd. services.
- User entities are responsible for immediately notifying Upollo Pty Ltd. of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.

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:

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

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

28

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 Upollo Pty Ltd. 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 Upollo Pty Ltd.'s 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 Upollo Pty Ltd..
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 Upollo Pty Ltd..

DC 7: Complementary Subservice Organization Controls (CSOCs)

Upollo Pty Ltd. uses GCP as a subservice organization for data center colocation services. Upollo Pty Ltd.'s 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 GCP.

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 GCP related to physical security and environmental protection, as well as backup, recovery, and redundancy controls related to availability. GCP physical security controls mitigate the risk of fires, power loss, climate, and temperature variabilities. Management of Upollo Pty Ltd. receives and reviews the GCP SOC 2 report annually. In addition, through its operational activities, Upollo Pty Ltd. management monitors the services performed by GCP 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 GCP management.

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

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

PRESCIENT
ASSURANCE

29

It is not feasible for the criteria related to the System to be achieved solely by Upollo Pty Ltd..
Therefore, each user entity's internal control must be evaluated in conjunction with Upollo Pty Ltd.'s
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.
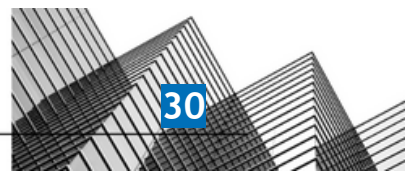
Criteria	Complementary Subservice Organization Controls
CC6.4	GCP is responsible for restricting data center access to authorized personnel.
CC6.4	GCP is responsible for the 24/7 monitoring of data centers by closed circuit cameras and security personnel.
CC7.2	GCP is responsible for the installation of fire suppression and detection, and environmental monitoring systems at the data centers.
CC7.2	GCP is responsible for protecting data centers against disruption in power supply to the processing environment by an uninterruptible power supply.
CC7.2	GCP 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: Disclosure of Significant Changes in Last 1 Year

No significant changes have occurred in the last 1 year.

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

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

PRESCIENT
ASSURANCE

30

SECTION 4

Applicable Trust Services Criteria and Related Control Activities

Trust ID	COSO Principle	Control Description
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	Upollo 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.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	Upollo has a formal Code of Conduct approved by management and accessible to all employees. All employees must accept the Code of Conduct upon hire.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	Upollo's new hires are required to pass a background check as a condition of their employment.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	Upollo has established a Data Protection Policy and requires all employees to accept it upon hire. Management monitors employees' acceptance of the policy.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	Upollo 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.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	Upollo requires its contractors to read and accept the Code of Conduct, read and accept the Acceptable Use Policy, and pass a background check.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Upollo engages with third-party to conduct vulnerability scans of the production environment regularly. Results are reviewed by management and high priority findings are tracked to resolution.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Upollo 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.
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.
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.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The company's board members have sufficient expertise to oversee management's ability to design, implement and operate information security controls. The board engages third-party information security experts and consultants as needed.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Management reviews security policies on an annual basis.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Upollo engages with third-party to conduct penetration tests of the production environment at least annually. Results are

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

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

PRESCIENT ASSURANCE

32

		reviewed by management and high priority findings are tracked to resolution.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Upollo conducts a Risk Assessment at least annually.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The company's board of directors has a documented charter that outlines its oversight responsibilities for internal control.
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.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Upollo reviews its organizational structure, reporting lines, authorities, and responsibilities in terms of information security on an annual basis.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Upollo 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.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Upollo requires its contractors to read and accept the Code of Conduct, read and accept the Acceptable Use Policy, and pass a background check.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	All Upollo 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 Upollo.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Upollo'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.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Upollo has established training programs for privacy and information security to help employees understand their obligations and responsibilities to comply with Upollo'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.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Upollo has a formal Code of Conduct approved by management and accessible to all employees. All employees must accept the Code of Conduct upon hire.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Upollo evaluates the performance of all employees through a formal, annual performance evaluation.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Upollo has a defined vendor management policy that establishes requirements of ensuring third-party entities meet the organization's data preservation and protection requirements.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Upollo's new hires are required to pass a background check as a condition of their employment.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Upollo has established training programs for privacy and information security to help employees understand their obligations and responsibilities to comply with Upollo's

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

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

PRESCIENT
ASSURANCE

33

		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.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Upollo has a formal Code of Conduct approved by management and accessible to all employees. All employees must accept the Code of Conduct upon hire.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Upollo 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.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Upollo evaluates the performance of all employees through a formal, annual performance evaluation.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Upollo ensures that file integrity monitoring (FIM) software is in place to detect whether operating system and application software files have been tampered with.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Upollo has an established policy and procedures that governs the use of cryptographic controls.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Upollo performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Upollo conducts continuous monitoring of security controls using Drata, and addresses issues in a timely manner.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Upollo authorizes access to information resources, including data and the systems that store or process customer data, based on the principle of least privilege.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Upollo maintains an accurate architectural diagram to document system boundaries to support the functioning of internal control.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Upollo has a defined policy that establishes requirements for the proper management and tracking of organizational assets.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Upollo conducts a Risk Assessment at least annually.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Upollo identifies, inventories, classifies, and assigns owners to IT assets.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Upollo has a defined Information Security Policy that covers policies and procedures to support the functioning of internal control.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Upollo 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.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Upollo 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.

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

PRESCIENT
ASSURANCE

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

34

CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Upollo 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.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Upollo has established a Data Protection Policy and requires all employees to accept it upon hire. Management monitors employees' acceptance of the policy.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Upollo has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Upollo provides a process to employees for reporting security, confidentiality, integrity, and availability features, incidents, and concerns, and other complaints to company management.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Upollo 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.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Upollo has established training programs for privacy and information security to help employees understand their obligations and responsibilities to comply with Upollo'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.	Upollo conducts continuous monitoring of security controls using Drata, and addresses issues in a timely manner.
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.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Upollo 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.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Upollo 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.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Upollo has a formal Code of Conduct approved by management and accessible to all employees. All employees must accept the Code of Conduct upon hire.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	Upollo tracks security deficiencies through internal tools and closes them within an SLA that management has pre-specified.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	Upollo 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.

PRESCIENT
ASSURANCE

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

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

35

CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	Upollo communicates system changes to customers that may affect security, availability, processing integrity, or confidentiality.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	Upollo has a defined vendor management policy that establishes requirements of ensuring third-party entities meet the organization's data preservation and protection requirements.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	Upollo 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.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	Upollo maintains a Terms of Service that is available to all external users and 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.	Upollo has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	Upollo maintains a Privacy Policy that is available to all external users and internal employees, and it details the company's confidentiality and privacy commitments.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	Upollo 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.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	Upollo's security commitments are communicated to external users, as appropriate.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	Upollo maintains a directory of its key vendors, including their compliance reports. Critical vendor compliance reports are reviewed annually.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	Upollo provides a process to external users for reporting security, confidentiality, integrity, and availability failures, incidents, concerns, and other complaints.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	Upollo maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	Upollo engages with third-party to conduct vulnerability scans of the production environment regularly. Results are reviewed by management and high priority findings are tracked to resolution.
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	Upollo 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.
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	Upollo 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.

PRESCIENT
ASSURANCE

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

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

36

CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	Upollo conducts a Risk Assessment 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.	Upollo conducts a Risk Assessment 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.	Upollo maintains a directory of its key vendors, including their compliance reports. Critical vendor compliance reports are reviewed 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.	Upollo 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.
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.	Upollo has a defined vendor management policy that establishes requirements of ensuring third-party entities meet the organization's data preservation and protection requirements.
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.	Upollo engages with third-party to conduct vulnerability scans of the production environment regularly. Results are reviewed by management and high priority findings are tracked to resolution.
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.	Upollo's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.
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.	Upollo maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	Upollo 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.
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	Upollo conducts a Risk Assessment at least annually.
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	Upollo's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	Upollo conducts a Risk Assessment at least annually.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	Upollo reviews its organizational structure, reporting lines, authorities, 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.	Upollo maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	Upollo engages with third-party to conduct vulnerability scans of the production environment regularly. Results are reviewed by management and high priority findings are tracked to resolution.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	Upollo has a defined vendor management policy that establishes requirements of ensuring third-party entities meet the organization's data preservation and protection requirements.

PRESCIENT ASSURANCE

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

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

37

CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	Upollo 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.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	Upollo 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.
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.	Upollo performs annual access control reviews.
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.	Upollo conducts a Risk Assessment at least annually.
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	Upollo maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.
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.	Upollo 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.
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.	Upollo engages with third-party to conduct vulnerability scans of the production environment regularly. Results are reviewed by management and high priority findings are tracked to resolution.
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.	Upollo 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.
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.	Upollo 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.
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.	Upollo maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.
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.	Upollo 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.
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.	Upollo has identified an incident response team that quantifies and monitors incidents involving security, 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.	Upollo engages with third-party to conduct vulnerability scans of the production environment regularly. Results are reviewed by management and high priority findings are tracked to resolution.
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.	Upollo 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.

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

PRESCIENT
ASSURANCE

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

38

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.	Upollo's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.
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.	Upollo 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.
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.	Upollo 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.
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.	Upollo 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.
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.	Upollo conducts a Risk Assessment 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.	Upollo 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.
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Upollo 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.
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Upollo reviews its organizational structure, reporting lines, authorities, and responsibilities in terms of information security on an annual basis.
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Upollo conducts a Risk Assessment at least annually.
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Upollo 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.
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Upollo 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.
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Upollo conducts continuous monitoring of security controls using Drata, and addresses issues in a timely manner.
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Upollo's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Upollo engages with third-party to conduct vulnerability scans of the production environment regularly. Results are reviewed by management and high priority findings are tracked to resolution.

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

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

PRESCIENT
ASSURANCE

39

CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	Upollo conducts continuous monitoring of security controls using Drata, and addresses issues in a timely manner.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	Upollo conducts a Risk Assessment at least annually.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	Upollo 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.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	Upollo 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.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	Upollo's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	Upollo engages with third-party to conduct vulnerability scans of the production environment regularly. Results are reviewed by management and high priority findings are tracked to resolution.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	Upollo 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.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	Upollo has an established policy and procedures that governs the use of cryptographic controls.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	Upollo has established training programs for privacy and information security to help employees understand their obligations and responsibilities to comply with Upollo'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.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	Upollo 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.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	Upollo authorizes access to information resources, including data and the systems that store or process customer data, based on the principle of least privilege.
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.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Upollo provides a process to employees for reporting security, confidentiality, integrity, and availability features, incidents, and concerns, and other complaints to company management.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Upollo conducts annual BCP/DR tests and documents according to the BCDR Plan.

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

PRESCIENT
ASSURANCE

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

40

CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Upollo has a formal Code of Conduct approved by management and accessible to all employees. All 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.	Upollo has a defined Information Security Policy that covers policies and procedures to support the functioning of internal control.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Upollo 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.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Upollo 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.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Upollo has an established Disaster Recovery Plan that outlines roles and responsibilities and detailed procedures for recovery of systems.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Upollo has a defined Business Continuity Plan that outlines the proper procedures to respond, recover, resume, and restore operations following a disruption.
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.	Upollo maintains an accurate network diagram that is accessible to the engineering team and is reviewed by management on an annual basis.
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.	Upollo's application user passwords are stored using a salted password hash.
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.	Upollo ensures that a password manager is installed on all company-issued laptops.
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.	Upollo has established formal guidelines for passwords to govern the management and use of authentication mechanisms.
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.
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.
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.	Upollo has an established key management process in place to support the organization's use of cryptographic techniques.
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.	Upollo has established a Data Protection Policy and requires all employees to accept it upon hire. Management monitors employees' acceptance of the policy.

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

PRESCIENT
ASSURANCE

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

41

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.	Upollo requires two factor authentication to access sensitive systems and applications in the form of user ID, password, OTP and/or certificate.
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.	Upollo stores customer data in databases that is encrypted at rest.
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.	Username and password (password standard implemented) or SSO required to authenticate into application, MFA optional for 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.	Upollo identifies, inventories, classifies, and assigns owners to IT assets.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Users can only access the production system remotely through the use of encrypted communication systems.
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.	Upollo ensures that company-issued laptops have encrypted hard-disks.
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.
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.	Upollo 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.
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.	Upollo has a defined policy that establishes requirements for the proper management and tracking of organizational assets.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Appropriate levels of access to infrastructure and code review tools are granted to new employees within one week of their start date.
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.	Upollo has a defined policy that establishes requirements for the use of cryptographic controls.
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.
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	Upollo uses a termination checklist to ensure that an employee's system access, including physical access, is

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

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

PRESCIENT
ASSURANCE

42

	entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	removed within a specified timeframe and all organization assets (physical or electronic) are properly returned.
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.	Upollo 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.
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.
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.
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.	External users must accept the Terms of Service prior to their account being created.
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.	Upollo performs annual access control reviews.
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.	Upollo performs annual access control reviews.
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 network, production machines, network devices, and support tools requires a unique ID.
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.	External users must accept the Terms of Service prior to their account being created.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information	Role-based security is in place for internal and external users, including super admin users.

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

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

PRESCIENT
ASSURANCE

43

	assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	
CC6.3	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.
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.	Upollo 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.
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.	Upollo 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.
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.
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.	Upollo performs annual access control reviews.
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.	Upollo maintains a directory of its key vendors, including their compliance reports. Critical vendor compliance reports are reviewed annually.
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.	Upollo 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.
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.	Upollo 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.
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.	Upollo 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.

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

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

PRESCIENT
ASSURANCE

44

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.	Upollo maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.
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.	Upollo 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.
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.	Upollo has formal policies and procedures in place to guide personnel in the disposal of hardware containing sensitive data.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	SSH users use unique accounts to access production machines. Additionally, the use of the "Root" account is not allowed.
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.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Upollo ensures that all company-issued computers use a screensaver lock with a timeout of no more than 15 minutes.
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.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Upollo ensures that all connections to its web application from its users are encrypted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Upollo automatically logs users out after a predefined inactivity interval and/or closure of the internet browser, and requires users to reauthenticate
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	WAF in place to protect Upollo's application from outside threats.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Upollo requires two factor authentication to access sensitive systems and applications in the form of user ID, password, OTP and/or certificate.
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.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	No public SSH is allowed.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Upollo has established formal guidelines for passwords to govern the management and use of authentication mechanisms.
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

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

PRESCIENT
ASSURANCE

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

45

CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Upollo uses configurations that ensure only approved networking ports and protocols are implemented, including firewalls.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Upollo maintains an accurate network diagram that is accessible to the engineering team and is reviewed by management on an annual basis.
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.	Upollo uses DLP (Data Loss Prevention) software to prevent unencrypted sensitive information from being transmitted over email
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.	Upollo has established a Data Protection Policy and requires all employees to accept it upon hire. Management monitors employees' acceptance of the policy.
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.	Upollo stores customer data in databases that is encrypted at rest.
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.
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.	Upollo ensures that company-issued laptops have encrypted hard-disks.
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.	Upollo ensures that company-issued removable media devices (USB drives) are encrypted.
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.	Upollo uses encryption to protect user authentication and admin sessions of the internal admin tool transmitted over the Internet.
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.	Upollo ensures that all connections to its web application from its users are encrypted.
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.	Upollo's customer data is segregated from the data of other customers
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.	SSH users use unique accounts to access production machines. Additionally, the use of the "Root" account is not allowed.
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.	Upollo ensures that file integrity monitoring (FIM) software is in place to detect whether operating system and application software files have been tampered with.
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.	Upollo requires antivirus software to be installed on workstations to protect the network against malware.

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

PRESCIENT ASSURANCE

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

46

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.	Upollo ensures that virtual machine OS patches are applied monthly.
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.	Upollo 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.
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.	Upollo's workstations operating system (OS) security patches are applied automatically.
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.	Upollo 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.
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.	Upollo conducts continuous monitoring of security controls using Drata, and addresses issues in a timely manner.
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.	Upollo engages with third-party to conduct vulnerability scans of the production environment regularly. Results are reviewed by management 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.	When Upollo's application code changes, code reviews and tests are performed by someone other than the person who made the code change.
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.	Upollo 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.
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
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.	Upollo 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.
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.	Upollo uses logging software that sends alerts to appropriate personnel. Corrective actions are performed, as necessary, in a timely manner.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of	Upollo has infrastructure logging configured to monitor web traffic and suspicious activity. When anomalous traffic

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

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

PRESCIENT
ASSURANCE

47

	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.	activity is identified, alerts are automatically created, sent to appropriate personnel and resolved, as necessary.
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.	Upollo 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.
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
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.	Upollo engages with third-party to conduct vulnerability scans of the production environment regularly. 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.	Upollo tracks and prioritizes security deficiencies through internal tools according to their severity by an independent technical resource.
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.	Upollo does not use Root Account on Infrastructure provider
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.	Upollo is using Drata to monitor the security and compliance of its cloud infrastructure configuration
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.	Upollo's cloud infrastructure is monitored through an operational audit system that sends alerts to appropriate personnel
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.	Upollo 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.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to	Upollo has an established Incident Response Plan that outlines management responsibilities and procedures to

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

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

PRESCIENT
ASSURANCE

48

	meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	ensure a quick, effective, and orderly response to information security incidents and annual testing.
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.	Upollo tracks and prioritizes security deficiencies through internal tools according to their severity by an independent technical resource.
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.
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.	Upollo has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company.
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.	Upollo 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.
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.	Upollo 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.
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.	Upollo 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.
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.	Upollo tracks and prioritizes security deficiencies through internal tools according to their severity by an independent technical resource.
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.	Upollo 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.
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.	Upollo has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Upollo has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Upollo performs backups daily and retains them in accordance with a predefined schedule in the Backup Policy.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Upollo has a defined Business Continuity Plan that outlines the proper procedures to respond, recover, resume, and restore operations following a disruption.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Upollo ensures that incident response plan testing is performed on an annual basis.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Upollo has an established Incident Response Plan that outlines management responsibilities and procedures to

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

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

PRESCIENT
ASSURANCE

49

		ensure a quick, effective, and orderly response to information security incidents and annual testing.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Upollo 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.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Upollo 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.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Upollo tracks and prioritizes security deficiencies through internal tools according to their severity by an independent technical resource.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Upollo has an established Disaster Recovery Plan that outlines roles and responsibilities and detailed procedures for recovery of systems.
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 Upollo's application code changes, code reviews and tests are performed by someone other than the person who made the code change.
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.	Upollo ensures that code changes are tested prior to deployment to ensure quality and security.
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.	Upollo 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.
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 Upollo's application
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 Upollo personnel can push or make changes to production code.
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.	Upollo ensures that releases are approved by appropriate members of management prior to production release.
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.	Upollo has developed policies and procedures governing the system development life cycle, including documented policies for tracking, testing, approving, and validating changes.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Upollo conducts annual BCP/DR tests and documents according to the BCDR Plan.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Upollo 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.

PRESCIENT
ASSURANCE

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

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

50

CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Upollo utilizes multiple availability zones to replicate production data across different zones.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Upollo has a defined backup policy that establishes the requirements for backup information, software and systems.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Upollo maintains cybersecurity insurance to mitigate the financial impact of business disruptions.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Upollo 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.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Upollo has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Upollo has an established Disaster Recovery Plan that outlines roles and responsibilities and detailed procedures for recovery of systems.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Upollo performs backups daily and retains them in accordance with a predefined schedule in the Backup Policy.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Upollo 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.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Upollo has a defined Business Continuity Plan that outlines the proper procedures to respond, recover, resume, and restore operations following a disruption.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Upollo 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.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	Upollo maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	Upollo has a defined vendor management policy that establishes requirements of ensuring third-party entities meet the organization's data preservation and protection requirements.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	Upollo maintains a directory of its key vendors, including their compliance reports. Critical vendor compliance reports are reviewed annually.

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

PRESCIENT
ASSURANCE

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

51