



A-ALIGN



Couchdrop Limited
Type 1 SOC 2
2021



couchdrop

**REPORT ON COUCHDROP LIMITED'S DESCRIPTION OF ITS SYSTEM AND ON THE
SUITABILITY OF THE DESIGN OF ITS CONTROLS RELEVANT TO SECURITY**

**Pursuant to Reporting on System and Organization Controls 2 (SOC 2)
Type 1 examination performed under AT-C 105 and AT-C 205**

October 31, 2021

Table of Contents

SECTION 1 ASSERTION OF COUCHDROP LIMITED MANAGEMENT	1
SECTION 2 INDEPENDENT SERVICE AUDITOR’S REPORT	3
SECTION 3 COUCHDROP LIMITED’S DESCRIPTION OF ITS SAAS SYSTEM AS OF OCTOBER 31, 2021	7
OVERVIEW OF OPERATIONS.....	8
Company Background	8
Description of Services Provided	8
Principal Service Commitments and System Requirements.....	8
Components of the System.....	9
Boundaries of the System.....	12
RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION, AND MONITORING	12
Control Environment.....	12
Risk Assessment Process	13
Information and Communications Systems.....	14
Monitoring Controls	14
Changes to the System in the Last 12 Months.....	14
Incidents in the Last 12 Months	14
Criteria Not Applicable to the System	14
Subservice Organizations	15
COMPLEMENTARY USER ENTITY CONTROLS	16
TRUST SERVICES CATEGORIES	17
CONTROL ACTIVITIES SPECIFIED BY THE SERVICE ORGANIZATION	18
TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY	18
SECTION 4 INFORMATION PROVIDED BY THE SERVICE AUDITOR	37
GUIDANCE REGARDING INFORMATION PROVIDED BY THE SERVICE AUDITOR	38

SECTION 1
ASSERTION OF COUCHDROP LIMITED MANAGEMENT

ASSERTION OF COUCHDROP LIMITED MANAGEMENT

December 1, 2021

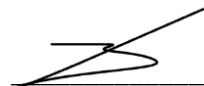
We have prepared the accompanying description of Couchdrop Limited's ('Couchdrop' or 'the Company') Software as a Service (SaaS) System titled "Couchdrop Limited's Description of Its SaaS System as of October 31, 2021" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria). The description is intended to provide report users with information about the SaaS System that may be useful when assessing the risks arising from interactions with Couchdrop's system, particularly information about system controls that Couchdrop has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Couchdrop uses Amazon Web Services ('AWS') and Digital Ocean to provide cloud hosting services (collectively, 'the subservice organizations'). The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Couchdrop, to achieve Couchdrop's service commitments and system requirements based on the applicable trust services criteria. The description presents Couchdrop's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Couchdrop's controls. The description does not disclose the actual controls at the subservice organizations.

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

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

- a. the description presents Couchdrop's SaaS System that was designed and implemented as of October 31, 2021, in accordance with the description criteria.
- b. the controls stated in the description were suitably designed as of October 31, 2021, to provide reasonable assurance that Couchdrop'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 Couchdrop's controls as of that date.



Jayden Bartram
Chief Executive Officer
Couchdrop Limited

SECTION 2
INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Couchdrop Limited

Scope

We have examined Couchdrop's accompanying description of its SaaS System titled "Couchdrop Limited's Description of Its SaaS System as of October 31, 2021" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design of controls stated in the description as of October 31, 2021, to provide reasonable assurance that Couchdrop's service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Couchdrop uses AWS and Digital Ocean to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Couchdrop, to achieve Couchdrop's service commitments and system requirements based on the applicable trust services criteria. The description presents Couchdrop's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Couchdrop's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

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

Service Organization's Responsibilities

Couchdrop 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 Couchdrop's service commitments and system requirements were achieved. Couchdrop has provided the accompanying assertion titled "Assertion of Couchdrop Limited Management" (assertion) about the description and the suitability of the design of controls stated therein. Couchdrop is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. 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 the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based the applicable trust services criteria
- Evaluating the overall presentation of the description

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

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report 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.

Other Matter

We did not perform any procedures regarding the operating effectiveness of controls stated in the description and, accordingly, do not express an opinion thereon.

Opinion

In our opinion, in all material respects,

- a. the description presents Couchdrop's SaaS System that was designed and implemented as of October 31, 2021, in accordance with the description criteria.
- b. the controls stated in the description were suitably designed as of October 31, 2021, to provide reasonable assurance that Couchdrop'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 Couchdrop's controls as of that date.

Restricted Use

This report is intended solely for the information and use of Couchdrop, user entities of Couchdrop's SaaS System as of October 31, 2021, business partners of Couchdrop subject to risks arising from interactions with the SaaS 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:

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

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

A-LIGN ASSURANCE

Tampa, Florida
December 1, 2021

SECTION 3

COUCHDROP LIMITED'S DESCRIPTION OF ITS SAAS SYSTEM AS OF OCTOBER 31, 2021

OVERVIEW OF OPERATIONS

Company Background

Since being founded in 2018, Couchdrop has enabled organizations globally through its SaaS solutions that simplify working with cloud storage. Couchdrop's products are delivered through self-service methods built on scalable and secure cloud infrastructure.

Couchdrop supports industries with their cloud storage requirements. These industries are, but not limited to, financial and insurance services, telecommunications, legal services, advertising, manufacturing, healthcare, retail, educational institutions, and government agencies.

Description of Services Provided

As of October 2021, Couchdrop provides two distinctive services. Couchdrop Cloud simple file transfer protocol (SFTP) and Movebot, the next generation data migration tool.

Couchdrop Cloud SFTP

Couchdrop Cloud SFTP is an SFTP server and MFT platform built for the cloud. SFTP is the standard protocol for transferring files securely and is widely used and accepted as the de facto standard for backend, automated, file transfers between systems and organizations.

Cloud platforms such as Dropbox, SharePoint, Amazon S3, offer inexpensive and scalable storage but do not support traditional protocols like SFTP, File Transfer Protocol (FTP) and SCP. Couchdrop makes these platforms accessible by providing a cloud SFTP solution, as a SaaS, that works directly with an organization's modern cloud storage and collaboration suite.

In addition to the SFTP solution, Couchdrop enables companies to automate their secure file transfers with workflows and scheduling as well as facilitates easy sharing and retrieval of files with external clients through secure web portals and other access methods.

Couchdrop is deployed as a simple SaaS solution that requires no software to be installed and minimal day to day management without sacrificing security and scalability.

Movebot

Movebot is a simple, fast and inexpensive cloud-to-cloud and on-premises to cloud file migration service. Until Movebot, moving data to the cloud and between cloud platforms had been complicated and prohibitively expensive. Movebot allows consumers, small businesses and large enterprises to move data between storage platforms at scale and with ease.

Movebot is deployed as a fully hosted cloud SaaS solution.

Principal Service Commitments and System Requirements

Couchdrop designs its processes and procedures related to its SaaS system to meet its objectives. Those objectives are based on the service commitments that Couchdrop makes to its customers.

Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online. Security and availability commitments are standardized and include, but are not limited to, the following:

- Ensure the service is available 99.9% of the time
- Use of end-to-end encryption to protect confidential data at rest and in transit
- Ensure logging is kept to a minimum and encrypted appropriately at rest
- Ensure best practices are followed to protect customer data
- Ensure data integrity is maintained

Couchdrop adopts operational processes and requirements that support the achievement of availability and security requirements. Such requirements are communicated in system policies and procedures, system design documentation and agreements 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, how to carry out specific manual and automated processes required in the operation and development of the system.

Components of the System

Infrastructure

Primary infrastructure used to provide Couchdrop’s SaaS System includes the following:

Primary Infrastructure		
Hardware	Type	Purpose
Databases	MongoDB, Postgres, Redis	Customer Data Storage
Firewalls	AWS and Digital Ocean	Network Protection
Servers	AWS and Digital Ocean	Software and Application Deployment
Computers	MacOS	Productivity and Staff Use
Load Balances	Nova Snap	Balance Load To Services and Manage Redundancy of Critical Services

Software

Primary software used to provide Couchdrop’s SaaS System includes the following:

Primary Software		
Software	Operating System	Purpose
Datadog	Cloud	Platform and Application Monitoring, Logging and Security Monitoring
Pingdom	Cloud	External Monitoring
GitHub	Cloud	Code Management
Docker Hub	Cloud	Code Image Repository
Zendesk	Cloud	Support Ticketing
Calendly	Cloud	Booking System

Primary Software		
Software	Operating System	Purpose
Doppler	Cloud	KMS
Trello	Cloud	Planning
1Password	Cloud	Password Management
Cluvio	Cloud	Business Reporting
HubSpot	Cloud	CRM and CMS
PagerDuty	Cloud	Alerting Platform
Google Analytics	Cloud	Web Performance Reporting
Docker	Cloud	Containerization

People

Couchdrop's staff are organized into the following business units but since Couchdrop's team is small, roles are often shared and are overlapping across team members:

- Executive Management - Responsible for overseeing company-wide activities, establishing and accomplishing goals, and managing objectives
- Engineering - Responsible for operational efficiencies, development, testing and implementation of changes, incident response, and overall security at Couchdrop
- Sales and Business Development - Responsible for expanding Couchdrop's business and supporting current relationships
- Human Resources (HR) and Legal - Facilitates day-to-day activities, including onboarding and offboarding relevant personnel to the corporate environment, workplace health, discipline, facilitation of security awareness training, and performance evaluations. Facilitates compliance across regulatory bodies and requirements

Data

Data refers to customer data held or transferred in the Couchdrop platform. This includes metadata pertaining to file transactions, user account details, events, billing details, files and storage tokens and credentials.

Couchdrop addresses data security with a range of approaches, depending on the type of data and its sensitivity classification.

Types of data stored by Couchdrop:

- Storage Tokens and Credentials - Details for accessing external storage is stored in a separate encrypted database and access is restricted to certain servers
- Metadata - User accounts, credentials, general configuration metadata is stored in a database environment of its own. Metadata is stored in the SFO2 region of Digital Ocean
- Customer Hosted Storage - Data stored in Couchdrop's hosted storage is stored in Amazon S3 buckets. Data is encrypted with SSE-C using customer-based tokens stored in the credential database. Customers can decide which region they wish to store their data in
- Data in Transit with Movebot - Customer files being migrated as part of a data migration are not retained and are only stored temporarily either in memory or on an encrypted disk. Customers can select several geographic regions to execute their migration in. Aside from the metadata required to run the migration, no data leaves the region specified

More information on Couchdrop's data security posture can be found in Couchdrop's security whitepapers.

Processes, Policies and Procedures

Procedures include the automated and manual procedures involved in the operation of the Couchdrop platform. Procedures are developed and documented by the respective teams for a variety of processes, including those relating to product management, engineering, technical operations, security, information technology (IT), and HR.

These procedures are drafted in alignment with the overall information security policies and are updated and approved as necessary to adapt to the changes in the business, but no less than annually.

Physical Security

Couchdrop has no physical office and data centers for hosting are provided by AWS and Digital Ocean.

Logical Access

Logical access to servers, networking equipment, databases and other hosted systems used to provide the platform is provided on an in-scope means and requires Chief of Technology Officer (CTO) approval.

Access levels are reviewed and where a staff member leaves, access is removed.

The following in-scope systems require unique usernames and password, certificate authentication or encrypted Secure Shell (SSH) keys for secure access:

- Network
- Couchdrop/Movebot
- Operating system access
- Database systems
- Cache systems
- AWS management console
- Digital Ocean management console

Multi-factor Authentication (MFA) is required and enforced for access to platforms that support MFA, including the following:

- AWS management console
- Digital Ocean

Resources are protected as appropriate with network firewalls and access monitoring.

Direct access to servers is provided via SSH and access is logged. SSH certificates are managed centrally and encrypted.

Computer Operations - Backups

Couchdrop's core databases are backed up daily and those backup snapshots are stored outside of Couchdrop's normal infrastructure.

Real-time monitoring and alerting ensures that the backup process is successful. Couchdrop regularly tests and restores backups to prove their validity and reviews the disaster recovery plan.

Computer Operations - Availability

Incident response systems and processes are in place to ensure that the platform remains available to customers.

Couchdrop monitors the capacity, performance, utilization and error rates of services and components with a combination of tools.

Incidents are automatically escalated and categorized to the appropriate team member for triage and remediation.

Change Control

Couchdrop has formally documented processes around software development, testing, deployment and bug fixes that govern how the company builds software.

Couchdrop's software and infrastructure change management process require that change requests are authorized, formally documented and tested prior to migration to production and peer reviewed.

Whereby there is a significant change that will impact customers, the company informs customers by e-mail prior to migration to production.

Data Communications

Server configurations are managed centrally through a configuration management system and are peer reviewed.

Systems must have their configurations managed, and most of them do not require operator intervention to add or remove new instances. In-scope Digital Ocean access is required to launch new servers, add new services, and modify other Digital Ocean resources used by servers.

Couchdrop relies on upstream security patches provided by the server operating system vendor.

In the case of severe vulnerabilities, Couchdrop can force updates to be applied sooner.

Boundaries of the System

The scope of this report includes the SaaS System performed in the remote working facilities.

This report does not include the cloud hosting services provided by AWS and Digital Ocean.

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

Control Environment

Integrity and Ethical Values

The effectiveness of controls and processes are limited by the team's ethical values inside the organization. Integrity and ethical values are an essential element of Couchdrop's control environment and business success. Couchdrop's team holds itself to the highest standards and encourages an open and transparent environment where honesty and integrity trumps process and controls.

Commitment to Competence

Couchdrop has well defined job descriptions that outline roles and responsibilities and the experience required to perform jobs in a competent and professional manner. Couchdrop hires not only for skill, but also cultural alignment and routinely evaluates employee performance and provides feedback and frameworks for growth and constant improvement.

Management's Philosophy and Operating Style

Couchdrop's management philosophy and operating style is best categorized as Agile and Lean. At its core, Couchdrop follows lean practices in its business planning, operations and management. Couchdrop responds quickly to changes in its business environment and reacts quickly to its customers' needs.

Couchdrop's lean management style is a competitive advantage, allowing the company to adapt to changing conditions and take advantage of their competitors bureaucracy and aversion to change.

As part of Couchdrop's lean management process it runs daily standups with the whole team and has monthly board meetings along with regular social outings and team building sessions.

Organizational Structure and Assignment of Authority and Responsibility

Couchdrop's organizational structure is best described as cross-functional with team members often sharing roles and responsibilities across the organization. This cross-functional approach suits a lean management style and encourages transparency.

Where needed, certain roles are explicitly assigned to team members and they are responsible for delivering on that control.

Human Resources Policies and Practices

Couchdrop's success is created and maintained by its team. New team members are provided with a clear framework that outlines Couchdrop's ethics and processes.

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

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

Risk Assessment Process

Couchdrop has a lean and cross-functional risk assessment process that utilizes both management and staff expertise to identify and remedy risks that could affect Couchdrop's ability to provide its service and meet its obligations to its customers.

Team members are instructed by general policy and processes to relate suspected or confirmed risks to the CTO and/or management for analysis and mitigation as appropriate. Staff are instructed that when in doubt, a matter should be reported and investigated.

Integration with Risk Assessment

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

Information and Communications Systems

Information is necessary for the Company to carry out almost responsibilities.

Couchdrop encourages lean, fast and honest communication over long winded correspondence. To communicate effectively Couchdrop uses a collection of tools for both internal and external communication. Communication tools include e-mails, collaborative documents, Zendesk, Trello, Slack and from time-to-time other tools.

Monitoring Controls

The Couchdrop management team meets on a regular basis to review the operational and financial performance of the Company. Ongoing evaluations, separate evaluations or some combination of the two are used to determine whether each of the components of an internal control is present and functioning effectively. Findings and issues are evaluated and adjusted or remedied as soon as possible.

The Company also uses software to track daily maintenance activities, infrastructure changes, code revisions, and customer requests and issues, which are maintained in a system and tracked through Couchdrop's development life cycle. Management performs regular reviews of tasks assigned to the team.

On-Going Monitoring

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

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

Reporting Deficiencies

An internal tracking tool is utilized to document and track the results of on-going monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool.

Changes to the System in the Last 12 Months

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

Incidents in the Last 12 Months

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

Criteria Not Applicable to the System

All Security criteria was applicable to the Couchdrop SaaS system.

Subservice Organizations

This report does not include the cloud hosting services provided by AWS and Digital Ocean.

Subservice Description of Services

Couchdrop uses AWS and Digital Ocean for managed services and hosting of its infrastructure. Management reviews the SOC 2 reports of both AWS and Digital Ocean.

Complementary Subservice Organization Controls

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

The following subservice organization controls should be implemented by AWS to provide additional assurance that the trust services criteria described within this report are met:

Subservice Organization - AWS		
Category	Criteria	Control
Common Criteria / Security	CC6.4	Physical access to datacentres is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		Physical access to datacentres is reviewed on a quarterly basis by appropriate personnel.
		Physical access points to server locations are recorded by closed circuit television camera (CCTV). Images are retained for 90 days, unless limited by legal or contractual obligations.
		Physical access points to server locations are managed by electronic access control devices.
		Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.

The following subservice organization controls should be implemented by Digital Ocean to provide additional assurance that the trust services criteria described within this report are met:

Subservice Organization - Digital Ocean		
Category	Criteria	Control
Common Criteria / Security	CC6.4	Physical access to data centers is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		Physical access points to server locations are recorded by closed circuit television camera (CCTV).

Subservice Organization - Digital Ocean		
Category	Criteria	Control
		Physical access points to server locations are managed by electronic access control devices.
		Physical access to assets is removed only after the ability to read or recover data and software from those assets has been diminished.

Couchdrop’s management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, Couchdrop performs monitoring of the subservice organization controls, including the following procedures:

- Reviewing attestation reports over services provided by vendors and subservice organizations
- Monitoring external communications, such as customer complaints relevant to the services provided by the subservice organizations

COMPLEMENTARY USER ENTITY CONTROLS

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

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

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

TRUST SERVICES CATEGORIES

In-Scope Trust Services Categories

Common Criteria (to the Security Category)

Security refers to the protection of

- i. information during its collection or creation, use, processing, transmission, and storage and
- ii. systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

CONTROL ACTIVITIES SPECIFIED BY THE SERVICE ORGANIZATION

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Control Environment		
CC1.0	Criteria	Control Activity Specified by the Service Organization
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	<p>The code of conduct is documented to communicate conduct standards and enforcement procedures.</p> <p>The code of conduct is signed off by new hires upon commencement of their role.</p> <p>Discipline policies and procedures define the consequences and method of handling misconduct.</p> <p>Background checks are completed for candidates prior to employment.</p> <p>Annual employee performance reviews are conducted.</p>
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	<p>Quarterly board of director meetings are held.</p> <p>Quarterly board of director meetings review company performance, and strategic initiatives, as applicable.</p> <p>The organizational chart documents the reporting lines, accountable executives, team and individual roles, and is updated whenever there are changes in personnel.</p>
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	<p>Quarterly management meetings are held to review the company operations.</p> <p>The organizational chart documents the reporting lines, accountable executives, team and individual roles, and is updated whenever there are changes in personnel.</p> <p>Job descriptions are documented for employees and management setting out the responsibilities, role requirements, and any key accountabilities.</p> <p>Business planning is performed at least annually to establish business requirements and objectives.</p> <p>The entity's third-party agreements outline and communicate; the scope of services, roles and responsibilities, terms of the business relationship, communication protocols, compliance requirements, service levels and just cause for terminating the relationship.</p> <p>Upon hire, employees are required to read and acknowledge the acceptable use policy.</p>
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	<p>New hire candidates are independently approved prior to selection and onboarding.</p> <p>Background checks are completed for candidates prior to employment.</p> <p>Quarterly management meetings are held to review the company operations.</p>

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY

Control Environment

CC1.0	Criteria	Control Activity Specified by the Service Organization
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	<p>Annual employee performance reviews are conducted.</p> <p>Annual security awareness training is provided to relevant employees based on job function.</p> <p>Discipline policies and procedures define the consequences and method of handling misconduct.</p> <p>The organizational chart documents the reporting lines, accountable executives, team and individual roles, and is updated whenever there are changes in personnel.</p> <p>Job descriptions are documented for employees and management setting out the responsibilities, role requirements, and any key accountabilities.</p> <p>Employment contracts are formed with employees.</p> <p>The contractor agreements outline and communicate the terms, conditions and responsibilities of the contractors.</p> <p>Annual employee performance reviews are conducted.</p>

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Information and Communication		
CC2.0	Criteria	Control Activity Specified by the Service Organization
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	<p>Job descriptions are documented for employees and management setting out the responsibilities, role requirements, and any key accountabilities.</p> <p>Organizational and information policies and procedures are made available to employees through the intranet.</p> <p>Information logs are maintained to track events and operating practices to support the internal control requirements.</p> <p>Couchdrop has documented system architecture to identify and document the relevant internal and external information sources of the system.</p>
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	<p>The code of conduct is signed off by new hires upon commencement of their role.</p> <p>Quarterly management meetings are held to review the company operations.</p> <p>Annual security awareness training is provided to relevant employees based on job function.</p> <p>Organizational and information policies and procedures are made available to employees through the intranet.</p> <p>On at least an annual basis, the approach to reporting and handling incidents, failures and security related matters is communicated to employees.</p> <p>The defined company objectives include a mix of strategic, financial and operational level objectives to guide functional areas and teams on how they support the company objectives and identify the risks that threaten achievement of the objectives.</p> <p>The company objectives are communicated to management and employees.</p> <p>The acceptable use policy sets out the roles, responsibilities and requirements to maintain the security of systems and data.</p> <p>Release notes for changes are sent to internal and external stakeholders, as applicable.</p>
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	<p>The contractor agreements outline and communicate the terms, conditions and responsibilities of the contractors.</p> <p>Changes to commitments, requirements, and responsibilities are communicated to third parties by the appointed account manager.</p> <p>Users of the system are provided support channels for reporting any requests, incidents, failures, or security-related matters.</p>

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY

Information and Communication

CC2.0	Criteria	Control Activity Specified by the Service Organization
		<p>User guide documentation is provided to users to guide them on the operation of the system.</p> <p>Customer's administrators are provided with training on how to administer the system and perform their responsibilities.</p> <p>Customer commitments, requirements, and responsibilities are outlined and communicated through service agreements.</p> <p>The entity's third-party agreements outline and communicate; the scope of services, roles and responsibilities, terms of the business relationship, communication protocols, compliance requirements, service levels and just cause for terminating the relationship.</p> <p>Management has assigned responsibility and accountability for the management of risks associated with third parties to appropriate personnel.</p> <p>Release notes for changes are sent to internal and external stakeholders, as applicable.</p>

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Risk Assessment		
CC3.0	Criteria	Control Activity Specified by the Service Organization
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	<p>The defined company objectives include a mix of strategic, financial and operational level objectives to guide functional areas and teams on how they support the company objectives and identify the risks that threaten achievement of the objectives.</p> <p>The company objectives are communicated to management and employees.</p> <p>Business planning is performed at least annually to establish business requirements and objectives.</p>
CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	<p>Documented policies and procedures are in place to guide personnel when performing a risk assessment.</p> <p>Management has defined risk assessment criteria with scales and guidance on how to measure and classify risks and provide a common language for comparing and prioritizing risks.</p> <p>The risk register is used to track and monitor the identified risks.</p> <p>Quarterly risk assessments are completed to identify and analyze the risks and identify any required mitigation actions.</p> <p>The risk assessments include consideration of risks related to systems and data security, third-party service providers, compliance obligations and operational risk.</p> <p>Identified risks are rated using a risk evaluation process and ratings are approved by management.</p> <p>Management has defined a third-party vendor risk management approach for evaluating third-party risks.</p> <p>Management develops third-party risk mitigation strategies to address risks identified during the risk assessment process.</p>
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	<p>The risk register is used to track and monitor the identified risks.</p> <p>The risk assessments include consideration of risks related to systems and data security, third-party service providers, compliance obligations and operational risk.</p> <p>The risk assessment process considers the potential for fraud including malicious acts of employees or other users of the system.</p>
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	<p>The risk register is used to track and monitor the identified risks.</p>

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY

Risk Assessment

CC3.0	Criteria	Control Activity Specified by the Service Organization
		<p>The risk assessments include consideration of risks related to systems and data security, third-party service providers, compliance obligations and operational risk.</p> <p>The risk assessment process identifies and assesses changes that could significantly impact the system of internal control.</p> <p>Management has assigned responsibility and accountability for the management of risks associated with third parties to appropriate personnel.</p>

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY

Monitoring Activities

CC4.0	Criteria	Control Activity Specified by the Service Organization
CC4.1	<p>COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.</p>	<p>The risk register is used to track and monitor the identified risks.</p> <p>Policies and processes are reviewed and updated at least annually to confirm their effectiveness and accuracy.</p> <p>Monitoring tools are used to identify and analyze system performance, capacity, and unusual system activity.</p> <p>Automated alerts are generated to notify IT personnel when thresholds or other criteria are met from the system monitoring tools.</p> <p>Daily vulnerability scans are performed. Identified vulnerabilities are addressed in line with the identified severity ratings.</p> <p>Management obtains and reviews attestation reports of vendors and third parties to evaluate the effectiveness of controls within the vendor or third parties environment.</p> <p>Annual employee performance reviews are conducted.</p> <p>Backup and restoration tests are performed on at least an annual basis to ensure the recovery controls are effective.</p>
CC4.2	<p>COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.</p>	<p>Quarterly board of director meetings are held.</p> <p>Quarterly board of director meetings review company performance, and strategic initiatives, as applicable.</p> <p>Policies and processes are reviewed and updated at least annually to confirm their effectiveness and accuracy.</p> <p>The control framework is reviewed at least annually by the control owners to ensure the control descriptions and owners are accurate, and that the controls are operating effectively as described.</p> <p>The third-party vendor register includes a listing of material vendors for tracking and monitoring.</p> <p>Management obtains and reviews attestation reports of vendors and third parties to evaluate the effectiveness of controls within the vendor or third parties environment.</p> <p>Management has assigned responsibility and accountability for the management of risks associated with third parties to appropriate personnel.</p>

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY

Monitoring Activities

CC4.0	Criteria	Control Activity Specified by the Service Organization
		<p>Security related change requirements based on vulnerabilities, security risk mitigation requirements, or other ongoing improvements have defined criteria to determine their relative priority or timeline for remediation.</p> <p>Management ensures control failures, breaches of policies and procedures, customer complaints and other issues are assessed, tracked, and monitored through to resolution, as applicable.</p>

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Control Activities		
CC5.0	Criteria	Control Activity Specified by the Service Organization
CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	<p>The risk register is used to track and monitor the identified risks.</p> <p>Quarterly risk assessments are completed to identify and analyze the risks and identify any required mitigation actions.</p> <p>The risk assessments include consideration of risks related to systems and data security, third-party service providers, compliance obligations and operational risk.</p> <p>The control framework is reviewed at least annually by the control owners to ensure the control descriptions and owners are accurate, and that the controls are operating effectively as described.</p> <p>The business continuity plan documents the to effectively manage critical events.</p> <p>The business continuity plan is tested at least annually to ensure the response plans to critical events are effective.</p>
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	<p>The control framework is reviewed at least annually by the control owners to ensure the control descriptions and owners are accurate, and that the controls are operating effectively as described.</p> <p>The risk register is used to track and monitor the identified risks.</p> <p>Quarterly risk assessments are completed to identify and analyze the risks and identify any required mitigation actions.</p> <p>The risk assessments include consideration of risks related to systems and data security, third-party service providers, compliance obligations and operational risk.</p> <p>Backup and restoration tests are performed at least annually to ensure the recovery controls are effective.</p> <p>The business continuity plan documents the to effectively manage critical events.</p> <p>The business continuity plan is tested at least annually to ensure the response plans to critical events are effective.</p> <p>The disaster recovery plan includes defined procedures to recover from significant events and is reviewed and updated at least annually.</p> <p>The disaster recovery plan is tested at least annually to confirm that recovery procedures are effective.</p>

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY

Control Activities

CC5.0	Criteria	Control Activity Specified by the Service Organization
CC5.3	<p>COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.</p>	<p>Job descriptions are documented for employees and management setting out the responsibilities, role requirements, and any key accountabilities.</p> <p>Documented policies and procedures are in place to guide personnel when performing a risk assessment.</p> <p>Policies and processes are reviewed and updated at least annually to confirm their effectiveness and accuracy.</p> <p>The control framework is reviewed at least annually by the control owners to ensure the control descriptions and owners are accurate, and that the controls are operating effectively as described.</p> <p>Management has defined a third-party vendor risk management approach for evaluating third-party risks.</p>

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Logical and Physical Access Controls		
CC6.0	Criteria	Control Activity Specified by the Service Organization
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.	<p>The security policies set out the requirements for managing security practices related to access control, network security, cryptography and systems and data security practices.</p> <p>New user access privileges to critical systems are approved by management prior to provisioning.</p> <p>Terminated user access is revoked from systems in a timely manner.</p> <p>Quarterly user access reviews are performed to confirm Couchdrop user access to the network, infrastructure and critical systems is appropriate.</p> <p>An inventory of system assets and components is maintained to classify and manage the information assets.</p> <p>Access to the network and infrastructure for Couchdrop employees requires authentication with strong password settings and multi-factor authentication.</p> <p>Access to Couchdrop platform for Couchdrop employees requires authentication with strong password settings.</p> <p>Access to Couchdrop platform for external users requires authentication with strong password settings.</p> <p>User access accounts to the network, infrastructure, Couchdrop platform and systems holding customer data are assigned to individual users.</p> <p>User access is based on the concept of least privilege to restrict access to only where there is a legitimate business need.</p> <p>Administrator account use is logged for retrospective investigation if required.</p> <p>Privileged access to sensitive resources is restricted to authorized personnel.</p>
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.	<p>The security policies set out the requirements for managing security practices related to access control, network security, cryptography and systems and data security practices.</p> <p>New user access privileges to critical systems are approved by management prior to provisioning.</p> <p>Terminated user access is revoked from systems in a timely manner.</p> <p>Quarterly user access reviews are performed to confirm Couchdrop user access to the network, infrastructure and critical systems is appropriate.</p>

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY

Logical and Physical Access Controls

CC6.0	Criteria	Control Activity Specified by the Service Organization
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, considering the concepts of least privilege and segregation of duties, to meet the entity's objectives.	<p>Privileged access to sensitive resources is restricted to authorized personnel.</p> <p>The security policies set out the requirements for managing security practices related to access control, network security, cryptography and systems and data security practices.</p> <p>New user access privileges to critical systems are approved by management prior to provisioning.</p> <p>Terminated user access is revoked from systems in a timely manner.</p> <p>Quarterly user access reviews are performed to confirm Couchdrop user access to the network, infrastructure and critical systems is appropriate.</p> <p>Privileged access to sensitive resources is restricted to authorized personnel.</p> <p>User access is based on the concept of least privilege to restrict access to only where there is a legitimate business need.</p> <p>Administrator account use is logged for retrospective investigation if required.</p>
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	This criterion is the responsibility of the subservice organizations. Refer to the Subservice Organizations section above for controls managed by the subservice organizations.
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.	<p>The security policies set out the requirements for managing security practices related to access control, network security, cryptography and systems and data security practices.</p> <p>The defined data disposal guidelines and requirements set out the process for ensuring data is erased prior to disposal of system assets.</p> <p>System assets are disposed of securely in line with the defined guidelines and requirements.</p>
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	<p>The security policies set out the requirements for managing security practices related to access control, network security, cryptography and systems and data security practices.</p> <p>Daily vulnerability scans are performed. Identified vulnerabilities are addressed in line with the identified severity ratings.</p> <p>Firewalls are used at external points of connectivity to the infrastructure and network.</p> <p>The firewall settings are maintained through restricted access to authorized administrators.</p>

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY

Logical and Physical Access Controls

CC6.0	Criteria	Control Activity Specified by the Service Organization
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.	<p>Security protocols are implemented through enforcement of policy requirements that mitigate the risk of malware and data leakage.</p> <p>Data at rest in the production databases is automatically encrypted.</p> <p>Data in transit to the infrastructure and Couchdrop platform is automatically encrypted.</p> <p>The security policies set out the requirements for managing security practices related to access control, network security, cryptography and systems and data security practices.</p> <p>Daily vulnerability scans are performed. Identified vulnerabilities are addressed in line with the identified severity ratings.</p> <p>Firewalls are used at external points of connectivity to the infrastructure and network.</p> <p>The firewall settings are maintained through restricted access to authorized administrators.</p> <p>Security protocols are implemented through enforcement of policy requirements that mitigate the risk of malware and data leakage.</p> <p>Data at rest in the production databases is automatically encrypted.</p> <p>Data in transit to the infrastructure and Couchdrop platform is automatically encrypted.</p>
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.	<p>The security policies set out the requirements for managing security practices related to access control, network security, cryptography and systems and data security practices.</p> <p>Daily vulnerability scans are performed. Identified vulnerabilities are addressed in line with the identified severity ratings.</p> <p>Security protocols are implemented through enforcement of policy requirements that mitigate the risk of malware and data leakage.</p> <p>Network security monitoring is performed to identify suspicious network activity.</p> <p>Incidents reported by external and internal users are logged in a central repository for monitoring through to closure.</p>

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY

System Operations

CC7.0	Criteria	Control Activity Specified by the Service Organization
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.	<p>Daily vulnerability scans are performed. Identified vulnerabilities are addressed in line with the identified severity ratings.</p> <p>Network security monitoring is performed to identify suspicious network activity.</p> <p>Monitoring tools are used to identify and analyze system performance, capacity, and unusual system activity.</p> <p>Automated alerts are generated to notify IT personnel when thresholds or other criteria are met from the system monitoring tools.</p> <p>Firewalls are used at external points of connectivity to the infrastructure and network.</p> <p>The firewall settings are maintained through restricted access to authorized administrators.</p> <p>Security protocols are implemented through enforcement of policy requirements that mitigate the risk of malware and data leakage.</p> <p>Incident management processes are defined and followed to resolve incidents.</p>
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.	<p>Network security monitoring is performed to identify suspicious network activity.</p> <p>Monitoring tools are used to identify and analyze system performance, capacity, and unusual system activity.</p> <p>Automated alerts are generated to notify IT personnel when thresholds or other criteria are met from the system monitoring tools.</p> <p>Incidents reported by external and internal users are logged in a central repository for monitoring through to closure.</p> <p>The incident management policies and procedures document the approach to identifying, reporting, evaluating, classifying and handling incidents.</p> <p>Incident management processes are defined and followed to resolve incidents.</p>
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.	<p>The risk assessments include consideration of risks related to systems and data security, third-party service providers, compliance obligations and operational risk.</p> <p>Incidents reported by external and internal users are logged in a central repository for monitoring through to closure.</p> <p>The incident management policies and procedures document the approach to identifying, reporting, evaluating, classifying and handling incidents.</p>

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY

System Operations

CC7.0	Criteria	Control Activity Specified by the Service Organization
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.	<p>Incident response plans are defined to provide guidelines for responding to major incidents including security breaches.</p> <p>Root cause analysis is conducted on high severity incidents to devise any lessons learned, updates to the incident response plans and raise change requests for permanent fixes to prevent recurrence, as applicable.</p> <p>Security related change requirements based on vulnerabilities, security risk mitigation requirements, or other ongoing improvements have defined criteria to determine their relative priority or timeline for remediation.</p> <p>Incidents reported by external and internal users are logged in a central repository for monitoring through to closure.</p> <p>The incident management policies and procedures document the approach to identifying, reporting, evaluating, classifying and handling incidents.</p> <p>Incident response plans are defined to provide guidelines for responding to major incidents including security breaches.</p> <p>Root cause analysis is conducted on high severity incidents to devise any lessons learned, updates to the incident response plans and raise change requests for permanent fixes to prevent recurrence, as applicable.</p>
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	<p>Incidents reported by external and internal users are logged in a central repository for monitoring through to closure.</p> <p>The incident management policies and procedures document the approach to identifying, reporting, evaluating, classifying and handling incidents.</p> <p>Incident response plans are defined to provide guidelines for responding to major incidents including security breaches.</p> <p>Root cause analysis is conducted on high severity incidents to devise any lessons learned, updates to the incident response plans and raise change requests for permanent fixes to prevent recurrence, as applicable.</p> <p>The business continuity plan documents the to effectively manage critical events.</p> <p>The business continuity plan is tested at least annually to ensure the response plans to critical events are effective.</p>

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY

System Operations

CC7.0	Criteria	Control Activity Specified by the Service Organization
		<p>The disaster recovery plan includes defined procedures to recover from significant events and is reviewed and updated at least annually.</p> <p>The disaster recovery plan is tested at least annually to confirm that recovery procedures are effective.</p>

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY

Change Management

CC8.0	Criteria	Control Activity Specified by the Service Organization
CC8.1	<p>The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.</p>	<p>System change requests are documented and tracked in a ticketing system.</p> <p>Documented change control policies and procedures are in place to guide personnel in the change management process.</p> <p>Development and test environments are logically separated from the production environment.</p> <p>Prior code is held in the source code repository for rollback capability if a system change does not function as intended.</p> <p>Code developments require a system enforced peer review prior to merging with the master code branch.</p> <p>Code developments are independently reviewed prior to merging with the master code branch.</p> <p>Releases are independently reviewed and approved prior to deployment.</p> <p>System changes are tested based on the type of change prior to implementation.</p> <p>Security related change requirements based on vulnerabilities, security risk mitigation requirements, or other ongoing improvements have defined criteria to determine their relative priority or timeline for remediation.</p> <p>Release notes for changes are sent to internal and external stakeholders, as applicable.</p>

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Risk Mitigation		
CC9.0	Criteria	Control Activity Specified by the Service Organization
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	<p>The business continuity plan documents the to effectively manage critical events.</p> <p>The business continuity plan is tested at least annually to ensure the response plans to critical events are effective.</p> <p>The disaster recovery plan includes defined procedures to recover from significant events and is reviewed and updated at least annually.</p> <p>The disaster recovery plan is tested at least annually to confirm that recovery procedures are effective.</p> <p>Management has defined risk assessment criteria with scales and guidance on how to measure and classify risks and provide a common language for comparing and prioritizing risks.</p> <p>The risk register is used to track and monitor the identified risks.</p> <p>Quarterly risk assessments are completed to identify and analyze the risks and identify any required mitigation actions.</p> <p>Couchdrop has purchased insurance to offset or compensate for the financial loss of an adverse event with the services.</p>
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	<p>The risk assessments include consideration of risks related to systems and data security, third-party service providers, compliance obligations and operational risk.</p> <p>Management has defined a third-party vendor risk management approach for evaluating third-party risks.</p> <p>The third-party vendor register includes a listing of material vendors for tracking and monitoring.</p> <p>The entity's third-party agreements outline and communicate; the scope of services, roles and responsibilities, terms of the business relationship, communication protocols, compliance requirements, service levels and just cause for terminating the relationship.</p> <p>Management develops third-party risk mitigation strategies to address risks identified during the risk assessment process.</p> <p>Management obtains and reviews attestation reports of vendors and third parties to evaluate the effectiveness of controls within the vendor or third parties environment.</p>

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Risk Mitigation		
CC9.0	Criteria	Control Activity Specified by the Service Organization
		Management has assigned responsibility and accountability for the management of risks associated with third parties to appropriate personnel.

SECTION 4
INFORMATION PROVIDED BY THE SERVICE AUDITOR

GUIDANCE REGARDING INFORMATION PROVIDED BY THE SERVICE AUDITOR

A-LIGN ASSURANCE's examination of the controls of Couchdrop was limited to the Trust Services Criteria, related criteria and control activities specified by the management of Couchdrop and did not encompass all aspects of Couchdrop's operations or operations at user entities. Our examination was performed in accordance with American Institute of Certified Public Accountants (AICPA) AT-C 105 and AT-C 205.

Our examination of the control activities was performed using the following testing methods:

TEST	DESCRIPTION
Inquiry	The service auditor made inquiries of service organization personnel. Inquiries were made to obtain information and representations from the client to determine that the client's knowledge of the control and corroborate policy or procedure information.
Observation	The service auditor observed application of the control activities by client personnel.
Inspection	The service auditor inspected among other items, source documents, reports, system configurations to determine performance of the specified control activity and in some instances the timeliness of the performance of control activities.
Re-performance	The service auditor independently executed procedures or controls that were originally performed by the service organization as part of the entity's internal control.

In determining whether the report meets the criteria, the user auditor should perform the following procedures:

- Understand the aspects of the service organization's controls that may affect the service commitments and system requirements based on the applicable trust services criteria;
- Understand the infrastructure, software, procedures and data that are designed, implemented and operated by the service organization;
- Determine whether the criteria are relevant to the user entity's assertions; and
- Determine whether the service organization's controls are suitably designed to provide reasonable assurance that its service commitments and system were achieved based on the applicable trust services criteria.