Plutoshift
Type 1 SOC 2
2020

REPORT ON PLUTOSHIFT'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

May 15, 2020

Table of Contents

SECTION 1

ASSERTION OF PLUTOSHIFT MANAGEMENT

plutoshift

ASSERTION OF PLUTOSHIFT MANAGEMENT

May 29, 2020

We have prepared the accompanying description of Plutoshift's ('the Company') Plutoshift Platform Services System titled "Plutoshift's Description of Its Plutoshift Platform Services System as of May 15, 2020" (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 Plutoshift Platform Services System that may be useful when assessing the risks arising from interactions with Plutoshift's system, particularly information about system controls that Plutoshift 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*).

Plutoshift uses Google Cloud Platform ('GCP' or 'subservice organization') 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 Plutoshift, to achieve Plutoshift's service commitments and system requirements based on the applicable trust services criteria. The description presents Plutoshift's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Plutoshift's controls. The description does not disclose the actual controls at the subservice organization.

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

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

a. the description presents Plutoshift's Plutoshift Platform Services System that was designed and implemented as of May 15, 2020, in accordance with the description criteria.
b. the controls stated in the description were suitably designed as of May 15, 2020, to provide reasonable assurance that Plutoshift'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 Plutoshift's controls as of that date.

Pjoshi

Prateek Joshi
CEO
Plutoshift

SECTION 2

INDEPENDENT SERVICE AUDITOR’S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Plutoshift

Scope

We have examined Plutoshift's accompanying description of its Plutoshift Platform Services System titled "Plutoshift's Description of Its Plutoshift Platform Services System as of May 15, 2020" (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 May 15, 2020, to provide reasonable assurance that Plutoshift'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*).

Plutoshift uses GCP 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 Plutoshift, to achieve Plutoshift's service commitments and system requirements based on the applicable trust services criteria. The description presents Plutoshift's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Plutoshift's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

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

Plutoshift 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 Plutoshift's service commitments and system requirements were achieved. Plutoshift has provided the accompanying assertion titled "Assertion of Plutoshift Management" (assertion) about the description and the suitability of the design of controls stated therein. Plutoshift 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 Plutoshift's Plutoshift Platform Services System that was designed and implemented as of May 15, 2020, in accordance with the description criteria.
b. the controls stated in the description were suitably designed as of May 15, 2020, to provide reasonable assurance that Plutoshift'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 Plutoshift's controls as of that date.

Restricted Use

This report is intended solely for the information and use of Plutoshift, user entities of Plutoshift's Plutoshift Platform Services System as of May 15, 2020, business partners of Plutoshift subject to risks arising from interactions with the Plutoshift Platform Services 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
May 29, 2020

SECTION 3

PLUTOSHIFT'S DESCRIPTION OF ITS PLUTOSHIFT PLATFORM SERVICES SYSTEM AS OF MAY 15, 2020

OVERVIEW OF OPERATIONS

Company Background

Plutoshift was launched in early 2017 with the objective of connecting the changing realities of the physical world with the monitoring power of intelligent software. Plutoshift provides automated performance monitoring for industrial processes by leveraging Artificial Intelligence. These solutions are delivered via a cloud-based solution that has been designed to help operators be more efficient.

The company is based in Palo Alto, California and has another office in Denver, Colorado. Industries served by Plutoshift include Food & Beverage, Oil & Gas, Chemicals, Water Services, and related manufacturing sectors.

Description of Services Provided

Plutoshift provides its services throughout the United States. Plutoshift's core application is a cloud-based solution that enables industrial companies to monitor the performance of processes. The Plutoshift platform ingests data from existing data collection systems and provides information to the operators. Here are the ways in which the solution is used:

- Compute key performance metrics for industrial processes
- Determine the root cause of anomalies
- Predict what's going to happen next with respect to the processes
- Communicate the information to the teammates
- Monitor the consumption of critical resources such as energy, chemicals, and water
- Forecast future consumption
- Generate reports
- Visualize data

Principal Service Commitments and System Requirements

Plutoshift designs its processes and procedures related to Plutoshift Platform Services to meet its objectives for its Artificial Intelligence (AI) product and services. Those objectives are based on the service commitments that Plutoshift makes to user entities, the laws and regulations that govern the provision of Plutoshift Platform Services, and the financial, operational, and compliance requirements that Plutoshift has established for the services. The Plutoshift Platform Services are subject to the security and privacy requirements of the client privacy requirements, including relevant regulations, as well as state privacy security laws and regulations in the jurisdictions in which Plutoshift operates. However, Plutoshift does not collect, store or process any PII, PCI, HIPAA relevant data.

Security commitments to user entities are documented and communicated in Statement of Work (SOW) and other customer agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following.

Security principles within the fundamental designs of the Plutoshift Platform Services 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.

Use of encryption technologies to protect customer data both at rest and in transit.

Plutoshift establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Plutoshift’s system policies and procedures, system design documentation, and contracts with customers.

Components of the System

Infrastructure

Primary infrastructure used to provide Plutoshift's Platform Services System includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Modem/Router	Comcast Business Router (CBR-T)	Provides internet to the Palo Alto office
Wi-Fi Router	Google H2D	Provides Wi-Fi to the Palo Alto office
Wi-Fi Access Point	Google H2E	Secondary Access point to provide Wi-Fi to the Palo Alto office
Google Cloud Platform (GCP)	Cloud	Primary cloud hosting network
Cloud SQL	GCP	Primary database

Software

Primary software used to provide Plutoshift's Platform Services System includes the following:

Primary Software		
Software	**Operating System**	**Purpose**
ClickUp	N/A	Issue Tracking
Gusto	N/A	Payroll
Expensify	N/A	Expense tracking
Google Drive	N/A	Cloud storage
Google E-mail	N/A	E-mail server
Google Calendar	N/A	Cloud calendar
Microsoft Office	N/A	Word processing, PowerPoints
Slack	N/A	Internal messaging
Bitbucket	N/A	Control Version System
Jenkins	Ubuntu	Build Server
Ansible	N/A	Configuration Management Software
Balsamiq	N/A	Wireframing tool
Digital Ocean	N/A	Company website hosting
GoDaddy	N/A	Secure Socket Layer (SSL) certifications
Freshworks	N/A	Helpdesk
Kubernetes	COS (Google)	Container Management software
Django	Debian	Backend server software
React	Debian	Frontend server software

Primary Software		
Software	**Operating System**	**Purpose**
GROUNDED AI	Ubuntu Linux	Primary application

People

Plutoshift has a staff of approximately 25 employees organized in the following functional areas:

- Executives. These individuals oversee the business and make sure that it runs efficiently
- New Business. These individuals go out find new customers for Plutoshift
- Client Engagement
- Customer Success. Interacting with existing clients to ensure Return on Investments (ROI) is being met and said customer's needs are being met
- Marketing
- Technology
- Data Science. These individuals are responsible for running the Exploratory Data Analysis (EDA) and Information Dispute Resolution (IDR) processes. They are also responsible for the data science built into the Plutoshift Platform
- Engineering. These individuals are responsible for creating the cloud infrastructure, Application Programming Interface (API)s and data visualization that make up the Plutoshift Platform

Data

Data, as defined by Plutoshift, constitutes the following:

- Time-series data
- Data Visualization diagrams
- System logs

Time-series data is collected from a client to build the Plutoshift Platform. This data is read only and is segregated from data of other clients. This data is currently contained within the platform and cannot be directly exported.

Data Visualization diagrams can be generated by using the platform to show trends over a given time frame.

System logs are collected and stored on GCP to show access as well as any errors that are produced by the platform.

Processes, Policies and Procedures

Formal IT policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. All teams are expected to adhere to the Plutoshift policies and procedures that define how services should be delivered. These are located on the Company's shared Google Drive and can be accessed by any Plutoshift team member.

<u>Physical Security</u>

The in-scope systems and infrastructure that supports Plutoshift are hosted by GCP. GCP is responsible for the physical controls around Plutoshift's in-scope systems and infrastructure.

<u>Logical Access</u>

Plutoshift uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. Resources are protected through the use of native system security and users are authenticated with a custom password.

Administrators of the Platform are responsible to give users access to specific Plants within the platform.

Plutoshift is all Cloud based, so all employees and clients must access the platform through a web browser that has proper internet access.

New users will only be given to the system by request of a Plutoshift administrator.

Internal employees of Plutoshift are only given access to each client's platform if upper management deems it necessary.

Computer Operations - Backups

Data Backup

To ensure that all data for the Plutoshift Platform can be restored in case of an emergency, Plutoshift enables various automated backups from GCP. All data can be restored through the GCP console.

The following is a breakdown of all the data that is backed up:

- GCP Engine Snapshot Schedule
- Cassandra cluster volumes
- Network File System (NFS) models volume
- GCP SQL Automated Backups

Computer Operations - Availability

To monitor its platform, Plutoshift utilizes Stackdriver Monitoring. This enables Plutoshift to be aware of anything that may be out of order of each individual platform.

The following configurations are enabled for each platform:

- Volume usage of Cassandra cluster volumes (triggered at 80% usage for 10 minutes in a row)
- Volume usage of NFS models volume (triggered at 80% usage for 10 minutes in a row)
- Central Processing Unit (CPU) utilization of the Cloud SQL server (triggered at 80% usage for 10 minutes in a row)
- Disk utilization of the Cloud SQL server (triggered at 80% usage for 10 minutes in a row)
- Memory utilization of the Cloud SQL server (triggered at 80% usage for 10 minutes in a row)
- CPU utilization of each Kubernetes node (triggered at 80% usage for 10 minutes in a row)
- Memory utilization of each Kubernetes node (triggered at 80% usage for 10 minutes in a row)

Change Control

Plutoshift has implemented a patch management process to ensure contracted customer and infrastructure systems are patched in accordance with vendor recommended operating system patches. Customers and Plutoshift system owners review proposed operating system patches to determine whether the patches are applied. Customers and Plutoshift systems are responsible for determining the risk of applying or not applying patches based upon the security and availability impact of those systems and any critical applications hosted on them. Plutoshift staff validate that all patches have been installed and if applicable that reboots have been completed.

Data Communications

Network address translation (NAT) functionality is utilized to manage internal IP addresses.

Redundancy is built into the cloud infrastructure in the GCP services to help ensure that there is no single point of failure that includes firewalls, containers, and load balancers. In the event that a primary system fails, the redundant software is configured to take its place.

Penetration testing is conducted to measure the security posture of the service. The third-party vendor uses an accepted industry standard penetration testing methodology specified by Plutoshift. The third-party vendor’s approach begins with a vulnerability analysis of the target system to determine what vulnerabilities exist on the system that can be exploited via a penetration test, simulating a disgruntled/disaffected insider or an attacker that has obtained internal access to the network. Once vulnerabilities are identified, the third-party vendor attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing includes network and application layer testing as well as testing of controls and processes around the networks and applications, and occurs from both outside (external testing) and inside the network.

Vulnerability scanning is performed by a third-party vendor on a daily basis in accordance with Plutoshift’s policy. The third-party vendor uses industry standard scanning technologies and a formal methodology specified by Plutoshift. These technologies are customized to test the organization's infrastructure and software in an efficient manner while minimizing the potential risks associated with active scanning. Retests and on-demand scans are performed on an as needed basis. Scans are performed during non-peak windows. Tools requiring installation in the Plutoshift system are implemented through the Change Management process. Scanning is performed with approved scanning templates and with bandwidth-throttling options enabled.

Boundaries of the System

The scope of this report includes the Plutoshift Platform Services System performed in the Palo Alto, California.

This report does not include the cloud hosting services provided by GCP at the various facilities.

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

Control Environment

Integrity and Ethical Values

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

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

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

Commitment to Competence

Plutoshift’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 particular jobs and how those levels translate into the requisite skills and knowledge.

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

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

Management’s Philosophy and Operating Style

Plutoshift’s management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management’s approach to taking and monitoring business risks, and management’s attitudes toward information processing, accounting functions, and personnel.

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

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

Organizational Structure and Assignment of Authority and Responsibility

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

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

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

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

Human Resource Policies and Practices

Plutoshift’s success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top quality personnel who ensures the service organization is operating at maximum efficiency. Plutoshift’s human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

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

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

Risk Assessment Process

Plutoshift's risk assessment process identifies and manages risks that could potentially affect Plutoshift's ability to provide reliable services to user organizations. This ongoing process requires that management identify significant risks inherent in products or services as they oversee their areas of responsibility. Plutoshift identifies the underlying sources of risk, measures the impact to organization, establishes acceptable risk tolerance levels, and implements appropriate measures to monitor and manage the risks.

This process has identified risks resulting from the nature of the services provided by Plutoshift, and management has implemented various measures designed to manage these risks. Risks identified in this process include the following:

- Operational risk - changes in the environment, staff, or management personnel
- Strategic risk - new technologies, changing business models, and shifts within the industry
- Compliance - legal and regulatory changes

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of Plutoshift's Platform; as well as the nature of the components of the system result in risks that the criteria will not be met. Plutoshift 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, Plutoshift'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 and communication is an integral component of Plutoshift's internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations. This process encompasses the primary classes of transactions of the organization, including the dependence on, and complexity of, information technology.

Various weekly calls are held to discuss operational efficiencies within the applicable functional areas and to disseminate new policies, procedures, controls, and other strategic initiatives within the organization. General updates to entity-wide security policies and procedures are usually communicated to the appropriate Plutoshift personnel via e-mail messages.

Specific information systems used to support Plutoshift's Platform Services are described in the Description of Services section above.

Monitoring Controls

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

On-Going Monitoring

Management's close involvement in Plutoshift'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 Plutoshift'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. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

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 end of the review period.

Incidents in the Last 12 Months

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

Criteria Not Applicable to the System

All Common/Security Criterion was applicable to the Plutoshift Platform Services System.

Subservice Organizations

This report does not include the cloud hosting services provided by GCP at the Los Angeles, California facilities.

Complementary Subservice Organization Controls

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

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

Subservice Organization - GCP		
Category	**Criteria**	**Control**
Common Criteria/ Security	CC6.4	Data center server floors network rooms and security systems are physically isolated from public spaces and/or delivery areas.
		Access to sensitive data center zones requires approval form authorized personnel and is controlled via badge access readers, biometric identification mechanism, and/or physical locks.

Subservice Organization - GCP		
Category	**Criteria**	**Control**
		Data center perimeters are defined and secured via physical barriers.
		Access lists to high security areas in data centers are reviewed on a periodic basis and inappropriate access is removed in a timely manner.
		Visitors to data center facilities must gain approval from authorized personnel, have their identity verified at the perimeter, and remain with an escort for the duration of the visit.
		Security measures utilized in data centers are assessed annually and the results are reviewed by executive management.
		Data centers are continuously staffed and monitored by security personnel through the use of real time video surveillance and/or alerts generated by security systems.
	CC6.5	Google sanitizes information system media prior to disposal, release out of organizational control, or release for reuse.
		Google sanitizes information system media, both digital and non-digital, prior to disposal, release out of organizational control, or release for reuse.

Plutoshift 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, Plutoshift performs monitoring of the subservice organization controls, including the following procedures:

- Reviewing and reconciling invoices
- Holding periodic discussions with vendors and the subservice organization
- Reviewing attestation reports over services provided by vendors and the subservice organization
- Monitoring external communications, such as customer complaints relevant to the services provided by the subservice organization

COMPLEMENTARY USER ENTITY CONTROLS

Plutoshift'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 of the Trust Services Criteria related to Plutoshift's services to be solely achieved by Plutoshift control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Plutoshift'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 Plutoshift.
2. User entities are responsible for notifying Plutoshift of changes made to technical or administrative contact information.

3. User entities are responsible for maintaining their own systems of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of Plutoshift 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 Plutoshift services.
6. User entities are responsible for providing Plutoshift with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying Plutoshift of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.

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.	Core values are communicated from executive management to personnel through policies, directives, guidelines, the code of conduct and the employee handbook. An employee handbook are documented to communicate workforce conduct standards and enforcement procedures. Upon hire, personnel are required to acknowledge the employee handbook. Upon hire, personnel are required to complete a background check. Personnel are required to acknowledge the employee handbook on an annual basis. Performance and conduct evaluations are performed for personnel on a quarterly basis. Sanction policies, which include probation, suspension and termination, are in place for employee misconduct. An anonymous hotline is in place to allow employees, third-parties, and customers to report unethical behavior in a confidential manner. The entity's third-party agreement requires that third-parties have a code of conduct and employee handbook in place.
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Executive management roles and responsibilities are documented and reviewed annually. Executive management defines and documents the skills and expertise needed among its members. Executive management evaluates the skills and expertise of its members annually. Executive management maintains independence from those that operate the key controls within the environment. Executive management meets annually with operational management to assess the effectiveness and performance of internal controls within the environment. Executive management evaluates the skills and competencies of those that operate the internal controls within the environment annually. Operational management assigns responsibility for and monitors the effectiveness and performance of internal controls implemented within the environment.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Control Environment		
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	A documented organizational chart is in place that defines organizational structures, lines of reporting, and areas of authority. Executive management reviews the organizational chart annually and makes updates to the organizational structure and lines of reporting, if necessary. Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's intranet. Executive management reviews job descriptions annually and makes updates, if necessary. Upon hire, personnel are required to acknowledge the employee handbook which requires adherence to the personnel's job role and responsibilities. Executive management has established proper segregations of duties for key job functions and roles within the organization. Roles and responsibilities defined in written job descriptions consider and address specific requirements relevant to the system. A vendor risk assessment is performed on an annual basis which includes reviewing the activities performed by third-parties.
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Policies and procedures are in place that outline the performance evaluation process as well as the competency and training requirements for personnel. Performance and conduct evaluations are performed for personnel on an annual basis. The entity evaluates the competencies and experience of candidates prior to hiring, and of personnel transferring job roles or responsibilities. The entity evaluates the competencies and experience of third-parties prior to working with them. Job requirements are documented in the job descriptions and candidates' abilities to meet these requirements are evaluated as part of the hiring or transfer process. The entity's third-party agreement requires that third-parties: • Consider the background, competencies and experience of its personnel • Provide regular training to its personnel as it relates to their job role and responsibilities

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.	The entity has a recruiting department that is responsible for attracting individuals with competencies and experience that align with the entity's goals and objectives. Executive management has created a training program for its employees. As part of the performance evaluation process, the entity rewards its personnel for exceeding expectations as it relates to their job role and responsibilities. The entity assesses training needs on an annual basis. Prior to employment, personnel are required to complete a background check. A documented organizational chart is in place that defines organizational structures, lines of reporting, and areas of authority. Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's intranet. Upon hire, personnel are required to acknowledge the employee handbook which requires adherence to the personnel's job role and responsibilities. Personnel are required to acknowledge the employee handbook on an annual basis. Policies and procedures are in place that outline the performance evaluation process as well as the competency and training requirements for personnel. Executive management has established performance measures, including the incentives and rewards for exceeding expectations, as it relates to job roles and responsibilities. Performance and conduct evaluations are performed for personnel on an annual basis. As part of the performance evaluation process, the entity rewards its personnel for exceeding expectations and performs disciplinary actions for its employees who do not meet expectations as it relates to their job role and responsibilities. Executive management reviews the job requirements and responsibilities documented within job descriptions annually and makes updates, if necessary. Executive management reviews the responsibilities assigned to operational personnel annually and makes updates, if necessary.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Control Environment		
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**
		Sanction policies which include probation, suspension and termination are in place for employee misconduct.

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.	Organizational and information security policies and procedures are documented for supporting the functioning of controls and processes and made available to its personnel through the entity's intranet.
		Edit checks are in place to prevent incomplete or incorrect data from being entered into the system.
		Data flow diagrams and narratives are documented and maintained by management to identify the relevant internal and external information sources of the system.
		Data that entered into the system, processed by the system and output from the system is protected from unauthorized access.
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.	Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's intranet.
		The entity's policies and procedures, code of conduct and employee handbook are made available to employees through the entity’s intranet.
		Upon hire, employees are required to read and acknowledge the information security policies and procedures and complete information security and awareness training.
		Current employees are required to read and acknowledge the information security policies and procedures and complete information security and awareness training on an annual basis.
		Upon hire, personnel are required to acknowledge the employee handbook and code of conduct.
		Personnel are required to acknowledge the employee handbook on an annual basis.
		Upon hire, personnel are required to acknowledge the employee handbook which requires adherence to the personnel's job role and responsibilities.
		Executive management meets annually with operational management to discuss the entity's objectives as well as roles and responsibilities.
		An anonymous hotline is in place to allow employees, third-parties, and customers to report unethical behavior in a confidential manner.
		Documented escalation procedures for reporting failures incidents, concerns and other complaints are in place and made available to employees through the entity's intranet.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Information and Communication		
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	The entity's objectives, including changes made to the objectives, are communicated to its personnel through the entity's intranet. Management tracks and monitors compliance with information security and awareness training requirements. The entity's third-party agreement delineates the boundaries of the system and describes relevant system components. The entity's third-party agreement communicates the system commitments and requirements of third-parties. The information security policies and procedures that communicate the system commitments and requirements of external users are provided to external users prior to allowing them access to the system. The entity's third-party agreement outlines and communicates the terms, conditions and responsibilities of third-parties. Customer commitments, requirements and responsibilities are outlined and communicated through service agreements. Changes to commitments, requirements and responsibilities are communicated to third-parties, external users, and customers via updated agreements or mass notifications. Documented escalation procedures for reporting failures incidents, concerns and other complaints are in place and shared with external parties. Executive management meets annually with operational management to discuss the results of assessments performed by third-parties. An anonymous hotline is in place to allow employees, third-parties, and customers to report unethical behavior in a confidential manner.

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.	The entity establishes organizational strategies and objectives that are used to determine entity structure and performance metrics. Executive management has documented objectives that are specific, measurable, attainable, relevant and time-bound (SMART). Executive management identifies and assesses risks that could prevent the entity's objectives from being achieved. Executive management reviews policies, procedures and other control documents for alignment to the entity's objectives on an annual basis. Executive management reviews and addresses control failures. Responsible parties are defined and assigned to coordinate and monitor compliance and audit activities. The entity has defined the desired level of performance and operation in order to achieve the established entity objectives. The operational reports reviewed by executive management define the acceptable level of operational performance and control failure. Business plans and budgets align with the entity's strategies and objectives. Entity strategies, objectives and budgets are assessed on an annual basis.
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.	Documented policies and procedures are in place to guide personnel when performing a risk assessment. Management has defined a formal risk assessment process that specifies the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances. A formal risk assessment is performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Risk Assessment		
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**
		The entity's risk assessment process includes: • Identifying the relevant information assets that are critical to business operations • Prioritizing the criticality of those relevant information assets • Identifying and assessing the impact of the threats to those information assets • Identifying and assessing the impact of the vulnerabilities associated with the identified threats • Assessing the likelihood of identified threats and vulnerabilities • Determining the risks associated with the information assets • Addressing the associated risks identified for each identified vulnerability Identified risks are rated using a risk evaluation process and ratings are approved by management. Risks identified as a part of the risk assessment process are addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk Management develops risk mitigation strategies to address risks identified during the risk assessment process. For gaps and vulnerabilities identified from the risk assessment, remediation efforts, including the implementation of controls, are assigned to process owners based on roles and responsibilities. The annual comprehensive risk assessment results are reviewed and approved by appropriate levels of management. As part of the annual risk assessment, management reviews the potential threats and vulnerabilities arising from its customers, vendors and third-parties.
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	On an annual basis, management identifies and assesses the types of fraud (e.g. fraudulent reporting, loss of assets, unauthorized system access, overriding controls) that could impact their business and operations.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Risk Assessment		
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**
		Identified fraud risks are reviewed and addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk As part of management's assessment of fraud risks, management considers key fraud factors such as incentives, pressures, opportunity for unauthorized access or use of data, and employee morale and attitude. As part of management's assessment of fraud risks, management considers how personnel could engage in or justify fraudulent activities. As part of management's assessment of fraud risks, management considers threats and vulnerabilities that arise from the use of IT (e.g. unauthorized access, inadequate segregation of duties, default accounts, inadequate password management, unauthorized changes).
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	Changes to the business structure and operations are considered and evaluated as part of the annual comprehensive risk assessment. Changes in key management and personnel are considered and evaluated as part of the annual comprehensive risk assessment. Changes to the entity's systems, applications, technologies, and tools are considered and evaluated as part of the annual comprehensive risk assessment. Changes in vendor and third-party relationships are considered and evaluated as part of the annual comprehensive risk assessment.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Monitoring Activities		
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC4.1	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.	Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. Management reviews policies, procedures and other control documents for accuracy and applicability on an annual basis. On an annual basis, management reviews the controls implemented within the environment for operational effectiveness and identifies potential control gaps and weaknesses. Backup restoration tests are performed on at least an annual basis. User access reviews are completed quarterly. Systems are scanned for vulnerabilities that could impair the environment and control gaps and vulnerabilities are identified on an annual basis. Evaluations of policies, controls, systems, tools, applications, and third-parties for effectiveness and compliance is required at least annually. Management reviews the frequency of compliance evaluations annually and adjusts it based on changes to the environment and operational performance. Penetration testing is completed on systems to identify and exploit vulnerabilities identified within the environment on an annual basis. Performance and conduct evaluations are performed for personnel on an annual basis. Management obtains and reviews attestation reports of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment. A formal risk assessment is performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.
CC4.2	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.	Senior management assesses the results of the compliance, control and risk assessments performed on the environment. Senior management is made aware of high-risk vulnerabilities, deviations and controls gaps identified as part of the compliance, control and risk assessments performed.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Monitoring Activities		
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**
		Vulnerabilities, deviations and control gaps identified from the compliance, control and risk assessments are communicated to those parties responsible for taking corrective actions.

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.	As part of the risk assessment process, controls within the environment are modified and implemented to mitigate identified vulnerabilities, deviations and control gaps. Controls within the environment are modified and implemented to mitigate vulnerabilities, deviations and control gaps identified as part of the various evaluations performed. Performance of the internal controls implemented within the environment are assigned to appropriate process owners and operational personnel based on roles and responsibilities. Prior to the development and implementation of internal controls into the environment, management considers the complexity, nature, and scope of its operations. Management has documented the relevant controls in place for each key business or operational process. Management has incorporated a variety of controls into their environment that include manual, automated, preventive, detective, and corrective controls. Management develops risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process. Business continuity plan is developed and updated on an annual basis. Business continuity and disaster recovery plans are tested on an annual basis.
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	Management has documented the relationship and linkage between business processes, the relevant technologies used to support the business processes, and the controls in place to help secure those business processes. Organizational and information security policies and procedures are documented and made available to employee's through the entity's intranet. Management has documented the controls implemented around the entity's technology infrastructure. As part of the risk assessment process, the use of technology in business processes is evaluated by management.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Control Activities		
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The internal controls implemented around the entity's technology infrastructure include, but are not limited to: • Restricting access rights to authorized users • Limiting services to what is required for business operations • Authentication of access • Protecting the entity's assets from external threats Management has established controls around the acquisition, development and maintenance of the entity's technology infrastructure. Organizational and information security policies and procedures are documented and made available to employee's through the entity's intranet. Job descriptions detail the day-to-day activities to be performed by personnel. Management has implemented controls that are built into the organizational and information security policies and procedures. Process owners and key management are assigned ownership to each key internal control implemented within the entity's environment. Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's intranet. Performance of the internal controls implemented within the environment are assigned to appropriate process owners and operational personnel based on roles and responsibilities. Process owners and management operate the controls implemented within the entity's environment based on the frequency defined in the organizational and information security policies and procedures. Effectiveness of the internal controls implemented within the environment are evaluated annually.

<table>
<tr><th colspan="3">TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY</th></tr>
<tr><th colspan="3">Logical and Physical Access Controls</th></tr>
<tr><th>CC6.0</th><th>Criteria</th><th>Control Activity Specified
by the Service Organization</th></tr>
<tr><td>CC6.1</td><td>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.</td><td>An inventory of system assets and components is maintained to classify and manage the information assets.
Privileged access to sensitive resources is restricted to authorized personnel.
Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.</td></tr>
<tr><td></td><td colspan="2"><b>Network (GCP)</b></td></tr>
<tr><td></td><td></td><td>Network user access is restricted via role based security privileges defined within the access control system.
Network administrative access is restricted to user accounts accessible by authorized personnel.
Networks are configured to enforce password requirements that include:
• Password length
• Complexity
Network audit logging settings are in place.
Network audit logs are maintained and can be pulled for review at any time.</td></tr>
<tr><td></td><td colspan="2"><b>Operating System (Linux)</b></td></tr>
<tr><td></td><td></td><td>Operating system user access is restricted via role based security privileges defined within the access control system.
Operating system administrative access is restricted to user accounts accessible by authorized personnel.
Operating systems are configured to enforce password lockout requirements.
Operating system audit logging settings are in place.
Operating system audit logs are maintained and can be pulled for review at any time.</td></tr>
<tr><td></td><td colspan="2"><b>Database (MySQL)</b></td></tr>
<tr><td></td><td></td><td>Database user access is restricted via role based security privileges defined within the access control system.
Database administrative access is restricted to user accounts accessible by authorized personnel.
Databases are configured to enforce password requirements.
Database audit logging settings are in place.</td></tr>
</table>

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Logical and Physical Access Controls		
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**
		Database audit logs are maintained and can be pulled for review upon request.
	Application	
		Application user access is restricted via role based security privileges defined within the access control system. Application administrative access is restricted to user accounts accessible by authorized personnel. The application is configured to enforce password requirements that include: • Password length • Complexity Application audit policy settings are in place. Application audit logs are maintained and can be pulled for review upon request. The entity's various networks are segmented to keep information and data isolated and restricted to authorized personnel. Data coming into the environment is secured and monitored through the use of firewalls and an intrusion detection software (IDS). Server certificate-based authentication is used as part of the SSL encryption with a trusted certificate authority. Stored passwords are encrypted. Critical data is stored in encrypted format using software supporting the Advanced Encryption Standard (AES). Encryption keys are protected during generation, storage, use, and destruction. The entity restricts access to its environment using the following mechanisms: • Classifying data (e.g. Public, private, restricted, etc.) • Port restrictions (via firewall rule settings) • Access protocol restrictions (via firewall rule settings) • User identification • Digital certifications User access reviews are performed on a quarterly basis. Logical access to systems is approved and granted to an employee as a component of the hiring process.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Logical and Physical Access Controls		
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**
		Logical access to systems is revoked as a component of the termination process.
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.	Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring. Logical access to systems is approved and granted to an employee as a component of the hiring process. Logical access to systems is revoked as a component of the termination process. User access reviews are performed on a quarterly basis. Privileged access to sensitive resources is restricted to authorized personnel.
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.	Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring. Logical access to systems is approved and granted to an employee as a component of the hiring process. Logical access to systems is revoked as a component of the termination process. Privileged access to sensitive resources is restricted to authorized personnel. User access reviews are performed on a quarterly basis.
	Network (GCP)	
		Network user access is restricted via role based security privileges defined within the access control system.
	Operating System (Linux)	
		Operating system user access is restricted via role based security privileges defined within the access control system.
	Database (MySQL)	
		Database user access is restricted via role based security privileges defined within the access control system.
	Application	
		Application user access is restricted via role based security privileges defined within the access control system.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Logical and Physical Access Controls		
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**
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 managed by the subservice organization. Please refer to the Subservice Organizations section for the controls managed by the subservice organization.
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.	Policies and procedures are in place to guide personnel in data disposal and destruction practices. Part of this this criterion is managed by the subservice organization. Please refer to the Subservice Organizations section for the controls managed by the subservice organization.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	NAT functionality is utilized to manage internal IP addresses. SSL and other encryption technologies are used for defined points of connectivity. Server certificate-based authentication is used as part of the SSL encryption with a trusted certificate authority. Transmission of digital output beyond the boundary of the system is encrypted. Logical access to stored data is restricted to authorized personnel. A firewall is in place to filter unauthorized inbound network traffic from the internet. The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule. An IDS is utilized to analyze network events and report possible or actual network security breaches. The IDS is configured to notify personnel upon intrusion detection. Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software. The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available. The antivirus software is configured to scan workstations on an ongoing basis. Critical data is stored in encrypted format using software supporting the AES.

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.	Logical access to stored data is restricted to authorized personnel. The ability to recall backed up data is restricted to authorized personnel. The entity secures its environment a using multi-layered defense approach that includes firewalls, an IDS, and antivirus software. SSL and other encryption technologies are used for defined points of connectivity. Server certificate-based authentication is used as part of the SSL encryption with a trusted certificate authority. A firewall is in place to filter unauthorized inbound network traffic from the internet. The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule. NAT functionality is utilized to manage internal IP addresses. An IDS is utilized to analyze network events and report possible or actual network security breaches. The IDS is configured to notify personnel upon intrusion detection. Critical data is stored in encrypted format using software supporting the AES. Backup media is stored in an encrypted format. Transmission of digital output beyond the boundary of the system is encrypted.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity’s objectives.	The ability to migrate changes into the production environment is restricted to authorized and appropriate users. File integrity monitoring (FIM) software is in place to ensure only authorized changes are deployed into the production environment. The FIM software is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected. Documented change control policies and procedures are in place to guide personnel in the change management process. Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Logical and Physical Access Controls		
CC6.0	Criteria	Control Activity Specified by the Service Organization
		The antivirus software provider pushes updates to the installed antivirus software as new updates are available. The antivirus software is configured to scan workstations on an ongoing basis. Information assets, software, hardware, tools, and applications introduced into the environment are scanned for vulnerabilities and malware prior to implementation into the environment.

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.	Management has defined configuration standards in the information security policies and procedures. Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. The monitoring software is configured to alert IT personnel when thresholds have been exceeded. An IDS is utilized to analyze network events and report possible or actual network security breaches. The IDS is configured to notify personnel upon intrusion detection. FIM software is in place to ensure only authorized changes are deployed into the production environment. The FIM software is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected. A firewall is in place to filter unauthorized inbound network traffic from the internet. The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule. Policies and procedures are in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment. Internal vulnerability scans and penetration tests are performed on at least an annual basis and remedial actions are taken where 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.	Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints. Policies and procedures are in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment. The monitoring software is configured to alert IT personnel when thresholds have been exceeded. Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. An IDS is utilized to analyze network events and report possible or actual network security breaches.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
System Operations		
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**
		The IDS is configured to notify personnel upon intrusion detection. FIM software is in place to ensure only authorized changes are deployed into the production environment. The FIM software is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected. A firewall is in place to filter unauthorized inbound network traffic from the internet. The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule. Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software. The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available. The antivirus software is configured to scan workstations on an ongoing basis. The entity's third-party agreement requires third-parties to implement detective controls and provide notice if the third-party's environment is compromised.
	Network (GCP)	
		Network account lockout settings are in place. Network audit logging settings are in place. Network audit logs are maintained and can be pulled for review at any time.
	Operating System (Linux)	
		Operating systems are configured to enforce password lockout requirements. Operating system audit logging settings are in place. Operating system audit logs are maintained and can be pulled for review at any time.
	Database (MySQL)	
		Databases are configured to enforce password requirements. Database audit logging settings are in place. Database audit logs are maintained and reviewed as-needed.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
System Operations		
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**
	Application	
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.	Application audit policy settings are in place. Application audit logs are maintained and reviewed as-needed. Management reviews reports on an annual basis summarizing incidents, root cause of incidents, and corrective action plans and as part of the review, management identifies the need for system changes and implementation of additional controls based on incident patterns and root causes. Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints. The incident response and escalation procedures are reviewed at least annually for effectiveness. The incident response policies and procedures define the classification of incidents based on its severity. Resolution of incidents are documented within the ticket and communicated to affected users. Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution. A security incident analysis is performed for critical incidents to determine the root cause, system impact and resolution. Identified incidents are reviewed, monitored and investigated by an incident response team. Incidents resulting in the unauthorized use or disclosure of personal information are communicated to the affected users. Identified incidents are analyzed, classified and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach.

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.	Roles and responsibilities for the design, implementation, maintenance, and execution of the incident response program are defined and documented. Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints. Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution. The actions taken to address identified security incidents are documented and communicated to affected parties. Documented incident response and escalation procedures are in place to guide personnel in addressing the threats posed by security incidents. Critical security incidents that result in a service/business operation disruption are communicated to those affected through e-mails. Resolution of incidents are documented within the ticket and communicated to affected users. Remediation actions taken for security incidents are documented within the ticket and communicated to affected users. Identified incidents are analyzed, classified and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach. A security incident analysis is performed for critical incidents to determine the root cause, system impact and resolution. The incident response and escalation procedures are reviewed at least annually for effectiveness. Management reviews reports on an annual basis summarizing incidents, root cause of incidents, and corrective action plans and as part of the review, management identifies the need for system changes and implementation of additional controls based on incident patterns and root causes.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
System Operations		
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Change management requests are opened for incidents that require permanent fixes. The entity restores system operations for incidents impacting the environment through activities that include, but are not limited to: • Rebuilding systems • Updating software • Installing patches • Removing unauthorized access • Changing configurations Data backup and restore procedures are in place to guide personnel in performing backup activities. Backup restoration tests are performed on at least an annual basis. Management reviews reports on an annual basis summarizing incidents, root cause of incidents, and corrective action plans and as part of the review, management identifies the need for system changes and implementation of additional controls based on incident patterns and root causes. A security incident analysis is performed for critical incidents to determine the root cause, system impact, and to determine the resolution. After critical incidents are investigated and addressed, lessons learned are documented and analyzed, and incident response plans and recovery procedures are updated based on the lessons learned. A business continuity and disaster recovery plan is documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations. The disaster recovery plan is tested on an annual basis.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Change Management		
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**
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.	Documented change control policies and procedures are in place to guide personnel in the change management process. System changes are communicated to both affected internal and external users. Access to implement changes in the production environment is restricted to authorized IT personnel. System changes are authorized and approved by management prior to implementation. Prior code is held in the source code repository for rollback capability in the event that a system change does not function as designed. Development and test environments are physically and logically separated from the production environment. System change requests are documented and tracked in a ticketing system. FIM software is utilized to help detect unauthorized changes within the production environment. Back out procedures are documented within each change implementation to allow for rollback of changes when changes impair system operation. System changes are tested prior to implementation. Types of testing performed depend on the nature of the change. System changes implemented for remediating incidents follow the standard change management process. Information security policies and procedures document the baseline requirements for configuration of IT systems and tools. Documented change control policies and procedures are in place to guide personnel in implementing changes in an emergency situation.

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.	Documented policies and procedures are in place to guide personnel in performing risk mitigation activities. Management has defined a formal risk assessment process that specifies the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances. A formal risk assessment is performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements. Identified risks are rated using a risk evaluation process and ratings are approved by management. Risks identified as a part of the risk assessment process are addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk Management develops risk mitigation strategies to address risks identified during the risk assessment process.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	Management has defined a third-party vendor risk management process that specifies the process for evaluating third-party risks based on identified threats and the specified tolerances. Management develops third-party risk mitigation strategies to address risks identified during the risk assessment process. Identified third-party risks are rated using a risk evaluation process and ratings are approved by management. The entity's third-party agreement outlines and communicates: • The scope of services • Roles and responsibilities • Terms of the business relationship • Communication protocols • Compliance requirements • Service levels • Just cause for terminating the relationship Management obtains and reviews attestation reports of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Risk Mitigation		
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**
		A formal third-party risk assessment is performed on an annual basis to identify threats that could impair system commitments and requirements. Management has assigned responsibility and accountability for the management of risks associated with third-parties to appropriate personnel. Management has established exception handling procedures for services provided by third-parties. The entity has documented procedures for addressing issues identified with third-parties. The entity has documented procedures for terminating third-party relationships.

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 Plutoshift was limited to the Trust Services Criteria, related criteria and control activities specified by the management of Plutoshift and did not encompass all aspects of Plutoshift'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.