People Data Labs

System and Organization Controls (SOC) 3

Report on PDL's Service System

Relevant to the Trust Services Criteria Security Category

For the Period
June 01, 2021 to September 30, 2021

Table of Contents

I. INDEPENDENT SERVICE AUDITORS' REPORT

Independent Service Auditor's Report

To Management of People Data Labs, Inc.

Scope

We have examined management's assertion, contained within the accompanying "Assertion of People Data Labs, Inc. Management" (assertion) that People Data Labs, Inc.'s controls over the PDL's Service System (system) were effective throughout the period June 01, 2021 to September 30, 2021, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the criteria relevant to security (applicable trust services criteria) set forth in the AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

Service Organization's Responsibilities

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

Service Auditors' Responsibilities

Our responsibility is to express an opinion on the assertion, 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 management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion, which includes: (1) obtaining an understanding of People Data Labs' relevant security policies, processes and controls, (2) testing and evaluating the operating effectiveness of the controls, and (3) performing such other procedures as we considered necessary in the circumstances. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence obtained during our examination is sufficient to provide a reasonable basis for our opinion.

Inherent Limitations

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that People Data Labs, Inc.'s service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions

about the suitability of the design or operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, People Data Labs, Inc.'s controls over the system were effective throughout the period June 01, 2021 to September 30, 2021, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the applicable trust services criteria.

JohansonGroup LLP

Colorado Springs, Colorado
October 15, 2021

II. ASSERTION OF PEOPLE DATA LABS, INC. MANAGEMENT

People Data Labs

Assertion of People Data Labs, Inc. Management

We are responsible for designing, implementing, operating, and maintaining effective controls within the People Data Labs Platform (system) throughout the period June 01, 2021 to September 30, 2021, to provide reasonable assurance that People Data Labs, Inc.'s service commitments and system requirements relevant to security were achieved. Our description of the boundaries of the system is presented in the section of this report titled, "People Data Labs, Inc. Description of the System," (description) and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period June 01, 2021 to September 30, 2021, to provide reasonable assurance that People Data Labs, Inc.'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*).

People Data Labs, Inc.'s objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in the accompanying system description.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period June 01, 2021 to September 30, 2021, to provide reasonable assurance that People Data Labs, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria.

People Data Labs, Inc. Management
October 15, 2021

III. DESCRIPTION OF PDL'S SERVICE SYSTEM

People Data Labs

Description of PDL's Service System

COMPANY BACKGROUND

Founded in 2015 by Henry Nevue and Sean Thorne, People Data Labs began as recruiting software, intended to help companies better understand and source candidates. Quickly, it became clear that our work extended far beyond recruiting. Henry and Sean began finding more and more diverse clients requesting access to PDL's raw data.

The PDL platform seeks to enable all companies to build compliant people data solutions. Our sole focus is on building the best data available by integrating thousands of compliantly sourced datasets into a single, developer friendly source of truth. Over 2.5 billion profiles are used by leading companies to enrich recruiting platforms, power AI models, create custom audiences, and more.

PDL was founded by a group of entrepreneurs from the SaaS space, with deep experience in data integration and simple, intuitive user experience, and is backed by Susa Ventures is an early-stage venture capital firm and a cadre of top-tier angel investors.

SERVICES PROVIDED

The PDL platform makes it incredibly easy for data teams and operators to enrich data from compliantly sourced datasets to augment their databases. PDL is delivered as a web API or licensed database. This allows engineering, data science, product, and other technical teams to build compliant, innovative, people data-based software solutions.

PDL also provides tools for creating new data models via API queries, browsing existing data, and enriching data pipelines.

PDL is designed to be secure by default, with an architecture designed to be compliant with NIST 800-53 standards and built on AWS best business practices.

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

PDL designs its processes and procedures related to its platform to meet its objectives for API services. Those objectives are based on the service commitments that PDL makes to user entities, the laws and regulations that govern the provision of PDL services, and the financial, operational, and compliance requirements that PDL has established for the services. The API services of PDL are subject to the security and privacy requirements of state and local privacy security laws and regulations in the jurisdictions in which PDL operates.

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

Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of the PDL platform that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role.
- Use of encryption technologies to protect customer data both at rest and in transit.

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

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

Our SLA uptime is 99.95% and we have an RTO and RPO of 24 hours.

COMPONENTS OF THE SYSTEM

Infrastructure

The primary infrastructure used to provide PDL's Services system includes the following:

Primary Infrastructure		
Platform	Type	Purpose
AWS	S3	Source Data Repository
	IAM / AWS SSO	User Access Management
	ECR	Services
	EC2 / VPC /ELB	Services
	RedShift	Data Warehouse
	RDS	Database Services
	Route53	DNS Services including DNSSEC
	AWS Firewall	Firewall /WAF
	Systems Manager	Maintain Security Patching
	CloudWatch	Log Monitoring
	Control Tower	Configuration management
	Lambada and Various others	Various uses
	Elastic Search	API Searching
Maintained by infrastructure as code		

Software

The primary software used to provide PDL's Services system includes the following:

Primary Software		
Software	Operating System	Purpose
Python	Linux	Primary development language/runtime for all PDL applications
PostgreSQL	Linux	Transactional database for PDL data
Redis	Linux	Used to maintain the PDL job queue, the core of our sync engine
Pulumi	SaaS	Infrastructure as Code

People

PDL has a staff of 75 employees and contractors organized into the following functional areas:

- **Management:** Individuals who are responsible for enabling other employees to perform their jobs effectively and for maintaining security and compliance across the environment.
- **Product Engineering:** Product managers and software engineers who design and maintain the PDL sync product, including the web interface, the proprietary sync engine, the job queuing infrastructure, and all debugging tools. This team designs and implements new PDL functionality assesses and remediates any issues or bugs found in the PDL product, and architects and deploys the underlying cloud infrastructure on which PDL runs. This team also implements new data warehouse and SaaS connections for the PDL sync engine. Members of the product team are responsible for peer reviews of code and infrastructure designed and authored within the team.
- **Infrastructure:** The monitoring and maintenance of the PDL product (once deployed) is handled by the operations role, which involves proactively designing and deploying monitoring software and tools to help identify errors or bugs in the PDL product and remediate them either directly or via feedback to the product team. The operations team responds to alerts generated by our system, identifies issues with both PDL's sync engine and the configurations and SQL queries created by PDL customers, and determines the best path to resolution. Operators also ensure that syncs are performing optimally (with high throughput and low latency) and that PDL is using the correct cloud infrastructure and scale to maintain high sync performance. Finally, operators are responsible for responding to any potential security issues with PDL and notifying affected customers if applicable.
- **Revenue Operations:** Individuals with commercial roles work to market, sell, and support PDL software. They are usually the primary point of contact to PDL customers. They help identify which parts of the PDL system are most useful to prospective customers, and what new product development or new sync connections need to be engineered to meet customer needs. In the marketing role, PDL employees identify best practices for automating business operations and provide that information to PDL customers and prospective customers via webinars, blog posts, white papers, and other channels. Finally, the PDL customer success team ensures that PDL customers can use the product effectively and without errors, by assisting PDL customers with onboarding into the product, helping identify useful

data sources and author SQL models, and proactively identifying any issues or bugs that occur when users try to sync their data.

Data

There are four major types of data used by PDL:

- **Configuration Data:** Data used to configure PDL syncs
- **Customer Data:** Data owned by PDL customers that PDL copies back and forth from data warehouses to SaaS applications
- **People Data:** Data that is our proprietary blend of commercial and open-source information on individuals and companies worldwide
- **Log Data:** Logs, traces, and samples produced by the PDL sync engine while performing customer-configured syncs

Configuration Data is stored in PDL primary PostgreSQL databases and includes:

- People Data Labs' customers' email addresses, names, and company names
- Credentials for accessing data warehouses, SaaS applications, and source code repositories, including usernames, passwords, OAuth tokens, and certificates
- The names of databases, schemata, tables, columns, custom objects, and custom fields in customers' data warehouses and SaaS applications
- Configuration objects that determine how data is copied between systems, including field mappings, update policies, and schedules
- Models (SQL queries) are stored in PDL by customers to provide logical views over data before being synced.
- Audit logs covering changes to each of the above items

Configuration Data is treated as sensitive by PDL. It is stored with a limited lifetime when possible. Access controls limit configuration data access to each customer's PDL organization. Customers can invite other people in their company to access their PDL organization and read and write configuration data. PDL operators may access configuration data to troubleshoot customer issues or to gather feedback for improving the PDL product.

Customer Data is sensitive data in the PDL system, and PDL does not store it longer than necessary. It is currently impossible for PDL to sync data from data warehouses directly to SaaS applications without handling customer data, so we attempt to limit that handling as much as possible and offload as much processing to customer infrastructure as we can. When PDL does handle customer data, it is restricted to roles-based access control. The data is never used for any other purposes than defined in our privacy statement.

People Data is the most valuable resource for PDL systems. It is the basis of our revenue generation. It is stored as long as it is relevant and has not been removed by a data subject via privacy request or GDPR request. It has a long lifetime and is protected by a layered defense system and backed up in multiple availability zones for redundancy.

Log Data is produced by the sync engine to make it easier for PDL operators to monitor the health of the system and track down any issues. Log data is a trace of the actions performed by the system in the course of normal operations. Log data will include snapshots of Configuration Data at the time the sync was performed, so operators can see what the sync engine was attempting to do. Log data also includes stack traces and samples of running code. Due to the nature of logging frameworks, there is a small possibility that log data can also include Customer Data captured by automatic tracers. People Data Labs endeavors to "scrub" logs of any Customer Data before they are persisted. Log data may be stored by vendors that PDL has entrusted for purposes like indexing, monitoring, and trending. Regardless of whether log data is stored within People Data Labs' internal databases or by vendors, it is given a limited lifetime and automatically removed. Log data is retained for 365 days by default; longer or shorter as required by specific contracts.

All data types processed by PDL are encrypted on the wire using TLS 1.2 with high-security protocols. No networking connections used by PDL for any purpose will ever send unencrypted data. In addition, all Configuration Data and Log Data, as well as samples of Customer Data are stored by PDL with encrypted at rest, in our internal databases, our caches, and our cloud storage. The encryption used will be upgraded as required to maintain compliance with NIST 800-53 moderate standards and industry best practices.

PROCESSES 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 PDL policies and procedures that define how services should be delivered. These are located on the Company's Notion intranet and can be accessed by any PDL team member. They are reviewed annually and modified as soon as required to maintain relevance to current operational requirements.

Physical Security

All data is hosted by Amazon Web Services (AWS) and backup servers by Opus systems. AWS data centers do not allow PDL employees physical access. At present, PDL does not maintain any office space, and all work is conducted remotely. All physical security is inherited by the provider.

Logical Access

PDL employees and contractors are granted access to infrastructure via a role-based access control system, to ensure uniform, least-privilege access to identified users and to maintain simple and repeatable user provisioning and de-provisioning processes.

PDL infrastructure runs entirely on cloud and SaaS-based systems, and as such, the resources used by employees to perform their roles are accounts and permissions within those systems. An employee can have one of their access levels to a SaaS or cloud service:

- Administrator – can alter policies and provision or de-provision users
- Engineering – Power User, can alter or maintain any part of AWS infrastructure except IAM, billing, and certain other functions
- Revenue – Limited to certain areas and S3 Buckets
- Finance-Admin – Full Control of billing and payment functions for AWS Services
- Billing – Access to billing and reporting
- Technical Services – Limited access to certain S3 buckets
- Audit/ReadOnly – Security Audit Level Privileges assigned to the security team and certain engineering members for troubleshooting.
- No access

Roles are reviewed on an annual basis by management and the security team to ensure least-privilege access.

PDL identifies employees primarily by their email address in Rippling.Com. Rippling functions as our HR System, corporate directory, and SSO provider. The PDL password policy mandates that employees and contractors use their Rippling credentials to sign in to SaaS and cloud tools when supported. When Rippling sign-in is not available, employees may authenticate using a strong, unique password, which must be stored in an approved password manager. We maintain Google Workspace and Github Credentials for specialty services that don't have SSO/SAML capabilities.

The PDL Rippling service requires users to use a multi-factor for authentication. In addition, any SaaS applications used by the company that doesn't use Rippling sign-in must be configured to use Google Workspace, Github, or a second factor when possible.

The HR team is responsible for onboarding new employees. Rippling is responsible for provisioning and deprovisioning Google Workplace and other SaaS accounts as dictated by the employee's role and after performing a background check, and the employee is responsible for reviewing PDL policies, completing a security training, and successfully gaining access to provisioned accounts (as well as enrolling a device for second-factor authentication). These steps must be completed within 30 days of hire.

When an employee is terminated, Rippling is responsible for removing or disabling the employee's accounts immediately and Information Security will audit that all access is terminated within 3 business days.

PDL employees must use a company-provided computer to perform their duties. Contractors may elect to "bring their own" device if that device is approved by the security team. Any computer (company-owned or BYOD) on which a PDL workforce member performs sensitive work must employ full-disk encryption, Rippling MDM, Vanta agent, and have an approved endpoint monitoring tool installed. On employee termination or end of a contract, management will ensure the return of company-owned devices and handle their de-provisioning or reprovisioning based on the company's Asset Management policy.

Computer Operations – Backups

Customer and People data is backed up by PDL's infrastructure team via automation. In the event of an exception, infrastructure personnel will perform troubleshooting to identify the root cause and then re-run the backup job immediately or as part of the next scheduled backup job.

Backup infrastructure is maintained in AWS, with physical access restricted according to applicable AWS policies. All backups are encrypted using KMS-managed encryption keys, with access restricted to key personnel via AWS IAM permissions.

Computer Operations – Availability

PDL maintains an Incident Response Policy that gives any PDL employee the ability to initiate a response to a potential security incident by notifying the internal security team through several channels and assists in classifying the severity of the incident.

External parties (customers and third-party security researchers) are also given a channel to send encrypted incident reports and responsibly disclose potential issues to the PDL security team.

Internally, the PDL operations team monitors the health of all applications, including the PDL web UI, sync engine, databases, and cloud storage. Monitoring includes the availability and performance of the web UI, the throughput and queuing latency of the job scheduler, and any faults or errors encountered by users while configuring PDL or while their data is being synced by PDL. Critical incidents are routed to an on-call operator who is responsible for acknowledging within one hour; if there is no acknowledgment, the incident is escalated to the rest of the operations team.

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

Change Control

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

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

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

Data Communications

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

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

People Data Labs engages an external security firm to perform annual penetration testing to look for unidentified vulnerabilities, and the product engineering team responds to any issues identified via the regular incident response and change management process.

PDL does not maintain a corporate network. PDL uses a VPN to connect to all infrastructure uses SaaS cloud applications hosted on the public internet and secured by TLS 1.2 or higher connections. All SaaS applications are protected by multifactor authentication and when possible IP whitelisting.

BOUNDARIES OF THE SYSTEM

The scope of this report includes the Services performed by PDL. This report does not include the data center hosting services provided by AWS or OPUS.

THE APPLICABLE TRUST SERVICES CRITERIA AND THE RELATED CONTROLS

Common Criteria (to the Security, Availability, and Confidentiality Categories)
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 removals of information or system resources, misuse of software licenses, and improper access to or use of, alteration, destruction, or disclosure of information.

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 PDL's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of PDL'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 and leadership 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 to sign an acknowledgment form indicating they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual.
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties is a component of the employee handbook.
- Background checks are performed for employees as a component of the hiring process.
- Annual and ongoing training on topics of Security Awareness, Secure Coding Principals, Privacy Act, GDPR, Ethics, and others are provided to all employees and tracking in the KnowBe4 application.

Commitment to Competence

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

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

- Management has considered the competence levels for 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.
- Corporate-wide "Hackathons" that involve all business units are scheduled to improve skills and understanding of the PDL applications stack.

Management's Philosophy and Operating Style

The PDL management team must balance two competing interests: continuing to grow and develop in a cutting-edge, rapidly changing technology space while remaining excellent and conservative stewards of the highly sensitive data and workflows our customers entrust to us.

The management team meets weekly to be briefed on technology changes that impact the way PDL can help customers build data workflows, as well as new security technologies that can help protect those workflows, and finally any regulatory changes that may require PDL to alter its software to maintain legal compliance. Major planned changes to the business are also reviewed by the management team to ensure they can be conducted in a way that is compatible with our core product offerings and duties to new and existing customers.

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

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

Organizational Structure and Assignment of Authority and Responsibility

PDL is currently organized into three major departments:
General / Administrative
Revenue Operations
Product and Engineering
Each major department has its own management team and reporting structure.
Specific control activities that the service organization has implemented in this area are described below:

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

Human Resource Policies and Practices

PDL'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. PDL's human resources policies and practices relating 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 acknowledgment 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.
- Employees are educated in PDL engineering and learn how it all works.

RISK ASSESSMENT PROCESS

PDL's risk assessment process identifies and manages risks that could potentially affect PDL's ability to provide reliable and secure services to our customers. As part of this process, PDL maintains a risk register to track all systems and procedures that could present risks to meeting the company's objectives. Risks are evaluated by likelihood and impact, and management creates tasks to address risks that score highly on both dimensions. The risk register is re-evaluated annually, and tasks are incorporated into the regular PDL product development process so they can be dealt with predictably and iteratively.

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of PDL's system; as well as the nature of the components of the system result in risks that the criteria will not be met. PDL 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, PDL'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 are integral components of PDL'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.

PDL uses several information and communication channels internally to share information with management, employees, contractors, and customers. PDL uses chat systems (Slack) and email as the primary internal and external communications channels.

Structured data is communicated internally via our SaaS applications and our project management tools (Asana). Finally, PDL uses in-person and Zoom video "all hands" meetings to communicate company priorities and goals from management to all employees.

MONITORING CONTROLS

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

also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

On-Going Monitoring

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

Management's close involvement in PDL's operations helps to identify significant variances from expectations regarding internal controls. Executive 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. This process aims to ensure legal compliance and maximize the performance of PDL's personnel.

Reporting Deficiencies

Our internal risk management tracking tool is utilized to document and track the results of ongoing monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks, and instructions for escalation are supplied to employees in company policy documents. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

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 date.

INCIDENTS IN THE LAST 12 MONTHS

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

CRITERIA NOT APPLICABLE TO THE SYSTEM

All relevant trust services criteria were applied to the PDL Services system.

SUBSERVICE ORGANIZATIONS

PDL's services are designed with the assumption that certain controls will be implemented by sub-service organizations. Such controls are called complementary sub-service organization controls. It is not feasible for all the trust services criteria related to PDL's services to be solely achieved by PDL control procedures.

Accordingly, subservice organizations, in conjunction with the services, should establish their independent internal controls or procedures to complement those of PDL.

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

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

PDL management, along with the sub-service organization, defines 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, PDL performs monitoring of the sub-service organization controls, including the following procedures

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

COMPLEMENTARY USER ENTITY CONTROLS

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

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