UHY LLP
Certified Public Accountants

Plivo

Cloud Communications Platform

SOC 3®

UHY LLP
www.uhy-us.com

The next level of service

TABLE OF CONTENTS

Section 1:

Independent Service Auditor's Report

Independent Service Auditor's Report

To the Management of:
Plivo, Inc.
Austin, TX

Scope

We have examined Plivo Inc.'s (Plivo) accompanying assertion titled "Plivo Inc.'s Management Assertion" (assertion) that the controls within the Plivo Cloud Communication Platform (the System) were effective throughout the period September 15, 2021 to December 15, 2021, to provide reasonable assurance that Plivo's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (the applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (trust services criteria).

Service Organization's Responsibilities

Plivo 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 Plivo's service commitments and system requirements were achieved. Plivo has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Plivo is responsible for selecting, and identifying, in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the System.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the System were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. 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. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the System and the service organization's service commitments and system requirements.
- Assessing the risks that controls were not effective to achieve Plivo's service commitments and system requirements based on the applicable trust services criteria.
- Performing procedures to obtain evidence about whether controls within the System were effective to achieve Plivo's service commitments and system requirements based the applicable trust services criteria.

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

Inherent Limitations

There are inherent limitations in the effectiveness of 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 the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the 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, management's assertion that the controls within the Plivo Cloud Communication Platform were effective throughout the period September 15, 2021 to December 15, 2021 to provide reasonable assurance that Plivo's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

April 11, 2022
West Des Moines, IA

Section 2:

Plivo, Inc.'s Management Assertion

Plivo Inc.'s Management Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within Plivo Cloud Communication Platform (the System) throughout the period September 15, 2021 to December 15, 2021, to provide reasonable assurance that Plivo's service commitments and system requirements relevant to security and availability were achieved. Our description of the boundaries of the System is presented in attachment A 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 September 15, 2021 to December 15, 2021, to provide reasonable assurance that Plivo's service commitments and system requirements were achieved based on the trust services criteria relevant to security, and availability (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).

Plivo'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 attachment B.

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 September 15, 2021 to December 15, 2021, to provide reasonable assurance that Plivo's service commitments and system requirements were achieved based on the applicable trust services criteria.

Management of Plivo

Attachment A:

Plivo's Description of the Boundaries of the Cloud Communications Platform

Attachment A: Plivo's Description of the Boundaries of the Cloud Communications Platform

Overview

Plivo Inc. (hereafter referred as the Company/Plivo) offers a Cloud Communication Platform as a Service (CPaaS) - a simple, quick, and scalable way to modernize customer communications.

Businesses of all sizes, from growing startups to public companies, have been relying on Plivo to deliver better customer experiences for over 10 years. Plivo's enterprise-grade communications platform includes a premium carrier network with connectivity in more than 190 countries, an API platform for messaging and voice calls, and solutions for sales and support teams. Plivo has over 200 employees.

Infrastructure

The Plivo Platform (the System or Platform) is a SaaS multi-tenant client-server application hosted in Amazon Web Services (AWS). Their data is logically separated and not accessible to other tenants to prevent unauthorized access.

Production environments for each component of the System are hosted in AWS and managed by the Plivo Engineering and DevOps team. These environments are separated logically and access to the production environment is strictly limited to authorized personnel. The Plivo application runs within AWS virtual private clouds (VPCs) using multiple availability zones for resiliency. The application runs on an Amazon Elastic Compute Cloud (EC2) instance hardened as per Center for Internet Security (CIS) standards.

Software

Plivo uses cloud storage and computing services from AWS. Plivo does not own or maintain hardware located in the AWS data centers and operates under a shared security responsibility model, where AWS is responsible for the security of the underlying cloud infrastructure (i.e. physical infrastructure, geographical regions, availability zones, edge locations, operating, managing and controlling the components from the host operating system, virtualization layer and storage) and Plivo is responsible for securing the application platform deployed in AWS (i.e. applications, identity access management, operating system and network virtual security groups configuration, network traffic, server-side encryption). Production servers and client-facing applications are logically secured.

People

The Company's control environment is implemented, maintained, and supported by Senior Management, Product, Engineering, DevOps, Security, Information Security (IT), Operations, Sales, Customer Support, Legal, PeopleOps, and Network and Security Operations.

Processes, Policies and Procedures

Logical and Physical Access

The Access Control Policy establishes the access control requirements for requesting and provisioning

user access for the System. The policy requires that access be denied by default, follow a least privilege principle, and be granted only upon business need. Each user account is unique and is identifiable to an individual user. Segregation of duties is established for critical functions within the environment to minimize the risk of unauthorized changes to production systems.

Access to the production environment is controlled through a designated set of jump servers and restricted to authorized individuals. Users are authenticated to virtual private network (VPN) as a first step using AWS Managed AD credentials and then to the jump server depending on where the production servers are located. Jump servers are accessed using username and SSH Key authentication which are restricted to authorized individuals and system processes based on job responsibilities.

Application Development

Software, system, and configuration changes including major releases, minor releases and hot fixes are managed through a change and release management procedure, and tracked using a centralized ticketing system. Changes are requested, approved, tracked, and implemented throughout the release life cycle, which can include product and engineering planning, release management, deployment, and post deployment support phases. Change requests are documented, assessed for their risks, and evaluated and approved for acceptance by the designated personnel.

Change Management

The Plivo development process is a formalized, process-driven approach intended to maintain the stability of production systems. This process dictates how changes to Plivo-developed systems are documented, tested, reviewed, approved, and deployed. Program change documents and security best practices are documented on the Plivo wiki and within the Engineering documentation repository.

Software Maintenance

Plivo has implemented a software maintenance standard for applying bug fixes and security updates to servers and specified applications. Maintenance changes are categorized into the following four (4) classifications: New Releases, Major Updates, Security Updates, and Bug Fixes.

Asset Management

Assets are tracked through their lifecycle from acquisition to final disposition. All such assets are assigned ownership by a designated department or team within the Company and prioritized based on the asset's business value and criticality to the Company. This classification process is owned by the Engineering and DevOps teams. Workstations and laptops have endpoint protections installed, including anti-malware/anti-virus software, full disk encryption, and personal firewalls and are subject to routine patching. The inventory of servers is also monitored and maintained by the Engineering and DevOps teams. In addition, network architecture is maintained as part of the inventory process.

System and Security Monitoring

Automated mechanisms and periodic scanning have been deployed to detect and troubleshoot exceptions or deviations in the production environment. The engineering reviews and updates configuration settings and baseline configurations quarterly.

Security Incident Management

An incident response plan defines roles, responsibilities, escalation paths, and communication requirements in case of incidents that affect the security, or availability of the System. Each identified incident is logged, investigated and rapidly remediated by the the Plivo team.

Vendor Management

Vendors that are considered subservice organizations are reviewed in the annual subservice organization review, which requires the review of a SOC report (or other certification reports) or completion of a vendor questionnaire. The Security Team reviews the compliance reports or questionnaires for issues that might impact the Platform and implements mitigating procedures, as necessary, to bring vendor risk to acceptable levels.

Business Continuity Management

The Company has designed and configured the Platform for high availability and redundancy. Production data hosted in AWS is configured in active-active setup. Snapshots of production data are taken daily and are retained in accordance with internal best practices. Backup restoration testing is performed annually to ensure the Platform disaster recovery plans are effective and to ensure data integrity is maintained after the restore.

Data

The following data is collected and supported by the System:

- Contact data (name, address, email, company, phone number, IP address)
- User feedback about our service
- Sending and receiving phone numbers and text content, including your current phone number
- Voice recordings
- Payment management information, including payment method and history of usage and payments
- E-mail address and name
- Cookie tracking, including IP address, device type, and location

Encryption is used to protect all system and customer data in transit and at rest, based on the data classification.

Complementary User Entity Controls (CUECs)

Plivo controls related to the Plivo Platform cover only a portion of overall internal control for each user entity of the Plivo Platform. The processes and services provided by the Company were designed with the assumption that certain controls would be implemented by user entities to meet their specific operational needs. In particular situations, the application of specified internal controls at user entities contribute significantly to the overall achievement of various trust services criteria included in this report. Therefore, each user entity's internal control should be evaluated in conjunction with the Company's controls, considering the related CUECs identified for the specific criterion. For user entities to rely on the controls reported herein, each user entity must evaluate its own internal control to determine whether the

identified CUECs have been implemented and are operating effectively.

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

Complementary User-Entity Controls	Applicable TSC
User entities are responsible for the accuracy, quality, integrity, legality, reliability, and appropriateness of all data entered to the System.	CC2.1
User entities are responsible for complying with their contractual obligations to Plivo.	CC2.3
User entities are responsible for ensuring their personnel adhere to the policies and procedures on the use of the System.	CC5.1, CC5.2
User entities are responsible for managing, rotating, and resetting passwords for all employee users with access to the System.	CC6.1
User entities are responsible for notifying Plivo when user entity data should be securely removed from the System. Termination of a contract does not automatically result in disposal of customer data.	CC6.2, C1.2
User entities are responsible for managing access (including provisioning and removing access) to their account using the administrator account within the System.	CC6.2
User entities are responsible for ensuring that only authorized individuals have the ability to access, modify, and delete information from the System.	CC6.2, CC6.3
User entities are responsible for using the Plivo Console to monitor user access to the System.	CC6.3
User entities are responsible for securing and monitoring the user entity's data and the usage of that data.	CC7.1, CC7.2
User entities are expected to notify Plivo if they suspect or learn of unauthorized access to the System.	CC7.3
User entities are responsible for reporting unusual or exceptional usage of the System immediately.	CC7.3
User entities are responsible for reporting to Plivo any incidents and breaches that may impact the System.	CC7.3
User entities are responsible for understanding the SLA for third-party systems that they purchase from such vendors that are integrated with the System.	CC9.2
User entities are responsible for establishing and communicating their privacy and security policies to their users and getting consent from end users toprovide any PII to the Company.	P2.1
User entities are responsible for amending or correcting inaccurate Personal Identifiable Information (PII) maintained by Plivo through the Plivo API or Plivo Console.	P5.1

Subservice Organizations and Complementary Subservice Organization Controls (CSOCs)

Plivo uses third-party service organizations to provide services related to the security and availability trust services criteria. This report includes only those controls at Plivo and does not include the controls of the subservice organizations set forth in the table below.

Subservice Organization Name	Service Provided
Amazon Web Services, Inc. (AWS)	Provide cloud infrastructure environment and storage of customer data.
Google LLC (Google)	Speech Recognition and Google Cloud Messaging (GCM) - Mobile SDK notifications for Android - Send push notifications.
Apple, Inc. (Apple)	Apple Push Notification Service (APNS) - Mobile SDK notifications for iOS - Send push notifications.
Redis Labs	Caching provider.

Although the subservice organizations have been carved out for the purposes of this report, certain service commitments, system requirements, and applicable criteria are intended to be met by controls at the subservice organizations. The Company monitors the services performed by subservice organizations by ensuring compliance with service agreements and performing a periodic vendor due diligence review which includes a review of the subservice organizations SOC 2 report.

The following complementary subservice organization controls are expected to be implemented at the subservice organizations; however, they should not be regarded as a comprehensive list of all the controls that should be employed by the subservice organizations.

Applicable Trust Services Criteria	Control Activity Expected to be Implemented by the Subservice Organizations
CC6.1, CC6.2, CC6.3, CC6.4, CC6.5, CC6.6, CC6.7, CC9.2	AWS, Google, Apple, and Redis Labs are responsible for restricting logical access to programs, data, and computer resources to authorized and appropriate users and ensuring those users are restricted to performing authorized and appropriate actions.
CC3.1, CC9.2	AWS, Google, Apple, and Redis Labs are responsible for implementing measures to prevent or mitigate threats consistent with the risk assessment.
CC6.1, CC6.6	AWS is responsible for maintaining segregation of Plivo's environments from other AWS clients.
C1.2, C.1.3, C1.4	AWS is responsible for the management of any third-party vendors with access to customer environments.
CC6.4, CC6.5	AWS is responsible for implementing physical security controls to restrict access to the data centers to authorized personnel.
CC7.2	AWS is responsible for monitoring and providing alerts of unauthorized access to network infrastructure and detected failures in the control environment.
CC8.1	AWS, Google, Apple, and Redis Labs are responsible for implementing change management procedures that engage the Company when changes are expected to impact the Plivo Platform.
A1.2	AWS is responsible for monitoring environmental conditions (temperature, fire, and water), leak detection, UPS battery life and capacity, and other key equipment to help maintain the availability of services.

Applicable Trust Services Criteria	Control Activity Expected to be Implemented by the Subservice Organizations
A1.2	AWS is responsible for the backup and recovery of data in their environment and to notify Tugboat Logic of any issues regarding the availability or integrity of their backup data.

Attachment B:

Plivo's Cloud Communication Platform Principal Service Commitments and System Requirements

Attachment B: Plivo's Cloud Communication Platform Principal Service Commitments and System Requirements

Scope of the System

The System description has been prepared to provide information on Plivo's control environment over its Cloud Communication Platform throughout the period September 15, 2021 to December 15, 2021 in relation to the security and availability trust services categories.

Principal Service Commitments and System Requirements

The Company's policies and procedures are based on the service commitments it makes to user entities; the laws and regulations that govern its services; and the financial, operational, and compliance requirements that Plivo has established for its services. The applicable use policy and the terms and conditions applicable to the Plivo services are as set forth at www.plivo.com/legal/tos/. Plivo privacy commitments are documented on the Plivo Website (www.plivo.com/legal/privacy/). Plivo may from time to time enter into master services agreements and other contracts with its customers, when necessary.

Plivo has developed and implemented standard operational procedures that support the achievement of its services, security, and privacy commitments; relevant laws and regulations; and other system requirements. Such requirements are communicated in the Company's policies and procedures, system design documentation, and contracts and/or other communications with clients.

Plivo principal service commitments and system requirements include the following:

Trust Services Category	Service Commitments	System Requirements
Security	● Plivo's principal security and availability service commitments include: – Security commitments are documented under a separate agreement or contract, where requested for by the user entity and/or customer. – Plivo will comply with all applicable laws and regulations in handling of customer data and performance of services. – Data is transmitted securely over SSL and stored in a database that is encrypted at rest using industry standard encryption algorithms.	● Logical access standards ● Physical access standards ● Employee provisioning and deprovisioning standards ● Access Control ● Access reviews ● Authentication ● Encryption standards ● Intrusion detection and prevention standards ● Risk and vulnerability management standards ● Configuration management ● Incident handling standards ● Change management standards ● Vendor management ● Endpoint Security Standard or Workstation Security ● Serverless Security ● Software Development LifeCycle

Trust Services Category	Service Commitments	System Requirements
(continued)	(continued)	• Environment Separation • Logging • Monitoring • CIS Standard Hardening and Patching Asset Management • Auditing • Security Awareness Training
Availability	• Plivo offers a service level committing to availability as documented and communication in SLA and other customer agreements.	• System Monitoring • Backup and Recovery • Replication • Business Continuity and Disaster Recovery • Continuity and Resilience