System and Organization Controls 3 (SOC3) Report

Report on Controls at Service Organization Relevant to Security, Availability, Confidentiality and Privacy

Throughout the period July 1, 2022, to December 31, 2022

Deloitte.

Deloitte Touche Tohmatsu
Certified Public Accountants LLP

30/F Bund Center
222 Yan An Road East
Shanghai 200002, PRC

Tel: + 86 (21) 6141 8888
Fax: + 86 (21) 6335 0003
www.deloitte.com

Report of Independent Service Auditors

To: Yealink Network Technology Co., Ltd.

Scope

We have examined Yealink Network Technology Co., Ltd. (the "Service Organization" or "Yealink") accompanying assertion titled "Assertion of Yealink Network Technology Co., Ltd.'s Management" (assertion) that the controls within Yealink's Device Management Cloud Service (system) were effective throughout the period July 1, 2022, to December 31, 2022, to provide reasonable assurance that Yealink's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, and privacy (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)*.

Service Organization's Responsibilities

Yealink 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 Yealink's service commitments and system requirements were achieved. Yealink has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Yealink 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 the International Standard on Assurance Engagements 3000 (Revised), Assurance Engagements Other Than Audits or Reviews of Historical Financial Information, issued by the International Auditing and Assurance Standards Board. The standard

requires 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 Yealink'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 Yealink'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 Yealink's Device Management Cloud Service system were effective throughout the period July 1, 2022, to December 31, 2022, to provide reasonable assurance that Yealink's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Deloitte Touche Tohmatsu Certified Public Accountants LLP

April 24, 2023

Assertion of Yealink Network Technology Co., Ltd.'s Management

We are responsible for designing, implementing, operating, and maintaining effective controls within Yealink Network Technology Co., Ltd.'s (Yealink's) Device Management Cloud Service system throughout the period July 1, 2022, to December 31, 2022, to provide reasonable assurance that Yealink's service commitments and system requirements relevant to security, availability, confidentiality, and privacy 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 July 1, 2022, to December 31, 2022, to provide reasonable assurance that Yealink's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, and privacy (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)*. Yealink'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 July 1,2022, to December 31, 2022, to provide reasonable assurance that Yealink's service commitments and system requirements were achieved based on the applicable trust services criteria.

Yealink Network Technology Co., Ltd.

April 24, 2023

Attachment A.

Yealink Network Technology Co., Ltd.'s Description of Yealink Device Management Cloud Service

Overview

Yealink Network Technology Co., Ltd. (the “Service Organization” or “Yealink”) is a listed company focusing on enterprise communication, providing cloud and terminal video conference service, IP voice communication services and collaboration solutions. Yealink’s Device Management Cloud Service provides a real-time, online, unified and graphical multi-level management platform based on Web for the enterprises and channels who use Yealink’s audio and video devices to efficiently deploy, manage, analyze, and monitor the devices.

Scope Boundary

This report only covers the system related to Device Management Cloud Service (public cloud platform(“YMCS”) and privatized deployment product(“YDMP”)) provided by Yealink.

Yealink uses the cloud computing service provided by Amazon Web Services (the “AWS”) (for Yealink global services) and Alibaba Cloud (the “ALI”) (for Yealink mainland China services) (the “Subservice Organizations”), including cloud servers, object storage services, VPC and cloud security service. This report does not include the services provided by Subservice Organizations related to Device Management Cloud Service.

Shared Responsibility

As a Software as a Service (SaaS) System, Yealink System is designed based on a shared responsibility model where both Yealink and the customers are responsible for aspects of Security, availability, Confidentiality and Privacy. To obtain the details of the customers' responsibilities, please email security@yealink.com.

Software and Infrastructure

Yealink takes advantage of information technology system and application system to support the effective implementation of control activities related to Yealink Device Management Cloud Service. Yealink has deployed a series of management information systems to support its operation and maintenance management, including human resource management, identity authentication, access management, change management, security vulnerability management, system operation monitoring, etc.

For regulating the standards and management related to software and infrastructure, Yealink formulates a series of official rules and regulations as well as control process, covering identification and access management, software development and program change management, data security management, security vulnerability and security incident management, availability management, and privacy protection, etc.

There are two main cloud service providers being used by Yealink, Amazon Web Services (the "AWS") (for Yealink global services) and Alibaba Cloud (the "ALI") (for Yealink mainland China services) as its Subservice Organizations (the "Subservice Organizations"), for the purpose of network transmission node over the internet, its virtual servers, network devices, and system data storage respectively. In order to monitor the effectiveness of the internal control of the subservice organization, the company performs an annual assessment to assess whether the cloud services used by the company are met. If any exception is noted, the company notifies the subservice organizations to take follow-up actions.

People

Yealink has established a comprehensive organizational structure and clearly defines the roles and responsibilities assigned to different positions within the organization structure. Meantime, Yealink utilizes the UME platform to maintain employees' information on their jobs and departments.

Yealink has established a structured onboarding process to help new employees understand their responsibilities in information security, code of conduct and performance evaluation mechanism. Background Check is conducted by the Human Resources Department before new employees are hired, based on the importance of different roles. The whole process complies with laws and regulations formulated by the country. In addition, new hires are required to sign confidentiality agreement and labor contract before onboarding and Yealink clarifies employees' duties on information security in the confidentiality agreement.

Yealink has established a series of information security training and learning mechanism to ensure that employees' information security awareness can meet the Company's requirements. Newly hired employees are required to participate in trainings on corporate culture, rules and regulations, information security, and performance evaluation. Meanwhile, the Company organizes trainings on a periodic basis, aiming at deepening employees' professional knowledge and skills and improving their information security awareness.

Process

Yealink has designed and implemented a series of procedures in its routine operation and management in terms of security, availability, confidentiality and privacy, including but not limited to:

- Control Environment
- Information and Communication
- Risk Assessment
- Monitoring
- Identity and Access Management
- Change Management
- Data Security Management
- Security Vulnerability and Security Incident Management
- Terminal Device Security
- Capacity, Backup and Business Continuity Management
- Privacy Protection

Data and Confidentiality

Yealink has established official policy to regulate the process of data security management. Meantime, Yealink has established a series of controls to ensure the security and confidentiality of data transmission and erasure process.

YMCS provides data transmission links that support encryption. Identity authentication information and operation commands are transmitted through secure hypertext transmission protocol.

Yealink clearly defines data security related terms in Privacy Terms, pertaining to data retention, confidentiality, data disclosure, etc. Yealink disposes corresponding data based on the requirements of data erasure and de-identification proposed by individual users and user entities.

Availability

Yealink has designed and implemented the management process to standardize the capability expansion and contraction management in daily operation and maintenance scenarios to ensure the availability of server resources.

Yealink has set up data backup, remote backup, backup monitoring and backup recovery testing strategies for Yealink Device Management Cloud Service to ensure the availability.

Yealink has developed business continuity management plan to provide guidelines of emergency response and recovery measures to scenarios that may lead to business disruption. Yealink has defined the emergency planning and response process for different emergent scenarios that may be involved in the Device Management Cloud Service, generating emergency response plan. The Company organizes emergency drill at least once a year for pre-defined scenarios that may lead to business disruption.

Privacy Protection

Yealink has developed Privacy Terms defining personal information and regulating the requirements of collection, usage, retention, disclosure and erasure of personal information. Meantime, Yealink assesses privacy compliance semi-annually to monitor the compliance with various data protection regulations.

Yealink provides users the ability to access and confirm their personal information. The company stipulates the channels to raise objections or complaints for the users in Privacy Terms. If a user has any objections or complaints about the Company's way to handle his or her information, the user can contact the Company via email or telephone. The Company responds to user's request in a timely manner and sends the handling results to the user.

In addition, Yealink has formulated official policy to regulate the response and emergency handling procedure of data leakage incidents.

Attachment B.

Principal Service Commitments and System Requirements

Yealink designs its processes and procedures related to the service systems to meet its service commitments and system requirements for Device Management Cloud Service. Those service commitments and system requirements are based on the service commitments that the Company makes to its user entities, and the operational, and compliance requirements that the Company has established for the services.

The Company has established communication channels according to the Company's policies and procedures, to ensure that the service commitments are effectively communicated to user entities. The Company has described its service commitments of its Device Management Cloud Service System related to security, availability, confidentiality and privacy by publishing Terms of Service and Privacy Terms.

The Company identifies the following objectives to support the security, availability, confidentiality and privacy commitments underlying their service commitments and system requirements. The objectives ensure the system operates and mitigates the risks that threaten the achievement of the service commitments and system requirements. The objectives include but not limited to:

- Integrating the security, availability, confidentiality and privacy principles into product design, and providing related functions to meet the user entities' requirements on security, availability, confidentiality and privacy;
- Applying secured change management processes;
- Applying management controls, operation controls and technological controls to protect business data and confidential information to guarantee the sustainable operation of business and application systems;
- Deploying encryption technologies to protect business data and confidential information at rest and in transit;
- Establishing corresponding service cycles and service availability commitments for Yealink Device Management Cloud Service to ensure the high availability of user entities' business and systems;
- Monitoring and periodically auditing the design and operating of controls within the system; and
- Applying management controls, operation controls and technological controls to ensure the compliance and security for personal information's collection, usage, retention, disclosure and disposal.

The Company establishes operational requirements that support the achievement of security, availability, confidentiality and privacy commitments and other system requirements. Such requirements are communicated in the Company's system policies and procedures and system

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