System and Organization Controls 3 (SOC 3) Report

Description of Tuya Inc.'s IoT Service System Relevant to Security, Availability, Confidentiality and Privacy

Throughout the Period January 1, 2023 to December 31, 2023

EY 安永

Ernst & Young Hua Ming LLP
Shanghai Branch
50/F, Shanghai World Financial Center
100 Century Avenue
Pudong New Area
Shanghai, China 200120

安永华明会计师事务所（特殊普通合伙）
上海分所
中国上海市浦东新区世纪大道100号
上海环球金融中心50楼
邮政编码: 200120

Tel 电话: +86 21 2228 8888
Fax 传真: +86 21 2228 0000
ey.com

Independent Service Auditor's Report

To the Management of Tuya Inc.

Scope

We have examined management's assertion, contained within the accompanying *Management's Report of Its Assertions on the Effectiveness of Its Controls over Tuya Inc.'s IoT Service System Based on the Trust Services Criteria for Security, Availability, Confidentiality and Privacy* (the "Assertion"), that Tuya Inc. ("Tuya" or the "Service Organization")'s controls over the IoT Service System (the "System") were effective throughout the period January 1, 2023 to December 31, 2023, to provide reasonable assurance that Tuya's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality and privacy set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (the "applicable trust services criteria").

Tuya uses Amazon Web Services, Inc., Microsoft Corporation, Tencent Cloud Computing (Beijing) Co., Ltd., Shanghai UCloud Information Technology Co., Ltd. and Google LLC to provide IT infrastructure hosting services (cloud computing). The service providers mentioned above are hereinafter collectively referred to as the "subservice organizations". The description of the boundaries of the System presented at *Attachment A* indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with related controls at Tuya, to provide reasonable assurance that Tuya's service commitments and system requirements are achieved based on the applicable trust service criteria. The description of the boundaries of the System presents the types of controls that the Service Organization assumes have been implemented, suitably designed, and operating effectively at the subservice organizations. Our procedures did not extend to the services provided by the subservice organizations and we have not evaluated whether the controls management assumes have been implemented at the subservice organizations have been implemented or whether such controls were suitably designed and operating effectively throughout the period January 1, 2023 to December 31, 2023.

Management's responsibilities

Tuya's management is responsible for its service commitments and system requirements, and for designing, implementing, operating, and monitoring effective controls within the System to provide reasonable assurance that Tuya's service commitments and system requirements were achieved. Tuya management is also responsible for providing the accompanying assertion about the effectiveness of controls within the System, selecting the trust services categories and associated criteria on which its assertion is based, and having a reasonable basis for its assertion. It is also responsible for:

- Identifying the System and describing the boundaries of the System.
- Identifying the service commitments and system requirements and the risks that would threaten the achievement of the principal service commitments and service requirements that are the objectives of the System.

Our 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 ("AICPA"). Those standards require that we plan and perform our examination to obtain reasonable assurance about whether the Assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about the Assertion, which includes: (1) obtaining an understanding of Tuya's relevant security, availability, confidentiality and privacy policies, processes and controls, (2) testing and evaluating the operating effectiveness of the controls, and (3) performing such other procedures as we consider 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.

Our examination was not conducted for the purpose of evaluating Tuya's cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

We are required to be independent of Tuya and to meet our other ethical responsibilities, in accordance with the relevant ethical requirements related to our examination engagement.

Inherent limitations

Because of their nature and inherent limitations, controls may not prevent, or detect and correct, all misstatements that may be considered relevant. Furthermore, the projection of any evaluations of effectiveness to future periods, or conclusions about the suitability of the design of the controls to achieve Tuya's service commitments and system requirements, is subject to the risk that controls may become inadequate because of changes in conditions, that the degree of compliance with such controls may deteriorate, or that changes made to the System or controls, or the failure to make needed changes to the System or controls, may alter the validity of such evaluations. Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal control at a vendor or business partner; and (c) persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity.

Opinion

In our opinion, Tuya's controls over the System were effective throughout the period January 1, 2023 to December 31, 2023, to provide reasonable assurance that its service commitments and system requirements were achieved based on the applicable trust services criteria.

Ernst & Young Hua Ming LLP Shanghai Branch

Ernst & Young Hua Ming LLP Shanghai Branch
February 20, 2024
Shanghai, China

Management's Report of Its Assertions on the Effectiveness of Its Controls over Tuya Inc.'s IoT Services System Based on the Trust Services Criteria for Security, Availability, Confidentiality and Privacy

February 20, 2024

We, as management of, Tuya Inc. ("Tuya" or "we") are responsible for:

- Identifying the IoT Services System (the "System") and describing the boundaries of the System, which are presented in *Attachment A*.
- Identifying our principal service commitments and system requirements.
- Identifying the risks that would threaten the achievement of our principal service commitments and service requirements that are the objectives of the System, which are presented in *Attachment A*.
- Identifying, designing, implementing, operating, and monitoring effective controls over the System to mitigate risks that threaten the achievement of the principal service commitments and system requirement.
- Selecting the trust services categories and associated criteria that are the basis of our assertion.

Tuya uses Amazon Web Services, Inc., Microsoft Corporation, Tencent Cloud Computing (Beijing) Co., Ltd., Shanghai UCloud Information Technology Ltd. and Google LLC to provide IT infrastructure hosting services (cloud computing). The service providers mentioned above are hereinafter collectively referred to as the "subservice organizations". The description of the boundaries of the System presented in *Attachment A* indicates that complementary controls at the subservice organizations that are suitably designed and operating effectively are necessary, along with controls at Tuya to achieve the service commitments and system requirements. The description of the boundaries of the System presents the types of complementary subservice organization controls assumed in the design of Tuya's controls. It does not disclose the actual controls at the subservice organizations.

We confirm to the best of our knowledge and belief that the controls over the System were effective throughout the period January 1, 2023 to December 31, 2023, to provide reasonable assurance that the service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality and privacy set forth in the AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

Very truly yours,

Tuya Inc.

Tuya Inc.
COMMON
SEAL

Overview of the Organization

Company Overview

Tuya Inc. ("Tuya" or the "Company") is a global leading service organization providing cloud development platform and "AI + IoT" developer platform, founded in 2014. It connects the intelligent needs of consumers, manufacturing brands, OEM manufacturers and chain retailers, and provides developers with one-stop PaaS solution of service combining artificial intelligence and internet of things (IoT). It also provides hardware development tools, global cloud and smart business platform, comprehensive ecological empowerment from technology to marketing channels, and the world's leading IoT Operating System ("IoT OS") product.

Products and Services

Based on Tuya "AI + IoT" Developer Platform (the "IoT Platform"), Tuya All-In-One Mobile APP (the "APP") and Tuya IoT Module (the "IoT Module"), Tuya provides the IoT Services for its user entities.

IoT Platform

The IoT Platform is a globally deployed IoT cloud platform that provides stable and secure smart experience and enables transformation to smart product. It provides proprietary high-performance IoT gateway and scalable distributed architecture that could support hundreds of millions of devices online simultaneously. It enables users to quickly implement smart hardware and IoT apps. Components like online device maintenance services, big data analysis services, SMS/phone services and smart after-sales services help users manage and monitor their IoT products and communicate with the Company.

APP

Tuya offers all-in-one app for which the users don't need to invest additional resources in software development. The APP is the necessary component in the smart ecosystem to connect and control smart devices and can integrate with various smart home scenarios and devices across brands and categories. Tuya provides regular maintenance, software update service and 24/7 technical support service for APP users. In addition to this, the APP provides home management function that enables users to share home access with family members, and device management functions including automatic devices detection, simple pairing and third-party voice control.

IoT Module

The IoT Module is a series of self-developed modules provided by the Company which realize the connections and controls of the IoT devices. The IoT Module supports multiple communication protocols including Wi-Fi, Bluetooth, Zigbee and NB-IoT.

Subservice Organizations

Tuya uses IT infrastructure hosting services (cloud computing) provided by Amazon Web Services, Inc. ("AWS"), Microsoft Corporation ("Microsoft Azure"), Tencent Cloud Computing (Beijing) Co., Ltd. ("Tencent Cloud"), UCloud Technology Co., Ltd ("UCloud") and Google LLC ("GCP") to support the IoT services in China, west-America, east-America, India and Europe.

Scope of the Report

The report only covers the IoT Platform, the APP and the IoT Module services (the "IoT Services") provided by Tuya. The Description of Tuya's System excludes IT infrastructure hosting services (cloud computing) provided by AWS, Microsoft Azure, Tencent Cloud, UCloud and GCP.

Principal Service Commitments and System Requirements

The Company designs its processes and procedures related to the IoT Services to meet its service commitments and system requirements. 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 identifies the following objectives to support the security, availability, confidentiality and privacy commitments underlying their service commitments and business 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:

- 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 in transit; 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 documentations. Information security policies define an approach about how systems and data in the report 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 operation of the above-mentioned service-supporting systems.

Entity Level Control

Tuya has established the Compliance Committee (the "Committee"), which is composed of sufficient and competent members, and also established *Compliance Committee Charter* to clarify its responsibilities in terms of Tuya's compliance and risk management.

Tuya has established *Tuya Internal Audit Policy*, to regulate the principles, frequency and management processes of internal audit and to ensure the effectiveness of internal control system.

Product Security

To ensure the reliability and confidentiality when accessing IoT Services, Tuya adopts HTTPS-based data transmission method for the APP and IoT Platform and AES-GCM based data encryption mechanism for transmitted data proceed within the IoT Module.

To ensure the security of Product's data, Tuya adopts data isolation mechanism and role-based access management function to prevent the data from unauthorized access and modifications.

Data Security Management

Tuya has established a series of mechanisms to ensure that confidential information that has been identified for destruction is disposed appropriately. Tuya encrypts the sensitive data stored in the databases and also designed and implemented a series of technical measures and management procedures for data security and information lifecycle management to ensure the security of users' data.

Vulnerability, Security Incident and Failure Management

In order to ensure that vulnerabilities, security incidents and failures identified can be promptly responded to and dealt with in a timely manner, Tuya has established procedures to support the stable operation of IoT Services and adopted a various of monitoring systems to monitor the operating status of IoT Services and related supporting systems.

Identity and Access Management

To protect all systems related to IoT Service from unauthorized intrusion and destruction by internal and external users, Tuya adopts the single sign-on (SSO) mechanism to realize the unified identity authentication within the Company. Employees must pass the appropriate identity authentication before logging into the application systems. Tuya also verifies the identity of a user based on the username and password when the user logs into the IoT Platform and the APP.

Change Management

Tuya integrates security concepts of change management throughout the development life cycle of Tuya's IoT Service, and implements strict controls in the processes of request collecting, request review, system development, testing, etc., to ensure stable operation and security of the

IoT Services. Tuya has also established a formal management process for the database project changes and a hierarchical approval process for the database configuration changes.

Privacy Protection

Tuya has established a series of policies and mechanisms to protect users' personal information. Tuya has established *Tuya Privacy Policy* and *Tuya Mobile Privacy Policy* that clearly explain the definition of personal information and describe the requirements in relating to collection, usage, retention, disclosure and disposal of personal information. Within third-party supplier management, Tuya has established a series of privacy management measures to ensure the data interaction between Tuya and third parties can satisfy the requirements as defined in privacy policies.