System and Organization Controls 3 (SOC 3)

Description of Lark Technologies Pte. Ltd.'s
Lark Suite System
Relevant to Security, Availability, Confidentiality and Privacy

Throughout the Period January 1, 2025 to December 31, 2025

Docusign Envelope ID: 420F2D64-5524-4C86-88FA-6C14C62FC864

Ernst & Young
27/F, One Taikoo Place
979 King's Road
Quarry Bay, Hong Kong

安永會計師事務所
香港制魚涌英皇道 979 號
太古坊一座 27 樓

Tel 電話: +852 2846 9888
Fax 傳真: +852 2868 4432
ey.com

Independent Service Auditor's Report

To the Board of Directors of Lark Technologies Pte. Ltd.

Scope

We have examined management's assertion, contained within the accompanying Management's Report of Its Assertions on the Effectiveness of Its Controls over Lark Technologies Pte. Ltd.'s Lark Suite System Based on the Trust Services Criteria for Security, Availability, Confidentiality and Privacy (the "Assertion"), that Lark Technologies Pte. Ltd. ("Lark Technologies" or the "Service Organization")'s controls over Lark Suite System (the "System") were effective throughout the period January 1, 2025 to December 31, 2025, to provide reasonable assurance that Lark Technologies' service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, privacy set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (the "applicable trust services criteria").

Lark Technologies uses Amazon Web Services, Inc. (the "subservice organization") to provide Cloud Computing Services, Cloud Storage Services, Database Services, Networking Services, and Security Services. 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 Lark Technologies, to provide reasonable assurance that Lark Technologies' 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 organization. Our procedures did not extend to the services provided by the subservice organization and we have not evaluated whether the controls management assumes have been implemented at the subservice organization have been implemented or whether such controls were suitably designed and operating effectively throughout the period January 1, 2025 to December 31, 2025.

Management's responsibilities

Lark Technologies' 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 Lark Technologies' service commitments and system requirements were achieved. Lark Technologies 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:

Docusign Envelope ID: 420F2D64-5524-4C86-88FA-6C14C62FC864

- 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 service commitments and system 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 Lark Technologies' 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 Lark Technologies' cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

Our examination was not conducted for the purpose of evaluating the performance or integrity of Lark Technologies Pte. Ltd.'s Artificial Intelligence ("AI") services . Accordingly, we do not express an opinion or any other form of assurance on the performance or integrity of Lark Technologies' AI services.

We are required to be independent of Lark Technologies 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 Lark Technologies' 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

Docusign Envelope ID: 420F2D64-5524-4C86-88FA-6C14C62FC864

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, Lark Technologies' controls over the System were effective throughout the period January 1, 2025 to December 31, 2025, to provide reasonable assurance that its service commitments and system requirements were achieved based on the applicable trust services criteria.

Ernst & Young
February 27, 2026
Hong Kong, China

Management's Report of its Assertions on the Effectiveness of Its Controls over Lark Technologies Pte. Ltd.'s Lark Suite System Based on the Trust Services Criteria for Security, Availability, Confidentiality and Privacy

February 27, 2026

We, as management of, Lark Technologies Pte. Ltd. ("Lark Technologies") are responsible for:

- Identifying Lark Suite System (the "System") and describing the boundaries of the System, which are presented in Attachment A.
- Identifying our service commitments and system requirements.
- Identifying the risks that would threaten the achievement of our service commitments and system 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 service commitments and system requirements.
- Selecting the trust services categories and associated criteria that are the basis of our assertion.

Lark Technologies uses Amazon Web Services, Inc. (the "subservice organization") to provide Cloud Computing Services, Cloud Storage Services, Database Services, Networking Services, and Security Services. The description of the boundaries of the System presented in Attachment A indicates that complementary controls at the subservice organization that are suitably designed and operating effectively are necessary, along with controls at Lark Technologies 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 Lark Technologies' controls. It does not disclose the actual controls at the subservice organization.

We confirm to the best of our knowledge and belief that the controls over the System were effective throughout the period January 1, 2025 to December 31, 2025, 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, in AICPA Trust Services Criteria (the "applicable trust services criteria").

Very truly yours,

Lark Technologies Pte. Ltd.

Attachment A — Lark Technologies Pte. Ltd.'s Description of the Boundaries of the Lark Suite

Company Overview

Founded in 2018, Lark Technologies Pte. Ltd. ("Lark Technologies" or the "Company") provides cloud-based Software-as-a-Service ("SaaS") solutions as its core services. The Company is committed to developing and providing secure, stable, and reliable cloud-based office suite solutions, with the mission of enabling user entities to transform their ways of working.

Services and Systems

Lark Technologies provides the next-generation office suite SaaS – Lark Suite System, which is a mobile- friendly solution that supports real-time collaboration and provides single sign-on ("SSO") capability. Lark Suite System helps user entities to improve work efficiency, reduce production and administrative costs, and to enable them to shift towards more efficient, better coordinated, and more secure businesses. Meanwhile, the Company has leveraged information technology and application systems to support the implementation of control activities related to the development and operation of Lark Suite System. Users of Lark Suite System can be classified into individual and enterprise users.

Services covered by the Description

Scope of services covered in the Description:

- Base
- Email
- Calendar
- OKR
- Messenger
- Minutes
- Approval
- Forms
- Slides
- Rooms
- Wiki
- AnyCross
- Docs
- Webinar
- Project
- Lark Developer
- Meetings
- Al Meeting Notes

Collaborative Office

Base

Base is an online database for storing and managing data. Unlike conventional spreadsheets, it facilitates not only data storage, analysis and visualization with real-time multi-person editing, annotations and discussions, but also workflow automation. Furthermore, its application mode enables users to build business pages using visual components, creating a complete business system based on Base data. This delivers an integrated experience spanning data management, process execution, and user interface.

Email

Email is integrated with Messenger as well as Calendar and can be shared to chat with just one click. In addition, team members can be invited to edit the email contents. These functions realize timely synchronization of information, thus improving the efficiency of email preparation. Besides, Email supports a smart sorting function, which effectively saves time for email managing. Email also supports

the authorization of shared Docs. Senders can grant read and/or edit rights to receivers when sharing the Docs through Email.

Calendar

Calendar is designed to help businesses and users for coordinating and arranging personnel, conference rooms, and other resources so as to achieve better synergy in schedule management. Calendar supports schedule creation, conference invitation, one-click conference group creation, schedule sharing, subscription to others' calendar, and public calendar creation. Calendar is integrated with Messenger and Docs, so that team members can easily plan and share schedules, stay synchronized, and organize meetings and projects more efficiently.

OKR

OKR is a tool developed by Lark Technologies based on the theory of goal and key results method to promote goal focus, encouraging cooperation and improving execution efficiency. Through OKR, users can understand the vision of the organization, participate in the development and discontinuation of strategies, actively seek implementation methods, collaborate with each other, classify individuals, and form an organization to promote goal focus.

Messenger

Messenger ("Lark") supports online communication, the transmission of text messages, documents, images, as well as voice and video communication via Messenger technology. The messages are stored in the cloud and synchronized to all devices automatically. When new members join the group, they can view historical messages anytime and anywhere. Messenger permits new members to integrate into teams and projects quickly, reducing communication costs and improving efficiency.

Minutes

Minutes automatically transcribes video meetings into transcripts that allow users to view, search, and collaborate on transcripts.

Approval

Approval allows users submitting and processing all types of approvals on a single platform. It provides an actionable approval center for making fast business decisions. Users can approve requests with one click.

Forms

Lark Forms is a flexible online form builder that lets users create custom surveys, polls, quizzes, and feedback forms without coding. It makes it easy to collect responses in real time, share forms directly with others, and integrate the collected data with Lark Base for analysis or automation.

Slides

Lark Slides is an online presentation tool that is part of the Lark productivity suite. It enables users to create, edit, and collaborate on presentations in real-time, with seamless integration across the Lark ecosystem. Designed for modern teams, it combines traditional presentation capabilities with cloud-based collaboration features.

Rooms

Lark Rooms is a conference room hardware solution designed to transform physical meeting spaces

into intelligent, integrated collaboration environments. It provides enterprises with dedicated hardware devices that seamlessly connect with the Lark collaboration platform, enabling effortless meeting room management and enhanced in-room meeting experiences.

Wiki
A knowledge management solution for organizations, where users can create, organize, manage and share a large pool of content with the entire team.

Anycross
AnyCross provides visual process arrangement capability for people, finance, and transactional processes in enterprises and other business systems. The platform breaks through the open capabilities of Lark account identity, Message, Cloud Document, Calendar, and other functions, making enterprise business system integration more standard, safer, and simpler, and solving the problems of internal application interconnection and business automation. By reducing the complexity and cost of internal system integration, AnyCross makes the transmission of information more efficient and makes the information within the enterprise fully interoperable.

Docs
Docs supports multiple users editing an online document simultaneously. Document formats include Docs are Word, Excel, and Mind Notes, etc. Multiple users can collaborate to edit the same document, and the document can be set as a private or shared document. By default, Docs are prohibited to be shared outside the tenant unless it is authorized by the owner. Docs supports the insertion of text, images, tables, files, videos, task lists, and other types of content.

Webinar
For large conference scenarios, Meetings has a webinar solution, that supports up to 10,000 participants cooperating at the same time and can flexibly manage the authorizations of guests and audiences, establish a variety of interactions with participants, and automatically generate data reports after the conference, making information transfer more efficient and organizing large-scale conferences easier.

Project
Project is a work management platform for complex team collaboration scenarios. It integrates various capabilities such as custom process management, demand management, defect management, and automated flow, as well as providing customized project management solutions for enterprises.

Lark developer
Lark Developer is the official developer platform of Lark Suite, designed to provide robust app development and system integration capabilities for enterprises and ISVs (Independent Software Vendors). It enables organizations to build custom applications, integrate existing business systems, and extend Lark's collaborative functionality to meet specific business needs.

Meetings
Meetings is integrated with Messenger and Calendar. Meetings can be initiated via group chat or a calendar meeting invitation. Meetings also provide intelligent meeting space solutions for offline Lark meeting rooms, which integrate audio and video conferences, local projection screens, sign-in boards, management console, and other functions. Supporting projection screen touch action, Meetings allow team members to communicate and collaborate in meetings anywhere.

AI Meeting Notes

AI Meeting Notes leverages artificial intelligence to generate meeting summaries in real-time, accurately capturing key decisions and discussion points. It automatically transforms meeting content into structured diagrams for intuitive understanding and follow-up. Meeting outcomes can be seamlessly saved as knowledge assets for team members to access and reuse. Furthermore, the system can assess meeting quality, providing data-driven insights to help organizations continuously improve meeting efficiency and effectiveness.

Supported OS

The Lark Suite System client is currently available for Android, iOS, Mac OS and Windows. Unless otherwise specified, the controls involved in the report apply to all products based on the above-mentioned operating systems.

Scope of the Report

The products covered in the report are supported by the Operating Systems Platforms deployed in Amazon Web Services, Inc. ("AWS") unless otherwise specified. The report excludes other controls, including elastic computing service, physical access, physical environmental security, etc. provided by AWS.

Principal Service Commitments and System Requirements

Lark Technologies designs its processes and procedures related to the service systems to meet its service commitments and system requirements for Lark Suite System. These are based on the service commitments made by the Company to its user entities, as well as the operational and compliance requirements established by the Company for the services.

Lark Technologies has established mature internal control practices by comprehensively considering corporate development objectives, industry best practices in operations management, and relevant legal and regulatory requirements. This ensures that service commitments related to security, availability, confidentiality, and privacy are effectively communicated to user entities. The Company has also coordinated the development of the Lark Suite system, which integrates and reinforces the internal control framework through five interconnected and mutually reinforcing components: the internal environment as the foundation, risk assessment as the key focus, control activities as the primary measures, information and communication as essential enablers, and internal monitoring as a critical safeguard.

Service commitments and system requirements are achieved by the Board, management, and all employees of Lark Technologies. To ensure organizational efficiency and operational effectiveness, the Company designs a scientific organizational structure that clearly defines roles, responsibilities, and job objectives, with internal departments rationally established. Meanwhile, Lark Technologies implements management requirements through a series of comprehensive and rigorous policies, processes, and documents, which are applied throughout the entire production activity lifecycle. The Company has established a series of formal regulations, policies, and controls to support this framework：

- Information Security Governance
- Information Security Governance
- Product Security
- Human Resources Management
- Network Security
- Endpoint Security
- Identity and Access Management
- User Authentication and Access Management
- Data Security Management
- Change Management
- Asset Management
- Security Vulnerability and Incident Management
- Business Continuity Management
- Supplier Management
- Availability
- Confidentiality
- Privacy Protection

Information Security Governance

Lark Technologies has established an information security and privacy management system compliant with ISO/IEC 27001 and 27701, covering security policies, asset management, and the information system lifecycle. The Company defines roles within its security organization, including compliance, auditing, and product security liaisons, who are responsible for monitoring, training, and risk assessments. Comprehensive policies have also been implemented, such as employee and supplier security manuals, access control, incident response, and emergency plans for network and data security, to ensure governance and business continuity.

Product Security

Lark Technologies has developed a comprehensive security management system and architecture, encompassing security development, training, and operational processes that cover lifecycle management, employee education, vulnerability management, and incident response. The Company has obtained multiple certifications, including ISO/IEC 27001 and 27701, and its Product Security Team oversees areas such as compliance, data security, and threat intelligence. The Lark Suite system ensures robust security through features like multi-factor authentication, abnormal login detection, and controlled access to chat groups and documents for both individual and enterprise users. Additionally, tenant administrators can manage sharing permissions, message recall, and watermarking to protect sensitive information.

Human Resources Management

The Human Resources Management Department at Lark Technologies supports organizational growth through recruitment, training, performance evaluation, and employee relations, while ensuring adherence to security and privacy standards. Key processes include structured onboarding, background check, and the proper documentation of employment contracts, confidentiality agreements, and resignation procedures. Employee performance is managed using the OKR methodology, supported by semi-annual reviews and regular training on topics such as information security and data protection. The department also enforces disciplinary measures for policy violations and maintains accurate employee records in the Human Resources Management System.

Network Security

Lark Technologies enforces strict network isolation, ensuring that production environments are segregated from development and testing environments, with no direct access allowed between them. The Company employs a Web Application Firewall (WAF) to block web vulnerabilities, which is regularly reviewed and updated by authorized engineers, and secures office networks with firewalls and restricted access controls. Network security incidents are monitored through the Security Operations Center platform, which alerts administrators for timely response and logs incident details for analysis.

Endpoint Security

Lark Technologies enforces office endpoint security through policies such as the Employee Information Security Manual and the Access Control Management Regulation. This is supported by the Endpoint Security Management System, which is integrated with the EDR Platform for intrusion and malware detection. The Company prohibits the use of unmanaged personal devices to access internal networks or store business data, with disciplinary actions taken for violations, and ensures data protection through full-disk encryption on office devices. Upon an employee's departure, the IT Department securely retrieves equipment and performs thorough data erasure to prevent information leakage.

Identity and Access Management

Lark Technologies governs identity and access management through policies such as the Employee Information Security Manual, adhering to the principles of least privilege and segregation of duties to prevent unauthorized access. Employee accounts are managed via the Identity Authentication Platform with SSO, requiring strong passwords and multi-factor authentication, while access rights are role-based and automatically deactivated upon resignation. Access to production environments and AWS is tightly controlled, requiring approvals and secure connections such as VPN, with high-risk operations monitored and logged for review. Regular audits ensure that privileged accounts align with job responsibilities, and any changes to access rights are required to be formally approved.

User Authentication and Access Management

Lark Technologies outlines user and the Company responsibilities in its Service Agreement and Privacy Policy, which users are required to acknowledge during account registration, ensuring compliance with password security requirements. Users, classified as individual or enterprise, can create tenants in the Lark Suite system, with designated contacts becoming tenant administrators responsible for configuration and access management. Tenant administrators manage organizational structures, assign roles, and control access, ensuring that terminated employees lose access to tenant information. The Lark Suite System isolates users across tenants using unique tenant IDs and UIDs, enabling a single user to have multiple identities in different tenants.

Data Security Management

Lark Technologies ensures comprehensive data security through established policies and controls across data access, transmission, storage, and deletion, guided by standards such as the Data Security Management Standard and the Cryptographic and Key Management Policy. Data is classified into four security levels, with strict access controls requiring time-limited approvals and encrypted transmission via HTTPS. Storage implements a multi-layered encryption system (root, master, and data keys) managed through a secure Key Management System. The company enforces secure data lifecycle practices, including automated monitoring, multi-copy redundancy, regular backups, and irreversible data erasure protocols for deletion requests, ensuring compliance and protection against breaches.

Change Management

Lark Technologies enforces a structured Change Management Policy to oversee modifications across software, infrastructure, and networks, ensuring rigorous testing, approvals, and documentation through dedicated tools. The software development life cycle integrates security evaluations, secure coding practices, QA testing, and deployment protocols, requiring code reviews and automated scans before production deployment. Infrastructure changes, including AWS instances and network configurations, require multi-level approvals and audits, while segregated environments (development, testing, production) and role-based access controls uphold the principle of least privilege. Annual internal audits and controlled source code access via approval workflows further ensure compliance and mitigate risks throughout all change processes.

Asset Management

Lark Technologies has implemented management guidelines and classification standards to regulate the identification, classification, and management of information assets, ensuring standardized procedures for acquisition, deployment, and disposal. The Company uses the Information Asset Inventory System to track asset status and changes, with Data-System Department responsible for maintaining the inventory, conducting annual reviews, and ensuring the accuracy and consistency of asset records. Proper authorization, testing, and documentation are required before any assets are deployed to production environments.

Security Vulnerability and Incident Management

Lark Technologies uses the Security Operation Center Platform to monitor and manage vulnerabilities, conducting regular scans for network services, code warehouses, and third-party libraries. Detected vulnerabilities are verified, tracked, and resolved by Security and Compliance Department, with major incidents reported quarterly. The Company also employs multiple monitoring platforms for real-time tracking of system operations, ensuring prompt incident response and post-resolution reviews. Security incidents are documented and analyzed, with follow-up actions and lessons learned properly recorded.

Business Continuity Management

Lark Technologies has established Business Continuity Security Management Regulation, creating a framework that includes business impact analysis, risk assessment, and the development of emergency response and business continuity plans. Annually, the Company conducts business impact analysis and risk assessments to identify critical processes, threats, and key metrics such as recovery time objectives, ensuring appropriate response strategies for potential disruptions. the Company also organizes annual disaster recovery drills, issues drill reports, and integrates its products into a unified disaster recovery system to maintain service availability. The Company regularly reviews and updates its business continuity plans, provides disaster recovery training to employees, and ensures that adequate resources are available to sustain critical processes during operational outages.

Supplier Management

Lark Technologies has implemented comprehensive policies for managing suppliers and outsourced personnel, including guidelines for supplier evaluation, information security, and performance management. Suppliers undergo qualification and security assessments and are required to sign a Service Agreement and a Confidentiality Agreement; their performance is reviewed regularly to determine continued engagement. Additionally, third-party applications on the Open Platform are subject to rigorous qualification reviews, periodic functional assessments, and removal in the event of inconsistencies.

Availability

Lark Technologies implements robust capacity management, including real-time monitoring, automated and manual scaling mechanisms, and detailed documentation to ensure sufficient resources. Backup and recovery processes are rigorously managed through weekly full backups, real-time incremental backups, and master-slave synchronization, with recovery testing conducted daily and failures promptly addressed. Additionally, the Company has established comprehensive business continuity management systems, including disaster recovery mechanisms and continuity plans, to maintain operational objectives and service availability.

Confidentiality

Lark Technologies prioritizes the security and confidentiality of user data by implementing robust privacy and data security policies aligned with industry best practices. These measures include encryption, logical access controls, and network configurations to prevent data breaches, loss, or unauthorized access. The Company employs a Key Management System with AES-256 encryption and maintains segregated production, testing, and development environments to safeguard user data. Additionally, the Company provides dedicated channels for users to request data deletion, ensuring that information is anonymized or rendered inaccessible upon verification.

Privacy Protection

Lark Technologies implements comprehensive technical and management controls to protect personal data throughout its lifecycle, ensuring compliance with privacy policies and relevant regulations. The Company requires user registration with verified credentials, enforces strict data handling practices, and provides tools for users to access, update, or delete their personal information. The Company's privacy policies are regularly reviewed and updated to align with legal requirements, and users are notified of significant changes. Additionally, the Company conducts annual privacy compliance assessments, performs emergency drills for data leakage incidents, and ensures that third-party applications adhere to stringent confidentiality and security standards.