Lark Security White Paper V1.1

Tabel of Contents

Foreword *3*
1. Security Team and Its Responsibilities *4*
2. Security Compliance Certification *5*
3. Personnel Security *8*
3.1 Human Resource Management Process 8
3.2 Security Training and Learning 8
3.3 Endpoint Security Management 9
4. Client-side Security *10*
4.1 Client-side Operating Environment Security 10
4.2 Client-side Data Security 10
4.3 Client-side Protection against Security Vulnerability 10
4.4 Product Security Capabilities 10
5. Network Security *12*
5.1 Network Access Control 12
5.2 Network Firewall 12
5.3 DDoS and Network Attack Defence 12
5.4 Network Transmission Encryption 12
6. Server Security *13*
6.1 Server Access Control 13
6.2 Vulnerability Scanning 13
6.3 Intrusion Detection 13
6.4 Anomaly Detection 13
7. Application Security *15*
7.1 Security Development Process 15
7.2 User Account Security 15
7.3 Vulnerability and Security Incident Management 15
8. Data Security *17*
8.1 Data Transmission 17
8.2 Data Storage 17
8.3 Data Access 18
8.4 Disposal of Data 18
8.5 Data Security Inspection 18
9. Infrastructure Security *19*
10. Disaster Recovery and Business Continuity *20*
10.1 Backup and Disaster Recovery 20
10.2 Business Continuity Guarantee 20
10.3 Emergency drills 20
11. Change Management *21*
11.1 Program Changes 21
11.2 Source Code Control 21
11.3 Infrastructure Changes 21
11.4 Change Monitoring 21
12. Open Platform Ecological Security *22*
12.1 Service Provider Access 22
12.2 App Development Review 22
12.3 Authority Classification and Approval 23
12.4 Security Monitoring Scanning 23
Version Change Record *24*

Foreword

Lark Technologies Pte. Ltd. (hereinafter referred to as “Lark”) provides the new generation of corporate office services: Lark Suite, which is characterized by “mobile friendliness, real-time collaboration, and uniform access”, helping businesses improve work efficiency, reduce production and management cost, and embrace the transition to more efficient, collaborative, and secure intelligent businesses.

Lark offers the office suite with functions such as instant messaging, cloud documents, cloud storage, smart calendars, audio and video conferences, open platforms, mailboxes, OKR, approvals, etc., all boasting high extensibility and availability. Lark applies industry-leading management and technical means to ensure the security of products and user data throughout the life cycle. The design, development, and operation of Lark products helps enterprise clients to meet the requirements of applicable laws, regulations and principles on network security, privacy, and data protection.

1. Security Team and Its Responsibilities

As a SaaS service provider, Lark has always taken the security of users' business and data as its top priority. With infrastructure security and business and data security protection systems for users, Lark can provide users with all-dimensional protection at an infrastructure, application and data level.

Lark's security team consists of full-time security management, compliance, business security, data security, emergency response, security tool development teams and other teams. Its responsibilities include security assessment for product design, code security review, vulnerability scanning, penetration testing, threat intelligence, intrusion detection, emergency response, data security, security compliance, and more.

2. Security Compliance Certification

Lark attaches great importance to product compliance and proactively benchmarks its products against the compliance requirements of the highest international standards. Lark has obtained a number of international compliance certifications, including ISO27001, ISO27017, ISO27018, ISO27701, DPF, CBPR & PRP & DPTM and completed SOC 2 Type II and SOC 3 service certification reports. This demonstrates that Lark has reached a more standardized and regulated level in areas such as information security, cloud security and privacy protection.

ISO27001 Information Security Management System: As a set of security management system standards widely recognized across the industry, it has always been regarded as the most authoritative and strictest international information security system certification standard widely accepted around the world. Lark's data center, management system, research and development, and functional departments have obtained this certification, which means that we have been aligned with international standards in the field of information security management.

ISO27017 Cloud Security Management System: It provides recommendations for the implementation of the cloud-specific information security control mechanism, supplements the guidance to the ISO 27002 and ISO 27001 standards. This implementation procedure provides more information security control implementation guidance for cloud service providers.

ISO27018 Public Cloud-based Personal Information Protection Management System: It is the first international certification standard focusing on the protection of personal information on the public cloud. It is based on the practical rules of ISO27002 information security management, and provides guidance for the security control system applicable to public cloud personally identifiable information (PII). Lark's having obtained this certification means that we have attained high-standard industry practices in terms of protecting corporate data, users' personal information, and preventing information leakage.

ISO27701 Privacy Information Management System: It is the first privacy information management system standard to build a complete PDCA operation closed-loop in its real sense. It stipulates in detail the requirements for establishing, implementing, maintaining and continuously improving the privacy information management system, and takes into consideration the privacy protection measures required for processing personally identifiable information (PII) on the basis of information security protection. In 2019, Lark took the lead in obtaining the ISO27701 privacy information management system certification issued by the top international certification body BSI (British Standards Institution), and was one of the first companies in the world to obtain this certification.

Lark has obtained **SOC 2 Type I, SOC 2 Type II and SOC 3 service audit reports**. System and Organization Controls (SOC) Reports are independent third-party examination reports about the internal control of the service organization issued by

professional third-party accounting firms, based on the relevant guidelines of the American Institute of Certified Public Accountants (AICPA). SOC2, one of the types, defines standards for managing customer data based on Trust Service Principles (security, availability, processing integrity, confidentiality, and privacy). Lark is regularly audited by third parties to verify that the products meet this standard, which indicates that our systems are reliable and secure.

Lark has attained **the Global Cross-Border Privacy Rules (CBPR) and the Global Privacy Recognition for Processors (PRP) Certificate.** CBPR and PRP Systems establishes an internationally recognized framework for safeguarding personal information across the participated jurisdictions. While the Global CBPR System enables organizations to demonstrate accountable cross-border data practices in line with participated jurisdictions recognized privacy and data protection standards, the Global PRP System complements this by assuring that data processors have the capacity and governance mechanisms to process personal information in a manner consistent with a controller's requirements under the CBPR framework.

By achieving certification under both the Global CBPR and PRP Systems, we have demonstrated that our privacy program not only meets rigorous standards for protecting personal information across participated jurisdictions, but also ensures that our processing practices are transparent, reliable, and aligned with the obligations of data controllers. This dual recognition underscores our commitment to privacy protection, reduces barriers to trusted cross-border data flows, and provides assurance to our customers, partners, and regulators that personal information entrusted to us is safeguarded under globally accepted principles.

In addition, Lark has been awarded the **Data Protection Trustmark (DPTM)** accredited by the Infocomm Media Development Authority (IMDA) in Singapore. This standard is formulated in accordance with Singapore's Personal Data Protection Act (PDPA) and international benchmarks and best practices. Securing this certification indicates that IMDA recognizes Lark's long-term commitment to formulating sound data protection policies and practices to protect clients' personal data.

Lark has been certified under the **Data Privacy Framework (DPF)**, further demonstrating its strong commitment to protecting personal data and complying with international privacy standards. This certification reinforces Lark's dedication to transparency, accountability, and responsible data handling, and facilitates the seamless and secure transfer of personal data from the EU, UK, and Switzerland to the United States in accordance with the DPF principles.

Lark has successfully completed **GDPR Validation** through TrustArc, an independent third-party assessment that verifies adherence to the requirements set forth under the European Union's General Data Protection Regulation (GDPR). The validation process involved a comprehensive review of our data protection policies, governance framework, and operational practices to confirm alignment with key GDPR obligations, including lawful bases for processing, data subject rights, data security, accountability, and cross-border transfer mechanisms.

By achieving GDPR Validation, we have demonstrated that our privacy management

program incorporates robust controls designed to meet regulatory requirements and industry best practices. This independent validation provides objective evidence of our compliance posture, ensuring that clients, partners, and regulators can rely on our commitment to maintaining high standards of data protection across our operations.

Lark proactively follows up on the international requirements for product compliance, and connects with regulators at all levels through security management and the compliance team to ensure that the products and services provided meet the requirements. In addition, a dedicated privacy team was put into place to review user privacy agreements, privacy protection design of products, collection and usage of users' private data, ensure that users' private data are properly used and processed, and maintain appropriate transparency for users. For more content on Lark's practices on privacy protection, please refer to Lark Trust Center.

3. Personnel Security

3.1 Human Resource Management Process

Lark has established a secure HR management process:

- The recruitment of new employees must be approved by the human resources specialist and the head of the job requirement department, and the recruitment process and outcome for new employees will be documented in the human resource system;
- Before employing a new employee, the Human Resources Department will conduct a background check on the employee according to the importance of the position and as permitted by national laws and regulations, to ensure that the employment of the employee complies with Lark's rules and regulations;
- New employees are required to sign the employment contracts and confidentiality agreements, which describe the responsibilities and obligations employees should undertake in terms of information security;
- The Legal Department shall review the terms enclosed in the employees' confidentiality agreements and third-party confidentiality agreements at least once a year, update them when necessary, and publish them through the internal knowledge platform after their being updated to ensure that all employees and relevant personnel can have access to the latest confidentiality agreements;
- The employee's resignation is required to be initiated in the human resource system by the employee himself/herself or the department head, and the official resignation can only be made after the application is reviewed by the human resource department and relevant functional departments. Before resignation, all accounts shall be cancelled and all hardware and software assets (such as computers, work documents, etc.) shall be returned.

3.2 Security Training and Learning

Lark has established a comprehensive training and learning system. New employees shall participate in training programs including corporate culture, rules and regulations, information security, and reward and punishment mechanisms. At the same time, Lark will organize training programs regarding employees' professional knowledge and skills and information security awareness aperiodically:

- Lark will organize information security-related training programs aperiodically to enhance employees' information security skills, at least once a year;
- Lark will hold information security activities periodically to publicize information security awareness, at least once a year;
- Lark will communicate security awareness to employees in multiple ways aperiodically, such as making publicity materials for security awareness and

conveying them to employees through the mail, posters, etc.

3.3 Endpoint Security Management

Lark has developed a sound security management and control strategy for terminal equipments of employees and deployed it to all equipments by default. Employees cannot delete or modify the security configuration by themselves. Antivirus software is installed on all computers of Lark's employees, and the back-end security configuration prevents employees from switching off, uninstalling, or modifying the configuration of the antivirus software. Only authorized personnel of the IT department have the administrator account of the anti-virus software to perform security configuration on the anti-virus software. The antivirus software is capable of updating virus database in real time, and periodically performing full-disk virus scanning of employees' terminal equipments. Lark exercises full-disk encryption over employees' terminal equipment disks to protect data and file security. Upon resignation, employees need to return their terminal equipment, and the IT department will erase the information on employees' equipment by erasing the hard disks.

4. Client-side Security

4.1 Client-side Operating Environment Security

Lark APP will stringently test the operating environment, including root detection, jailbreak detection, debugging detection, injection detection, etc. The purpose of such detections is to ensure that the client-side terminal runs in a trusted environment to prevent the programs from being cracked or exploited by malware.

4.2 Client-side Data Security

Lark APP adopts the security mechanism embedded in the operating system to isolate permissions between APPs. Local information on the client-side is encrypted for storage. The full-link communications between the client-side and the server are encrypted using HTTPS or WSS.

Lark has integrated self-developed data security solution on the client-side, providing system-level capabilities for encrypting the client-side's local private data and the unique binding function between data and devices. Even if an attacker steals the user's encrypted data, he cannot decrypt such data to use them in his own devices. As a result, the user's data security boundary has been enhanced significantly, and the chance of user data leakage has been greatly reduced.

4.3 Client-side Protection against Security Vulnerability

Lark has a full-time mobile security vulnerability mining team, which conducts security assessments and vulnerability mining on Android, iOS, Windows, MacOS, Linux and other client sides, and at the same time conducts vulnerability detection on the third-party components (library, SDK) used, so as to locate the loopholes in the applications to ensure the security of the client side. In addition, Lark regularly invites external professional thirdparty security companies to conduct security penetration tests on Lark and follow up on fixing and solving problems in a timely manner.

4.4 Product Security Capabilities

Lark provides security capabilities in account security, access security, data security and other aspects, including but not limited to:

Account Security:
Ensure account security through two-factor authentication (2FA) and safeguard application access via Single Sign-On (SSO) authentication.

Access Security:
Enforce access conditions and capabilities to restrict Lark logins to only trusted environments.

Data Security:
Protect enterprise information through classification labels, file operation permissions, Lark’s self-developed DLP, mobile file encryption, screenshot and screen recording protection, and customizable watermarks.

Email Security:
Provide anti-phishing, anti-spam, blacklist/whitelist management, and data protection rules for secure email communication.

Tenant Switching Restriction:
Only Lark tenant accounts associated with the enterprise may be accessed in trusted environments. Logging into unrelated tenants (e.g., personal or other organizations' tenants) is prohibited.

Audit Logs:
Support data leak traceability by retaining and reviewing detailed operation logs related to potential leaks.

Lark’s product security capabilities are updated rapidly. For the latest features, you can refer to the official website introduction or contact customer service for consultation.

5. Network Security

5.1 Network Access Control

Lark uses access control lists (ACLs) for network isolation. Different network areas such as guest networks, office networks, development test networks, and production networks are divided internally. All employees who are outside Lark's network borders need to access Lark's internal resources through a VPN connection. Lark's internal audit department will audit access logs, etc., find and trace non-compliant operation records, and impose corresponding penalties.

Lark has strict employee access control policies in place to limit access to internal resources. Employees need identity-authentication to access internal resources. After the identity is confirmed, employees only have the least privilege by default. The request of new permissions needs to be approved and recorded by the relevant responsible personnel. Permissions have a validity period, and the system will automatically revoke the permissions after the validity period expires. Employees operate online services through the bastion host, and all operation logs are kept for at least 180 days and audited by the internal audit department.

5.2 Network Firewall

Lark uses a network firewall to intercept common network security vulnerability attacks in the Lark suite system, and only authorized security and compliance engineers can uniformly configure the protection rules of the network firewall. Lark has set up a combination of automatic and manual methods to update the network firewall configuration.

5.3 DDoS and Network Attack Defence

Lark service provides customers with network access through CDN and dynamic acceleration, and accesses back-end services through company load balancing; Lark has deployed industry-leading anti-DDoS services, which can effectively target traffic-type and connection-type attacks, etc. to defence.

5.4 Network Transmission Encryption

Lark uses HTTPS and WSS for encrypted transmission in both the internal and external networks, ensuring the security of the transmission process and prevents eavesdropping and tampering.

6. Server Security

Lark has adopted a series of security control measures for the servers used to ensure the safety of server production and effectively prevent malicious network attacks.

6.1 Server Access Control

Lark regularly scans server assets, closes unnecessary ports and services in a timely manner, minimizes external permissions, filters unsafe services, and reduces security risks. Security personnel conduct weak password detection on a regular basis, and urge server operation and maintenance personnel to increase the complexity of passwords to prevent brute force cracking. All access to the server must be operated and audited through the bastion host. Lark uses the whitelist to control the access source of business services to ensure that only trusted sources can access the service.

6.2 Vulnerability Scanning

Lark uses automated vulnerability scanning tools to regularly detect server vulnerabilities. After the confirmation by security personnel, it will be notified to relevant personnel for processing and repair. The operation and maintenance personnel will regularly update the system patches to effectively ensure the stable operation of the server.

6.3 Intrusion Detection

Lark's physical servers are fully deployed with HIDS (Host-based Intrusion Detection System), which can monitor server file baseline changes in real time, discover abnormal processes, capture active abnormal external links, Trojan backdoors and other abnormal behaviours, and respond in a timely manner. In addition, all traffic from the client end is detected and verified by WAF (Web Application Firewall) to ensure its security and legality, and to block malicious requests in real time. The security team will closely track the security situation and the latest attack methods, study intrusion characteristics, and regularly upgrade defence strategies.

6.4 Anomaly Detection

Built on the big data platform and machine learning platform, the security team conducts multi-dimensional security analysis on the massive host logs generated by the server and the data collected by the self-developed HIDS, establishes an anomaly detection model, and timely discovers risky operations and abnormal processes on the server, malicious network connections and other abnormal behaviours, and responds in a timely manner. The security team will closely track the security situation and the latest attack methods, continuously iterate the security algorithm model, update the abnormal behaviour characteristics, and regularly

upgrade the defence strategy.

7. Application Security

7.1 Security Development Process

Lark strives to control security risks from the source of security vulnerabilities. By making security courses and providing training in the form of on-site and online programs, all developers and product managers must receive security training to understand the causes of relevant security vulnerabilities and strengthen coding knowledge. When the project starts, the security team communicates with the project manager to ensure that security requirements and security tests are reflected in the project plan. At the same time, the security team will evaluate the third-party libraries and tools used by the product, and discover vulnerabilities to ensure that there are no vulnerabilities introduced by the supply chain. The security team conducts design and code security reviews with the product team. Before the product goes online, a penetration test and a security assessment of deployment will be conducted to ensure the security of the service.

7.2 User Account Security

The user's access to the Lark system is authenticated through a password plus a dynamic verification code. For logins initiated on unidentified devices, the risk control strategy will increase the difficulty of login verification. At the same time, the accounting system has defence capabilities against abnormal and violent login attempts.

Lark is connected to the self-developed risk control and anti-cheating system, which has protection functions such as anti-malicious registration, anti-crash database, and anti-violent login cracking. Users use password + dynamic password multi-factor authentication to log in to reduce the risk of account breaches caused by compromised passwords.

7.3 Vulnerability and Security Incident Management

Lark monitors internal and external security vulnerabilities and threat intelligence information through various means. The security team uses automated security scanning tools to scan its own services and operating systems, and conducts security checks on application systems through regular penetration tests. After the vulnerability and threat intelligence information is confirmed, the risk level will be determined according to the hazard situation, and it will be pushed to the relevant team for repair and processing as soon as possible. Lark has a complete vulnerability lifecycle management strategy, and a professional security team follows up on all security problem solving.

At the same time, Lark's security team maintains close cooperation and communication with the industry's top third-party evaluation companies and White Hat Communities. It will occasionally invite external companies and white hats to conduct penetration tests on the service and reward them to find out as many

security holes as possible.

Lark has a complete incident management process and implements a 7*24 emergency response strategy. When a security incident occurs, the security team will quickly classify the incident according to the security emergency plan and start the emergency response process to prevent the security incident from expanding. After the security incident is processed, the incident will be reviewed. The content of the review includes the cause of the incident, the process and results of the incident handling, the main person in charge of the incident, and follow-up measures, etc., and record the results of the review and follow-up measures to ensure a closed loop of events. When a security incident affects users or customers, we will promptly notify users, customers or other relevant parties in accordance with the incident handling process.

8. Data Security

Lark has complete data life cycle management, and has a clear process and technical guarantees from the creation, storage, transmission, use, and destruction of data. Lark has corresponding control measures to ensure data transmission, data storage, and data access and the security of the data destruction process.

8.1 Data Transmission

Lark provides users with data transmission links that support strong encryption protocols. Data transmissions such as message extraction, identity verification, and operation instructions are all encrypted using HTTPS and using 2048-bit RSA keys; the transmitted data is encrypted and protected; the video chat adopts DTLS-based end-server encryption to ensure the security of data transmission.

8.2 Data Storage

Lark uses a secure key mechanism to encrypt and store data, and has encrypted and stored all customer data such as messages and documents.

Lark has developed a comprehensive data classification management method, and has implemented strict classification and classification management of user information collected by Lark and tenant information in the backend management system, encrypted all sensitive information stored in the system, effectively protecting users' information security.

The encryption algorithm is embedded in the source code of each application; the key is generated by the key management system (referred to as "KMS system") and called by each application. The KMS service is responsible for the lifecycle management of keys and sensitive configuration information, including creation, storage, distribution, use, update, deletion, etc. The master key used for data encryption of tenants and various other sensitive information of Lark services (such as database accounts, passwords, etc.) are stored in the KMS system maintained by Lark, and access must be performed through KMS access. The root key of the KMS system is maintained by a hardware security module (HSM). The management of the HSM requires the cooperation of multiple keys. These keys are distributed to different functional roles for management. The KMS system uses envelope encryption to encrypt and decrypt data. The master keys used by different tenants are isolated from each other.

In addition to using the standard tenant master key and the AES-256 algorithm to encrypt data and data keys, Lark supports customer-independent keys, that is, KMS generates data keys, and uses customer-defined master keys for data and data keys. The key and the specified encryption algorithm are encrypted and stored in the database. Customers can choose the encryption algorithm and control the key rotation independently.

8.3 Data Access

Access to user data is strictly isolated with permissions. Users cannot access each other without authorization. Access to data must be explicitly authorized by the data owner, such as sharing operations, etc. (for example, the document created by user A is only visible to user A by default, unless he actively grants access to others).

By default, employees of Lark do not have access to any user data, and all operations of employees are strictly restricted and audited.

8.4 Disposal of Data

Individual users can request deleting personal accounts and information. After receiving the application for account or personal information deletion, Lark will delete or anonymize the relevant data of the deleted account.

For enterprise users, when an employee resigns, the organization's administrator can manage the resignation through the enterprise management console. As part of this process, the administrator may choose to delete the employee's data or anonymize the employee's personal information.

When Lark signed a cooperation agreement with the user organization, it agreed with the user organization that when the cooperation is terminated, Lark will process account-related data in accordance with laws and regulations, including but not limited to deletion and anonymization.

All data deletion and anonymization technical means comply with the prevailing industry standards and the requirements of laws and regulations.

8.5 Data Security Inspection

The login behaviour, operation behaviour, server security baseline file changes, access rights changes, and data access behaviours of all servers in Lark's online environment will be recorded. By establishing user behaviour portraits and abnormal behaviour models, the security team realizes the identification, analysis and correlation of abnormal behaviours, and automatically detects various abnormal data access behaviours in real time, such as inappropriate access to data, malicious data crawling and risky operations, log in abnormalities, privilege escalation, etc., and issues alarms or block them.

9. Infrastructure Security

Lark uses AWS cloud services, and AWS is responsible for operating, managing and controlling its hardware and software facilities. As the world's leading cloud service provider, AWS has the industry's top security capabilities to protect users' infrastructure security. See https://docs.aws.amazon.com/pdfs/whitepapers/latest/aws-overview-security-processes/aws-overview-security-processes.pdf for more information on cloud service infrastructure protection provided by AWS.

10. Disaster Recovery and Business Continuity

10.1 Backup and Disaster Recovery

Lark has formulated relevant regulations to standardize database backup strategies, backup data storage, and backup recovery testing. The business databases have regular snapshots and backups, and the data is stored in two places and three backups. At the same time, Lark has deployed a backup execution monitoring mechanism to ensure the integrity of data backups, and regularly conducts backup data recovery tests.

Full data backup is performed once a week, and incremental backup is performed automatically in real time. Lark has deployed a backup execution monitoring mechanism. If the database backup task fails, an alarm will be automatically sent to the database administrator through the Lark push function, and the database administrator will check the cause of the failure and handle it.

Lark extracts backup data every day for recovery testing. The R&D personnel raise the request of backup data recovery through the database operation and maintenance platform. After being reviewed by the person in charge of R&D, the database administrator will restore the data, and the R&D personnel will verify whether the backup data is available.

10.2 Business Continuity Guarantee

The access layer of the business system is accessed in a high-availability manner through the public gateway service provided by the basic service provider. The backend adopts multi-instance access to ensure service reliability, carry out meticulous monitoring of traffic and faults, and adopt degraded operation mode to ensure business availability when traffic bursts or faults occur.

Lark has emergency response and recovery measures in place for scenarios that could result in business disruption. Business impact analysis and risk assessment are performed once a year to identify important business processes and threats that may disrupt Lark's business and resources, define indicators such as maximum tolerable interruption time, recovery time objectives, and minimum service levels; formulate responses to different business interruption scenarios strategy.

10.3 Emergency drills

Lark has a complete emergency drill mechanism, and regularly conducts drills.

Participants include business teams, security teams, and operation and maintenance teams. Disaster recovery drill is conducted at least once a year for situations that may cause business interruptions to ensure data availability.

11. Change Management

11.1 Program Changes

Lark has established comprehensive change management controls, and clarified the change management requirements and process, including change plan, change approval, and change the implementation. Operations that have known or potential impacts on the stability, availability, and security of online services fall within the scope of online changes. Lark product development strictly controls the change operation to prevent the change operation from affecting the stability of the service. Online operations must have an operation request, which can only be carried out after approval. Lark has deployed independent development, testing, and production environments for each product-related application. The change operation follows the grayscale release and goes online. A small traffic test is required before the official release, so as to ensure the stability and security of the service.

11.2 Source Code Control

Lark has established a strict source code management process, and research personnel can only access and manage the code warehouse corresponding to their team. Each project code warehouse in the code warehouse has a person in charge of the code warehouse. If the R&D personnel need to apply for access to the code warehouse other than their team, they must submit the application in the code warehouse, and after the approval of the department head and the person in charge of the applied code warehouse, the corresponding permissions can be granted.

11.3 Infrastructure Changes

Lark deploys an access control list at the border of the public network to control network access. If it is necessary to change the ACL configuration baseline and network access control list, the operation and maintenance personnel submit an application through the platform, and professional engineers will perform the operation after assessing the rationality of the change. Only authorized engineers have the permission to perform changes to the network access configuration.

11.4 Change Monitoring

Lark conducts internal audits every year to check the operation of Lark's internal control system, which covers the implementation effectiveness of control related to change management, and summarizes the results in the internal audit report. If abnormalities are found, the internal audit department and the relevant responsible team will communicate and follow up on the rectification results. Segregation of duties exists in the change management process, including change development, testing, approval, release, and monitoring.

12. Open Platform Ecological Security

Lark is committed to creating a diverse, safe and reliable application ecosystem platform to provide enterprises with a more diverse SaaS service experience and meet the needs of different businesses. In this model, the Lark platform, application developers, customers and users form a multi-party responsibility system. Lark protects the security of applications, the health of the ecosystem, and the privacy of users from the aspects of service provider onboarding, application development review, permission classification and approval, and regular security inspections.

12.1 Service Provider Access

Lark has established a stringent onboarding mechanism for ecosystem application service providers to ensure that service providers have the ability to guarantee the security of user data. For example, the enterprise has been established for a certain number of years, the product has matured and commercialized, and the number of customers has served exceeds a certain number.

All Independent Software Vendors (ISVs) undergo a qualification review during onboarding. The review content includes but is not limited to: company qualifications, R&D capabilities, core members, past experience, customer groups, social reputation, etc.

12.2 App Development Review

Lark has formulated detailed development documents to provide developers with a set of safe and reliable development methods, and guided ISVs to develop safe, reliable and compliant applications from the development stage. In the store app launch stage, Lark will conduct an overall acceptance of the app deployment environment, app security, compliance privacy, security defence products, etc., and confirm the security compliance of the app through supplier questionnaires and app walkthroughs.

Lark conducts strict reviews of each application before it is put on the shelves, and grades it according to the risks of third-party applications. It is divided into three levels according to the permissions obtained by the application, the number of tenants or users used, and each level covers the deployment environment, application security, compliance privacy, security defence products and many other aspects.

- A1: Bottom line requirements: Applicable to all applications on the shelves
- A2: Enhanced security requirements: Applicable to apps with sensitive permissions and high usage
- A3: Recommended Security Measures: Recommended head application implementation

12.3 Authority Classification and Approval

Based on user and customer data security considerations, applications on the Lark open platform need to apply for permissions, and only after being reviewed by the open platform or tenant administrators can the open capabilities of permission binding be used. We divide permissions into normal permissions and advanced permissions:

- Ordinary permissions: permissions with general data sensitivity levels. Such as obtaining the user ID of the user, sending a message as an application, etc.
- Advanced permissions: The data accessed is highly sensitive. Such as obtaining user organizational structure information, obtaining a calendar, schedule and busy/leisure information, etc.

For enterprise self-built applications and store applications, Lark adopts different levels of permission application and approval strategies to ensure that the use of permissions is reasonable and minimally necessary under the premise of operability. For store apps, all permission operations need to go through two review processes: the app listing process and the tenant installation process. The listing is reviewed by the open platform, and the installation is reviewed by the tenant administrator when the version is updated. The tenant administrator configures audit-free rules based on the tenant's actual data control requirements to reduce the audit burden.

Based on relevant laws and regulations and operating system requirements, obtaining some sensitive personal information or invoking system-sensitive permissions may require separate authorization from the user, such as obtaining the user's geographic location, accessing the microphone, etc.

12.4 Security Monitoring Scanning

Lark uses automated vulnerability scanning for third-party applications to perform security scanning to detect whether the server uses vulnerable or vulnerable services, and continuously conducts risk monitoring and vulnerability detection for third-party applications.

The Lark security team conducts security tests on third-party applications aperiodically, simulating the behaviour of hackers, and conducts in-depth security assessments on app store applications to help third-party applications discover risks before hackers.

Version Change Record

Date	Version	Explanation
December 23, 2022	V1.0	English version finalized
September 1, 2025	V1.1	Updated with additions and changes