Lark Security 白皮書 V1.1

目錄

前言

Lark Technologies Pte. Ltd.（以下簡稱「Lark」）提供新一代企業辦公服務：Lark Suite，特色為「行動友善、即時協作及統一存取」，幫助企業提升工作效率、降低生產與管理成本，並迎向更高效、協作與安全的智慧型企業轉型。

Lark 提供辦公套件，具備即時通訊、雲端文件、雲端儲存、智慧行事曆、音視頻會議、開放平台、郵箱、OKR、審批等功能，且皆擁有高度的擴展性與可用性。Lark 採用業界領先的管理和技術手段，確保產品和用戶數據在整個生命週期中的安全。Lark 產品的設計、開發與運營，協助企業客戶符合適用法律、法規及網路安全、隱私與數據保護原則的要求。

1. 安全團隊及其職責

作為一個SaaS服務提供商，Lark始終將用戶的業務和數據安全視為首要任務。憑藉基礎設施安全以及業務和數據安全保護系統，Lark能夠在基礎設施、應用和數據層面為用戶提供全方位的保護。

Lark 的安全團隊由全職的安全管理、合規、業務安全、數據安全、應急響應、安全工具開發團隊及其他團隊組成。其職責包括產品設計的安全評估、代碼安全審查、漏洞掃描、滲透測試、威脅情報、入侵檢測、應急響應、數據安全、安全合規等多項工作。

2. 安全合規認證

Lark 非常重視產品合規，並積極將其產品與最高國際標準的合規要求進行對標。Lark 已獲得多項國際合規認證，包括 ISO27001、ISO27017、ISO27018、ISO27701、DPF、CBPR & PRP & DPTM，並完成了 SOC 2 Type II 和 SOC 3 服務認證報告。這表明 Lark 在資訊安全、雲端安全及隱私保護等領域已達到更為標準化和規範化的水平。

ISO27001 資訊安全管理系統：作為一套在業界廣泛認可的安全管理系統標準，它一直被視為最具權威性且最嚴格的國際資訊安全系統認證標準，並被全球廣泛接受。Lark 的數據中心、管理系統、研發及功能部門已取得此項認證，這意味著我們在資訊安全管理領域已與國際標準接軌。

ISO27017 雲端安全管理系統：它提供雲端專屬資訊安全控制機制的實施建議，補充了對 ISO 27002 與 ISO 27001 標準的指導。本實施程序為雲端服務提供者提供更多資訊安全控制實施指引。

ISO27018 公有雲個人資訊保護管理系統：這是首個聚焦於公有雲個人資訊保護的國際認證標準。它基於 ISO27002 資訊安全管理的實務規範，並為適用於公有雲個人可識別資訊（PII）的安全控制系統提供指導。Lark 獲得此認證代表我們在保護企業資料、用戶個人資訊及防止資訊外洩方面，達到了高標準的產業實務。

ISO27701 隱私信息管理系統：它是首個真正建立完整 PDCA 運作閉環的隱私信息管理系統標準。該標準詳細規定了建立、實施、維護及持續改進隱私信息管理系統的要求，並在信息安全保護的基礎上，考慮了處理個人可識別信息（PII）所需的隱私保護措施。2019 年，Lark 領先獲得由國際頂尖認證機構 BSI（英國標準協會）頒發的 ISO27701 隱私信息管理系統認證，成為全球首批獲得該認證的企業之一。

Lark 已獲得 SOC 2 Type I、SOC 2 Type II 及 SOC 3 服務審核報告。系統和組織控制（SOC）報告是由獨立第三方針對服務組織內部控制發出的檢查報告。

專業的第三方會計師事務所，依據美國註冊會計師協會（AICPA）的相關指導方針進行審核。SOC2 是其中一種類型，根據信任服務原則（安全性、可用性、處理完整性、機密性及隱私）訂定管理客戶資料的標準。Lark 定期接受第三方審計，以驗證產品符合此標準，顯示我們的系統可靠且安全。Lark 已獲得全球跨境隱私規則（CBPR）及全球資料處理者隱私認證（PRP）證書。CBPR 及 PRP 系統建立了國際公認的框架，用於保護參與司法管轄區內的個人資料。全球 CBPR 系統使組織能夠展現符合參與司法管轄區公認的隱私與資料保護標準的跨境資料負責實務；全球 PRP 系統則補充此點，確保資料處理者具備能力與治理機制，能依據 CBPR 框架下資料控制者的要求處理個人資料。透過同時取得全球 CBPR 及 PRP 系統的認證，我們展示了隱私計劃不僅符合嚴格標準以保護參與司法管轄區內的個人資料，同時確保處理實務透明、可靠，並符合資料控制者的義務。此雙重認可強調我們對隱私保護的承諾，降低跨境資料流的信任障礙，並向客戶、合作夥伴及監管機構保證受託個人資訊根據全球公認原則受到保護。此外，Lark 亦獲得新加坡資訊通信媒體發展局（IMDA）認可的資料保護信任標章（DPTM）。該標準依據新加坡《個人資料保護法》（PDPA）以及國際基準與最佳實務制定。取得此認證代表 IMDA 認可 Lark 長期致力於制定健全的資料保護政策與實務，保障客戶個人資料。Lark 已通過資料隱私框架（DPF）的認證，進一步展現其對保護個人資料及符合國際隱私標準的堅定承諾。此認證強化了 Lark 對透明性、問責制及負責任資料處理的投入，並促進依據 DPF 原則，將個人資料從歐盟、英國及瑞士無縫且安全地傳輸至美國。Lark 已成功完成由 TrustArc 進行的 GDPR 驗證，該獨立第三方評估機構確認我們遵守歐盟《一般資料保護條例》（GDPR）所訂定的要求。驗證過程涵蓋對我們資料保護政策、治理架構及操作實務的全面檢視，以確認符合 GDPR 主要義務，包括處理的合法依據、資料主體權利、資料安全、問責制以及跨境傳輸機制。

program 包含強而有力的控制措施，旨在符合監管要求和行業最佳實踐。這項獨立驗證提供了客觀的合規狀況證據，確保客戶、合作夥伴及監管機構能夠信賴我們在整個營運中維持高標準資料保護的承諾。

Lark 積極追蹤產品合規的國際要求，並透過安全管理與合規團隊與各級監管機構保持聯繫，確保所提供的產品與服務符合相關要求。此外，設立了專門的隱私團隊，負責審查用戶隱私協議、產品隱私保護設計、用戶私密資料的收集與使用，確保用戶私密資料被妥善使用與處理，並維持對用戶的適當透明度。關於 Lark 隱私保護相關實踐的更多內容，請參閱 Lark Trust Center。

3. 人員安全

3.1 人力資源管理流程

Lark 已建立安全的人力資源管理流程：

· 新員工的招聘必須經人力資源專員及職缺部門主管批准，且新員工的招聘流程與結果將記錄於人力資源系統；

· 在人力資源部根據職位的重要性及國家法律法規允許的範圍內，於聘用新員工前，將對該員工進行背景調查，以確保員工的聘用符合Lark的規章制度；

· 新員工需簽署聘用合約及

· 法律部門應至少每年審查員工保密協議及第三方保密協議中的條款，必要時進行更新，並在更新後透過內部知識平台發布，以確保所有員工及相關人員能夠取得最新的保密協議；

· 員工離職須由員工本人或部門主管在人力資源系統中提出申請，經人力資源部門及相關職能部門審核後，方可正式辭職。離職前，須取消所有帳號並歸還所有硬體及軟體資產（如電腦、工作文件等）。

3.2 安全培訓與學習

Lark 已建立完善的培訓與學習系統。新進員工需參加包括企業文化、規章制度、資訊安全及獎懲機制等培訓課程。同時，Lark 也會不定期舉辦有關員工專業知識與技能及資訊安全意識的培訓課程：

· Lark 將不定期舉辦資訊安全相關培訓課程，以提升員工的資訊安全技能，至少每年一次；

· Lark 將定期舉辦資訊安全活動以宣傳資訊安全意識，至少每年一次；

· Lark將以多種方式定期向員工傳達安全意識，例如製作安全意識宣傳資料及

透過郵件、海報等方式傳達給員工。

3.3 端點安全管理

Lark 已針對員工的終端設備制定完善的安全管理與控制策略，並預設部署於所有設備上。員工無法自行刪除或修改安全配置。所有 Lark 員工的電腦均安裝了防病毒軟體，後端安全配置防止員工關閉、卸載或修改防病毒軟體的設定。僅有 IT 部門授權人員擁有防病毒軟體的管理員帳號，以執行防病毒軟體的安全配置。該防病毒軟體能夠即時更新病毒資料庫，並定期對員工的終端設備進行全盤病毒掃描。Lark 對員工終端設備的磁碟執行全盤加密，以保障資料與檔案的安全。員工離職時需歸還終端設備，IT 部門將透過擦除硬碟的方式刪除員工設備上的資料。

4. 客戶端安全性

4.1 用戶端作業環境安全

Lark APP 將嚴格檢測運行環境，包括 root 偵測、越獄偵測、除錯偵測、注入偵測等。這些檢測的目的是確保客戶端終端在受信任的環境中運行，以防止程式被破解或遭惡意軟體利用。

4.2 用戶端資料安全

Lark APP 採用作業系統內建的安全機制來隔離 APP 之間的權限。用戶端本地資訊進行加密存儲。用戶端與伺服器之間的全鏈路通訊均使用 HTTPS 或 WSS 進行加密。

Lark 已在客戶端整合了自研的數據安全解決方案，提供系統級的能力來加密客戶端本地的私人數據以及數據與裝置之間的獨特綁定功能。即使攻擊者竊取了用戶的加密數據，也無法在自己的裝置上解密並使用這些數據。如此一來，用戶的數據安全邊界得到了顯著加強，用戶數據洩漏的機率也大幅降低。

4.3 用戶端防範安全漏洞

Lark 擁有一支全職的行動安全漏洞挖掘團隊，對 Android、iOS、Windows、MacOS、Linux 及其他客戶端進行安全評估與漏洞挖掘，並同時對所使用的第三方組件（庫、SDK）進行漏洞檢測，以定位應用程式中的漏洞，確保客戶端的安全。此外，Lark 也定期邀請外部專業的第三方安全公司對 Lark 進行安全滲透測試，並及時跟進修復和解決問題。

4.4 產品安全功能

Lark 在帳戶安全、訪問安全、數據安全等多方面提供安全能力，包括但不限於：

帳戶安全：
透過雙重身份驗證（2FA）確保帳戶安全，並透過單一登入（SSO）認證保護應用程式存取權限。

存取安全：
強制訪問條件和能力，以限制 Lark 登入僅限於受信任的環境。

資料安全：
透過分類標籤、檔案操作權限、Lark 自主研發的 DLP、行動檔案加密、螢幕截圖與錄影保護，以及可自訂的浮水印，保護企業資訊。

電子郵件安全：
提供防釣魚、防垃圾郵件、黑名單/白名單管理及資料保護規則，以確保電子郵件通訊安全。

租戶切換限制：
只有與企業相關聯的 Lark 租戶帳號才能在受信任環境中存取。禁止登入無關的租戶（例如個人或其他組織的租戶）。

稽核日誌：
支援資料外洩追蹤，透過保留並審查與潛在外洩相關的詳細操作日誌。

Lark 的產品安全功能更新迅速。欲了解最新功能，您可以參考官方網站介紹或聯繫客服諮詢。

5. 網路安全

5.1 網路存取控制

Lark 使用存取控制清單（ACL）來進行網路隔離。不同的網路區域，例如訪客網路、辦公網路、開發測試網路和生產網路，皆在內部分開。所有位於 Lark 網路邊界之外的員工皆需透過 VPN 連線來存取 Lark 的內部資源。Lark 的內部稽核部門將會稽核存取日誌等資料，查找並追蹤不合規的操作紀錄，並施加相應的處罰。

Lark 有嚴格的員工訪問控制政策，以限制對內部資源的訪問。員工需要進行身份認證才能訪問內部資源。身份確認後，員工默認只具有最小權限。新增權限的請求需經相關負責人員批准並記錄。權限具有有效期限，系統會在有效期限到期後自動撤銷權限。員工通過堡壘機操作線上服務，所有操作日誌至少保存 180 天，並由內部審計部門進行審核。

5.2 網路防火牆

Lark 使用網路防火牆攔截 Lark 套件系統中常見的網路安全漏洞攻擊，並且只有被授權的安全與合規工程師能統一配置網路防火牆的保護規則。Lark 採取自動與手動相結合的方式來更新網路防火牆配置。

5.3 DDoS 和網路攻擊防禦

Lark 服務透過 CDN 與動態加速為客戶提供網路存取，並透過公司負載平衡存取後端服務；Lark 已部署業界領先的防 DDoS 服務，能有效針對流量型與連線型攻擊等進行防禦。

5.4 網路傳輸加密

Lark 在內部網路和外部網路中均使用 HTTPS 和 WSS 進行加密傳輸，確保傳輸過程的安全，防止竊聽和篡改。

6. 伺服器安全性

Lark 已採取一系列安全控制措施來確保伺服器生產的安全，並有效防止惡意網路攻擊。

6.1 伺服器存取控制

Lark定期掃描伺服器資產，及時關閉不必要的埠口和服務，將外部權限降至最低，過濾不安全的服務，降低安全風險。安全人員定期進行弱密碼檢測，並督促伺服器運維人員提高密碼的複雜度，以防止暴力破解。所有對伺服器的訪問必須通過堡壘主機操作並審計。Lark使用白名單控制業務服務的訪問來源，確保只有受信任的來源能夠訪問服務。

6.2 弱點掃描

Lark 使用自動化漏洞掃描工具定期檢測伺服器漏洞。經安全人員確認後，會通知相關人員進行處理和修復。運維人員會定期更新系統補丁，以有效確保伺服器的穩定運行。

6.3 入侵偵測

Lark 的物理伺服器全面部署了 HIDS（主機入侵偵測系統），能即時監控伺服器檔案基線變化，發現異常程序，捕捉主動異常外部連結、木馬後門及其他異常行為，並及時響應。此外，所有來自客戶端的流量均經由 WAF（網頁應用防火牆）檢測與驗證，以確保其安全性和合法性，並即時阻擋惡意請求。安全團隊將密切追蹤安全狀況與最新攻擊手法，研究入侵特徵，並定期升級防禦策略。

6.4 異常檢測

基於大數據平台和機器學習平台，安全團隊對伺服器產生的大量主機日誌以及自研HIDS收集的數據進行多維度安全分析，建立異常檢測模型，及時發現伺服器上的風險操作和異常進程、惡意網路連接等異常行為，並及時響應。安全團隊將密切追蹤安全狀況和最新攻擊手法，持續迭代安全演算法模型，更新異常行為特徵，並定期

升級防禦策略。

7. 應用程式安全

7.1 安全開發流程

Lark 致力於從安全漏洞的源頭控制安全風險。透過製作安全課程並提供現場及線上培訓，所有開發人員和產品經理必須接受安全培訓，以了解相關安全漏洞的成因並加強程式碼知識。當專案啟動時，安全團隊會與專案經理溝通，確保安全需求和安全測試反映在專案計畫中。同時，安全團隊將評估產品使用的第三方函式庫和工具，發現漏洞以確保供應鏈不會引入漏洞。安全團隊會與產品團隊進行設計及程式碼安全審查。在產品上線前，將進行滲透測試及部署的安全評估，以確保服務的安全。

7.2 使用者帳戶安全

使用者對 Lark 系統的存取是透過密碼加上動態驗證碼進行身份驗證。對於在未識別裝置上發起的登入，風險控制策略將提高登入驗證的難度。同時，帳務系統具備防禦異常及暴力登入嘗試的能力。

Lark 連接了自主開發的風險控制與反作弊系統，具有防止惡意註冊、防止數據庫崩潰以及防止暴力破解登入等保護功能。使用者採用密碼+動態密碼多因素驗證方式登入，以降低因密碼外洩而導致帳號被入侵的風險。

7.3 漏洞與安全事件管理

Lark透過多種方式監控內部及外部的安全漏洞與威脅情報。安全團隊使用自動化安全掃描工具對自身的服務和作業系統進行掃描，並透過定期滲透測試對應用系統進行安全檢查。在確認漏洞及威脅情報後，將根據危害情況判定風險等級，並儘速推送給相關團隊進行修復與處理。Lark擁有完整的漏洞生命週期管理策略，專業的安全團隊會持續追蹤所有安全問題的解決。

同時，Lark 的安全團隊與業界頂尖的第三方評估公司及 WhiteHat 社群保持密切合作與溝通，並會不定期邀請外部公司及白帽駭客對服務進行滲透測試，並給予獎勵，以發現更多漏洞。

盡可能地減少安全漏洞。

Lark 擁有完善的事件管理流程，並實施 7*24 緊急響應策略。當發生安全事件時，安全團隊會根據安全緊急預案快速對事件進行分類，並啟動緊急響應流程，以防止安全事件擴大。安全事件處理完成後，將對事件進行復盤。復盤內容包括事件原因、事件處理過程與結果、事件主要負責人及後續措施等，並記錄復盤結果及後續措施，以確保事件的閉環管理。當安全事件影響用戶或客戶時，我們將根據事件處理流程及時通知用戶、客戶或其他相關方。

8. 資料安全

Lark 擁有完整的資料生命週期管理，並且在資料的建立、儲存、傳輸、使用及銷毀等各個階段，具備明確的流程與技術保障。Lark 採取相應的控制措施，以確保資料傳輸、資料儲存、資料存取以及資料銷毀過程的安全。

8.1 數據傳輸

Lark 為用戶提供支援強加密協議的數據傳輸連結。數據傳輸如訊息擷取、身份驗證及操作指令，皆透過 HTTPS 並使用 2048 位元 RSA 金鑰進行加密；傳輸的數據皆被加密並受到保護；視訊聊天採用基於 DTLS 的端到端伺服器加密，確保數據傳輸的安全。

8.2 資料儲存

Lark 使用安全金鑰機制來加密和儲存資料，並已對所有客戶資料如訊息和文件進行加密儲存。

Lark 已制定全面的數據分類管理方法，並在後台管理系統中對 Lark 收集的用戶信息及租戶信息進行嚴格的分類和分類管理，對系統中存儲的所有敏感信息進行加密，有效保護用戶的信息安全。

加密演算法嵌入於每個應用程式的原始碼中；金鑰由金鑰管理系統（稱為「KMS系統」）生成並由各應用程式呼叫。KMS服務負責金鑰與敏感配置資訊的生命週期管理，包括建立、儲存、分發、使用、更新、刪除等。租戶的資料加密主金鑰及 Lark 服務的各種其他敏感資訊（如資料庫帳號、密碼等）皆儲存在由 Lark 維護的 KMS 系統中，且存取必須透過 KMS 存取。KMS 系統的根金鑰由硬體安全模組（HSM）維護。HSM的管理需要多把金鑰合作完成，這些金鑰分別由不同的功能角色管理。KMS 系統使用封套加密（envelope encryption）來加密及解密資料。不同租戶使用的主金鑰彼此隔離。

除了使用標準的租戶主密鑰和 AES-256 演算法來加密資料和資料密鑰之外，Lark 支援使用客戶獨立管理的金鑰，也就是由 KMS 生成資料密鑰，並使用客戶自訂的主密鑰來加密資料及資料密鑰。該密鑰及指定的加密演算法會被加密並儲存在資料庫中。客戶可以自行選擇加密演算法並控制金鑰輪換。

8.3 資料存取

使用者資料的存取嚴格依權限隔離。使用者無法在未經授權的情況下存取彼此資料。資料存取必須由資料擁有者明確授權，例如透過分享操作等。（例如，userA 所建立的文件預設僅 userA 可見，除非他主動授權他人存取）。

預設情況下，Lark 的員工無法存取任何用戶資料，且所有員工的操作皆受到嚴格限制與審核。

8.4 資料處置

個人用戶可以申請刪除個人帳戶及資訊。收到帳戶或個人資訊刪除申請後，Lark 將刪除或匿名化被刪除帳戶的相關資料。

對於企業用戶，當員工離職時，組織的管理員可以通過企業管理控制台管理離職流程。作為此流程的一部分，管理員可以選擇刪除員工的數據或將員工的個人資訊匿名化。

當 Lark 與用戶組織簽訂合作協議時，雙方同意在合作終止時，Lark 將依照法律法規處理與帳戶相關的數據，包括但不限於刪除和匿名化。

所有資料刪除及匿名化技術手段均符合現行產業標準及法律法規的要求。

8.5 資料安全檢查

Lark 線上環境中所有伺服器的登入行為、操作行為、伺服器安全基線檔案變更、存取權限變更及資料存取行為皆會被記錄。透過建立使用者行為畫像及異常行為模型，安全團隊得以辨識、分析及關聯異常行為，並即時自動偵測各類異常資料存取行為，如不當資料存取、惡意資料爬取及風險操作、異常登入、權限提升等，並發出警報或進行封鎖。

9. 基礎設施安全

Lark 使用 AWS 雲端服務，AWS 負責操作、管理及控制其硬體和軟體設施。作為全球領先的雲端服務提供者，AWS 擁有業界頂尖的安全能力，以保護使用者的基礎設施安全。參見

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. 災難復原與業務持續性

10.1 備份與災難復原

Lark 已制定相關規定，以規範資料庫備份策略、備份資料存儲及備份恢復測試。，業務資料庫定期進行快照和備份，並將資料儲存在兩地三備的架構中。同時，Lark 部署了備份執行監控機制，以確保資料備份的完整性，並定期進行備份資料恢復測試。

完整資料備份每週執行一次，增量備份則自動進行且為即時。Lark 已部署備份執行監控機制，若資料庫備份任務失敗，會透過 Lark 推送功能自動發出警報給資料庫管理員，資料庫管理員將檢查失敗原因並進行處理。

Lark每天提取備份數據進行恢復測試。研發人員通過數據庫運維平台提出備份數據恢復請求。經研發負責人審核後，數據庫管理員將恢復數據，研發人員將驗證備份數據是否可用。

10.2 企業持續營運保證

業務系統的接入層透過基礎服務提供商提供的公共網關服務以高可用方式接入。後端採用多實例接入以確保服務可靠性，對流量和故障進行細緻監控，並在流量突發或故障發生時採用降級運行模式以確保業務可用性。

Lark已制定緊急應變與復原措施，應對可能導致業務中斷的情境。每年進行一次業務影響分析與風險評估，以識別重要的業務流程和可能中斷Lark業務與資源的威脅，定義最大可容忍中斷時間、復原時間目標和最低服務水平等指標；並針對不同的業務中斷情境制定應對策略。

10.3 緊急演習

Lark 擁有完善的應急演練機制，並定期進行演練。參與者包括業務團隊、安全團隊以及運維團隊。災難復原演練至少每年進行一次，針對可能導致業務中斷的情況，以確保資料可用性。

11. 變更管理

11.1 程式變更

Lark 已建立完善的變更管理控制，並明確變更管理的要求與流程，包括變更計劃、變更審批及變更實施。對線上服務的穩定性、可用性與安全性有已知或潛在影響的操作，均屬於線上變更的範圍。Lark 產品開發嚴格控制變更操作，以防止變更操作影響服務穩定性。線上操作必須有操作申請，且僅能在審批通過後執行。Lark 為每個產品相關應用部署獨立的開發、測試和生產環境。變更操作遵循灰度發布後上線，正式發布前需進行小流量測試，以確保服務的穩定性與安全性。

11.2 原始碼控制

Lark 已建立嚴格的原始碼管理流程，研發人員僅能訪問並管理其團隊所對應的代碼倉庫。代碼倉庫中的每個專案代碼倉庫皆有專人負責。如研發人員需申請訪問非所屬團隊的代碼倉庫，須在代碼倉庫中提交申請，經部門主管及申請代碼倉庫負責人批准後，方可授予相應權限。

11.3 基礎設施變更

Lark 在公共網路邊界部署存取控制清單以管理網路存取。若需變更 ACL 配置基線及網路存取控制清單，運維人員必須通過平台提交申請，專業工程師將在評估變更合理性後執行操作。僅有授權工程師擁有執行網路存取配置變更的權限。

11.4 變更監控

Lark 每年進行內部審計，以檢查 Lark 內部控制系統的運作情況，該系統涵蓋與變更管理相關控制的實施效能，並將結果彙總於內部審計報告中。如發現異常，內部審計部門與相關負責團隊將進行溝通並跟進整改結果。變更管理流程中設有職責分離，包括變更開發、測試、批准、發布及監控。

12. 開放平台生態安全

Lark 致力於打造多元、安全且可靠的應用生態系統平台，為企業提供更豐富的 SaaS 服務體驗，並滿足不同業務的需求。在此模式中，Lark 平台、應用開發者、客戶及用戶共同構成多方責任體系。Lark 從服務提供者入駐、應用開發審核、權限分類與審批，以及定期安全檢查等方面，保障應用的安全、生態系統的健康及用戶的隱私。

12.1 服務提供者存取

Lark 已建立嚴謹的生態系統應用服務提供者上線機制，以確保服務提供者具備保障用戶數據安全的能力。例如，企業成立已有一定年限，產品已成熟並商業化，且服務的客戶數量超過一定數量。

所有獨立軟體供應商（ISVs）在加入時都會接受資格審查。審查內容包括但不限於：公司資質、研發能力、核心成員、過往經驗、客戶群、社會聲譽等。

12.2 應用程式開發審查

Lark 制定了詳細的開發文件，為開發者提供一套安全且可靠的開發方法，並指導 ISV 在開發階段開發安全、可靠且合規的應用程式。在商店應用啟動階段，Lark 將對應用部署環境、應用安全、合規隱私、安全防禦產品等進行全面驗收，並通過供應商問卷和應用檢查確認應用的安全合規性。
環境、應用程式安全、合規隱私、安全防護產品等，並通過供應商問卷調查和應用程式演練確認應用程式的安全合規性。

Lark 在上架每個應用程式之前，都會進行嚴格審查，並根據第三方應用程式的風險進行評級。根據應用程式獲得的權限、使用的租戶或用戶數量，分為三個等級，每個等級涵蓋部署環境、應用程式安全、合規隱私、安全防護產品等多個方面。
應用程式安全、合規隱私、安全防禦產品及其他多個方面。

- A1：基本要求：適用於所有上架的應用程式
- A2：強化安全需求：適用於具有敏感權限和高使用率的應用程式
- A3：建議的安全措施：建議的頭部應用實施

12.3 權限分類與核准

基於用戶和客戶數據安全的考量，Larkopen 平台上的應用程式需申請權限，並且只有在經過 theopen 平台或租戶管理員審核通過後，才能使用權限綁定的開放能力。我們將權限分為一般權限與進階權限：

· 普通權限：具有一般數據敏感度級別的權限。例如獲取用戶的用戶ID、以應用程式身份發送訊息等。

· 進階權限：所存取的資料屬於高度敏感。例如
訊、取得行事曆、行程及忙碌/閒暇資訊等。

對於企業自建應用和應用商店應用，Lark 採用不同層級的權限申請和審批策略，以確保在可操作性前提下，權限的使用合理且達到最小必要。對於商店應用，所有權限操作都需經過兩個審核流程：應用上架流程和租戶安裝流程。上架由開放平台審核，安裝則由租戶管理員在版本更新時審核。租戶管理員根據租戶的實際數據控制需求配置免審規則，以減輕審核負擔。

根據相關法律法規及作業系統要求，
取得一些敏感的個人資訊或調用系統敏感權限
權限可能需要用戶另外授權，例如獲取用戶的地理位置、使用麥克風等。

12.4 安全監控掃描

Lark 使用自動化漏洞掃描對第三方應用程式進行安全掃描，以檢測伺服器是否使用了易受攻擊的服務，並持續對第三方應用程式進行風險監控和漏洞檢測。

Lark 安全團隊定期對第三方應用程式進行安全測試，模擬駭客的行為，並對應用程式商店的應用進行深入的安全評估，協助第三方應用程式在駭客之前發現風險。

版本變更記錄

日期	版本	說明
2022年12月23日	V1.0	英文版本定稿
2025年9月1日	V1.1	更新並新增內容與修改事項