源思科技股份有限公司

資訊安全管理暨隱私保護制度

雲端服務安全白皮書

發行單位:資訊安全管理委員會

文件編號:LoFT-GR-FM-077

發布日期:2026/03/03

版本編號:1.0.0

紀錄版本:1.1.0

修訂紀錄

紀錄版本	修訂日期	修訂內容摘要
1.0.0	2026/01/30	因應新增ISO/IEC 27017/27018 要求，修訂本文件。
1.1.0	2026/03/03	調整聯絡窗口

目錄

1. 前言與適用範圍

源思科技股份有限公司(以下稱「本公司」)提供企業級雲端通訊與協作平台 Juiker, 屬軟體即服務(SaaS)之雲端服務。

本白皮書旨在說明本公司作為雲端服務供應商(Cloud Service Provider, CSP)如何落實資訊安全與個人資料保護之管理與技術措施, 並揭露雲端服務客戶(以下稱「客戶」) 在共享責任模型下應配合之事項。

本文件為公開版, 本文件為 公開版(Public Edition), 適用於:

- 政府、企業、教育機構等使用 Juiker 之雲端服務客戶與潛在客戶;
- 監管機關、合作夥伴與稽核關係人;
- 一般使用者了解 Juiker 對安全與資料保護之承諾。

2. 安全與隱私治理架構

2.1. 資安治理

本公司設置「資訊安全與隱私保護管理委員會」, 由資訊安全長(CISO)領導, 負責制定安全與資料保護政策、年度風險評估、稽核追蹤與持續改善;並定期檢視管理系統之有效性與認證維護狀態。

2.2. 資安團隊與職能

本公司配置專職資安與合規人力, 涵蓋安全管理、合規、業務安全、資料安全、應急響應與安全工具研發等職能, 以確保從基礎設施到應用與資料層的全方位防護。

主要工作項目包含(但不限於):

- 產品設計安全評估、程式碼安全審查與安全上線評估。

- 弱點掃描、滲透測試、威脅情報與入侵偵測。
- 資安事件應變、協助鑑識與修復改善。
- 資料安全與雲端服務合規要求之落實與稽核準備。

2.3. 共享責任模型

Juiker 採共享責任模型，安全責任之劃分原則如下，實際責任範圍仍以契約、SLA、資料處理協議（DPA）或與相關約定為準。

範疇	Juiker (CSP) 責任	客戶 (CSC) 責任
平台架構安全	維護系統與網路安全、修補漏洞	依客戶端使用情境配合（例如：端點安全、網路環境）
使用者與存取管理	提供帳號權限機制與記錄	設定、授權與審查使用者權限
資料管理與保護	提供安全儲存與刪除機制	決定蒐集、保留與刪除內容
合規與稽核支援	維持平台合規管理機制，並依契約或客戶合理需求提供透明揭露與合規佐證。	依自身法規遵循資料蒐集目的

3. 雲端架構與虛擬化隔離

3.1. 架構概覽

Juiker 之主運行節點位於台灣資料中心；另設置災難備援節點以支援故障復原。為提升使用體驗與韌性，本公司可採用第三方雲端服務提供內容快取與備援等輔助能力。

- 所有通訊流量採 TLS 加密通道傳輸（含行動端與網頁端）。
- 採用標準化時間同步機制（NTP），並監測時間偏移，以確保稽核與

事件追蹤一致性。

3.2. 多租戶隔離

針對客戶型態服務模式，網路隔離及安全機制定義如下:

客戶型態	網路隔離措施	實施方式與說明
一般用戶 （公共服務）	不進行網路隔離	採應用層邏輯隔離，以帳號、權限與品牌區分使用者資料。
企業用戶 （無特殊網路要求）	應用層隔離	與一般用戶相同，另以企業識別碼Corpid進行邏輯分群。
企業用戶 （要求網路隔離）	虛擬網路隔離	於 CSP 環境內建立專屬 VPC/VNet/Subnet，設定防火牆與 VPN，確保與其他租戶流量隔離。
企業用戶 （要求內部部署）	實體隔離	系統部署於客戶自有機房或指定設備上;維運依契約責任界面執行。

3.3. 安全設計則

Juiker 在虛擬化環境中落實三層防禦:

- 技術隔離(技術面):容器、網段、金鑰與存取權限分層與隔離。
- 邏輯隔離(應用面):租戶資料與服務認證分離，採最小權限原則。
- 組織隔離(人員面):維運人員權限受限，避免直接讀取客戶資料內容。

4. 人員安全與資安意識

4.1. 招募、任用與離職管理

本公司建立人力資源安全管理流程，包含招募核准、(依法)背景查核、聘僱合約與保密義務、離職交接與帳號停用等，確保人員生命週期安全控管。

4.2. 資安訓練

新進人員需完成資訊安全與制度訓練;並定期(至少每年一次)辦理資安意識與專業訓練，以提升全員安全素養。

4.3. 終端設備安全

員工終端設備採防毒等端點安全管理要求，並由管理機制控管安全設定;離職時依程序回收設備並執行資料抹除

5. 網路與基礎設施安全

5.1. 網路存取控制與分區

內部網路依訪客、辦公、開發測試、正式等區域分段隔離;位於公司網路邊界外之人員需透過 VPN 存取內部資源，並留存稽核紀錄。

5.2. 防火牆與 DDoS 防護

採用網路防火牆、WAF 與抗 DDoS 服務等措施，阻擋常見網路攻擊與惡意流量;防護規則由授權人員統一管理並定期更新。

6. 伺服器與主機安全

本公司針對正式環境主機與伺服器建立維運安全管理與技術防護控制，重點包含:

- 資產管理、弱點管理與組態強化:建立資產清冊，定期執行弱點掃描、修補與風險評估;依組態強化基準關閉非必要連接埠/服務，並控管預設帳密、管理介面與遠端存取。
- 特權帳號集中控管與遠端維運管制:正式環境維運採特權帳號集

中控管與維運遠端控管機制，落實最小權限、分權分責、授權期限、帳號到期註銷、操作紀錄保存與稽核追蹤。

- 主機端防護、日誌與偵測回應:部署主機端防護與偵測機制(如主機入侵偵測/防護、日誌蒐集、檔案完整性監控、行為/異常偵測)，並納入事件處理流程以進行告警分析、阻斷與改善。

7. 應用安全與安全開發流程

7.1. 開發生命週期管理

本公司於產品規劃、設計、開發、測試、部署與上線各階段導入安全要求，包含:第三方元件風險評估、程式碼/變更審核，以及上線前必要之安全測試與部署設定檢視。

7.2. 弱點管理與資安事件處理

本公司定期監控弱點資訊與威脅情資，依風險分級訂定修補時程並追蹤至結案;如發生資安事件，依既定流程進行通報、處置、調查、復原與改善，並保留相關紀錄以利稽核追蹤。

8. 資料安全與加密

8.1. 資料生命週期管理

本公司針對資料建立、儲存、傳輸、使用到銷毀建立管理流程與技術措施，確保資料於各階段之機密性、完整性與可用性。

8.2. 傳輸中資料加密

- 傳輸中資料:訊息與通訊資料於傳輸過程中採用安全通訊協定(如TLS)，並依循國家資通安全研究院之相關資安指引，確保資料於傳輸期間之機密性與完整性。

- 儲存中資料:系統所儲存之檔案與訊息內容均採用業界通用之高

強度加密機制進行保護;檔案識別資訊以非可識別方式產生，以降低未授權存取風險。

- 金鑰管理:金鑰集中於專責管理系統進行控管，依服務模式由 Juiker 或客戶負責管理，並採多層級權限與身分驗證機制，確保金鑰安全與存取可控。
- 金鑰更新:金鑰定期進行更新與輪替，並留存相關紀錄以供查核。

8.3. 資料存取控管

租戶資料依權限嚴格隔離;預設情況下，員工不具備客戶資料內容之存取權限。任何必要之系統操作將受核准流程、最小權限與稽核紀錄約束，並加強日誌檢視機制對非法存取與高風險操作進行稽核。

客戶使用 Juiker 服務時，應依本公司提供之服務功能、管理介面及授權範圍操作，不得使用未授權工具、繞過存取控制、濫用權限，或從事可能影響雲端服務安全與穩定性之行為。

9. 備份、災難復原與營運持續

本公司制定備份與復原策略，定期執行全量/增量備份並加密保存於與主系統不同之儲存位置;並定期進行復原測試與演練，以驗證備份資料可用性與復原程序有效性。

本公司亦依業務衝擊分析(BIA)與風險評估結果，規劃營運持續措施與應急回復策略，並至少每年進行一次災難復原演練。

10. 個資處理與刪除政策

本公司依客戶授權與契約約定處理個人資料，不將客戶資料用於未經授權之分析或行銷用途。

- 資料最小化:僅保存提供服務所需之最小資料;

- 刪除機制:客戶終止服務或提出刪除要求時,將於合規時間內刪除資料及備份副本,並可提供完成紀錄供查驗;
- 資料可攜:服務終止時,可依客戶要求提供資料導出或轉移協助,以標準格式取回資料。

11. 跨境傳輸與揭露

本公司原則上以台灣境內資料中心進行主要資料處理與儲存;若為內容快取、備援或維運需要而使用境外雲端服務,將依契約與法規要求揭露資料處理地點與分包情形,並採取適當加密與存取控管措施。

如因法律或主管機關要求需進行資料揭露,本公司將依相關法令辦理,並於法令允許範圍內事前通知客戶。

12. 事件通報與應變

若發生資料外洩、未授權存取或重大系統異常,本公司將依事件管理程序啟動分級處理與應變流程,並:

- 原則上於 72 小時內通報客戶。
- 事件概要、影響評估與改善計畫;
- 若涉及個人資料事件,協助客戶完成主管機關通報與後續處置;
- 結案後進行檢討,列管改善事項並追蹤完成
- 本公司定期辦理通報與應變演練,以確保跨部門反應時效。

13. 變更通知與透明揭露

本公司建立正式之變更管理程序,確保影響系統、應用服務或個人資料處理之重大變更均經評估與核准後實施。

可能涉及之平台層級變更項目包含:

- 虛擬化底層版本更新與資安修補
- 防火牆韌體更新與資安修補
- 容器平台與作業系統更新與資安修補
- 資料庫系統更新與資安修補
- 個人資料存放地點或分包商變更

其通知方式與原則如下:

- 屬例行維運與資安修補者,將以公告方式通知,且其維護時段不納入 SLA 可用度計算。
- 涉及平台架構、服務模式或資料治理之重大變更者,應於事前通知客戶並說明影響評估。
- 涉及個人資料處理地點或跨境移轉之變更者,應依法及契約約定進行通知。
- 變更完成後,Juiker 將視需要更新相關公開文件或透明性說明資料。(網路公告)
- 例行性維護或不影響雲端服務客戶使用之更新,將透過平台維運公告方式說明。

14. 分包供應商與資料處理地點

本公司如使用分包供應商提供機房、備援或內容快取等服務,將採取供應商管理與安全要求(例如:評估、契約安全條款、定期審查),並揭露主要資料處理地點。下表為網站公告版之摘要,詳細資訊可於簽

署 NDA 後提供。

項次	供應商名稱	服務類型	處理行為	資料處理地點	說明
1	台灣大哥大股份有限公司	IDC 機房／雲端基礎設施服務	提供機房場地、電力、網路、環境控制及實體設施維運，供 Juiker 自行架設與營運主系統伺服器；供應商不介入系統操作，亦不直接存取或處理 Juiker 資料內容。	台灣（台北資料中心）	主運行節點；系統與資料由 Juiker 自行管理與控制
2	Google Cloud Platform（Google LLC）	雲端運算與災難備援服務	依 Juiker 設定提供災難備援、系統復原與必要之資料同步儲存服務，資料處理行為受 Juiker 管理與控管	台灣（彰濱區域）	災難備援節點；平時非主要營運系統
3	Amazon Web Services, Inc. (AWS)	安裝檔案快取加速服務	依 Juiker 設定提供 Log備份、安裝檔快取（CDN）加速服務。	新加坡/日本	用於安裝檔案快取最佳化

15. 法規遵循與第三方查核

本公司依 Juiker 服務型態與客戶需求，持續對標並導入雲端安全與個資保護相關國際標準，包含 ISO/IEC 27001、ISO/IEC 27017、ISO/IEC 27018 等；並依契約與稽核需求提供合規佐證之申請與查閱流程。

第三方稽核報告與合規證書可於客戶簽署 NDA 後查閱。

16. 聯絡窗口

資安事件通報: service@juiker.tw

個資查詢與刪除:service@juiker.tw

合約與法遵洽詢:service@juiker.tw