個人資料檔案安全維護計畫

好記 Hoki AI 輔助諮商紀錄系統

文件編號：HOKI-SEC-001 ｜ 版本：3.0 ｜ 生效日期：2026 年 2 月 21 日

一、目的

本計畫依據《個人資料保護法》第 27 條第 1 項及《個人資料保護法施行細則》第 12 條之規定，針對「好記 Hoki」AI 輔助諮商紀錄系統（以下簡稱「本系統」）所蒐集、處理及利用之個人資料，訂定安全維護措施，以防止個人資料被竊取、竄改、毀損、滅失或洩漏。

二、適用範圍

本計畫適用於本系統之所有個人資料處理作業，包括：

- 使用者帳號資料（帳號、密碼雜湊、顯示名稱）
- 諮商相關資料（錄音、逐字稿、去識別化諮商紀錄、個案編號）
- 系統使用紀錄（使用時間、次數、模板使用）
- 稽核紀錄（操作事件、IP 位址、時間戳）

三、組織與權責

角色	權責	擔當
個資管理負責人	統籌個人資料保護政策之制定、執行與監督	系統開發者（張益善）
系統管理員（Superadmin）	帳號管理、稽核紀錄查閱、資料庫備份、安全事故通報。**不可存取個案之諮商紀錄內容或原始錄音。**	系統開發者或委託人指定人員
心理師（Therapist）	遵守系統使用規範、保護案主隱私	使用本系統之心理師

四、資料分級

等級	定義	資料範例	保護措施

機密	涉及案主之敏感個人資料	諮商錄音、逐字稿	處理後立即刪除，不保存
限制	經去識別化之諮商資料	去識別化諮商紀錄、個案編號	加密儲存、存取權限控制
內部	系統營運相關資料	帳號資料、使用紀錄、稽核紀錄	加密儲存、角色權限控制

五、技術安全措施

5.1 存取控制

- 採二層角色權限架構：系統管理員（Superadmin）、心理師（Therapist）。系統管理員不可存取個案之諮商紀錄內容
- 所有 API 端點於處理請求前驗證使用者身分與角色權限
- 使用者認證採 Token 機制，Token 有效期為 7 日，以 HttpOnly Cookie 儲存
- 所有使用者帳號均強制啟用兩步驟驗證（TOTP MFA）
- 閒置超過 15 分鐘自動登出
- API 速率限制：每 IP 每分鐘 60 次，登入 API 每分鐘 10 次

5.2 加密措施

項目	技術	說明
傳輸加密	HTTPS / TLS	使用者與伺服器間所有通訊皆加密
儲存加密	SQLCipher (256-bit AES)	資料庫檔案全磁碟加密
密碼儲存	bcrypt 雜湊	密碼不以明文保存，含隨機鹽值
加密金鑰管理	Google Cloud Secret Manager	金鑰不寫入程式碼，透過 Secret Manager 注入

5.3 去識別化

- **第一層（AI 辨識）**：大型語言模型自動辨識逐字稿中的人名、地名等，以代號替換
- **第二層（正規表達式）**：以 pattern matching 移除電話、電子郵件、日期、中文常見姓氏等

5.4 HTTP 安全標頭

- **Content-Security-Policy (CSP)**：限制可執行的腳本來源，防止跨站腳本攻擊 (XSS)
- **Strict-Transport-Security (HSTS)**：強制瀏覽器使用 HTTPS 連線
- **X-Content-Type-Options**：防止 MIME 類型嗅探

- **X-Frame-Options**：防止頁面被嵌入 iframe（防止 Clickjacking）
- **Referrer-Policy**：限制 HTTP Referrer 資訊洩漏

5.5 自動刪除機制

- 錄音檔：經客戶端加密上傳後，於伺服器記憶體（tmpfs）中解密處理，語音轉文字完成後立即自動刪除，全程不寫入磁碟
- 逐字稿：僅暫存於伺服器記憶體，不寫入資料庫或檔案系統
- 暫存檔案：處理過程中產生之暫存檔案使用 tmpfs（記憶體檔案系統），無論成功或失敗皆自動清除

5.6 稽核軌跡

系統自動記錄以下事件類型：

事件類型	說明
LOGIN_SUCCESS / LOGIN_FAILURE	登入成功 / 失敗
LOGOUT	使用者登出
DATA_ACCESS	諮商資料存取
USER_CREATE / USER_DELETE	帳號建立 / 刪除
USER_RESET_PW	密碼重設
TEMPLATE_CREATE / UPDATE / DELETE	模板操作
RETENTION_UPDATE	資料保留期間設定變更
BACKUP	資料庫備份

每筆稽核紀錄包含：事件類型、使用者 ID、使用者名稱、詳細說明、IP 位址、時間戳。僅系統管理員可查閱稽核紀錄。

5.7 資料備份

- 系統管理員可透過管理介面或命令列工具執行加密資料庫備份
- 備份自動排除諮商紀錄（DELETE + VACUUM），僅保留系統管理資料，貫徹資料最小化原則
- 備份檔案保持 SQLCipher 加密狀態，檔名含時間戳以利版本管理
- 備份操作自動記錄於稽核紀錄
- 建議備份頻率：每日一次或依機構資料量調整

- 保留最近 14 日之備份

5.8 客戶端加密

- 音訊資料於瀏覽器端以 AES-256-GCM 對稱加密，AES 金鑰再以 RSA-4096 公鑰包裝後上傳
- 每次上傳產生新的隨機 AES 金鑰與 IV，具備前向安全性
- 僅伺服器持有 RSA 私鑰可解密，傳輸中間節點（包含 CDN/Tunnel）無法還原明文
- 使用 Web Crypto API（瀏覽器原生），不依賴第三方函式庫

5.9 資料殘留防護

- Docker 暫存目錄使用 tmpfs（記憶體檔案系統），容器停止後自動清除
- 關閉 swap（mem_swappiness=0），防止敏感資料被交換至磁碟
- 停用 core dump（ulimit core=0），防止程序崩潰時記憶體內容外洩
- AI 模型處理完成後立即釋放記憶體（推理完成即清空）

5.10 數位浮水印

- 匯出之 DOCX 文件內嵌隱藏浮水印，記錄匯出使用者與時間戳
- 浮水印以極小字元嵌入文件頁尾，不影響閱讀但可供事後追溯

5.11 資料保留與自動清除

資料類別	保留期間	清除方式
諮商錄音	處理完成後即刪	系統自動（finally 區塊）
逐字稿	僅存記憶體	請求結束後自動釋放
去識別化諮商紀錄	2 天	系統自動清除（purge_expired_data）
使用紀錄	90 天	系統自動清除
稽核紀錄	365 天	系統自動清除

> **設計原則**：本系統為輔助筆記工具，非法定紀錄保存系統。諮商紀錄僅供心理師短期參考，保留期間最小化以降低資料外洩風險。心理師應於紀錄生成後儘速匯出至正式紀錄系統。

六、管理安全措施

6.1 人員管理

- 系統使用者需經系統管理員授權或透過線上註冊管道自助註冊方可開通帳號
- 使用者不再使用本系統時，應停用或刪除其帳號
- 新進人員應接受系統操作與隱私保護教育訓練

6.2 密碼政策

- 密碼長度至少 12 個字元，須包含大寫字母、小寫字母、數字及特殊字元，並檢查常見密碼黑名單
- 密碼超過 90 天未更換時，系統將於登入時提醒使用者更新
- 密碼以 bcrypt 雜湊加鹽儲存，不保留明文
- 密碼重設操作記錄於稽核紀錄

6.3 設備管理

- 系統部署於 Google Cloud Platform 台灣區域（asia-east1），受 Google 資料中心實體安全保護，並透過 IAM 存取控制、VPC 防火牆規則及 IAP 通道存取管理
- 伺服器作業系統應定期更新安全修補程式
- 使用者操作設備（電腦、手機）應設定螢幕鎖定

七、安全事故通報與應變

詳細事故應變流程請參閱《事故應變 SOP》（文件編號：HOKI-SEC-002）。重點摘要如下：

1. **發現通報**：任何人員發現或懷疑個人資料安全事故，應立即通報系統管理員
2. **初步處置**：系統管理員應於 1 小時內進行初步評估並採取緊急處置
3. **通報機制**：確認事故後 24 小時內通知受影響之委託人，72 小時內通報主管機關
4. **事後改善**：事故處理完成後進行根因分析，修訂安全措施

八、定期檢視與稽核

8.1 定期檢視項目

- [ ] 檢視使用者帳號清單，停用閒置帳號（每季）
- [ ] 檢視稽核紀錄，確認無異常存取模式（每月）
- [ ] 確認資料庫備份正常執行且可還原（每月）
- [ ] 檢視伺服器作業系統與軟體之安全更新（每月）

- [ ] 確認 HTTPS/TLS 憑證有效期（每季）
- [ ] 確認 SQLCipher 加密金鑰管理正常（每季）
- [ ] 重新評估安全維護計畫之適當性（每年）

8.2 稽核紀錄檢視要點

- 多次登入失敗是否來自同一 IP（潛在暴力破解攻擊）
- 非上班時間之異常資料存取
- 短時間內大量資料匯出
- 未授權角色嘗試存取受限功能

九、教育訓練

對象	訓練內容	頻率
系統管理員	系統安全設定、稽核紀錄判讀、備份還原操作、事故應變流程	到職時 + 每年一次
心理師	系統操作、知情同意流程、個資保護注意事項	到職時 + 每年一次

十、文件管理

本計畫相關文件清單：

文件編號	文件名稱	說明
HOKI-SEC-001	個人資料檔案安全維護計畫	本文件
HOKI-SEC-002	個人資料安全事故應變 SOP	事故應變流程
HOKI-LEG-001	隱私權政策	公開之隱私政策說明
HOKI-LEG-002	AI 輔助諮商紀錄知情同意書	案主簽署用
HOKI-LEG-003	個人資料委託處理契約	與委託人（個人或機構）簽訂
HOKI-GDPR-001	個人資料處理活動紀錄 (ROPA)	GDPR 第 30 條處理活動紀錄
HOKI-DPIA-001	資料保護影響評估 (DPIA)	GDPR 第 35 條資料保護影響評估

版本紀錄

版本	日期	修訂內容	修訂人
1.0	2025-02-15	初版制定	張益善
2.0	2026-02-21	RBAC 改為二層；密碼政策 12+；新增客戶端加密、資料殘留防護、數位浮水印、資料保留與自動清除；備份排除諮商紀錄；移除機構管理員角色	張益善
3.0	2026-02-21	SOAP→諮商紀錄統一用語；個人/機構雙模式支援；錄音 tmpfs 記憶體處理補述；委託處理契約說明更新；人員管理個人模式適用	張益善

本計畫依《個人資料保護法》第 27 條第 1 項及《個人資料保護法施行細則》第 12 條之規定訂定