資安是智生活產品開發與治理的最高準則
守護用戶資料與隱私，是我們最重要、也最不可退讓的責任

智生活

針對近期媒體報導及消基會公布之資安檢測結果，對於外界疑慮，我們不找藉口—無論是版本不同或測試條件差異，保護資料安全就是我們的責任，為此提出具體修補與可驗證結果對外負責。已於2/15與2/16 發布 V4.13.1 Hotfix 更新版本。同步啟動「雙重第三方驗證」機制，3/4收到實驗室初步提供檢測文件。
截至 3/24，已陸續完成雙實驗室之檢測與複測結果，以下提供最消基會指稱項目的最新處理進度報告

最新處理進度報告(更新時間2026/03/30 18:30)

	消基會指稱不合格項目	目前狀態	資安強化行動(持續進行)	檢測項目編號
	行動應用程式應於蒐集敏感性資料前取得使用者同意	雙重第三方驗證通過	**【2026/03/17】雙平台同時通過兩間第三方實驗室檢測通過** 【2026/03/03】完成使用者同意流程優化，完成使用服務前即可清楚了解相關條款與資料使用方式 調整為於蒐集敏感性資料前即完成明確告知與同意程序，強化資訊揭露透明度與流程完整性。 同時新增《行動裝置資源存取說明》，進一步說明 App 使用裝置權限之情境與目的。 上述優化將隨後續版本更新正式上線。 【2026/02/14】完成《隱私權政策》《個人資料使用授權說明》指引更新，並部署至正式線上環境 未來將持續強化資安防範，包含 (1)敏感資料： 儲存前取得同意、儲存內容加密保護。 (2)交易安全： 執行交易時強制身分鑑別。 (3)防護機制： 具備畫面擷取（截圖）警示功能。 (4)系統層級： 確保 Session ID 亂數規則安全、第三方函式庫引用安全。	4.1.2.1.1
	行動應用程式應於儲存敏感性資料前取得使用者同意	雙重第三方驗證通過		4.1.2.3.1
	行動應用程式函式庫引用安全	雙重第三方驗證通過	**【2026/03/17】雙平台同時通過兩間第三方實驗室檢測通過** 【2026/03/03】已完成行動應用程式第三方函式庫之全面安全盤點與強化作業。 針對 App 所使用之第三方元件與技術套件進行版本確認與風險評估。經檢查，部分套件已有更新版本可供升級，已完成更新至官方最新穩定版本，並同步進行必要之安全修補與風險控管。相關調整將隨下一版本更新正式發布。 同時，為強化第三方套件之生命週期管理與弱點控管能力，我們已建立持續性管理機制，包括： (1)定期盤點第三方函式庫版本 (2)持續追蹤國際公開漏洞資訊（CVE） (3)依風險等級即時進行更新與安全強化	4.1.5.3.1
	行動應用程式應避免在 IPC 機制中洩漏敏感性資料	雙重第三方驗證通過	**【2026/03/17】雙平台同時通過兩間第三方實驗室檢測通過** 【2026/03/03】完成 IPC 機制安全強化調整說明 針對行動應用程式 IPC 機制之安全性要求，已完成相關元件設定盤點與風險控管作業。將併入下一版本更新正式發布。 本次強化措施包括： (1) 收斂不必要對外暴露之應用元件存取權限 (2) 調整元件匯出設定，避免非授權應用程式存取 (3) 補充各元件功能用途說明與對應防護措施	4.1.2.3.12
	敏感性資料應避免出現於行動應用程式之程式碼	雙重第三方驗證通過	**【2026/03/03】雙平台同時通過兩間第三方實驗室檢測通過** 【2026/02/16】Android 與 iOS 最新版本 v4.13.1 已正式上架至應用程式商店 1.查證結果：報告提到的 API Key 為研發測試用參數 2.是否影響用戶？ 不會，報告提到的 API Key 為研發測試用參數僅存在公司內部封閉測試環境，未用於正式 App／正式系統 3.安全控管：權限嚴格限縮並留存稽核紀錄，避免誤用或外流 4.後續措施：已完成測試參數盤點與加嚴管理，管理制度會持續清理非必要測試設定	4.1.2.3.8
	行動應用程式應於交易收款時主動通知使用者	雙重第三方驗證完成	**【2026/03/03】經雙實驗室檢測，智生活 App 未提供收款功能，僅有付款功能，判定不適用此檢測項目。** 【2026/02/14】已完成版本更新，並部署至正式線上環境 為提升交易資訊透明度與使用者體驗，並確保使用者能即時掌握交易狀態與明細內容，我們仍進行相關功能強化，包括： (1) 新增「付款成功即時提示」機制，於交易完成頁面明確顯示付款成功訊息，並同步揭露交易時間、交易品項及交易金額等資訊。 (2) 於付款前增加交易資訊確認機制，確保使用者可再次檢視最終交易內容。 (3) 強化「訂單明細查詢」功能，交易完成後可即時查閱訂單內容與完整交易資訊。	4.1.3.1.3
	行動應用程式應避免在關閉及登出後將敏感性資料儲存於冗餘檔案或日誌檔案中	雙重第三方驗證通過	**【2026/03/03】雙平台同時通過兩間第三方實驗室檢測通過** L3 等級檢測係依 4.1.2.3.5 條款進行驗證，相關檢測與改善作業均依適用規範辦理並完成驗證。 4.1.2.3.4 為其他分級適用條款。我們亦參酌相關條款精神，針對登出與關閉情境進行資料清理與風險盤點，以強化敏感資料管理機制。	4.1.2.3.4
	行動應用程式敏感性資料分享權限控管	雙重第三方驗證通過	**【2026/03/03】雙平台同時通過兩間第三方實驗室檢測通過** 經全面盤點，確認部分早期導入之輔助模組在「資料暫存管理」上仍有可再強化之處 1.已完成改善：相關套件已升級至新版，並同步調整裝置端資料儲存與清除邏輯，提升敏感資料保護強度、降低潛在風險 2.驗證現況：依既有資安監控與檢測紀錄，目前未發現敏感資訊外洩情形 未來將透過版本管理與定期檢測機制，持續強化行動應用程式在資料存取與暫存管理上的安全性	4.1.2.5.3
	行動應用程式應針對螢幕覆蓋攻擊進行防護（只適用 Android)	雙重第三方驗證通過	**【2026/03/03】雙平台同時通過兩間第三方實驗室檢測通過** 【2026/02/16】Android 與 iOS 最新版本 v4.13.1 已正式上架至應用程式商店 鑑於 Android 平台可能存在螢幕覆蓋（Overlay）攻擊風險，為避免惡意應用程式透過畫面覆蓋干擾使用者操作或誘導誤觸，已啟動相關風險強化措施。 優化方向：於不影響正常使用體驗之前提下，強化 Android 端整體應用程式之覆蓋攻擊防護機制，包括： (1) 啟用應用程式全域防覆蓋機制，避免畫面遭第三方應用程式覆蓋顯示 (2) 偵測異常覆蓋情境時限制互動操作並進行風險提示 (3) 完成相關弱點掃描與情境測試驗證	4.1.5.1.3
	行動應用程式應於發布時說明欲存取之敏感性資料、資源與用途	雙重第三方驗證通過	**【2026/03/24】雙平台通過第三方實驗室檢測** 【2026/03/03】完成使用者同意流程優化，完成使用服務前即可清楚了解相關條款與資料使用方式 調整為於蒐集敏感性資料前即完成明確告知與同意程序，強化資訊揭露透明度與流程完整性。 同時新增《行動裝置資源存取說明》，進一步說明 App 使用裝置權限之情境與目的。 上述優化將隨後續版本更新正式上線。	4.1.1.1.2
New!	行動應用程式冗餘檔案或日誌檔案敏感性資料儲存限制	雙重第三方驗證通過	**【2026/03/24】雙平台通過第三方實驗室檢測** 【2026/03/03】完成裝置端資料暫存機制優化調整，強化暫存資料清理與生命週期管理。 【2026/02/16】Android 與 iOS 最新版本 v4.13.1 已正式上架至應用程式商店 1.盤點結果：經全面盤點，確認部分早期導入之輔助模組在「資料暫存管理」上仍有可再強化之處 2.已完成改善：相關套件已升級至新版，並同步調整裝置端資料儲存與清除邏輯，提升敏感資料保護強度、降低潛在風險 3.驗證現況：依既有資安監控與檢測紀錄，目前未發現敏感資訊外洩情形 4.持續強化：未來將透過版本管理與定期檢測機制，持續強化行動應用程式在資料存取與暫存管理上的安全性	4.1.2.3.5
	行動應用程式敏感性資料儲存保護	雙重第三方驗證通過		4.1.2.3.6
	行動應用程式中的使用者介面應避免洩漏敏感性資料	雙重第三方驗證通過	**【2026/03/24】雙平台通過第三方實驗室檢測** 【2026/03/03】完成使用者同意流程優化，完成使用服務前即可清楚了解相關條款與資料使用方式 【2026/02/14】已完成版本更新，並部署至正式線上環境 1. 關於訂單頁面顯示姓名與電話一事 (1) 設計目的：讓用戶在付款前可核對配送與聯絡資訊，保障交易確認與消費者權益 (2) 必要性考量：避免因資訊遮蔽導致聯絡資料錯誤、配送失敗或後續交易爭議 (3) 揭露原則：僅在最小必要範圍內顯示本次訂單所需資訊，並搭配權限與存取控管，降低不當使用風險 (4) 制度與告知：導入 ISO 27701 隱私資訊管理制度時，已同步修訂《隱私權政策》，並於相關條款說明交易/配送情境下的資料使用目的與範圍，確保透明與用戶知情 2. 關於支付資訊顯示一事 (1) 原因說明：信用卡資訊顯示疑慮，經查係第三方金流回傳資料的遮蔽格式未即時同步，導致前端顯示未達保護標準 (2) 已完成修正：已於 2026/02/12 21:00 完成 WebView 前端遮蔽機制優化 (3) 修正方式：前端介面改為獨立執行遮蔽（masking），已調整信用卡資訊顯示方式，僅保留卡號後四碼供識別使用，其餘資訊將進行遮蔽處理，確保敏感財務欄位於顯示層即受保護 (4) 防護效果：任何敏感財務資訊不會在使用者介面上完整呈現，降低資訊暴露風險 即使資料來源為第三方回傳，我們仍以平台端顯示層保護為責任邊界，已加嚴防護以避免類似情況再次發生	4.1.2.3.13
	行動應用程式應於使用交易資源時進行使用者身分鑑別	雙重第三方驗證通過	**【2026/03/24】雙平台通過第三方實驗室檢測** 【2026/03/03】交易身分鑑別機制強化 現行交易機制已具備既有安全控管措施。為進一步提升交易安全性與使用者身分確認強度，我們正規劃新增交易驗證機制，於使用已綁定信用卡進行交易時，導入額外身分確認程序（如交易密碼驗證），強化每筆交易之使用者鑑別。 本項強化措施係屬風險防護層級提升，目的在於增進交易安全保障與使用者權益保護。 相關優化將於完成測試與驗證後併入後續版本更新。	4.1.3.2.1
New!	行動應用程式畫面擷取警示	雙重第三方驗證通過	**【2026/03/24】雙平台通過一間第三方實驗室檢測** 【2026/03/03】完成雙平台全面導入畫面擷取提醒機制 當使用者於 App 內進行截圖時，系統將即時提示，提醒使用者留意畫面中可能包含之個人資料或敏感資訊，進一步提升用戶資料保護透明度與使用安全性。將併入下一版本更新正式發布。 【2026/02/16】Android 與 iOS 最新版本 v4.13.1 已正式上架至應用程式商店 完成截圖阻擋頁面，[個人頁、訂單詳情、服務聯絡資訊、服務常用收件人]更新	4.1.2.3.9
New!	行動應用程式應避免使用具有規則性之交談識別碼	雙重第三方驗證通過	**【2026/03/24】雙平台通過一間第三方實驗室檢測** 【2026/03/03】交談識別碼安全強化說明 為提升行動應用程式交談識別碼（Session ID）之安全控管強度，我們已完成相關存取機制優化調整。 本次強化重點包括： (1) 優化 API 存取憑證有效期限設定 (2) 強化逾時失效與重新驗證機制 透過上述調整，可進一步降低識別碼遭重複利用或未授權存取之風險，強化整體系統層級安全防護能力。 相關優化已完成驗證，並將隨後續版本更新正式上線。	4.1.4.2.1

資安是一項持續精進的工程，後續我們將持續推進下列工作
•外部稽核 × 內部監控並行：啟動「雙重公正第三方驗證」，並委請第二家公正專業機構進行交叉檢視與比對。
•落實國際標準：依ISO 27001 、 ISO 27701 隱私資訊管理系統，持續強化個資治理、流程控管與透明揭露。
•零信任思維：強化最小權限、分層防護與持續監測為原則，提升高風險路徑的控管強度。
我們將以可驗證的改善與定期檢測機制，持續提供用戶更安全、可信賴的數位服務環境。

備註：
1.ISO 27001 資訊安全管理制度 (ISMS)：通過國際標準認證，認證機構為台灣德國萊因技術監護顧問股份有限公司 (TÜV Rheinland)。
2.ISO 27701 隱私資訊管理制度 (PIMS)：通過國際標準認證，認證機構為台灣德國萊因技術監護顧問股份有限公司 (TÜV Rheinland)。
3.支付安全合規：信用卡交易全程經由符合 PCI DSS 最高合規標準之第三方金流服務商 TapPay 進行技術串接，並由聯合信用卡處理中心 (NCCC) 執行收單作業，確保交易環境安全無虞。