附錄：檢測實驗室 APP 檢測報告自我檢核表參考範例

依據：依行動應用資安聯盟113年9月5日行動應用 App 基本資安檢測基準 V4.0

L1檢測項：25項，L2檢測項：31項，L3檢測項：39項，F 檢測項：9項。

F 類檢測為加測項目，視送檢單位之需求自行選擇是否加測。

本表使用符號說明：「★」表示檢測項目；「－」表示參考項目。

檢測項目	編號	資訊安全技術要求事項	技術要求	各類型行動應用程式必要符合檢測項目			
				L1	L2	L3	F
4.1.1 行動應用程式發布安全	1	4.1.1.1.行動應用程式發布	4.1.1.1.2.行動應用程式應於發布時說明欲存取之安全敏感性資料、行動裝置資源及宣告之權限用途。	★	★	★	－
4.1.1 行動應用程式發布安全	2	4.1.1.1.行動應用程式發布	4.1.1.1.3行動應用程式應於顯著位置(如官網、應用程式下載頁面等)提示使用者於行動應用裝置上安裝防護軟體。	－	－	－	★
4.1.1 行動應用程式發布安全	3	4.1.1.3.行動應用程式安全性問題回報	4.1.1.3.1.行動應用 APP 開發者應提供回報安全性問題之管道。	－	★	★	－
4.1.2. 敏感性資料保護	4	4.1.2.1.敏感性資料蒐集	4.1.2.1.1.行動應用程式應於蒐集敏感性資料前，取得使用者同意。	★	★	★	－
4.1.2. 敏感性資料保護	5	4.1.2.1.敏感性資料蒐集	4.1.2.1.2.行動應用程式應提供使用者拒絕蒐集敏感性資料之權利。	★	★	★	－
4.1.2. 敏感性資料保護	6	4.1.2.2敏感性資料利用	4.1.2.2.3.行動應用程式如採用密碼認證，應主動提醒使用者設定較複雜之密碼。	－	－	－	★
4.1.2. 敏感性資料	7	4.1.2.2敏感性資料利用	4.1.2.2.4.行動應用程式應提醒使用者定期更	－	－	－	★

檢測項目	編號	資訊安全技術要求事項	技術要求	各類型行動應用程式必要符合檢測項目			
				L1	L2	L3	F
保護			改密碼。				
4.1.2. 敏感性資料保護	8	4.1.2.3.敏感性資料儲存	4.1.2.3.1.行動應用程式應於儲存敏感性資料前，取得使用者同意。	★	★	★	—
4.1.2. 敏感性資料保護	9	4.1.2.3.敏感性資料儲存	4.1.2.3.2.行動應用程式應提供使用者拒絕儲存敏感性資料之權利。	★	★	★	—
4.1.2. 敏感性資料保護	10	4.1.2.3.敏感性資料儲存	4.1.2.3.4.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。	★	★	—	—
4.1.2. 敏感性資料保護	11	4.1.2.3.敏感性資料儲存	4.1.2.3.5.行動應用程式應避免將敏感性資料儲存於冗餘檔案或日誌檔案中。	—	—	★	—
4.1.2. 敏感性資料保護	12	4.1.2.3.敏感性資料儲存	4.1.2.3.6.敏感性資料應採用適當且有效之金鑰長度與加密演算法，進行加密處理再儲存。	★	★	★	—
4.1.2. 敏感性資料保護	13	4.1.2.3.敏感性資料儲存	4.1.2.3.7.敏感性資料應儲存於受作業系統保護之區域，以防止其他應用程式未經授權之存取。	★	★	★	—
4.1.2. 敏感性資料保護	14	4.1.2.3.敏感性資料儲存	4.1.2.3.8.敏感性資料應避免出現於行動應用程式之程式碼。	★	★	★	—
4.1.2. 敏感性資料保護	15	4.1.2.3.敏感性資料儲存	4.1.2.3.9.行動應用程式於非使用者主動進行的畫面擷取時應主動警示使用者。	—	—	★	—

檢測項目	編號	資訊安全技術要求事項	技術要求	各類型行動應用程式必要符合檢測項目			
				L1	L2	L3	F
4.1.2. 敏感性資料保護	16	4.1.2.3.敏感性資料儲存	4.1.2.3.10.行動應用程式應將個人可識別資訊、使用者憑證及加密金鑰等敏感性資料儲存於系統憑證儲存設施。	–	–	–	★
4.1.2. 敏感性資料保護	17	4.1.2.3.敏感性資料儲存	4.1.2.3.11.行動應用程式應於使用者輸入敏感性資料時將鍵盤的快取機制關閉。	–	★	★	–
4.1.2. 敏感性資料保護	18	4.1.2.3.敏感性資料儲存	4.1.2.3.12.行動應用程式應避免在 IPC 機制中洩漏敏感性資料。	★	★	★	–
4.1.2. 敏感性資料保護	19	4.1.2.3.敏感性資料儲存	4.1.2.3.13.行動應用程式中的使用者介面應避免洩漏敏感性資料。	–	★	★	–
4.1.2. 敏感性資料保護	20	4.1.2.3.敏感性資料儲存	4.1.2.3.14.行動裝置作業系統的備份資料中不應存有行動應用程式的敏感性資料。	–	–	★	–
4.1.2. 敏感性資料保護	21	4.1.2.3.敏感性資料儲存	4.1.2.3.16.行動應用程式應避免將敏感性資料儲存或輸出於系統日誌。	★	★	★	—
4.1.2. 敏感性資料保護	22	4.1.2.4.資料傳輸安全	4.1.2.4.1.行動應用程式透過網路傳輸資料，應使用適當且有效之金鑰長度與加密演算法進行安全加密。	★	★	★	–
4.1.2. 敏感性資料保護	23	4.1.2.5.敏感性資料分享	4.1.2.5.1.行動裝置內之不同行動應用程式間，應於分享敏感性資料前，取得使用者同意。	★	★	★	–

檢測項目	編號	資訊安全技術要求事項	技術要求	各類型行動應用程式必要符合檢測項目			
				L1	L2	L3	F
4.1.2. 敏感性資料保護	24	4.1.2.5.敏感性資料分享	4.1.2.5.2.行動應用程式應提供使用者拒絕分享敏感性資料之權利。	★	★	★	–
4.1.2. 敏感性資料保護	25	4.1.2.5.敏感性資料分享	4.1.2.5.3.行動應用程式分享敏感性資料時，應避免未授權之行動應用程式存取。	★	★	★	–
4.1.3.交易資源控管安全	26	4.1.3.1.交易資源使用	4.1.3.1.1.行動應用程式應於使用交易資源時主動通知使用者。	–	–	★	–
4.1.3.交易資源控管安全	27	4.1.3.1.交易資源使用	4.1.3.1.2.行動應用程式應提供使用者拒絕使用交易資源之權利。	–	–	★	–
4.1.3.交易資源控管安全	28	4.1.3.1.交易資源使用	4.1.3.1.3. 行動應用程式應於交易收款時主動通知使用者。	—	—	★	
4.1.3.交易資源控管安全	29	4.1.3.2.交易資源控管	4.1.3.2.1.行動應用程式應於使用交易資源時進行使用者身分鑑別。	–	–	★	–
4.1.3.交易資源控管安全	30	4.1.3.2.交易資源控管	4.1.3.2.2.行動應用程式應提供使用交易資源之交易記錄。	–	–	★	–
4.1.3.交易資源控管安全	31	4.1.3.2.交易資源控管	4.1.3.2.3.行動應用程式應提供預授權交易之記錄。	—	—	★	—
4.1.4.行動應用程式使用者身分鑑別、授權與連線管理安全	32	4.1.4.1.使用者身分鑑別與授權	4.1.4.1.1.行動應用程式應有適當之身分鑑別機制，確認使用者身分。	–	★	★	–

檢測項目	編號	資訊安全技術要求事項	技術要求	各類型行動應用程式必要符合檢測項目			
				L1	L2	L3	F
4.1.4.行動應用程式使用者身分鑑別、授權與連線管理安全	33	4.1.4.1.使用者身分鑑別與授權	4.1.4.1.2.行動應用程式應依使用者身分授權。	–	★	★	–
4.1.4.行動應用程式使用者身分鑑別、授權與連線管理安全	34	4.1.4.2.連線管理機制	4.1.4.2.1.行動應用程式應避免使用具有規則性之交談識別碼。	–	★	★	–
4.1.4.行動應用程式使用者身分鑑別、授權與連線管理安全	35	4.1.4.2.連線管理機制	4.1.4.2.2.行動應用程式應確認伺服器憑證之有效性。	★	★	★	–
4.1.4.行動應用程式使用者身分鑑別、授權與連線管理安全	36	4.1.4.2.連線管理機制	4.1.4.2.3.行動應用程式應確認伺服器憑證為可信任之憑證機構所簽發。	★	★	★	–
4.1.4.行動應用程式使用者身分鑑別、授權與連線管理安全	37	4.1.4.2.連線管理機制	4.1.4.2.4.行動應用程式封包流向應與所宣告的內容一致。	★	★	★	—
4.1.5.行動應用程	38	4.1.5.1.防範惡意程式碼	4.1.5.1.1.行動應用程式應避免含有惡意程式	★	★	★	–

檢測項目	編號	資訊安全技術要求事項	技術要求	各類型行動應用程式必要符合檢測項目			
				L1	L2	L3	F
式碼安全		與避免資訊安全漏洞	碼。				
4.1.5.行動應用程式碼安全	39	4.1.5.1.防範惡意程式碼與避免資訊安全漏洞	4.1.5.1.2.行動應用程式應避免資訊安全漏洞。	★	★	★	–
4.1.5.行動應用程式碼安全	40	4.1.5.1.防範惡意程式碼與避免資訊安全漏洞	4.1.5.1.3.行動應用程式應針對螢幕覆蓋攻擊進行防護。	★	★	★	—
4.1.5.行動應用程式碼安全	41	4.1.5.3.函式庫引用安全	4.1.5.3.1.行動應用程式於引用之函式庫有更新時，應備妥對應之更版本，更新方式請參酌 4.1.1.行動應用程式發布安全。	★	★	★	–
4.1.5.行動應用程式碼安全	42	4.1.5.4.使用者輸入驗證	4.1.5.4.1.行動應用程式應針對使用者於輸入階段之字串，進行安全檢查。	★	★	★	–
4.1.5.行動應用程式碼安全	43	4.1.5.4.使用者輸入驗證	4.1.5.4.2.行動應用程式應提供相關注入攻擊防護機制。	★	★	★	–
4.1.5.行動應用程式碼安全	44	4.1.5.5.防止動態分析及竄改	4.1.5.5.1.行動應用程式須偵測行動作業系統保護層是否有被破解(如：Root、Jailbreak)或保護不當之情形，如有，應主動通知使用者或關閉應用程式。	–	–	–	★
4.1.5.行動應用程式碼安全	45	4.1.5.5.防止動態分析及竄改	4.1.5.5.6.行動應用程式應有程式碼混淆機制。	–	–	–	★
4.1.5.行動應用程式碼安全	46	4.1.5.5.防止動態分析及竄改	4.1.5.5.7.行動應用程式須偵測當前的執行環境是否為模擬器。	—	—	—	★
4.1.5.行動應用程式碼安全	47	4.1.5.5.防止動態分析及竄改	4.1.5.5.8.行動應用程式須偵測行動裝置是否開啟 USB 偵錯模式。	—	—	—	★

檢測項目	編號	資訊安全技術要求事項	技術要求	各類型行動應用程式必要符合檢測項目			
				L1	L2	L3	F
4.1.5.行動應用程式碼安全	48	4.1.5.5.防止動態分析及竄改	4.1.5.5.9.行動應用程式應將偵錯模式(Debug mode)設為關閉。	—	—	—	★
4.2.2 伺服器端安全檢測	49	4.2.2.1.Webview 安全檢測	4.2.2.1.2.行動應用程式於 Webview 呈現功能時，所連線之網域應執行安全檢測。	★	★	★	–

填寫人：_____ 單位主管：