行動應用APP基本資安檢測基準V4.0基準修改對照

孫宏民教授

資訊安全實驗室

國立清華大學資訊工程系

Outline

- 基準V4.0與V3.2修改對照

標準詳細修改內容比較表

行動應用App基本資安檢測基準 V3.2	行動應用App基本資安檢測基準 V4.0 （ NEW Version. ）

修改目錄

- 補上”系統日誌”

修改目錄

- ”多工模式”修改為”螢幕背景模式”

基本資安檢測基準

- 僅供開發者參考，非實際執行檢測之項目。↵

參考項目詳見「附錄五、 行動應用 App 基本資安參考項目」。↵

「行動應用 App 基本資安規範」及「基本資安檢測基準」為針對行動應用程式之功能分類，訂定各類別之安全要求範圍，分為三類以及一類加測類別：↵

L1：無須使用者身分鑑別之行動應用程式，須檢測之項目共 23 項。↵

L2：須使用者身分鑑別之行動應用程式，須檢測之項目共 29 項。↵

L3：含有交易行為之行動應用程式，須檢測之項目共 35 項。↵

F:屬於安全性需求較高之行動應用程式，為加測項目，須檢測之項目共 6 項。↵

- 僅供開發者參考，非實際執行檢測之項目。↵

參考項目詳見「附錄五、 行動應用 App 基本資安參考項目」。↵

「行動應用 App 基本資安規範」及「基本資安檢測基準」為針對行動應用程式之功能分類，訂定各類別之安全要求範圍，分為三類以及一類加測類別：↵

L1：無須使用者身分鑑別之行動應用程式，須檢測之項目共 25 項。↵

L2：須使用者身分鑑別之行動應用程式，須檢測之項目共 31 項。↵

L3：含有交易行為之行動應用程式，須檢測之項目共 39 項。↵

F ：屬於安全性需求較高之行動應用程式，為加測項目，須檢測之項目共 9 項。↵

- 增加L1, L2, L3, 檢測項目

前言修改

為協助行動應用程式開發者妥適遵循「行動應用 App 基本資安規範」，維護行動應用程式之安全開發品質，經濟部工業局專案委託財團法人資訊工業策進會並協同中華民國資訊安全學會為執行單位，於民國 107 年 8 月修訂「行動應用 App 基本資安檢測基準 V3.0」，民國 108 年 09 月更新修訂「行動應用 App 基本資安檢測基準 V3.1」，並於民國 111 年 01 月由台北市電腦公會為執行單位，更新修訂「行動應用 App 基本資安檢測基準 V3.2」（下稱本檢測基準），以測試並確保行動應用程式之安全性。本檢測基準主要依據「行動應用 App 基本資安規範」之行動應用程式分類，並參考 OWASP（開放 Web 軟體安全計畫）「Mobile Security Testing Guide」中 OWASP Mobile Application Security Verification Standard 1.2 版本、CSA MAST「Cloud Security Alliance - Mobile Application Security Testing」及 NIST（美國國家標準技術研究所）「Special Publication 800-163 Vetting the Security of Mobile Applications」，針對行動應用程式安全風險評估與審驗，訂定基本資安檢測項目、依檢測項目所須檢測之各項檢查事項、預期之檢測結果及各結果之形成條件等。

為協助行動應用 App 開發者妥適遵循「行動應用 App 基本資安規範」，維護行動應用程式之安全開發品質，經濟部工業局(民國 111 年數位發展部數位產業署承接)專案委託財團法人資訊工業策進會並協同中華民國資訊安全學會為執行單位，於民國 107 年 8 月修訂「行動應用 App 基本資安檢測基準 V3.0」，民國 108 年 09 月更新修訂「行動應用 App 基本資安檢測基準 V3.1」，民國 111 年 01 月更新修訂「行動應用 App 基本資安檢測基準 V3.2」，民國 113 年 03 月由台北市電腦公會為執行單位，更新修訂「行動應用 App 基本資安檢測基準 V4.0」（下稱本檢測基準）以測試並確保行動應用程式之安全性。本檢測基準主要依據「行動應用 App 基本資安規範」之行動應用程式分類，並參考 OWASP（開放 Web 軟體安全計畫）「Mobile Application Security Testing Guide（MASTG） V1.7.0」、「Mobile Application Security Verification Standard（MASVS）V2.0」、CSA MAST「Cloud Security Alliance - Mobile Application Security Testing」及 NIST（美國國家標準技術研究所）「Special Publication 800-163 Vetting the Security of Mobile Applications」，針對行動應用程式安全風險評估與審驗，訂定基本資安檢測項目、依檢測項目所須檢測之各項檢查事項、預期之檢測結果及各結果之形成條件等。

更新修訂日期及參考之OWASP MASTG、MASVS版本

3.3 個人資料

3.3. 個人資料（Personal Data）↵

指主要依「個人資料保護法」上定義之所有得以直接或間接方式識別該個人之資料，包括但不限於自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、帳戶餘額、社會活動。↵

3.3. 個人資料（Personal Data）↵

指主要依「個人資料保護法」上定義之所有得以直接或間接方式識別該個人之資料，包括但不限於自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動。↵

修改定義（刪除帳戶餘額）

3.4 敏感性資料

3.4. –敏感性資料（Sensitive Data）

指依使用者行為或行動應用程式之運作，於行動裝置及其附屬儲存媒介建立、儲存或傳輸之資訊，其中對個人隱私資料之存取便屬於蒐集、儲存於本地空間內即屬儲存，而該資訊之洩漏有對使用者造成損害之虞，除包括 3.3 內定義之個人資料之外，並包括但不限於~~通行碼~~密碼、金鑰、視訊、照片、通話、錄音檔、即時通訊訊息、通話~~紀錄~~記錄、簡訊、備忘錄、通訊錄、筆記、地理位置、行事曆及裝置識別符等有關個人隱私之資料。

修改定義

3.5 密碼

3.5. 通行碼（Password）↵

指一組能讓使用者使用系統或用以識別使用者身分之字元串，包括本機儲存資料加密檔案密碼、自身帳號及密碼、遠端網路服務帳號及密碼。↵

3.5. 密碼（Password）↵

指一組能讓使用者使用系統或用以識別使用者身分之字元串。

通行碼改成密碼、今後所有使用到通行碼之詞彙皆改為密碼

3.6 交易資源

3.6. 交易資源（Transaction Resource）

指透過行動應用程式內所提供購買功能，並可直接或間接取得之額外功能、內容或訂閱項目，凡有牽涉金流者，不論是虛擬或實體貨幣（包含點數或序號）等有價值物品皆視為交易資源。如售票系統 App 內購買票券得到一組 QRcode 可做為票券的憑證；如網路書店 App 內購買電子書得到電子書的內容可供閱讀；如訂閱或訂購 App 內的交易服務項目，於交易後提供新的功能、移除使用限制功能或移除廣告功能等；或繳費網 App 提供繳費功能、銀行類型 App 提供轉帳或 App 提供購買實體或虛擬商品之功能。股票下單等有風險的敏感操作行為亦須為使用者留下紀錄，以保障消費者權益。

3.6. 交易資源（Transaction Resource）

指透過行動應用程式內所提供涉及交易行為之項目，包括但不限於實體貨幣、虛擬貨幣(包含點數或序號)、票券(包含股票)等有價值項目。

修改定義

新增 3.7 交易記錄, 3.8 預授權交易

3.7. 交易記錄（Transaction Record）

指透過行動應用程式進行交易時，與達成交易有關之資料，包含交易對象、交易商品名稱、交易時間、交易金額、支付方式（例如：信用卡、電子支付）及交易狀態（例如：交易完成、交易中、交易取消）。

3.8. 預授權交易（Pre-authorization Transaction）

指使用者事先對應用程式開放特定交易類型的授權，使得在後續符合授權範圍與條件的情況下，交易得自動執行，而無須再次取得使用者同意。此授權須明確界定可執行的交易範疇（如例行性付款、固定金額扣款），且使用者可隨時查看、取消或變更該預授權設定。

新增定義

新增 3.10 JWT, 3.11 生物特徵身份鑑別, 3.12 一次性密碼

3.10. JWT（JSON Web Token）

指一種開放標準（RFC 7519），透過 HMAC、RSA、ECDSA 等演算法進行簽章，經常用於對使用者進行身分驗證，使用者透過 JWT 向資源伺服器請求資源，若該 JWT 為有效，則使用者能獲得相對應的資源。

3.11. 生物特徵身分鑑別（Biometric Authentication）

指使用者透過其身體的生物特徵進行身分認證。生物特徵可以包括指紋、虹膜、臉部、聲紋等。

3.12. 一次性密碼（One Time Password, OTP）

指行動應用裝置或其他數位裝置上只能使用一次的密碼，有效期為單次登錄使用。

新增定義

新增 3.16 網路釣魚，3.17 殭屍網路，3.18 間諜軟體，3.19 下載器

3.16. 網路釣魚（Phishing）

此種類型之惡意程式主要是將使用者導入釣魚網站，並且誘導使用者輸入相關資訊，以竊取個人資料。

3.17. 殭屍網路（Botnet）

此種惡意程式可以在行動裝置後台運作，和殭屍控制主機（botmaster）聯繫並執行命令，使用者不易察覺。

3.18. 間諜軟體（Spyware）

此種應用程式會監控和記錄使用者的設備資訊或行為資訊，例如簡訊、電子郵件、電話記錄、聯絡人、地理位置等訊息，並分享給遠端的伺服器。

3.19. 下載器（Downloader）

此種應用程式自身並非惡意程式，但會隱身於 APP 中，負責下載其他的惡意程式到使用者行動裝置中。

新增定義

新增 3.21 螢幕覆蓋攻擊

3.21. 螢幕覆蓋攻擊（Screen Overlay Attack）↵

指攻擊者的應用程式會在行動應用程式上繪製一個視窗，誤導使用者將自己點擊的入侵視窗當作正常視窗。↵

新增定義

新增 3.27 模擬器，3.28 USB 偵錯模式，3.29 偵錯模式

3.27. 模擬器（Emulator）

指在電腦或是其他非行動裝置之設備上，模擬行動裝置之執行環境，用於在非行動裝置上執行行動應用程式。

3.28. USB 偵錯模式（USB Debugging Mode）

指在 Android 行動裝置可啟用的一個功能，可讓 Android 行動裝置與運行 Android SDK 的電腦進行通訊，目的為方便開發人員透過 USB 連線到 Android 行動裝置，並對行動應用程式進行偵錯或測試。

3.29. 偵錯模式（Debug Mode）

指一種在行動應用程式的開發模式，提供額外的偵錯功能，方便開發者對該行動應用程式進行偵錯。

新增定義

新增 3.31 常見弱點列舉

3.31. 常見弱點列舉（Common Weakness Enumeration）↵

簡稱「CWE」，由美國國土安全部網路與基礎設施安全局所贊助，由非營利的研發機構 MITRE 負責管理的弱點列表。這些弱點列表提供評估軟體安全的共通語言，羅列各種軟體弱點、識別方法、緩解與預防工作的知識。↵

新增定義

新增 3.33 身分鑑別

3.19. 身分鑑別（Authentication）

指對個體所宣稱之身分提供保證。

3.33. 身分鑑別（Authentication）↵

指對個體所宣稱之身分提供證明。↵

修改定義

新增 3.34 ChaCha20加密演算法

3.34. ChaCha20 加密演算法↵

指一種串流加密算法，由丹麥計算機科學家 Daniel J. Bernstein 於 2008 年開發，使用一個 128 位的密鑰和一個 64 位的初始向量（IV）作為輸入，並生成一個 256 位的密鑰流（Keystream）。然後，將密鑰流與明文數據進行 XOR 運算。↵

新增定義

3.37 橢圓曲線加密演算法

3.22. 橢圓曲線密碼學（Elliptic Curve Cryptography）↵

指一種建立公開金鑰加密的演算法，基於橢圓曲線所生成之加法群或數學結構。橢圓曲線在密碼學中的使用是在 1985 年由 Neal Koblitz 和 Victor Miller 分別獨立提出的。↵

3.37. 橢圓曲線加密演算法（Elliptic Curve Cryptography）↵

指一種建立公開金鑰加密的演算法，基於橢圓曲線所生成之加法群或數學結構。橢圓曲線在密碼學中的使用是在 1985 年由 Neal Koblitz 和 Victor Miller 分別獨立提出的。↵

修改定義標題

新增 3.41 加殼

3.41. 加殼（Packing）

指將行動應用程式原始碼進行加密，並在行動應用程式執行期間進行解密的技術，目的是防止攻擊者利用逆向工程技術獲得行動應用程式的原始碼。

新增定義

新增 3.43 日誌檔案

3.43. 日誌檔案（Log File）↵

僅供於進行除錯使用之應用程序日誌、安全日誌、除錯日誌或自定義日誌檔。↵

新增定義

新增 3.44 系統日誌

3.44. 系統日誌（System Logs）↵

指作業系統記錄各種事件、錯誤、警告等的日誌文件，用於開發者除錯應用程式、分析系統崩潰問題、以及系統維護。↵

新增定義

新增 3.45 裝置識別符

3.45. 裝置識別符 （Device Identifier）

指硬體或軟體之唯一識別資訊，包括國際行動設備識別碼（International Mobile Equipment Identity, IMEI）、行動設備識別碼（Mobile Equipment Identifier, MEID）、國際行動用戶識別碼（International Mobile Subscriber Identity, IMSI）、積體電路卡識別碼（Integrated Circuit Card Identifier, ICCID）、媒體存取控制位址（Media Access Control Address, MAC Address）、安卓系統識別碼（Android Identifier, Android ID）、安卓系統廣告識別碼（Android Advertising ID, AID）、iOS IFAID（Identifier for Advertisers Identifier, IFAID）及 Windows Phone Device ID。

3.45. 裝置識別符（Device Identifier）

指硬體或軟體之唯一識別資訊，包括國際行動設備識別碼（International Mobile Equipment Identity, IMEI）、行動設備識別碼（Mobile Equipment Identifier, MEID）、國際行動用戶識別碼（International Mobile Subscriber Identity, IMSI）、積體電路卡識別碼（Integrated Circuit Card Identifier, ICCID）、媒體存取控制位址（Media Access Control Address, MAC Address）、安卓系統識別碼（Android Identifier, Android ID）、安卓系統廣告識別碼（Android Advertising ID, AAID）、iOS IDFA（Identifier for Advertisers, IDFA）及 Windows Phone Device ID。

修正縮寫

新增 3.48 處理間通信

3.48. 處理間通信（Inter-Process Communication）↵

簡稱「IPC」，是不同的程序之間的通訊機制，允許不同的程序之間進行資訊交換，以實現共享資源的目的。↵

新增定義

3.55 安全亂數產生函式

3.37. 安全亂數產生函式 (Secure Random Number Generator)↵

符合或引用 ANSI X9.17、FIPS 140-2、NIST SP 800-22 以及 SP 800-90A (CAVP Testing: Random Number Generators) 至少其中一項標準之亂數產生函式。↵

3.55. 安全亂數產生函式（Secure Random Number Generator）↵

符合或引用 ANSI X9.17、FIPS 140-3、NIST SP 800-22 及 SP 800-90A (CAVP Testing: Random Number Generators) 至少其中一項標準之亂數產生函式。↵

修改定義

3.56 安全網域

3.38. 安全網域 (Secure Domain)↵

範圍包括開發商、客戶所屬網域或一般熟知之公共安全網域，一般熟知之公共安全網域包括 Facebook、Google 或 Twitter 等支援 OAuth 2.0 協定之應用。↵

3.56. 安全網域（Secure Domain）↵

一般熟知之公共安全網域包括 Facebook、Google 或 Twitter。

刪除OAuth2.0之敘述

3.57 安全加密函式

3.39. 安全加密函式 (Secure Encryption Function)

符合 FIPS 140-2 Annex A 之加密函式。↵

3.57. 安全加密函式（Secure Encryption Function）↵

符合 FIPS 140-3 SP800-140C 所列舉之加密函式，並且禁止使用三重資料加密演算法。↵

修改定義

3.59 App切換模式（App Switching Mode）

3.59. 多工模式（Multitasking Mode）

指一個行動設備（如智慧手機或平板電腦）的執行模式，其中使用者可以同時預覽多個應用程式。

3.59. App切換模式（App Switching Mode）

指一個行動設備（如智慧手機或平板電腦）的執行模式，其中使用者可以同時預覽多個應用程式。iOS 中稱為 App 切換器（App Switcher），Android 則為「切換畫面與應用程式」功能。

修改定義名稱、定義

檢測項目欄位說明表格

檢測依據	依據「行動應用 App 基本資安規範」之「4.技術要求」及 OWASP「Mobile Security Testing Guide」(MSTG)相對應之行動應用程式資訊安全技術要求事項

檢測依據	依據「行動應用 App 基本資安規範」之「4.技術要求」及 OWASP「Mobile Application Security Verification Standard」(MASVS)相對應之行動應用程式資訊安全技術要求事項

修改檢測依據

所有檢測項檢測依據更新

檢測編號	4.1.1.1.2
檢測項目	行動應用程式發布說明
檢測分類	L1、L2、L3
檢測依據	「行動應用 App 基本資安規範」4.1.1.1 行動應用程式發布、MSTG-PLATFORM-1、MSTG-STORAGE-12
技術要求	行動應用程式應於發布時說明欲存取之敏感性資料、行動裝置資源及宣告之權限用途

檢測編號	4.1.1.1.2
檢測項目	行動應用程式發布說明
檢測分類	L1、L2、L3
檢測依據	「行動應用 App 基本資安規範」4.1.1.1 行動應用程式發布、MASVS-PLATFORM-1、MASVS-PRIVACY-1
技術要求	行動應用程式應於發布時說明欲存取之敏感性資料、行動裝置資源及宣告之權限用途

由MSTG-XXXX修改為MASVS-XXXX

以下檢測依據之內容皆通用

所有檢測結果敘述修改

檢測結果	符合要求：符合所有檢測基準，或行動應用程式未儲存敏感性資料 不符合要求：任一檢測基準不符合，或於檢測基準 4.1.2.3.1 之檢測結果因未聲明欲儲存之所有敏感性資料而不符合 不適用：行動應用程式不公開發布，則此項不須檢測

檢測結果	符合要求：符合所有檢測基準，或行動應用程式未儲存敏感性資料。 不符合要求：不符合任一檢測基準，或於檢測基準 4.1.2.3.1 之檢測結果因未聲明欲儲存之所有敏感性資料而不符合。

任一檢測基準不符合改為不符合任一檢測基準

以下檢測結果之內容通用

檢測項目欄位說明表格下方文字說明

	會上架。 2. 不公開：係指行動應用程式在企業內部使用，不論是否上架。
備註	其他說明事項

所有須「取得使用者同意」之檢測項目，可於信任之行動應用程式商店以「使用者下載安裝使用即視為同意」之聲明方式或行動應用程式至少於第一次執行時，以「主動提供說明及同意與不同意選項」方式，取得使用者同意，當送檢之行動應用程式同時提供上述兩種取得使用者同意之方式時，以行動應用程式內取得使用者同意之方式為檢測判定是否符合之依據。

	b、尚未發布：係指行動應用程式屬於開發階段，未來可能會上架。 2. 不公開：係指行動應用程式在企業內部使用，不論是否上架。
備註	其他說明事項

所有須「取得使用者同意」的檢測項目，皆適用於下列三種應用程式發布狀態：公開發布、尚未發布與不公開發布。

若行動應用程式已發布，檢查行動應用程式所有蒐集之敏感性資料，是否於應用程式商店內聲明，且於行動應用程式內聲明及取得使用者同意。

若行動應用程式尚未發布，檢查調查表內是否有填寫「需要之行動裝置敏感性資料類型(資源、權限)、用途說明、是否儲存於 裝置內以及是否與其他應用分享」並說明將如何取得使用者同 意，且在行動應用程式內聲明及取得使用者同意。

若行動應用程式不公開發布，檢查是否於行動應用程式內聲明及取得使用者同意。

針對「取得使用者同意」詳細說明公開發布、尚未發布與不公開發布等三種應用程式發布狀態

4.1.1

行動應用程式發布安全

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)提示使用者於行動裝置上安裝防護軟體。

檢測編號	4.1.1.1.3
檢測項目	行動應用程式提示資訊
檢測分類	F
檢測依據	「行動應用 App 基本資安規範」4.1.1.1 行動應用程式發布
技術要求	行動應用程式應於顯著位置(如官網、應用程式下載頁面等)提示使用者於行動裝置上安裝防護軟體
檢測基準	若行動應用程式已發布，檢查行動應用程式是否於顯著位置(如官網、應用程式下載頁面或應用程式內等)提示使用者於行動裝置上安裝防護軟體。 若行動應用程式尚未發布，檢查調查表內是否有填寫「提醒安裝防護軟體之聲明內容及預計聲明位置(非尚未發布不須填寫)」，並說明預計提醒位置以及預計提醒內容。 如為「是」則符合檢測基準；「否」則不符合檢測基準
檢測結果	符合要求：符合檢測基準 不符合要求：不符合檢測基準 不適用：行動應用程式不公開發布，則此項不須檢測
備註	無

檢測編號	4.1.1.1.3
檢測項目	行動應用程式提示資訊
檢測分類	F
檢測依據	「行動應用 App 基本資安規範」4.1.1.1 行動應用程式發布
技術要求	行動應用程式應於顯著位置(如官網、應用程式下載頁面等)提示使用者於行動裝置上安裝防護軟體
檢測基準	若行動應用程式已發布，檢查行動應用程式是否於顯著位置(如官網、應用程式下載頁面或應用程式內等)提示使用者於行動裝置上安裝防護軟體。 若行動應用程式尚未發布，檢查調查表內是否有填寫「提醒安裝防護軟體之聲明內容及預計聲明位置已發布不須填寫」，並說明預計提醒位置以及預計提醒內容。 如為「是」則符合檢測基準；「否」則不符合檢測基準
檢測結果	符合要求：符合檢測基準 不符合要求：不符合檢測基準 不適用：行動應用程式不公開發布，則此項不須檢測
備註	無

將非尚未發布改為已發布

4.1.2

敏感性資料保護

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

檢測編號	4.1.2.1.1
檢測項目	行動應用程式敏感性資料蒐集聲明
檢測分類	L1、L2、L3
檢測依據	「行動應用 App 基本資安規範」4.1.2.1.敏感性資料蒐集、MSTG-STORAGE-12、MSTG-PLATFORM-1
技術要求	行動應用程式應於蒐集敏感性資料前，取得使用者同意
檢測基準	若行動應用程式已發布，檢查行動應用程式所有蒐集之敏感性資料，是否於應用程式商店內聲明，或於行動應用程式內聲明及取得使用者同意。 若行動應用程式尚未發布，檢查調查表內是否有填寫「需要之行動裝置敏感性資料類型(資源、權限)、用途說明、是否儲存於裝置內以及是否與其他應用分享」並說明將如何取得使用者同意，或在行動應用程式內聲明及取得使用者同意。 如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準
檢測結果	符合要求：符合檢測基準，或行動應用程式未蒐集敏感性資料 不符合要求：不符合檢測基準 不適用：行動應用程式不公開發布，則此項不須檢測
備註	應用程式商店之宣告以行動裝置之商店介面為主

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

檢測編號	4.1.2.1.1
檢測項目	行動應用程式敏感性資料蒐集聲明
檢測分類	L1、L2、L3
檢測依據	「行動應用 App 基本資安規範」4.1.2.1. 敏感性資料蒐集、MASVS-STORAGE-1、MASVS-PRIVACY-3
技術要求	行動應用程式應於蒐集敏感性資料前，取得使用者同意
檢測基準	若行動應用程式已發布，檢查行動應用程式所有蒐集之敏感性資料，是否於應用程式商店內聲明，且於行動應用程式內聲明及取得使用者同意。 若行動應用程式尚未發布，檢查調查表內是否有填寫「需要之行動裝置敏感性資料類型（資源、權限）、用途說明、是否儲存於裝置內以及是否與其他應用分享」並說明將如何取得使用者同意，且在行動應用程式內聲明及取得使用者同意。 如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。 若行動應用程式不公開發布，檢查是否於行動應用程式內聲明及取得使用者同意。
檢測結果	符合要求：符合檢測基準，或行動應用程式未蒐集敏感性資料。 不符合要求：不符合檢測基準。
備註	應用程式商店之宣告以行動裝置之商店介面為主。

將或改成且，刪除不適用之敘述。補充說明：4.1.2.1.1如果是公開發布要在商城+應用程式內聲明，如果不公開發布則是要在應用程式內聲明，因為一4.1.2.1.1有聲明了，所以4.1.2.1.2不管是否公開發布，都需要讓使用者有拒絕的權利。

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

檢測編號	4.1.2.1.2
檢測項目	行動應用程式提供使用者拒絕敏感性資料蒐集機制
檢測分類	L1、L2、L3
檢測依據	「行動應用 App 基本資安規範」4.1.2.1.敏感性資料蒐集、MSTG-STORAGE-12
技術要求	行動應用程式應提供使用者拒絕蒐集敏感性資料之權利
檢測基準	(1)檢查行動應用程式是否提供使用者拒絕蒐集敏感性資料之功能。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準
	(2)檢查在使用者拒絕敏感性資料蒐集的情況下，行動應用程式是否未檢出蒐集敏感性資料。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準
檢測結果	符合要求：符合所有檢測基準，或行動應用程式未檢出蒐集敏感性資料 不符合要求：任一檢測基準不符合，或於檢測基準 4.1.2.1.1 之檢測結果因未聲明所有敏感性資料而不符合 不適用：行動應用程式不公開發布，則此項不須檢測
備註	於檢測基準 4.1.2.1.1 之檢測結果因未聲明所有敏感性資料，致使使用者無法對未聲明之敏感性資料行使拒絕權利

檢測編號	4.1.2.1.2
檢測項目	行動應用程式提供使用者拒絕敏感性資料蒐集機制
檢測分類	L1、L2、L3
檢測依據	「行動應用 App 基本資安規範」4.1.2.1.敏感性資料蒐集、MASVS-STORAGE-1、MASVS-PRIVACY-4
技術要求	行動應用程式應提供使用者拒絕蒐集敏感性資料之權利
檢測基準	(1)檢查行動應用程式是否提供使用者拒絕蒐集敏感性資料之功能。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。
	(2)檢查在使用者拒絕敏感性資料蒐集的情況下，行動應用程式是否未檢出蒐集敏感性資料。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。
檢測結果	符合要求：符合所有檢測基準，或行動應用程式未檢出蒐集敏感性資料。 不符合要求：不符合任一檢測基準。
備註	於檢測基準 4.1.2.1.1 之檢測結果因未聲明所有敏感性資料，致使使用者無法對未聲明之敏感性資料行使拒絕權利

修改檢測結果之敘述：刪除不適用之敘述，新增不公開之檢測基準

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

4.1.2.2.3. 行動應用程式如採用通行碼認證，應主動提醒使用者設定較複雜之通行碼

檢測編號	4.1.2.2.3
檢測項目	行動應用程式通行碼認證機制
檢測分類	F
檢測依據	「行動應用 App 基本資安規範」4.1.2.2.敏感性資料利用、MSTG-STORAGE-11、MSTG-AUTH-5
技術要求	行動應用程式如採用通行碼認證，應主動提醒使用者設定較複雜之通行碼
檢測基準	(1) 檢查行動應用程式於通行碼設定頁面是否提醒使用者通行碼至少 6 個字元。如為「是」則符合檢測基準，如為「否」不符合檢測基準。 (2) 檢查行動應用程式於通行碼設定頁面是否提醒使用者避免使用個人相關資料做為通行碼。如為「是」則符合檢測基準，如為「否」不符合檢測基準。
檢測結果	符合要求：符合所有檢測基準 不符合要求：任一檢測基準不符合 不適用：行動應用程式未採用任何通行碼機制。
備註	(1)個人相關資料如：身分證字號、帳號、姓名、電子郵件、出生年月日等。 (2)參考 NIST SP800 標準，建議大於等於 8 個字元。

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

檢測編號	4.1.2.2.3
檢測項目	行動應用程式密碼強度認證機制
檢測分類	F
檢測依據	「行動應用 App 基本資安規範」4.1.2.2.敏感性資料利用、NIST SP 800-63B、MASVS-AUTH-2
技術要求	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
檢測基準	(1) 檢查行動應用程式於密碼設定頁面是否提醒使用者密碼至少 8 個字元。如為「是」則符合檢測基準，如為「否」不符合檢測基準。 行動應用程式業者得舉證主管機關相關公文或證明，並依其主管機關之規定作為判定基準。 (2) 檢查行動應用程式於密碼設定頁面是否提醒使用者避免使用個人相關資料做為密碼。如為「是」則符合檢測基準，如為「否」不符合檢測基準。
檢測結果	符合要求：符合所有檢測基準。 不符合要求：不符合任一檢測基準。 不適用：行動應用程式未採用任何密碼機制。
備註	個人相關資料如：身分證字號、帳號、姓名、電子郵件、出生年月日等。

修改通行碼之敘述改為密碼、修改檢測依據、修改檢測基準的密碼長度限制、刪除備註(2)

4.1.2.2.4 行動應用程式應提醒使用者定期更改密碼

4.1.2.2.4. 行動應用程式應提醒使用者定期更改通行碼

檢測編號	4.1.2.2.4
檢測項目	行動應用程式通行碼認證機制
檢測分類	F
檢測依據	「行動應用 App 基本資安規範」4.1.2.2.敏感性資料利用
技術要求	行動應用程式應提醒使用者定期更改通行碼
檢測基準	檢查行動應用程式是否提醒使用者定期更改通行碼，至多不超過 90 天。如為「是」則符合檢測基準，如為「否」不符合檢測基準。
檢測結果	符合要求：符合所有檢測基準 不符合要求：不符合檢測基準 不適用：行動應用程式未採用任何通行碼機制
備註	無

4.1.2.2.4. 行動應用程式應提醒使用者定期更改密碼

檢測編號	4.1.2.2.4
檢測項目	行動應用程式密碼期限認證機制
檢測分類	F
檢測依據	「行動應用 App 基本資安規範」4.1.2.2.敏感性資料利用
技術要求	行動應用程式應提醒使用者定期更改密碼
檢測基準	檢查行動應用程式是否提醒使用者定期更改密碼，至多不超過 90 天。如為「是」則符合檢測基準，如為「否」不符合檢測基準。 行動應用程式業者得舉證主管機關相關公文或證明，並依其主管機關之規定作為判定基準。
檢測結果	符合要求：符合所有檢測基準。 不符合要求：不符合檢測基準。 不適用：行動應用程式未採用任何密碼機制。
備註	無

修改通行碼之敘述改為密碼、修改密碼更改時間之規範

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

檢測編號	4.1.2.3.1
檢測項目	行動應用程式敏感性資料儲存聲明
檢測分類	L1、L2、L3
檢測依據	「行動應用 App 基本資安規範」4.1.2.3.敏感性資料儲存、MSTG-STORAGE-12、MSTG-PLATFORM-1
技術要求	行動應用程式應於儲存敏感性資料前，取得使用者同意
檢測基準	若行動應用程式已發布，檢查行動應用程式所有儲存之敏感性資料，是否於應用程式商店內聲明，或於行動應用程式內聲明及取得使用者同意。 若行動應用程式尚未發布，檢查調查表內是否有填寫「需要之行動裝置敏感性資料類型(資源、權限)、用途說明、是否儲存於裝置內以及是否與其他應用分享」，並說明將如何取得使用者同意，或在行動應用程式內聲明及取得使用者同意。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準
檢測結果	符合要求：符合檢測基準 不符合要求：不符合檢測基準 不適用：行動應用程式不公開發布，則此項不須檢測
備註	應用程式商店之宣告以行動裝置之商店介面為主

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

檢測編號	4.1.2.3.1
檢測項目	行動應用程式敏感性資料儲存聲明
檢測分類	L1、L2、L3
檢測依據	「行動應用 App 基本資安規範」4.1.2.3. 敏感性資料儲存、MASVS-PLATFORM-1、MASVS-STORAGE-1、MASVS-PRIVACY-4
技術要求	行動應用程式應於儲存敏感性資料前，取得使用者同意
檢測基準	若行動應用程式已發布，檢查行動應用程式所有儲存之敏感性資料，是否於應用程式商店內聲明，且於行動應用程式內聲明及取得使用者同意。 若行動應用程式尚未發布，檢查調查表內是否有填寫「需要之行動裝置敏感性資料類型（資源、權限）、用途說明、是否儲存於裝置內以及是否與其他應用分享」，並說明將如何取得使用者同意，且在行動應用程式內聲明及取得使用者同意。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。 若行動應用程式不公開發布，檢查是否於行動應用程式內聲明及取得使用者同意。
檢測結果	符合要求：符合檢測基準，或行動應用程式未儲存敏感性資料。 不符合要求：不符合檢測基準。
備註	應用程式商店之宣告以行動裝置之商店介面為主。

將或改成且、刪除不適用之敘述，新增不公開發布之檢測基準

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

檢測編號	4.1.2.3.2
檢測項目	行動應用程式提供使用者拒絕敏感性資料儲存機制
檢測分類	L1、L2、L3
檢測依據	「行動應用 App 基本資安規範」4.1.2.3.敏感性資料儲存、MSTG-STORAGE-12
技術要求	行動應用程式應提供使用者拒絕儲存敏感性資料之權利
檢測基準	(1)檢查行動應用程式是否提供使用者拒絕儲存敏感性資料之功能。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準
	(2)檢查在使用者拒絕敏感性資料儲存的情況下，行動應用程式是否未儲存敏感性資料於行動裝置。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準
檢測結果	符合要求：符合所有檢測基準，或行動應用程式未儲存敏感性資料 不符合要求：任一檢測基準不符合，或於檢測基準 4.1.2.3.1 之檢測結果因未聲明欲儲存之所有敏感性資料而不符合 不適用：行動應用程式不公開發布，則此項不須檢測
備註	於檢測基準 4.1.2.3.1 之檢測結果因未聲明欲儲存之所有敏感性資料，致使使用者無法對未聲明之敏感性資料行使拒絕權利

檢測編號	4.1.2.3.2
檢測項目	行動應用程式提供使用者拒絕敏感性資料儲存機制
檢測分類	L1、L2、L3
檢測依據	「行動應用 App 基本資安規範」4.1.2.3.敏感性資料儲存、MASVS-STORAGE-1、MASVS-PRIVACY-4
技術要求	行動應用程式應提供使用者拒絕儲存敏感性資料之權利
檢測基準	(1)檢查行動應用程式是否提供使用者拒絕儲存敏感性資料之功能。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。
	(2)檢查在使用者拒絕敏感性資料儲存的情況下，行動應用程式是否未儲存敏感性資料於行動裝置。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。
檢測結果	符合要求：符合所有檢測基準，或行動應用程式未儲存敏感性資料。 不符合要求：不符合任一檢測基準，或於檢測基準 4.1.2.3.1 之檢測結果因未聲明欲儲存之所有敏感性資料而不符合。
備註	於檢測基準 4.1.2.3.1 之檢測結果因未聲明欲儲存之所有敏感性資料，致使使用者無法對未聲明之敏感性資料行使拒絕權利

刪除不適用之敘述

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

4.1.2.3.5. 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

檢測編號	4.1.2.3.5
檢測項目	行動應用程式敏感性資料儲存限制
檢測分類	L3
檢測依據	「行動應用 App 基本資安規範」4.1.2.3.敏感性資料儲存、MSTG-STORAGE-3、MSTG-STORAGE-13
技術要求	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
檢測基準	(1)檢查行動應用程式是否未檢出將敏感性資料儲存於冗餘檔案。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準
	(2)檢查行動應用程式是否未檢出將敏感性資料儲存於日誌檔案。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準
	(3)檢查行動應用程式是否將敏感性資料儲存於冗餘檔案或日誌檔案且已用符合 FIPS 140-2 Annex A 之安全之加密函式保護。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準
檢測結果	符合要求：檢測基準(1)、(2)皆符合或符合檢測基準(3) 不符合要求：檢測基準(1)或(2)不符合且檢測基準(3)不符合
備註	受作業系統保護之區域亦不可檢出

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

檢測編號	4.1.2.3.5
檢測項目	行動應用程式冗餘檔案或日誌檔案敏感性資料儲存限制
檢測分類	L3
檢測依據	「行動應用 App 基本資安規範」4.1.2.3.敏感性資料儲存、MASVS-STORAGE-2
技術要求	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
檢測基準	(1)檢查行動應用程式是否未檢出將敏感性資料儲存於冗餘檔案。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。
	(2)檢查行動應用程式是否未檢出將敏感性資料儲存於日誌檔案。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。
	(3)檢查行動應用程式是否將敏感性資料儲存於冗餘檔案或日誌檔案且已用安全加密函式保護。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。
檢測結果	符合要求：檢測基準(1)、(2)皆符合或符合檢測基準(3)。 不符合要求：檢測基準(1)或(2)不符合且檢測基準(3)不符合。
備註	根據美國國家標準技術研究院建議：於 2023 年 12 月 31 日以後不允許對 Triple DES (3DES、DES3) 加密之支援。故將 3DES 加密從基準中剔除。

修改檢測項目名稱、修改檢測基準、修改備註

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

檢測基準	(1) 檢查行動應用程式之非冗餘檔案及非日誌檔案內之敏感性資料是否採用金鑰有效長度為 128 位元（含）以上之先進加密標準（AES）或三重資料加密演算法（Triple DES）。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。
	(2) 檢查行動應用程式所使用之加密函式之金鑰是否採用符合 ANSI X9.17、FIPS 140-2、NIST SP 800-22 及 SP 800-90A (CAVP Testing: Random Number Generators) 至少其中一項之安全的亂數產生函式。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準
檢測結果	符合要求：符合所有檢測基準，或行動應用程式未儲存敏感性資料 不符合要求：任一檢測基準不符合。
備註	受作業系統保護之區域亦不可檢出

檢測基準	(1)檢查行動應用程式之非冗餘檔案及非日誌檔案內之敏感性資料是否僅採用金鑰有效長度為 128 位元（含）以上之先進加密標準（AES），或使用 ChaCha20。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。
	(2)檢查行動應用程式所使用之加密函式之金鑰是否僅採用符合 ANSI X9.17、FIPS 140-3、NIST SP 800-22 及 SP 800-90A (CAVP Testing: Random Number Generators) 至少其中一項之安全的亂數產生函式。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。
檢測結果	符合要求：符合所有檢測基準，或行動應用程式未儲存敏感性資料。 不符合要求：不符合任一檢測基準。
備註	(1)受作業系統保護之區域亦不可檢出。 (2)根據美國國家標準技術研究院建議: 於 2023 年 12 月 31 日以後不允許對 Triple DES (3DES、DES3) 加密之支援。故將 3DES 加密從基準中剔除。

修改允許使用的加密演算法、修改檢測基準、增加備註

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

檢測編號	4.1.2.3.9
檢測項目	行動應用程式畫面擷取警示
檢測分類	L3
檢測依據	「行動應用 App 基本資安規範」4.1.2.3.敏感性資料儲存、MSTG-STORAGE-12
技術要求	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
檢測基準	檢查行動應用程式於非使用者主動進行的畫面擷取時是否主動警示使用者。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準
檢測結果	符合要求：符合檢測基準 不符合要求：不符合檢測基準 不適用：iOS 作業系統之應用程式
備註	無

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

檢測編號	4.1.2.3.9
檢測項目	行動應用程式畫面擷取警示
檢測分類	L3
檢測依據	「行動應用 App 基本資安規範」4.1.2.3. 敏感性資料儲存、MASVS-PLATFORM-3
技術要求	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
檢測基準	(1) 若畫面擷取是由應用程式自身觸發或其他應用程式觸發，而非使用者明確要求：檢查行動應用程式是否主動警示使用者或遮蔽畫面。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。 (2) 若應用程式處於App切換模式下，並且自動擷取畫面，而非使用者明確要求：檢查行動應用程式是否遮蔽畫面。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。
檢測結果	符合要求：Android 行動應用程式須符合所有檢測基準，iOS 行動應用程式須符合檢測基準(2)。 不符合要求：不符合檢測基準。
備註	無

增加iOS對應檢測項目、修改檢測結果敘述

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

4.1.2.3.10. 行動應用程式應適當使用系統憑證儲存設施儲存敏感性資料

檢測編號	4.1.2.3.10
檢測項目	行動應用程式應適當使用系統憑證儲存設施儲存敏感性資料。
檢測分類	L1、L2、L3
檢測依據	「行動應用 App 基本資安規範」4.1.2.3.敏感性資料儲存、MSTG-STORAGE-1、MSTG-STORAGE-14
技術要求	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。
檢測基準	檢查行動應用程式是否將可儲存於系統憑證儲存設施之敏感性資料儲存於內。如為「是」則符合檢測基準，如為「否」不符合檢測基準。
檢測結果	符合要求：符合檢測基準，或行動應用程式未檢出儲存敏感性資料 不符合要求：不符合檢測基準。
備註	根據系統不同，所提供之「系統憑證儲存設施」能儲存之資料限制不同，應依照不同系統之設計檢測是否有適當儲存敏感性資料。

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

檢測編號	4.1.2.3.10
檢測項目	行動應用程式應適當使用系統憑證儲存設施儲存敏感性資料
檢測分類	F
檢測依據	「行動應用 App 基本資安規範」4.1.2.3. 敏感性資料儲存、MASVS-STORAGE-1
技術要求	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
檢測基準	檢查行動應用程式是否將可儲存於系統憑證儲存設施之敏感性資料儲存於內。如為「是」則符合檢測基準，如為「否」不符合檢測基準。
檢測結果	符合要求：符合檢測基準，或行動應用程式未檢出儲存敏感性資料。 不符合要求：不符合檢測基準。
備註	根據系統不同，所提供之「系統憑證儲存設施」能儲存之資料限制不同，應依照不同系統之設計檢測是否有適當儲存敏感性資料。

將此檢測項移至F類別、修改檢測項名稱

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

檢測編號	4.1.2.3.11
檢測項目	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。
檢測分類	L2、L3
檢測依據	「行動應用 App 基本資安規範」4.1.2.3.敏感性資料儲存、MSTG-STORAGE-5、MSTG-PLATFORM-11
技術要求	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。
檢測基準	檢查行動應用程式是否在輸入敏感性資料欄位中將鍵盤快取機制關閉： (1) 檢查行動應用程式於使用者輸入敏感性資料時，是否未自動修正且未帶入可能字串。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。 (2) 檢查行動應用程式是否未將敏感性資料儲存在鍵盤快取檔案中。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。
檢測結果	符合要求：符合所有檢測基準，或行動應用程式未檢出蒐集敏感性資料。 不符合要求：不符合任一檢測基準。
備註	無

檢測編號	4.1.2.3.11
檢測項目	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
檢測分類	L2、L3
檢測依據	「行動應用 App 基本資安規範」4.1.2.3. 敏感性資料儲存、MASVS-STORAGE-2
技術要求	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
檢測基準	檢查行動應用程式是否在輸入敏感性資料欄位中將鍵盤快取機制關閉： 檢查行動應用程式於使用者輸入敏感性資料時，是否未自動修正且未帶入可能字串。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。
檢測結果	符合要求：符合所有檢測基準，或行動應用程式未提供字串輸入介面 不符合要求：不符合任一檢測基準。
備註	無

刪除檢測基準(2)、修改檢測結果之敘述

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

4.1.2.3.13. 行動應用程式中的使用者介面應避免洩漏敏感性資料

檢測編號	4.1.2.3.13
檢測項目	行動應用程式中的使用者介面應避免洩漏敏感性資料。
檢測分類	L2、L3
檢測依據	「行動應用 App 基本資安規範」4.1.2.3.敏感性資料儲存、MASVS-PLATFORM-3
技術要求	行動應用程式中的使用者介面應避免洩漏敏感性資料。
檢測基準	檢查行動應用程式執行時，是否對於敏感性資料進行防護，顯示於使用者介面之敏感性資料（至少包含通行碼與信用卡卡號）應有遮蔽設計。若有敏感性資料項不進行遮蔽，應敘明原因。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。
檢測結果	符合要求：符合檢測基準。 不符合要求：不符合檢測基準。
備註	無

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

檢測編號	4.1.2.3.13
檢測項目	行動應用程式中的使用者介面應避免洩漏敏感性資料
檢測分類	L2、L3
檢測依據	「行動應用 App 基本資安規範」4.1.2.3. 敏感性資料儲存、MASVS-PLATFORM-3
技術要求	行動應用程式中的使用者介面應避免洩漏敏感性資料
檢測基準	檢查行動應用程式執行時，是否對於敏感性資料進行防護，顯示於使用者介面之敏感性資料（至少包含密碼與信用卡卡號）應有遮蔽設計。若有敏感性資料項不進行遮蔽，應敘明原因。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。
檢測結果	符合要求：符合檢測基準。 不符合要求：不符合檢測基準。
備註	無

檢測項目改為”避免”洩漏敏感性資料

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

檢測編號	4.1.2.3.14
檢測項目	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。
檢測分類	L3
檢測依據	「行動應用 App 基本資安規範」4.1.2.3.敏感性資料儲存、MSTG-STORAGE-8
技術要求	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。
檢測基準	檢查行動裝置的系統備份檔案中是否未含有行動應用程式中的敏感性資料，如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。
檢測結果	符合要求：符合檢測基準，或行動應用程式未蒐集敏感性資料。 不符合要求：不符合檢測基準。
備註	系統備份是指行動裝置中的行動作業系統所提供的備份功能，其行動裝置內部及外部的備份檔案不應含有該行動應用程式的敏感性資料。

檢測編號	4.1.2.3.14
檢測項目	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
檢測分類	L3
檢測依據	「行動應用 App 基本資安規範」4.1.2.3.敏感性資料儲存、MASVS-STORAGE-2
技術要求	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。
檢測基準	(1)若行動應用程式有進行檔案備份，則檢查行動裝置的系統備份檔案中是否未含有行動應用程式中的敏感性資料，如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。 (2)若行動應用程式無進行檔案備份或設定不允許備份，則符合本項檢測基準，否則不符合本項檢測基準。
檢測結果	符合要求：符合任一檢測基準。 不符合要求：不符合所有檢測基準。
備註	系統備份是指行動裝置中的行動作業系統所提供的備份功能，其行動裝置內部及外部的備份檔案不應含有該行動應用程式的敏感性資料。

增加檢測基準(2)

4.1.2.3.16. 行動應用程式應避免將敏感性資料輸出於系統日誌

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

檢測編號	4.1.2.3.16
檢測項目	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
檢測分類	L1、L2、L3
檢測依據	「行動應用 App 基本資安規範」4.1.2.3. 敏感性資料儲存、MASVS-STORAGE-2、 MASVS-PLATFORM-1
技術要求	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
檢測基準	檢查行動應用是否將敏感性資料儲存或輸出於系統日誌中，如為「是」則不符合本項檢測基準；「否」則符合本項檢測基準。
檢測結果	符合要求：符合檢測基準。 不符合要求：不符合檢測基準。
備註	無

新增檢測項

4.1.2.3.16. 行動應用程式應避免將敏感性資料輸出於系統日誌

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

檢測編號	4.1.2.3.16
檢測項目	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
檢測分類	L1、L2、L3
檢測依據	「行動應用 App 基本資安規範」4.1.2.3. 敏感性資料儲存、MASVS-STORAGE-2、 MASVS-PLATFORM-1
技術要求	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
檢測基準	檢查行動應用是否將敏感性資料儲存或輸出於系統日誌中，如為「是」則不符合本項檢測基準；「否」則符合本項檢測基準。
檢測結果	符合要求：符合檢測基準。 不符合要求：不符合檢測基準。
備註	無

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

檢測編號	4.1.2.3.16
檢測項目	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
檢測分類	L1、L2、L3
檢測依據	「行動應用 App 基本資安規範」4.1.2.3. 敏感性資料儲存、MASVS-STORAGE-2、 MASVS-PLATFORM-1
技術要求	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
檢測基準	檢查行動應用程式是否將敏感性資料儲存或輸出於系統日誌中，如為「是」則不符合本項檢測基準；「否」則符合本項檢測基準。
檢測結果	符合要求：符合檢測基準。 不符合要求：不符合檢測基準。
備註	無

修改檢測基準，檢查行動應用「程式」是否將敏感性資料儲存或輸出於系統日誌中

4.1.2.4. 資料傳輸安全

4.1.2.4. 敏感性資料傳輸

針對「敏感性資料傳輸」之檢測項目，L1、L2、L3 行動應用程式於「4.1.2.4.1. 行動應用程式透過網路傳輸敏感性資料，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。」檢測結果須為「符合」，始符合本資訊安全技術要求事項；否則未符合本資訊安全技術要求事項。

4.1.2.4.1. 行動應用程式透過網路傳輸敏感性資料，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

4.1.2.4 資料傳輸安全

針對「資料傳輸安全」之檢測項目，L1、L2、L3 行動應用程式於「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。」檢測結果須為「符合」，始符合本資訊安全技術要求事項；否則未符合本資訊安全技術要求事項。根據 Mobile Application Security Testing Guide（MASTG）V1.7.0，禁止明文傳輸任何資料。

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

修改標題，因OWASP規定所有傳輸皆須加密

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

檢測編號	4.1.2.4.1
檢測項目	行動應用程式敏感性資料傳輸
檢測分類	L1、L2、L3
檢測依據	「行動應用 App 基本資安規範」4.1.2.4.敏感性資料傳輸、MSTG-STORAGE-4、MSTG-NETWORK-1、MSTG-NETWORK-2
技術要求	行動應用程式透過網路傳輸敏感性資料，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
檢測基準	(1)檢查行動應用程式是否採用 TLS 1.2（含）以上版本加密協定傳輸敏感性資料。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準
	(2)檢查行動應用程式是否採用金鑰有效長度為 2048 位元（含）以上之 RSA 加密演算法，或採用金鑰有效長度為 224 位元（含）以上之橢圓曲線加密演算法（Elliptic Curve Cryptography）。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準
	(3)檢查行動應用程式是否採用金鑰有效長度為 128 位元（含）以上之進階加密標準（AES），或採用三重資料加密演算法（Triple DES）。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準
檢測結果	符合要求：符合所有檢測基準，或行動應用程式未傳輸敏感性資料 不符合要求：任一檢測基準不符合
備註	無

修改檢測基準，所有傳輸皆須加密、增加備註

檢測編號	4.1.2.4.1
檢測項目	行動應用程式資料傳輸安全
檢測分類	L1、L2、L3
檢測依據	「行動應用 App 基本資安規範」4.1.2.4.資料傳輸安全、MASVS-STORAGE-2、MASVS-NETWORK-1
技術要求	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
檢測基準	(1)檢查行動應用程式是否僅採用 TLS 1.2（含）以上版本加密協定傳輸資料。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。
	(2)檢查行動應用程式是否僅採用金鑰有效長度為 2048 位元（含）以上之 RSA 加密演算法，或採用金鑰有效長度為 224 位元（含）以上之橢圓曲線加密演算法（Elliptic Curve Cryptography）。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。
	(3)檢查行動應用程式是否僅採用金鑰有效長度為 128 位元（含）以上之進階加密標準（AES），或使用 TLS1.2 所支援的加密演算法（含 ChaCha20）。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。
檢測結果	符合要求：符合所有檢測基準。 不符合要求：不符合任一檢測基準。
備註	根據美國國家標準技術研究院建議：於 2023 年 12 月 31 日以後不允許對 Triple DES (3DES、DES3) 加密之支援。故將 3DES 加密從基準中剔除。

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

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

檢測編號	4.1.2.5.1
檢測項目	行動應用程式敏感性資料分享聲明
檢測分類	L1、L2、L3
檢測依據	「行動應用 App 基本資安規範」4.1.2.5.敏感性資料分享、MSTG-STORAGE-12
技術要求	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
檢測基準	若行動應用程式已發布，檢查行動裝置內之不同行動應用程式間，分享敏感性資料前，是否於應用程式商店內聲明，或於行動應用程式內聲明及取得使用者同意。 若行動應用程式尚未發布，檢查調查表內是否有填寫「行動應用程式分享敏感性資料之預計分享內容、用途說明及如何取得使用者同意、分享之應用程式(非尚未發布不須填寫)」，並說明將如何取得使用者同意，或在行動應用程式內聲明及取得使用者同意。 如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準
檢測結果	符合要求：符合檢測基準，或行動應用程式未分享敏感性資料 不符合要求：不符合檢測基準 不適用：行動應用程式不公開發布，且行動應用程式內亦未提供，則此項不須檢測
備註	無

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

檢測編號	4.1.2.5.1
檢測項目	行動應用程式敏感性資料分享聲明
檢測分類	L1、L2、L3
檢測依據	「行動應用 App 基本資安規範」4.1.2.5. 敏感性資料分享、MASVS-STORAGE-2、MASVS-PRIVACY-3
技術要求	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
檢測基準	若行動應用程式已發布，檢查行動裝置內之不同行動應用程式間，分享敏感性資料前，是否於應用程式商店內聲明，且於行動應用程式內聲明及取得使用者同意。 若行動應用程式尚未發布，檢查調查表內是否有填寫「行動應用程式分享敏感性資料之預計分享內容、用途說明及如何取得使用者同意、分享之應用程式（已發布不須填寫）」，並說明將如何取得使用者同意，且在行動應用程式內聲明及取得使用者同意。 若行動應用程式不公開發布，檢查是否於行動應用程式內聲明及取得使用者同意。
	如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。
檢測結果	符合要求：符合檢測基準，或行動應用程式未分享敏感性資料。 不符合要求：不符合檢測基準。
備註	無

刪除不適用之檢測結果，新增不公開發布之檢測基準

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

檢測編號	4.1.2.5.2
檢測項目	行動應用程式提供使用者拒絕敏感性資料分享機制
檢測分類	L1、L2、L3
檢測依據	「行動應用 App 基本資安規範」4.1.2.5.敏感性資料分享、MSTG-STORAGE-12
技術要求	行動應用程式應提供使用者拒絕分享敏感性資料之權利
檢測基準	(1)檢查行動應用程式是否提供使用者拒絕分享敏感性資料之功能。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準
	(2)檢查在使用者拒絕敏感性資料分享的情況下，行動應用程式是否未分享敏感性資料。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準
檢測結果	符合要求：符合所有檢測基準，或行動應用程式未分享敏感性資料 不符合要求：任一檢測基準不符合 不適用：行動應用程式不公開發布，且行動應用程式內亦未提供，則此項不須檢測
備註	無

檢測編號	4.1.2.5.2
檢測項目	行動應用程式提供使用者拒絕敏感性資料分享機制
檢測分類	L1、L2、L3
檢測依據	「行動應用 App 基本資安規範」4.1.2.5.敏感性資料分享、MASVS-STORAGE-2、MASVS-PRIVACY-4
技術要求	行動應用程式應提供使用者拒絕分享敏感性資料之權利
檢測基準	(1)檢查行動應用程式是否提供使用者拒絕分享敏感性資料之功能。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。
	(2)檢查在使用者拒絕敏感性資料分享的情況下，行動應用程式是否未分享敏感性資料。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。
檢測結果	符合要求：符合所有檢測基準，或行動應用程式未分享敏感性資料。 不符合要求：不符合任一檢測基準。
備註	無

刪除不適用之檢測結果

4.1.3.

交易資源控管安全

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

檢測編號	4.1.3.1.1
檢測項目	行動應用程式交易資源使用聲明
檢測分類	L3
檢測依據	「行動應用 App 基本資安規範」4.1.3.1.交易資源使用、MSTG-STORAGE-12
技術要求	行動應用程式應於使用交易資源時主動通知使用者
檢測基準	檢查行動應用程式內於交易時，是否主動通知使用者，且資訊至少包含交易資源名稱、金額及交易方式。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準
檢測結果	符合要求：符合檢測基準 不符合要求：不符合檢測基準
備註	行動應用程式應於「應用程式交易前」主動通知使用者，意即行動應用程式於交易前是否主動通知使用者。

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

檢測編號	4.1.3.1.1
檢測項目	行動應用程式交易資源使用聲明
檢測分類	L3
檢測依據	「行動應用 App 基本資安規範」4.1.3.1._交易資源使用
技術要求	行動應用程式應於使用交易資源時主動通知使用者
檢測基準	(1)線上交易：檢查行動應用程式於交易時，是否主動通知使用者，且資訊至少包含交易商品名稱、金額及交易方式。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。僅限外匯、期貨與虛擬貨幣，可在事前宣告風險並取得使用者同意的狀況下，不針對每筆交易額外主動通知使用者。 (2)現場交易：使用者在現場購買商品或服務，交易資訊未顯示在應用程式的頁面上，但使用者在現場確認並授權交易（特別是行動支付的情境下），則視為符合本項檢測基準，否則視為不符合本項檢測基準。
檢測結果	符合要求：符合所有檢測基準，或行動應用程式僅使用上述其中一項交易模式，則僅需符合該項檢測基準。 不符合要求：不符合檢測基準。 不適用：行動應用程式僅涉及收款行為。
備註	行動應用程式應於「應用程式交易前」主動通知使用者，意即行動應用程式於交易前是否主動通知使用者。

增加檢測基準(2)、修改檢測基準(1)之敘述

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

檢測編號	4.1.3.1.2
檢測項目	行動應用程式拒絕交易資源使用機制
檢測分類	L3
檢測依據	「行動應用 App 基本資安規範」4.1.3.1.交易資源使用、MSTG-STORAGE-12
技術要求	行動應用程式應提供使用者拒絕使用交易資源之權利
檢測基準	(1) 檢查行動應用程式內於交易時，是否提供使用者拒絕交易之功能。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準
	(2) 檢查在使用者拒絕交易的情況下，行動應用程式是否未進行交易。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準
檢測結果	符合要求：符合所有檢測基準 不符合要求：任一檢測基準不符合
備註	無

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

檢測編號	4.1.3.1.2
檢測項目	行動應用程式拒絕交易資源使用機制
檢測分類	L3
檢測依據	「行動應用 App 基本資安規範」4.1.3.1. 交易資源使用
技術要求	行動應用程式應提供使用者拒絕使用交易資源之權利
檢測基準	(1)檢查行動應用程式於交易時，是否提供使用者拒絕交易之功能。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。僅限外匯、期貨與虛擬貨幣，可在事前宣告風險並取得使用者同意的狀況下，不針對每筆交易額外具有拒絕的步驟。
	(2)檢查在使用者拒絕交易的情況下，行動應用程式是否未進行交易。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。
檢測結果	符合要求：符合所有檢測基準。 不符合要求：不符合任一檢測基準。 不適用：行動應用程式僅涉及收款行為。
備註	無

修改檢測依據、修改檢測基準(1)之敘述、增加檢測結果之不適用敘述

4.1.3.1.3. 行動應用程式應提供使用者拒絕使用交易資源之權利

4.1.3.1.3. 行動應用程式應於交易收款時主動通知使用者

檢測編號	4.1.3.1.3
檢測項目	行動應用程式交易收款聲明
檢測分類	L3
檢測依據	「行動應用 App 基本資安規範」4.1.3.1. 交易資源使用
技術要求	行動應用程式應於交易收款時主動通知使用者
檢測基準	檢查行動應用程式於交易收款時，是否主動通知使用者，且資訊至少包含交易對象、交易時間、交易金額及交易商品資訊。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。
檢測結果	符合要求：符合檢測基準。 不符合要求：不符合檢測基準。 不適用：行動應用程式無收款行為。
備註	無

新增檢測項

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

檢測編號	4.1.3.2.1
檢測項目	行動應用程式交易資源使用者身分鑑別
檢測分類	L3
檢測依據	「行動應用 App 基本資安規範」4.1.3.2.交易資源控管、MSTG-AUTH-7、MSTG-AUTH-10、MSTG-NETWORK-5
技術要求	行動應用程式應於使用交易資源時進行使用者身分鑑別
檢測基準	檢查行動應用程式於交易前，是否提供有效的身分鑑別機制。如為「是」則符合檢測基準；「否」則不符合檢測基準
檢測結果	符合要求：符合檢測基準 不符合要求：不符合檢測基準
備註	除首次交易須身分鑑別外，若屬同一連線 (session)，則第二次之後的交易不須再進行身分鑑別。若連線 (session) 改變，則須要重新進行身分鑑別

檢測編號	4.1.3.2.1
檢測項目	行動應用程式交易資源使用者身分鑑別
檢測分類	L3
檢測依據	「行動應用 App 基本資安規範」4.1.3.2.交易資源控管、MASVS-AUTH-3
技術要求	行動應用程式應於使用交易資源時進行使用者身分鑑別
檢測基準	檢查行動應用程式於交易前，是否提供有效的身分鑑別機制。如為「是」則符合檢測基準；「否」則不符合檢測基準。
檢測結果	符合要求：符合檢測基準。 不符合要求：不符合檢測基準。 不適用：行動應用程式僅有預授權交易行為。
備註	(1)除首次交易須身分鑑別外，若屬同一連線 (session)，則第二次之後的交易不須再進行身分鑑別。若連線 (session) 改變，則須要重新進行身分鑑別。 (2)身分鑑別機制包括但不限於 OTP、生物特徵身分鑑別及 Google Authenticator。

增加不適用 、增加備註的說明

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

檢測編號	4.1.3.2.2
檢測項目	行動應用程式交易資源紀錄
檢測分類	L3
檢測依據	「行動應用 App 基本資安規範」4.1.3.2.交易資源控管
技術要求	行動應用程式應記錄使用之交易資源與時間
檢測基準	檢查行動應用程式於交易後，是否提供查詢交易資源交易紀錄之管道，且交易資源交易紀錄至少包含交易資源名稱、交易時間及交易金額之記錄。如為「是」則符合檢測基準；「否」則不符合檢測基準
檢測結果	符合要求：符合檢測基準 不符合要求：不符合檢測基準
備註	規範中所述之「交易資源與時間」於基準定義為「交易記錄」，即檢查行動應用程式是否提供交易記錄及記錄之內容

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

檢測編號	4.1.3.2.2
檢測項目	行動應用程式交易記錄
檢測分類	L3
檢測依據	「行動應用 App 基本資安規範」4.1.3.2. 交易資源控管
技術要求	行動應用程式應提供使用交易資源之交易記錄
檢測基準	檢查行動應用程式於交易後，是否提供查詢交易記錄之管道，且交易記錄至少包含交易商品名稱、交易時間及交易金額之記錄。如為「是」則符合檢測基準；「否」則不符合檢測基準。
檢測結果	符合要求：符合檢測基準。 不符合要求：不符合檢測基準。 不適用：行動應用程式僅有預授權交易行為。
備註	無

修改檢測項目名稱、增加不適用的檢測結果、刪除備註、

4.1.3.2.3. 行動應用程式應提供預授權交易之記錄

4.1.3.2.3. 行動應用程式應提供預授權交易之記錄

檢測編號	4.1.3.2.3
檢測項目	行動應用程式授權交易
檢測分類	L3
檢測依據	「行動應用 App 基本資安規範」4.1.3.2. 交易資源控管
技術要求	行動應用程式應提供預授權交易之記錄
檢測基準	(1)檢查行動應用程式預授權交易之功能，是否提供查詢交易記錄之管道，包括交易之金額。如為「是」則符合檢測基準；「否」則不符合檢測基準。
	(2)檢查行動應用程式預授權交易之功能，是否提供使用者取消預授權之功能。如為「是」則符合檢測基準；「否」則不符合檢測基準。
	(3)檢查行動應用程式預授權交易之功能，是否於取得使用者提供之授權時進行宣告。如為「是」則符合檢測基準；「否」則不符合檢測基準。
檢測結果	符合要求：符合所有檢測基準。 不符合要求：不符合任一檢測基準。 不適用：行動應用程式無預授權交易行為。
備註	無

新增檢測項

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

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

4.1.4.2.1. 行動應用程式應避免使用具有規則性之交談識別碼

檢測編號	4.1.4.2.1
檢測項目	行動應用程式交談識別碼規則性
檢測分類	L2、L3
檢測依據	「行動應用 App 基本資安規範」4.1.4.2.連線管理機制、MSTG-AUTH-1、MSTG-AUTH-2、MSTG-AUTH-4、MSTG-AUTH-7
技術要求	行動應用程式應避免使用具有規則性之交談識別碼
檢測基準	(1) 檢查行動應用程式是否採用長度為 128 位元（含）以上之交談識別碼。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準
	(2) 檢查行動應用程式使用之交談識別碼是否未與時間、使用者提交資料、具規則性之數字或字串有直接關聯或難以偽造。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準
	(3) 檢查行動應用程式使用之交談識別碼是否具備登出失效機制。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準
檢測結果	符合要求：符合所有檢測基準，或行動應用程式未使用交談識別碼 不符合要求：任一檢測基準不符合
備註	本項檢測基準所述之交談識別碼為使用者身分鑑別後所使用

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

檢測編號	4.1.4.2.1
檢測項目	行動應用程式交談識別碼規則性
檢測分類	L2、L3
檢測依據	「行動應用 App 基本資安規範」4.1.4.2.連線管理機制、MASVS-AUTH-1
技術要求	行動應用程式應避免使用具有規則性之交談識別碼
檢測基準	(1) 檢查行動應用程式是否採用長度為 128 位元（含）以上之交談識別碼。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。
	(2) 檢查行動應用程式使用之交談識別碼是否未與時間、使用者提交資料、具規則性之數字或字串有直接關聯或難以偽造。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。
	(3) 檢查行動應用程式使用之交談識別碼是否具備登出失效機制。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。
檢測結果	符合要求：符合所有檢測基準，或行動應用程式未使用交談識別碼。 不符合要求：不符合任一檢測基準。
備註	(1) 本項檢測基準所述之交談識別碼為使用者身分鑑別後所使用。 (2) 因 JWT 具備難以偽造的特性，亦納入檢測範疇內。

增加備註之敘述

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

檢測編號	4.1.4.2.3
檢測項目	行動應用程式伺服器憑證簽發來源
檢測分類	L1、L2、L3
檢測依據	「行動應用 App 基本資安規範」4.1.4.2.連線管理機制、MSTG-NETWORK-3
技術要求	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
檢測基準	檢查行動應用程式是否驗證並確保伺服器憑證為行動作業系統內建可信任之憑證機構所簽發。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準
檢測結果	符合要求：符合檢測基準。 不符合要求：不符合檢測基準
備註	行動作業系統內建之可信任憑證機構為行動作業系統廠商所安裝受信任之憑證簽發單位 若行動應用程式僅運用於封閉式內網連線，則企業自行簽發的憑證亦可視為可信任之憑證

檢測編號	4.1.4.2.3
檢測項目	行動應用程式伺服器憑證簽發來源
檢測分類	L1、L2、L3
檢測依據	「行動應用 App 基本資安規範」4.1.4.2.連線管理機制、MASVS-NETWORK-1
技術要求	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
檢測基準	檢查行動應用程式是否驗證並確保伺服器憑證為行動作業系統內建可信任之憑證機構所簽發。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。
檢測結果	符合要求：符合檢測基準。 不符合要求：不符合檢測基準。
備註	(1)行動作業系統內建之可信任憑證機構為行動作業系統業者所安裝受信任之憑證簽發單位。 (2)若行動應用程式僅運用於封閉式內網連線，則企業自行簽發的憑證亦可視為可信任之憑證。

修改備註之敘述

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

4.1.4.2.4. 行動應用程式封包流向應與所宣告的內容一致

檢測編號	4.1.4.2.4
檢測項目	行動應用程式封包流向
檢測分類	L1、L2、L3
檢測依據	「行動應用 App 基本資安規範」4.1.4.2. 連線管理機制、MASVS-NETWORK-2
技術要求	行動應用程式封包流向應與所宣告的內容一致
檢測基準	檢查行動應用程式封包流向是否與「行動應用 APP 基本資安檢測資料調查表上」宣告的封包流向一致。如為「是」則符合檢測基準;「否」則不符合檢測基準。
檢測結果	符合要求：符合檢測基準。 不符合要求：不符合檢測基準。
備註	須於「行動應用程式基本資料調查表」(附錄三、 行動應用 App 基本資安檢測資料調查表) 宣告封包的流向國家和網域名稱。

新增檢測項

4.1.5.

行動應用程式碼安全

4.1.5.1.1. 行動應用程式應避免含有惡意程式碼

檢測編號	4.1.5.1.1
檢測項目	行動應用程式惡意程式碼
檢測分類	L1、L2、L3
檢測依據	「行動應用 App 基本資安規範」4.1.5.1.防範惡意程式碼與避免資訊安全漏洞、MSTG-ARCH-10、MSTG-CODE-6、MSTG-CODE-7
技術要求	行動應用程式應避免含有惡意程式碼
檢測基準	(1)檢查行動應用程式是否未針對其他行動應用程式或行動作業系統之檔案，在未授權情況下，嘗試進行查詢、新增、修改、刪除、存取遠端服務、提權等行為。如為「是」則符合檢測基準；「否」則不符合檢測基準
	(2)檢查行動應用程式是否未包括可導致行動作業系統，發生未預期錯誤、資源明顯耗損、重新啟動或關閉等行為。如為「是」則符合檢測基準；「否」則不符合檢測基準
檢測結果	符合要求：符合所有檢測基準 不符合要求：任一檢測基準不符合
備註	無

檢測編號	4.1.5.1.1
檢測項目	行動應用程式惡意程式碼
檢測分類	L1、L2、L3
檢測依據	「行動應用 App 基本資安規範」4.1.5.1.防範惡意程式碼與避免資訊安全漏洞
技術要求	行動應用程式應避免含有惡意程式碼
檢測基準	(1)檢查行動應用程式是否未針對其他行動應用程式或行動作業系統之檔案，在未授權情況下，嘗試進行查詢、新增、修改、刪除、存取遠端服務、提權等行為。如為「是」則符合檢測基準；「否」則不符合檢測基準。
	(2)檢查行動應用程式是否未包括可導致行動作業系統，發生未預期錯誤、資源明顯耗損、重新啟動或關閉等行為。如為「是」則符合檢測基準；「否」則不符合檢測基準。
檢測結果	符合要求：符合所有檢測基準。 不符合要求：不符合任一檢測基準。
備註	常見的行動應用惡意程式類型包括但不限於: 網路釣魚(Phishing)、殭屍網路(Bots)、間諜軟體(Spyware)、下載器(Downloader)。

增加備註之敘述

4.1.5.1.3. 行動應用程式應針對螢幕覆蓋攻擊進行防護

4.1.5.1.3. 行動應用程式應針對螢幕覆蓋攻擊進行防護

檢測編號	4.1.5.1.3
檢測項目	行動應用程式針對螢幕覆蓋攻擊進行防護
檢測分類	L1、L2、L3
檢測依據	「行動應用 App 基本資安規範」4.1.5.1.防範惡意程式碼與避免資訊安全漏洞、MASVS-PLATFORM-3
技術要求	行動應用程式應針對螢幕覆蓋攻擊進行防護
檢測基準	檢查行動應用程式是否針對螢幕覆蓋攻擊(Screen Overlay Attack)進行防護或主動警示使用者，如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。
檢測結果	符合要求：符合檢測基準。 不符合要求：不符合檢測基準。 不適用：iOS 作業系統之應用程式。
備註	無

新增檢測項

4.1.5.5.5. 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

4.1.5.5.5. 屬於該行動應用程式的可執行檔案以及函式庫都應在檔案層級中加密或者在可執行檔案中重要的程式碼區段以及資料區段都應加密或加殼，使得一般的靜態分析不易取出重要的程式碼或資料。

檢測編號	4.1.5.5.5
檢測項目	屬於該行動應用程式的可執行檔案以及函式庫都應在檔案層級中加密或者在可執行檔案中重要的程式碼區段以及資料區段都應加密或加殼，使得一般的靜態分析不易取出重要的程式碼或資料
檢測分類	F
檢測依據	「行動應用 App 基本資安規範」4.1.5.5 防止動態分析及竄改、MSTG-RESILIENCE-11
技術要求	屬於該行動應用程式的可執行檔案以及函式庫都應在檔案層級中加密或者在可執行檔案中重要的程式碼區段以及資料區段都應加密或加殼，使得一般的靜態分析不易取出重要的程式碼或資料。
檢測基準	檢查該行動應用程式在檔案層級中的可執行檔案以及函式庫是否加密或者在可執行檔案中重要的程式碼區段以及資料區段是否加密或加殼，使得一般的靜態分析不易取出重要的程式碼或資料，如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。
檢測結果	符合要求：符合檢測基準。 不符合要求：不符合檢測基準。
備註	(1)實際檢測中可由受測方提供兩種行動應用程式，其一為無任何防禦機制之行動應用程式，而其一為有所有防禦機制之行動應用程式，並呈現有保護及未保護的兩支行動應用程式之各自雜湊值及相同功能切結書，以保障雙方權益。 (2)檢測實驗室可自行宣告具有解殼之能力。

4.1.5.5.5 屬於該行動應用程式的可執行檔案以及函式庫都應在檔案層級中加密或者在可執行檔案中重要的程式碼區段以及資料區段都應加密或加殼，使得一般的靜態分析不易取出重要的程式碼或資料。

參考編號	REF-15
依據	「行動應用 App 基本資安規範」 4.1.5.5 防止動態分析及竄改
技術要求	屬於該行動應用程式的可執行檔案以及函式庫都應在檔案層級中加密或者在可執行檔案中重要的程式碼區段以及資料區段都應加密或加殼，使得一般的靜態分析不易取出重要的程式碼或資料。
參考說明	參考原因：因檢測所須時間、複雜度或目前尚無通用檢測方法，造成檢測難以執行或重複檢測時結果不一致。 說明：由於已要求行動應用程式需進行程式碼混淆，故不強制行動應用程式需於程式碼區段進行加殼。
參考來源	「行動應用 App 基本資安規範」 4.1.5.5 防止動態分析及竄改、OWASP MASVS-RESILIENCE-2
備註	無

將加殼之檢測項移至參考項

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

4.1.5.5.7. 行動應用程式須偵測當前的執行環境是否為模擬器

檢測編號	4.1.5.5.7
檢測項目	行動應用程式執行環境是否為模擬器
檢測分類	F
檢測依據	「行動應用 App 基本資安規範」4.1.5.5. 防止動態分析及竄改、MASVS-RESILIENCE-1
技術要求	行動應用程式須偵測當前的執行環境是否為模擬器，如是，應主動通知使用者或關閉應用程式
檢測基準	當行動應用程式執行環境為模擬器時，行動應用程式是否能主動偵測並提醒使用者或中止執行該行動應用程式或行動應用程式無法安裝成功。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。
檢測結果	符合要求：符合檢測基準。 不符合要求：不符合檢測基準。
備註	無

新增檢測項

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

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

檢測編號	4.1.5.5.8
檢測項目	行動應用程式偵測是否開啟 USB 偵錯模式
檢測分類	F
檢測依據	「行動應用 App 基本資安規範」4.1.5.5. 防止動態分析及竄改、MASVS-RESILIENCE-2
技術要求	行動應用程式須偵測行動裝置是否開啟 USB 偵錯模式，如是，應主動通知使用者或關閉應用程式
檢測基準	當行動裝置於設定中開啟 USB 偵錯模式時，檢查行動應用程式是否能主動偵測並提醒使用者或者中止執行該行動應用程式。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。
檢測結果	符合要求：符合檢測基準。 不符合要求：不符合檢測基準。 不適用：iOS 行動應用程式。
備註	無

新增檢測項

4.1.5.5.9. 行動應用程式應將偵錯模式(Debug mode)設為關閉

4.1.5.5.9. 行動應用程式應將偵錯模式(Debug mode)設為關閉

檢測編號	4.1.5.5.9
檢測項目	行動應用程式應關閉偵錯模式
檢測分類	F
檢測依據	「行動應用 App 基本資安規範」4.1.5.5. 防止動態分析及竄改、MASVS-RESILIENCE-4
技術要求	行動應用程式應將偵錯模式設為關閉
檢測基準	檢查行動應用程式是否將偵錯模式的屬性設為關閉。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。
檢測結果	符合要求：符合檢測基準。 不符合要求：不符合檢測基準。
備註	無

新增檢測項

Webview安全檢測

Manual, OSSTMM），參考連結為 https://www.isecom.org/research.html。

- SANS（System Administration, Networking, and Security Institute）的滲透測試相關文件，參考連結為 http://pen-testing.sans.org/。

4.2.2.1. Webview 安全檢測

針對「Webview 安全檢測」之檢測項目，L1、L2、L3 行動應用程式於

「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」檢測結果須為「符合要求」，始符合本資訊安全技術要求事項，否則未符合本資訊安全技術要求事項。

4.2.2.1.1. 行動應用程式應使用 Webview 與遠端伺服器進行網頁資源交換

此項為建議參考項目，詳見「附錄五、行動應用 App 基本資安參考項目」。

修改4.2.2.1.2敘述文字

4.2.2.1.2. 行動應用程式於Webview呈現功能時，所連線之網域應為安全網域

檢測編號	4.2.2.1.2
檢測項目	行動應用程式之 Webview 安全檢測
檢測分類	L1、L2、L3
檢測依據	「行動應用 App 基本資安規範」4.2.2.1 Webview 安全檢測、MSTG-ARCH-2、MSTG-NETWORK-4、MSTG-PLATFORM-5、MSTG-PLATFORM-6、MSTG-PLATFORM-7
技術要求	行動應用程式於 Webview 呈現功能時，所連線之網域應為安全網域
檢測基準	(1)檢查行動應用程式使用 Webview 呈現功能時，所連線之網域是否為安全網域且與開發商於資料調查表中宣稱實際所連線之網域一致。如為「是」則符合檢測基準；「否」則不符合檢測基準 (2)檢查行動應用程式使用 Webview 呈現功能時，連線時是否使用 HTTPS 且進行憑證綁定。若無法預期使用者所連線之網站，則應提示連線目標有變更並有提醒使用者即將連線至其他網站之設計。如為「是」則符合檢測基準；「否」則不符合檢測基準。 (3)檢查行動應用程式使用 Webview 呈現功能時，其網頁伺服器弱點掃描須驗證 Cross-Site Scripting 以及 Injection Flaws 檢查是否全數通過。如為「是」則符合檢測基準；「否」則不符合檢測基準
檢測結果	符合要求：符合所有檢測基準，或行動應用程式於 Webview 呈現功能時無連網，若連線並未傳輸敏感資料可不進行憑證綁定、HTTPS 連線 不符合要求：不符合任一檢測基準 不適用：行動應用程式無使用 Webview 呈現功能
備註	有關弱點掃描之詳細說明請參照「6. 補充說明 (一)」

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

檢測編號	4.2.2.1.2
檢測項目	行動應用程式之 Webview 安全檢測
檢測分類	L1、L2、L3
檢測依據	「行動應用 App 基本資安規範」4.2.2.1 Webview 安全檢測、MASVS-NETWORK-2、MASVS-PLATFORM-2
技術要求	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
檢測基準	檢查行動應用程式使用 Webview 呈現功能時，其網頁伺服器弱點掃描須驗證 Injection Flaws 檢查是否全數通過。如為「是」則符合檢測基準；「否」則不符合檢測基準。 若所連線之網域為安全網域且與行動應用 App 開發者於資料調查表中宣稱實際所連線之網域一致，該網域不需進行網頁伺服器弱點掃描。
檢測結果	符合要求：符合檢測基準，或行動應用程式於 Webview 呈現功能時無連網。 不符合要求：不符合檢測基準。 不適用：行動應用程式無使用 Webview 呈現功能。
備註	(1)有關弱點掃描之詳細說明請參照「6. 補充說明（一）」。 (2)關於檢測基準第一點，Cross-Site Scripting 已納入 Injection Flaws。 (3)安全網域可參照行動應用資安聯盟所提供之白名單列表。

將Cross-site Scripting 併入Injection Flaws、修改檢測項名稱、檢測結果之敘述、修改檢測基準、修改技術要求之敘述

參考資料

8. 參考資料

[1] 行動應用 App 基本資安規範，經濟部工業局，民國 104 年 4 月 20 日

[2] 個人資料保護法，民國 104 年 12 月 30 日

[3] Vetting the Security of Mobile Applications, NIST Special Publication 800-163, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-163.pdf, 2015

[4] Technical Guide to Information Security Testing and Assessment, NIST Special Publication 800-115, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf, 2008

[5] Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, NIST Special Publication 800-131A, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-131a.pdf, 2011

[6] Cryptographic Algorithm Validation Program （CAVP）, http://csrc.nist.gov/groups/STM/cavp/, NIST

[7] Cryptographic Module Validation Program （CMVP）, http://csrc.nist.gov/groups/STM/cmvp/, NIST

[8] 移動智慧終端安全能力技術要求, YD/T 2407-2013, 2013

[9] 移動智慧移終端安全能力測試方法, YD/T 2408-2013, 2013

[10] Common Vulnerabilities and Exposures （CVE）, https://cve.mitre.org/

[11] Common Weakness Enumeration（CWE）, https://cwe.mitre.org/

[12] Device Administration - Minimum password length,

8. 參考資料

[1] 行動應用 App 基本資安規範，經濟部工業局，民國 104 年 4 月 20 日

[2] 個人資料保護法，民國 104 年 12 月 30 日

[3] Vetting the Security of Mobile Applications, NIST Special Publication 800-163, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-163.pdf, 2015

[4] Technical Guide to Information Security Testing and Assessment, NIST Special Publication 800-115, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf, 2008

[5] Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, NIST Special Publication 800-131A, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-131a.pdf, 2011

[6] Cryptographic Algorithm Validation Program （CAVP）, http://csrc.nist.gov/groups/STM/cavp/, NIST

[7] Cryptographic Module Validation Program （CMVP）, http://csrc.nist.gov/groups/STM/cmvp/, NIST

[8] Common Vulnerabilities and Exposures （CVE）, https://cve.mitre.org/

[9] Common Weakness Enumeration（CWE）, https://cwe.mitre.org/

[10] Device Administration - Minimum password length, http://developer.android.com/guide/topics/admin/device-admin.html

[11] OWASP Mobile App Security Checklist v1.7.0, https://mas.owasp.org/checklists/

刪除部分參考資料

附錄三、 行動應用App基本資安檢測資料調查表

※本表填寫內容均須與應用程式商店公開之資訊一致。

編號	項目		內容
1.	送檢單位名稱		
2.	連絡資訊		
3.	受測行動應用程式資訊	通用名稱	
4.		唯一識別名稱	
5.		App 雜湊值	格式： MD5：XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX SHA1: XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX SHA256：XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX
6.		作業系統	☐Android 版本：_____ ☐iOS 版本：_____ ☐Windows 版本：_____ ☐其他_____
7.		程式版本	
8.	APP 類別		請勾選符合之安全分類 APP 類別 ☐L1：無須使用者身分鑑別之行動應用程式 ☐L2：須使用者身分鑑別之行動應用程式 ☐L3：含有交易行為之行動應用程式
9.	發布狀態		☐內部使用，不公開發布

※本表填寫內容均須與應用程式商店公開之資訊一致。

編號	項目		內容
1.	送檢單位名稱		
2.	連絡資訊		
3.	受測行動應用程式資訊	通用名稱	
4.		唯一識別名稱	
5.		App 雜湊值	格式： MD5：XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX SHA1: XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX SHA256：XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX
6.		作業系統	☐Android 版本：_____ ☐iOS 版本：_____ ☐其他_____
7.		程式版本	
8.	APP 類別		請勾選符合之安全分類 APP 類別 ☐L1：無須使用者身分鑑別之行動應用程式 ☐L2：須使用者身分鑑別之行動應用程式 ☐L3：含有交易行為之行動應用程式 ☐F：屬於安全性需求較高之行動應用程式（此項為加測項目）

修改受測行動應用程式資訊、APP類別增加F類別

附錄二、 行動應用App基本資安檢測項目表

資訊安全技術要求面向	資訊安全技術要求事項	各類型之行動應用程式必要符合檢測項目				技術要求
		L1	L2	L3	F	
					★	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。
					★	4.1.5.5.8.行動應用程式須偵測行動裝置是否開啟USB偵錯模式。
					★	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	4.2.2.1. Webview 安全檢測	–	–	–	–	4.2.2.1.1.行動應用程式應使用 Webview 與遠端伺服器進行網頁資源交換。
		★	★	★	–	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。

修改4.2.2.1.2技術要求

附錄三、 行動應用App基本資安檢測資料調查表

18.	App 是否為免費版	☐ 是 ☐ 否
19.	是否使用 Webview	☐ 是，網域名稱：_____ （如：www.moeaidb.gov.tw）

編號	項目	內容
		☐ 否
20.	封包流向國家宣告	☐ 國內 ☐ 其他國家，包括：_____ (如:日本、英國等國家名稱)
21.	備註	

18.	App 是否為免費版	☐ 是 ☐ 否
19.	是否使用 Webview	☐ 是，網域名稱：_____ （如：www.moeaidb.gov.tw） ☐ 否
20.	封包流向國家宣告	☐ 國內 ☐ 其他國家，包括：_____

編號	項目	內容
		(如:日本、英國等國家名稱)
21.	封包流向網域名稱	
22.	備註	

新增編號21項

附錄四、 行動應用App基本資安檢測報告參考格式

報告編號		
檢測依據		
送檢單位名稱		
開發商名稱		
受測行動應用程式資訊	通用名稱	
	唯一識別名稱	
	作業系統	
	程式版本	
	檢測分類	
檢測結果		
檢測起始日期		
檢測完成日期		
報告日期		
報告版本		

報告編號		
檢測依據		
送檢單位名稱		
行動應用App開發者名稱		
受測行動應用程式資訊	通用名稱	
	唯一識別名稱	
	作業系統	
	程式版本	
	封包流向國家(所有)	
	封包流向網域名稱	
	檢測分類	
檢測結果		
檢測起始日期		
檢測完成日期		
報告日期		
報告版本		

增加行動應用App基本資安檢測報告項目

4.1.2.3.15.行動應用程式應避免重複使用相同的對稱式加密金鑰

4.1.2.3.15. 行動應用程式應避免重複使用相同的對稱式加密金鑰

參考編號	REF-9.
依據	「行動應用 App 基本資安規範」4.1.2.3.敏感性資料儲存、MASVS-CRYPTO-2
技術要求	行動應用程式所使用對稱式加密金鑰不應重複使用於多種用途
參考說明	參考原因：因檢測所須時間、複雜度或目前尚無通用檢測方法，造成檢測難以執行或重複檢測時結果不一致。
參考來源	MASVS-CRYPTO-2
備註	無

新增參考項

6. 補充說明

(一) 針對檢測項目 4.2.2.1.2，各實驗室必須提供網頁伺服器端之弱點掃描資訊，並於報告中加註弱點掃描對應之檢測項目，其中弱點掃描部份應由各實驗室自行檢測，或由各實驗室委託信賴的第三方廠商檢測。在合格證明與標章期限內若有伺服器端網頁資訊改版，開發商有義務主動通知實驗室再次做弱點掃描。實驗室檢測時要將所有此一問題發生處彙總，並註記於檢測報告的專一章節。↵

(一) 針對檢測項目 4.2.2.1.2，各實驗室必須提供網頁伺服器端之弱點掃描資訊，並於報告中加註弱點掃描對應之檢測項目，其中弱點掃描部份應由各實驗室自行檢測，或由各實驗室委託信賴的第三方廠商檢測。在合格證明與標章期限內若有伺服器端網頁資訊改版，行動應用 App 開發者有義務主動通知實驗室再次做弱點掃描。實驗室檢測時要將所有此一問題發生處彙總，並註記於檢測報告的專一章節。↵

開發商修改為行動應用App開發者

4.1.1.2. 行動應用程式更新

4.1.1.2. 行動應用程式更新↵

針對「行動應用程式更新」之檢測項目皆為參考項目，僅供開發者參考。↵

4.1.1.2.1. 行動應用程式應於可信任來源之行動應用程式商店發布更新↵

此項為建議參考項目，詳見附錄五、 行動應用 App 基本資安參考項目。↵

4.1.1.2. 行動應用程式更新↵

針對「行動應用程式更新」之檢測項目皆為參考項目，僅供行動應用 App 開發者參考。↵

4.1.1.2.1. 行動應用程式應於可信任來源之行動應用程式商店發布更新↵

此項為建議參考項目，詳見「附錄五、 行動應用 App 基本資安參考項目」。↵

開發者修改為行動應用App開發者

4.1.1.3. 行動應用程式安全性問題回報

4.1.1.3. 行動應用程式安全性問題回報

針對「行動應用程式安全性問題回報」之檢測項目，L2 及 L3 行動應用程式於「4.1.1.3.1. 行動應用程式開發者應提供回報安全性問題之管道」檢測結果須為「符合要求」，始符合本資訊安全技術要求事項；否則未符合本資訊安全技術要求事項。

4.1.1.3.1. 行動應用程式開發者應提供回報安全性問題之管道

4.1.1.3. 行動應用程式安全性問題回報

針對「行動應用程式安全性問題回報」之檢測項目，L2 及 L3 行動應用程式於「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」檢測結果須為「符合要求」，始符合本資訊安全技術要求事項；否則未符合本資訊安全技術要求事項。

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

行動應用程式開發者修改為行動應用App開發者

4.1.1.3. 行動應用程式安全性問題回報

4.1.1.3.1. 行動應用程式開發者應提供回報安全性問題之管道

檢測編號	4.1.1.3.1
檢測項目	行動應用程式問題回報
檢測分類	L2、L3
檢測依據	「行動應用 App 基本資安規範」4.1.1.3. 行動應用程式安全性問題回報
技術要求	行動應用程式開發者應提供回報安全性問題之管道
檢測基準	若行動應用程式已發布，檢查行動應用程式是否於應用程式商店或行動應用程式內，提供聯絡網頁、留言板、電子郵件、電話或其他類型聯絡方式，並經測試可實際聯絡成功。 若行動應用程式尚未發布，檢查調查表內是否有說明預計提供回報安全性問題之管道與聯絡方式，並經測試可實際聯絡成功。 如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準

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

檢測編號	4.1.1.3.1
檢測項目	行動應用程式問題回報
檢測分類	L2、L3
檢測依據	「行動應用 App 基本資安規範」4.1.1.3. 行動應用程式安全性問題回報
技術要求	行動應用 App 開發者應提供回報安全性問題之管道
檢測基準	若行動應用程式已發布，檢查行動應用程式是否於應用程式商店或行動應用程式內，提供聯絡網頁、留言板、電子郵件、電話或其他類型聯絡方式，並經測試可實際聯絡成功。 若行動應用程式尚未發布，檢查調查表內是否有說明預計提供回報安全性問題之管道與聯絡方式，並經測試可實際聯絡成功。 如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。

行動應用程式開發者修改為行動應用App開發者

8. 參考資料

▪8. 參考資料↵

[1] 行動應用 App 基本資安規範，經濟部工業局，民國 104 年 4 月 20 日↵

▪8. 參考資料↵

[1] 行動應用 App 基本資安規範，經濟部工業局(民國 111 年數位發展部數位產業署承接)，民國 104 年 4 月 20 日↵

新增民國111年數位發展部數位產業署承接

附錄二 新增4.1.5.5.5.之敘述

4.1.5.5.5.屬於該行動應用程式的可執行檔案以及函式庫都應在檔案層級中加密或者在可執行檔案中重要的程式碼區段以及資料區段都應加密或加殼，使得一般的靜態分析不易取出重要的程式碼或資料。↵