行動應用App基本資安檢測基準

V2.1

經濟部工業局
中華民國 106 年 02 月

目　次

表　目　次

1. 前言

行動裝置成為國人生活不可或缺的設備，各類行動應用程式（Mobile Application, App）應運而生，惟部分程式開發缺乏資安意識，恐造成使用者資料外洩或財務損失之風險。經濟部工業局依據103年6月24日行政院國家資通安全會報第26次委員會議決議，參照國際相關資安規範，並公開徵詢各界意見，完成制訂「行動應用App基本資安規範」，供業界開發行動應用程式自主遵循參考。

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制訂「行動應用App基本資安檢測基準（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」之安全分類，並參考OWASP（開放Web軟體安全計畫）「Mobile Security Project - Top Ten Mobile Risks」，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。

本檢測基準為提供第三方機構針對行動應用程式，進行資訊安全檢測及評估其安全水準之依據，藉由行動應用程式符合本檢測基準要求，以建立國人對行動應用程式使用之安全信賴感。

2. 適用範圍

本檢測基準項目適用於非特定領域及「行動應用 App 基本資安規範」中所有類別之行動應用程式，以確保受測行動應用程式符合現階段資訊安全水準要求。資訊安全本質為風險控管概念，即使行動應用程式檢測結果通過本檢測基準定義之檢測分級，仍不能完全保證行動應用程式不被惡意破解或利用，使用者亦需善盡相關使用與管理個人相關資料之責任，如帳號、密碼保管及保密等，以降低因蓄意或個人行為疏失所造成之風險及危害。

3. 用語及定義

本章節中文技術用語譯名主要採用國家教育研究院雙語詞彙、學術名詞暨辭書資訊網之翻譯用語：

3.1. 行動應用程式（Mobile Application）

指一種設計給智慧型手機、平板電腦和其他行動裝置使用之應用程式，本文中亦簡稱「行動應用 App」。

3.2. 行動應用程式商店（Application Store）

指行動裝置使用者透過內建在裝置中之行動應用程式商店或透過網站對應用程式、音樂、雜誌、書籍、電影、電視節目進行瀏覽、下載或購買。

3.3. 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，而該資訊之洩漏有對使用者造成損害之虞，包括個人資料、通行碼、金鑰、即時通訊訊息、筆記、備忘錄、通訊錄、地理位置、行事曆、通話紀錄及簡訊。

3.4. 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。

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、自身帳號密碼、遠端網路服務帳號密碼。

3.6. 付費資源（Payment Resource）

指透過行動應用程式購買功能取得之額外功能、內容及訂閱項目。

3.7. 交談識別碼（Session Identification, Session ID）

指在建立連線時，指派給該連線之識別碼，並做為連線期間之唯一識別碼；當連線結束時，該識別碼可釋出並重新指派給新之連線。

3.8. 伺服器憑證（Server Certificate）

指載有簽章驗證資料，提供行動應用程式鑑別伺服器身分及資料傳輸加密使用。

3.9. 憑證機構（Certification Authority）

指簽發憑證之機關、法人。

3.10. 惡意程式碼（Malicious Code）

指在未經使用者同意之情況下，侵害使用者權益，包括任何具有惡意特徵或行為之程式碼。

3.11. 資訊安全漏洞（Vulnerability）

指行動應用程式安全方面之缺陷，使得系統或行動應用程式資料之保密性、完整性、可用性面臨威脅。

3.12. 函式庫（Library）

指將一些繁複或者牽涉到硬體層面之程式包裝成函式（Function）或物件（Object）收集在一起，編譯成二進位碼提供程式設計者使用。

3.13. 注入攻擊（Code Injection）

指因行動應用程式設計缺陷而執行使用者所輸入之惡意指令，包括但不限於命令注入（Command Injection）及資料隱碼攻擊（SQL Injection）。

3.14. 行動作業系統（Mobile Operating System）

指在行動裝置上運作的作業系統。

3.15. 行動裝置資源（Mobile Resource）

指行動裝置提供之功能或服務，包括相機、相片、麥克風、無線網路、感應器及地理位置。

3.16. 行動應用程式內部更新（In-App Update）

指不更動發布於行動應用程式商店之主要版本，透過自訂的方法更新行動應用程式內容與功能。

3.17. 常見弱點與漏洞（Common Vulnerabilities and Exposures）

簡稱「CVE」，由美國國土安全部贊助之弱點管理計畫，針對每一弱點項目給予全球認可之唯一共通編號。

3.18. 脆弱加密演算法（Weak Cryptographic Algorithm）

指具 CVE 編號之加密演算法。

3.19. 已知安全性漏洞（Known Vulnerabilities）

指具 CVE 編號之漏洞。

3.20. 身分認證（Authentication）

即身分鑑別，指對個體所宣稱之身分提供保證。

3.21. 進階加密演算法（Advanced Encryption Standard）

指美國國家標準與技術研究院（National Institute of Standards and Technology, NIST）於 2001 年發佈於 AES（Advanced Encryption Standard）加密演算法，文件編號為 FIPS PUB 197 標準，並在 2002 年正式實施此標準。AES 可以支援 128 位元資料區塊（Data Block），並支援 128、192 與 256 位元金鑰長度（Key Size），提高安全性，AES 的加解密包含十個以上的回合數（Round Number），每個回合包含四個主要基本單元。

3.22. 三重資料加密演算法（Triple Data Encryption Standard）

指一種乘積密碼法，使用三重資料加密標準（Triple Data Encryption Standard），處理 64 位元的資料區塊。

3.23. 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，其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。

3.24. 憑證綁定（Certificate Pinning）

指將伺服器憑證預先存放於應用程式內，用於連線時確認是否與伺服器憑證相符。

3.25. 雜湊（Hash）

指由一串資料中經過演算法計算出來的資料指紋，經常用來識別檔案與資料是否有被竄改，以保證檔案與資料確實是由原創者所提供。

3.26. 混淆（Obfuscation）

指將行動應用程式原始碼，在不影響功能執行的情況下，轉換為難以閱讀

之形式。

3.27. 使用敏感性資料 （Use Sensitive Data）

指包含應用程式本身及提供給第三方進行之應用。

3.28. 紀錄檔 （Log）

指系統日誌或自定義日誌，可用來進行除錯使用，刪除時不影響行動應用程式再次執行時的功能與表現。

3.29. 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 Identifer, Android ID），安卓系統廣告識別碼（Android Advertising ID, AID），iOS IFAID(Identifier for Advertisers Identifier, IFAID)，Windows Phone Device ID。

3.30. 暫存檔（Temporary File）

指行動應用程式運作產生的檔案，通常於應用程式結束時刪除，該檔案存在與否，不影響行動應用再次執行時的功能與表現。

3.31. 設定檔（Configuration File）

指行動應用程式儲存相關設定的檔案，刪除時會影響行動應用程式再次執行時功能的表現。

3.32. 編碼（Encode）

指將數據轉換為代碼或字符的動作，且該代碼或字符可以譯（解）碼成原來數據。

3.33. 解碼（Decode）

指將編碼後的代碼或字符轉譯成原來數據的動作。

3.34. 酬載（Payload）

指封包、訊息或程式碼內容中的有效資料或指令。

3.35. 蒐集敏感性資料（Collect Sensitive Data）

指行動應用程式取得手機內建或使用者輸入之敏感性資料。

3.36. 儲存敏感性資料（Store Sensitive Data）

指行動應用程式將敏感性資料以檔案形式寫入行動裝置或其附屬儲存媒介。

3.37. 通用漏洞評分系統（Common Vulnerability Scoring System）

簡稱「CVSS」，使用 IT 漏洞的特點與影響進行評分，由美國國家基礎建設諮詢委員會負責研究（National Infrastructure Advisory Council, NIAC），現轉由資安事件應變小組論壇（Forum of Incident Response and Security Teams, FIRST）發展，目前為第 3 版。

4. 基本資安檢測基準

「行動應用 App 基本資安檢測基準」之檢測項目係依據「行動應用 App 基本資安規範」之「4.技術要求」資訊安全技術要求事項內容，主要提供資安檢測業者檢測遵循依據；基本資安規範主要提供行動應用程式開發商參考，故非所有基本資安規範之要求事項於檢測基準中皆須檢測。

檢測基準項目分為檢測項目及參考項目兩類，檢測項目為必要符合之項目，行動應用程式符合本檢測基準之檢測項目，代表使用者在未破解行動應用裝置之作業系統層保護時（如：root、jailbreak），行動應用程式具有基本資安水準，檢測項目詳見「4.1. 行動應用程式基本資安檢測基準」；參考項目因下列原因，故不要求進行實際檢測，僅供參考：

- 與品質有關，未直接影響行動應用程式安全性。
- 因檢測所需時間、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。
- 僅供開發者參考，非實際執行檢測之項目。

參考項目詳見「附錄四、行動應用 App 基本資安參考項目」。

「行動應用 App 基本資安規範」為針對行動應用程式之屬性分類，訂定各分類之安全要求項目，分為三類：第一類為純功能性，第二類為具認證功能、具連網行為，第三類為具交易功能（包含認證、連網行為）；「基本資安檢測基準」為針對行動應用程式之功能性對安全要求程度，訂定檢測安全等級，再依其檢測安全等級訂定檢測項目，檢測安全等級分為三個等級，各檢測分級定義如下：

「初級」檢測項目：主要檢測無連網之基礎功能安全性，檢測方式可採自動化工具檢測，並輔以適當之人工檢測，或純人工檢測；

「中級」檢測項目（含初級）：主要檢測連網及認證安全性，檢測方式採人工檢測方式為主；

「高級」檢測項目（含中級）：主要檢測付費資源安全性，檢測方式採人工檢測方式為主。

各檢測項目之檢測分級詳見「附錄一、行動應用 App 基本資安檢測項目表」。

因應行動應用程式改版快速的特性，本檢測基準於初級檢測項目主要以可採自動化工具檢測，並輔以適當人工檢測之項目，以縮短檢測所需時間達成快速檢測目的，其中有 9 項屬純功能之安全性檢測項目（請參閱附錄一、行動應用 App 基本資安檢測項目表），由於須採人工檢測方式進行，故將其納入中級檢測項目。由於不同自動化檢測工具其特性不盡相同，故自動化檢測工具可檢測之敏感性資料，以透過行動裝置內建 API 取得，並可規則化之敏感性資料為原則，故於初級檢測之敏感性資料主要類型，可包含：國民身分證統一編號、電子郵件地址、電話號碼與裝置識別符等。

行動應用程式通過其所屬安全等級之要檢測項目，即表示具備該安全等級之基本安全技術要求。第一類純功能性行動應用程式可送測初級（含）以上之安全檢測、第二類具認證功能與連網行為行動應用程式可送測中級（含）以上之安全檢測，第三類具交易功能行動應用程式須送測高級之安全檢測，其行動應用程式分類與檢測基準安全等級之對應表格如下：

表1　行動應用程式規範分類與基準分級檢測對應表

檢測基準安全等級 行動應用程式分類	初級 檢測功能相關之安全性	中級 檢測連網及認證安全性	高級 檢測交易相關之安全性
第一類 純功能性	★	V	V
第二類 具認證功能與連網行為	－	★	V
第三類 具交易功能（包含認證、連網行為）	－	－	★
註：★為必要送測之檢測等級，V 為可自由選擇通過之檢測等級			

各檢測項目之檢測分級詳見「附錄一、行動應用 App 基本資安檢測項目表」。

行動應用程式送測時，須詳實宣告並填寫於附錄二之「行動應用 App 基本資安檢測資料調查表」，一方面可促使送測廠商先自行檢視所需之敏感性資料與權限之合理性，另一方面可加速檢測人員了解行動應用程式之商業邏輯及其相關功能，以利檢測進行。

4.1. 行動應用程式基本資安檢測基準

本章節針對不同面向之行動應用程式安全訂定基本資安檢測基準，其中包括五大面向，分別詳述於4.1.1.行動應用程式發布安全、4.1.2.敏感性資料保護、4.1.3.付費資源控管安全、4.1.4.行動應用程式使用者身分認證、授權與連線管理安全及4.1.5.行動應用程式碼安全各章節。

針對每一檢測項目，訂定其檢測編號、檢測項目、檢測分級、檢測依據、技術要求、檢測基準及檢測結果等欄位並說明如表2。

表2　檢測項目欄位說明

欄位名稱	欄位說明
檢測編號	依據「行動應用 App 基本資安規範」之「4.技術要求」編號項次，檢測編號由5碼組成，分別為4.1.x.y.z，「4.1.」表示為「行動應用程式基本資安檢測基準」，「x.y.z」分別為其向下所展開之次編號項目
檢測項目	參照「行動應用 App 基本資安規範」之「4.技術要求」內容，訂定檢測摘要簡稱
檢測分級	「初級」檢測項目：主要檢測無連網之基礎功能安全性，檢測方式採自動化工具為主 「中級」檢測項目（含初級）：主要檢測連網及認證安全性，檢測方式採人工檢測方式為主 「高級」檢測項目（含中級）：主要檢測付費資源安全性，檢測方式採人工檢測方式為主
檢測依據	依據「行動應用 App 基本資安規範」之「4.技術要求」相對應之行動應用程式資訊安全技術要求事項
技術要求	依據「行動應用 App 基本資安規範」之「4.技術要求」相對應之行動應用程式資訊安全技術要求事項「內容」
檢測基準	依檢測項目所須檢測之各項檢查事項
檢測結果	依據檢查事項，預期之檢測結果及各結果之形成條件。預期之檢測結果包括「符合要求」與「不符合要求」
備註	其他說明事項

所有需「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。

4.1.1. 行動應用程式發布安全

本面向主要適用於發布行動應用程式之相關資訊安全檢測基準，包括發布、更新與問題回報等。

4.1.1.1. 行動應用程式發布

針對「行動應用程式發布」之檢測項目於「4.1.1.1.2. 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」中級檢測結果須為「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。

4.1.1.1.1. 行動應用程式應於可信任來源之行動應用程式商店發布

此項為建議參考項目，詳見附錄四、行動應用 App 基本資安參考項目。

4.1.1.1.2. 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
檢測分級	中級
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
檢測基準	檢查行動應用程式是否於可信任之應用程式商店，依實際需要說明欲存取之敏感性資料、行動裝置資源及宣告權限用途。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，或行動應用程式尚未發布，但於調查表內有說明預計提供欲存取之敏感性資料、行動裝置資源及宣告權限用途之說明
備註	須於「行動應用程式基本資料調查表」(附錄二、行動應用App基本資安檢測資料調查表)自我宣告發布來源 可信任之應用程式商店詳見附錄四、行動應用App基本資安參考項目REF-1 應用程式商店之宣告以行動裝置之商店介面為主

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，詳見附錄四、行動應用 App 基本資安參考項目。

4.1.1.2.2. 行動應用程式應提供更新機制

此項為建議參考項目，詳見附錄四、行動應用 App 基本資安參考項目。

4.1.1.2.3. 行動應用程式應於安全性更新時主動公告

此項為建議參考項目，詳見附錄四、行動應用 App 基本資安參考項目。

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，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」中級檢測結果須為「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

檢測編號	4.1.1.3.1
檢測項目	行動應用程式問題回報
檢測分級	中級
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	檢查行動應用程式是否於可信任之應用程式商店或行動應用程式內，提供聯絡網頁、電子郵件、電話或其他類型聯絡方式，並可實際聯絡成功。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準
檢測結果	符合要求：符合檢測基準 不符合要求：不符合檢測基準或調查表內未說明 不適用：行動應用程式不公開發布，或行動應用程式尚未發布，但於調查表內有說明預計提供回報安全性問題之管道與聯絡方式
備註	可信任之應用程式商店詳見附錄四、行動應用 App 基本資安參考項目 REF-1

4.1.1.3.2. 行動應用程式開發者應於適當期間內回覆問題並改善

此項為建議參考項目，詳見附錄四、行動應用 App 基本資安參考項目。

4.1.2. 敏感性資料保護

本面向主要適用於敏感性資料與個人資料保護之相關資訊安全檢測基準，包括敏感性資料蒐集、利用、儲存、傳輸、分享及刪除等。

4.1.2.1. 敏感性資料蒐集

針對「敏感性資料蒐集」之檢測項目，於「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」、「4.1.2.1.2. 行動應用程式應提供使用者拒絕蒐集敏感性資料之權利」中級檢測結果皆須為「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。

4.1.2.1.1. 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
檢測分級	中級
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
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	檢查行動應用程式所有蒐集之敏感性資料，是否皆已於可信任之應用程式商店或行動應用程式內聲明，並取得使用者同意。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，或行動應用程式尚未發布，但於調查表內有說明預計於應用程式商店宣告之敏感性資料蒐集聲明並取得使用者同意
備註	可信任之應用程式商店詳見附錄四、行動應用 App 基本資安參考項目 REF-1 應用程式商店之宣告以行動裝置之商店介面為主

4.1.2.1.2. 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
檢測分級	中級
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
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選項。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
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

4.1.2.2. 敏感性資料利用

針對「敏感性資料利用」之項目，僅供開發者參考。

4.1.2.2.1. 行動應用程式應於使用敏感性資料前，取得使用者同意

此項為建議參考項目，詳見附錄四、行動應用 App 基本資安參考項目。

4.1.2.2.2. 行動應用程式應提供使用者拒絕使用敏感性資料之權利

此項為建議參考項目，詳見附錄四、行動應用 App 基本資安參考項目。

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

此項為建議參考項目，詳見附錄四、行動應用 App 基本資安參考項目。

4.1.2.2.4. 行動應用程式應提醒使用者定期更改通行碼

此項為建議參考項目，詳見附錄四、行動應用 App 基本資安參考項目。

4.1.2.3. 敏感性資料儲存

針對「敏感性資料儲存」之檢測項目，於「4.1.2.3.4.行動應用程式應避免將敏感性資料儲存於暫存檔或紀錄檔中」、「4.1.2.3.5.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」、「4.1.2.3.6.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」、「4.1.2.3.7.敏感性資料應避免出現於行動應用程式之程式碼」初級檢測結果須為「符合要求」；於「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」、「4.1.2.3.2.行動應用程式應提供使用者拒絕儲存敏感性資料之權利」中級檢測結果須為「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。

4.1.2.3.1. 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
檢測分級	中級
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
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	(1)檢查行動應用程式是否於可信任之應用程式商店或行動應用程式內聲明。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於可信任之應用程式商店或行動應用程式內取得使用者同意。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 不適用：行動應用程式不公開發布，或行動應用程式尚未發布，但於調查表內有說明預計於應用程式商店宣告之敏感性資料儲存聲明並取得使用者同意
備註	可信任之應用程式商店詳見附錄四、行動應用 App 基本資安參考項目 REF-1 應用程式商店之宣告以行動裝置之商店介面為主

4.1.2.3.2. 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
檢測分級	中級
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
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選項。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
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

4.1.2.3.3. 行動應用程式儲存之敏感性資料，應僅用於其使用聲明之用途

此項為建議參考項目，詳見附錄四、行動應用 App 基本資安參考項目。

4.1.2.3.4. 行動應用程式應避免將敏感性資料儲存於暫存檔或紀錄檔中

檢測編號	4.1.2.3.4
檢測項目	行動應用程式敏感性資料儲存限制
檢測分級	初級
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
技術要求	行動應用程式應避免將敏感性資料儲存於暫存檔或紀錄檔中
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系統日誌。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

4.1.2.3.5. 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

檢測編號	4.1.2.3.5
檢測項目	行動應用程式敏感性資料儲存保護
檢測分級	初級
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
技術要求	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）。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：符合任一檢測基準，或行動應用程式未儲存敏感性資料 不符合要求：所有檢測基準皆不符合 不適用：若敏感性資料之儲存僅於檢測基準 4.1.2.3.4 之檢測結果為不符合則此項不須檢測
備註	符合檢測基準 4.1.2.3.4 之形成條件為「不得檢出」儲存敏感性資料，故無敏感性資料加密處理後再儲存議題 受作業系統保護之區域亦不可檢出

4.1.2.3.6. 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

檢測編號	4.1.2.3.6
檢測項目	行動應用程式敏感性資料儲存控管
檢測分級	初級
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
技術要求	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
檢測基準	檢查行動應用程式是否儲存敏感性資料於其他行動應用程式預設無法存取之區域。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，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 不適用：若敏感性資料之儲存僅於檢測基準 4.1.2.3.4 之檢測結果為不符合則此項不須檢測
備註	符合檢測基準 4.1.2.3.4 之形成條件為「不得檢出」儲存敏感性資料，故無儲存敏感性資料於其他行動應用程式預設無法存取之區域議題

4.1.2.3.7. 敏感性資料應避免出現於行動應用程式之程式碼

檢測編號	4.1.2.3.7
檢測項目	行動應用程式敏感性資料硬碼（Hard Code）
檢測分級	初級
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
技術要求	敏感性資料應避免出現於行動應用程式之程式碼
檢測基準	檢查行動應用程式之程式碼與行動應用程式安裝檔內其他檔案，是否未檢出密碼、身分驗證資訊或對稱式加解密演算法之金鑰。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	參考 CWE 揭露之 Hard code 弱點類型（如：CWE-259、CWE-321、CWE-798）

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，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。」中級檢測結果須為「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

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
檢測分級	中級
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
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 1.1（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	參酌支付卡產業安全標準委員會（Payment Card Industry Security Standards Council, PCI SSC）於 2015 年 12 月對 TLS 1.0 使用期限展延之公告（https://blog.pcisecuritystandards.org/migrating-from-ssl-and-early-tls），於 2018 年 6 月 30 日前，行動應用程式於不支援

	TLS 1.1（含）以上加密協定之 Android 作業系統，可支援使用 TLS 1.0，唯仍不可支援使用 SSL v3.0（含）以下之加密協定。實驗室若檢出行動應用程式可支援使用 TLS 1.0 應於檢測報告中加註說明，並建請開發者於 2018 年 7 月 1 日後停止支援使用 自 2018 年 7 月 1 日起，行動應用程式執行於不支援 TLS 1.1（含）以上加密協定之 Android 作業系統，亦不得檢出支援使用 TLS 1.0，開發商應考量相關配套設計與措施

4.1.2.5. 敏感性資料分享

針對「敏感性資料分享」之檢測項目，於「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」、「4.1.2.5.2.行動應用程式應提供使用者拒絕分享敏感性資料之權利」、「4.1.2.5.3.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」中級檢測結果須為「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。

4.1.2.5.1. 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
檢測分級	中級
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
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	(1) 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，是否於行動應用程式內或可信任之應用程式商店聲明。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準
	(2) 檢查行動裝置內之不同行動應用程式間，分享敏感性資料前，是否於行動應用程式內或可信任之應用程式商店取得使用者同意。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：行動應用程式尚未發布或不公開發布，且行動應用程式內亦未提供
備註	可信任之應用程式商店詳見附錄四、行動應用 App 基本資安參考項目 REF-1

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
檢測分級	中級
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
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選項。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
備註	無

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

檢測編號	4.1.2.5.3
檢測項目	行動應用程式敏感性資料分享權限控管
檢測分級	中級
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
技術要求	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
檢測基準	檢查分享敏感性資料之行動應用程式，是否限定特定行動應用程式可存取敏感性資料。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，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

4.1.2.6. 敏感性資料刪除

針對「敏感性資料刪除」之檢測項目其檢測分級皆為參考項目，僅供開發者參考。

4.1.2.6.1. 行動應用程式如涉及儲存使用者敏感性資料，應提供使用者刪除之功能

此項為建議參考項目，詳見附錄四、行動應用 App 基本資安參考項目。

4.1.3. 付費資源控管安全

本面向主要適用於付費資源控管之相關資訊安全檢測基準，包括付費資源之使用與控管等。

4.1.3.1. 付費資源使用

針對「付費資源使用」之檢測項目，於「4.1.3.1.1.行動應用程式應於使用付費資源前主動通知使用者」、「4.1.3.1.2.行動應用程式應提供使用者拒絕使用付費資源之權利」高級檢測結果皆須為「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。

4.1.3.1.1. 行動應用程式應於使用付費資源前主動通知使用者

檢測編號	4.1.3.1.1
檢測項目	行動應用程式付費資源使用聲明
檢測分級	高級
檢測依據	「行動應用 App 基本資安規範」4.1.3.1.付費資源使用
技術要求	行動應用程式應於使用付費資源前主動通知使用者
檢測基準	檢查行動應用程式內於付費前，是否主動通知使用者，且資訊至少包含付費資源名稱、數量、金額及付費方式。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，或行動應用程式無付費功能 不符合要求：不符合檢測基準
備註	規範中所述之「使用付費資源前」於基準定義為「付費前」，即檢查行動應用程式於付費前是否主動通知使用者

4.1.3.1.2. 行動應用程式應提供使用者拒絕使用付費資源之權利

檢測編號	4.1.3.1.2
檢測項目	行動應用程式拒絕付費資源使用機制
檢測分級	高級
檢測依據	「行動應用 App 基本資安規範」4.1.3.1.付費資源使用
技術要求	行動應用程式應提供使用者拒絕使用付費資源之權利
檢測基準	(1) 檢查行動應用程式內於付費時，是否提供使用者拒絕付費之選項。如為「是」則符合本項檢測基準;「否」則不符合本項檢測基準
	(2) 檢查在使用者拒絕付費的情況下，行動應用程式是否未進行付費。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，或行動應用程式無付費功能 不符合要求：任一檢測基準不符合
備註	規範中所述之「使用付費資源前」於基準定義為「付費時」，即檢查行動應用程式於付費前是否主動提供使用者拒絕付費選項

4.1.3.2. 付費資源控管

針對「付費資源控管」之檢測項目，於「4.1.3.2.1.行動應用程式應於使用付費資源前進行使用者認證」、「4.1.3.2.2.行動應用程式應記錄使用之付費資源與時間」高級檢測結果皆須為「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。

4.1.3.2.1. 行動應用程式應於使用付費資源前進行使用者認證

檢測編號	4.1.3.2.1
檢測項目	行動應用程式付費資源使用者認證
檢測分級	高級
檢測依據	「行動應用 App 基本資安規範」4.1.3.2.付費資源控管
技術要求	行動應用程式應於使用付費資源前進行使用者認證
檢測基準	檢查行動應用程式於付費時，是否提供身分認證機制。
檢測結果	符合要求：符合檢測基準，或行動應用程式無付費功能 不符合要求：不符合檢測基準
備註	規範中所述之「使用付費資源前」於基準定義為「付費時」，即檢查行動應用程式於付費前是否進行使用者認證

4.1.3.2.2. 行動應用程式應記錄使用之付費資源與時間

檢測編號	4.1.3.2.2
檢測項目	行動應用程式付費資源紀錄
檢測分級	高級
檢測依據	「行動應用 App 基本資安規範」4.1.3.2.付費資源控管
技術要求	行動應用程式應記錄使用之付費資源與時間
檢測基準	檢查行動應用程式於付費後，是否提供查詢交易紀錄之管道，且交易紀錄至少包含付費資源名稱、付費時間及付費金額之記錄。
檢測結果	符合要求：符合檢測基準，或行動應用程式無付費功能 不符合要求：不符合檢測基準
備註	規範中所述之「付費資源與時間」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

4.1.4. 身分認證、授權與連線管理安全

本面向主要適用於行動應用程式身分認證、授權與連線管理之相關資訊安全檢測基準，包括使用者身分認證與授權及連線管理機制等。

4.1.4.1. 使用者身分認證與授權

針對「使用者身分認證與授權」之檢測項目，於「4.1.4.1.1.行動應用程式應有適當之身分認證機制，確認使用者身分」、「4.1.4.1.2.行動應用程式應依使用者身分授權」中級檢測結果須為「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。

4.1.4.1.1. 行動應用程式應有適當之身分認證機制，確認使用者身分

檢測編號	4.1.4.1.1
檢測項目	行動應用程式使用者身分認證機制
檢測分級	中級
檢測依據	「行動應用 App 基本資安規範」4.1.4.1.使用者身分認證與授權
技術要求	行動應用程式應有適當之身分認證機制，確認使用者身分
檢測基準	如行動應用程式存取與個人資料相關之敏感性資料，檢查行動應用程式是否提供認證機制。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：符合檢測基準，或行動應用程式未存取使用者個人資料相關之敏感性資料 不符合要求：不符合檢測基準
備註	無

4.1.4.1.2. 行動應用程式應依使用者身分授權

檢測編號	4.1.4.1.2
檢測項目	行動應用程式使用者身分授權
檢測分級	中級
檢測依據	「行動應用 App 基本資安規範」4.1.4.1.使用者身分認證與授權
技術要求	行動應用程式應依使用者身分授權
檢測基準	如行動應用程式存取與個人資料相關之敏感性資料，檢查行動應用程式是否提供身分授權機制。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：符合檢測基準，或行動應用程式未存取使用者個人資料相關之敏感性資料 不符合要求：不符合檢測基準
備註	無

4.1.4.2. 連線管理機制

針對「連線管理機制」之檢測項目，於「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」、「4.1.4.2.2.行動應用程式應確認伺服器憑證之有效性」、「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、政府機關或企業簽發」、「4.1.4.2.4.行動應用程式應避免與未具有效憑證之伺服器，進行連線與傳輸資料」中級檢測結果須為「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。

4.1.4.2.1. 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
檢測分級	中級
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
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認證後所使用

4.1.4.2.2. 行動應用程式應確認伺服器憑證之有效性

檢測編號	4.1.4.2.2
檢測項目	行動應用程式伺服器憑證有效性
檢測分級	中級
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
技術要求	行動應用程式應確認伺服器憑證之有效性
檢測基準	(1) 檢查行動應用程式是否使用伺服器憑證仍於有效期間內、未被註銷（Revoke），且憑證之主體名稱與主體別名包含連線之伺服器網域名稱。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使用憑證綁定（Certificate Pinning）方式驗證，以確保連線之伺服器為行動應用程式開發者所指定。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安全加密傳輸協定 不符合要求：任一檢測基準不符合
備註	無

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、政府機關或企業簽發

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
檢測分級	中級
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
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、政府機關或企業簽發
檢測基準	如行動應用程式使用安全加密傳輸協定，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、政府機關、企業簽發。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，或行動應用程式未使用安全加密傳輸協定 不符合要求：不符合檢測基準
備註	憑證簽發單位說明如下： 1. 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 2. 政府機關：為政府單位成立之憑證簽發單位 3. 企業：企業自行成立之憑證簽發單位

4.1.4.2.4. 行動應用程式應避免與未具有效憑證之伺服器，進行連線與傳輸資料

檢測編號	4.1.4.2.4
檢測項目	行動應用程式連線安全
檢測分級	中級
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
技術要求	行動應用程式應避免與未具有效憑證之伺服器，進行連線與傳輸資料
檢測基準	(1) 如不符合檢測編號 4.1.4.2.2 或 4.1.4.2.3 之技術要求，檢查行動應用程式是否未與伺服器進行連線與傳輸敏感性資料。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使用符合檢測編號 4.1.4.2.2 與 4.1.4.2.3 之憑證與伺服器進行連線與傳輸敏感性資料。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：符合任一檢測基準，或行動應用程式未使用安全加密傳輸協定 不符合要求：所有檢測基準不符合
備註	無

4.1.5. 行動應用程式碼安全

本面向主要適用於行動應用程式開發之相關資訊安全檢測基準，包括防範惡意程式碼與避免資訊安全漏洞、行動應用程式完整性、函式庫引用安全與使用者輸入驗證等。

4.1.5.1. 防範惡意程式碼與避免資訊安全漏洞

針對「防範惡意程式碼與避免資訊安全漏洞」之檢測項目，於「4.1.5.1.1.行動應用程式應避免含有惡意程式碼」初級檢測結果須為「符合要求」，於「4.1.5.1.2.行動應用程式應避免資訊安全漏洞」中級檢測結果須為「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。

4.1.5.1.1. 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
檢測分級	初級
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)檢查是否符合檢測編號 4.1.2.1.1 之技術要求。如為「是」則符合檢測基準；「否」則不符合檢測基準
	(2)檢查是否符合檢測編號 4.1.2.3.1 之技術要求。如為「是」則符合檢測基準；「否」則不符合檢測基準
	(3)檢查是否符合檢測編號 4.1.2.5.1 之技術要求。如為「是」則符合檢測基準；「否」則不符合檢測基準
	(4)檢查是否符合檢測編號 4.1.3.1.1 之技術要求。如為「是」則符合檢測基準；「否」則不符合檢測基準
	(5)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
	(6)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

4.1.5.1.2. 行動應用程式應避免資訊安全漏洞

檢測編號	4.1.5.1.2
檢測項目	行動應用程式資訊安全漏洞
檢測分級	中級
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資訊安全漏洞
檢測基準	(1)檢查是否符合檢測編號 4.1.2.3.4 之技術要求。如為「是」則符合檢測基準；「否」則不符合檢測基準
	(2)檢查是否符合檢測編號 4.1.2.3.5 之技術要求。如為「是」則符合檢測基準；「否」則不符合檢測基準
	(3)檢查是否符合檢測編號 4.1.2.3.7 之技術要求。如為「是」則符合檢測基準；「否」則不符合檢測基準
	(4)檢查是否符合檢測編號 4.1.2.4.1 之技術要求。如為「是」則符合檢測基準；「否」則不符合檢測基準
	(5)檢查是否符合檢測編號 4.1.2.5.3 之技術要求。如為「是」則符合檢測基準；「否」則不符合檢測基準
	(6)檢查是否符合檢測編號 4.1.4.1.1 之技術要求。如為「是」則符合檢測基準；「否」則不符合檢測基準
	(7)檢查是否符合檢測編號 4.1.4.2.4 之技術要求。如為「是」則符合檢測基準；「否」則不符合檢測基準
	(8)檢查是否符合檢測編號 4.1.5.3.1 之技術要求。如為「是」則符合檢測基準；「否」則不符合檢測基準
	(9)檢查是否符合檢測編號 4.1.5.4.1 之技術要求。如為「是」則符合檢測基準；「否」則不符合檢測基準
	(10)檢查是否符合檢測編號 4.1.5.4.2 之技術要求。如為「是」則符合檢測基準；「否」則不符合檢測基準
	(11)檢查行動應用程式是否不存在已知安全性漏洞。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	檢查事項(11)中所述不符合本項檢測基準之已知安全性漏洞，為具 CVE 編號且 CVSS v3.0 分數大於等於 7 之漏洞。 TLS 1.0 相關之弱點於 2018 年 6 月 30 日(含)前不適用本檢測項目。

4.1.5.2. 行動應用程式完整性

針對「行動應用程式完整性」之檢測項目其檢測分級皆為參考項目，僅供開發者參考。

4.1.5.2.1. 行動應用程式應使用適當且有效之完整性驗證機制，以確保其完整性

此項為建議參考項目，詳見附錄四、行動應用 App 基本資安參考項目。

4.1.5.3. 函式庫引用安全

針對「函式庫引用安全」之檢測項目，於「4.1.5.3.1.行動應用程式於引用之函式庫有更新時，應備妥對應之更新版本，更新方式請參酌 4.1.1.行動應用程式發布安全」中級檢測結果須為「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。

4.1.5.3.1. 行動應用程式於引用之函式庫有更新時，應備妥對應之更新版本，更新方式請參酌 4.1.1.行動應用程式發布安全

檢測編號	4.1.5.3.1
檢測項目	行動應用程式函式庫引用安全
檢測分級	中級
檢測依據	「行動應用 App 基本資安規範」4.1.5.3.函式庫引用安全
技術要求	行動應用程式於引用之函式庫有更新時，應備妥對應之更新版本，更新方式請參酌 4.1.1.行動應用程式發布安全
檢測基準	檢查行動應用程式引用之函式庫是否不存在已知安全性漏洞。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」(附錄二、行動應用 App 基本資安檢測資料調查表)自我宣告引用函式庫名稱及版本資訊

4.1.5.4. 使用者輸入驗證

針對「使用者輸入驗證」之檢測項目，於「4.1.5.4.1.行動應用程式應針對使用者輸入之字串，進行安全檢查」初級檢測結果須為「符合要求」，於「4.1.5.4.2.行動應用程式應提供相關注入攻擊防護機制」中級檢測結果須為「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。

4.1.5.4.1. 行動應用程式應針對使用者輸入之字串，進行安全檢查

檢測編號	4.1.5.4.1
檢測項目	行動應用程式使用者輸入檢查
檢測分級	初級
檢測依據	「行動應用 App 基本資安規範」4.1.5.4.使用者輸入驗證
技術要求	行動應用程式應針對使用者輸入之字串，進行安全檢查
檢測基準	(1)檢查行動應用程式是否針對預期使用者輸入之字串驗證型別。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針對使用者輸入字串驗證長度。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：任一檢測基準不符合
備註	無

4.1.5.4.2. 行動應用程式應提供相關注入攻擊防護機制

檢測編號	4.1.5.4.2
檢測項目	行動應用程式注入攻擊防護機制
檢測分級	中級
檢測依據	「行動應用 App 基本資安規範」4.1.5.4.使用者輸入驗證
技術要求	行動應用程式應提供相關注入攻擊防護機制
檢測基準	(1)檢查行動應用程式是否防護使用者輸入 SQL Injection 字串之設計。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防護使用者輸入 JavaScript Injection 字串之設計。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防護使用者輸入 Command Injection 字串之設計。如為「是」則符合本項檢測基準;「否」則不符合本項檢測基準
	(4)檢查行動應用程式是否防護使用者輸入 Local File Inclusion 字串之設計。如為「是」則符合本項檢測基準;「否」則不符合本項檢測基準
	(5)檢查行動應用程式是否防護使用者輸入 XML Injection 字串之設計。如為「是」則符合本項檢測基準;「否」則不符合本項檢測基準
	(6)檢查行動應用程式是否防護使用者輸入 Format String Injection 字串之設計。如為「是」則符合本項檢測基準;「否」則不符合本項檢測基準
	(7)檢查行動應用程式是否防護使用者輸入 Intent Injection 字串之設計。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：任一檢測基準不符合
備註	未來如有新型 Injection 攻擊手法，亦納入檢測基準 有效的注入攻擊防護機制應於伺服端對使用者輸入之字串進行處理，基於防禦縱深概念，且本檢測基準檢測範圍為行動應用程式本身，實驗室至少須於行動應用程式對於輸入注入攻擊字串是否有初步防護設計進行檢測

4.2. 伺服端基本資安檢測基準

依據「行動應用 App 基本資安規範」4.2 章節描述：「本規範旨在針對行動應用程式安全提出基本資訊安全要求，如行動應用程式涉及伺服端之資訊安全需求，建議應由業者自我宣告或切結其伺服端資訊安全防護與管理措施，或對於其伺服端服務之資訊安全防護與管理，出具第三方檢測通過證明。」，故伺服端基本資安檢測基準不於本檢測基準訂之。

4.2.1. 伺服端安全管理

伺服端安全建議應以提供之應用與服務為出發點，進行應用與服務整體之威脅模型分析，找出對服務造成的安全性風險，以實施必要與有效的後續管控措施。若伺服端採租用 IDC 機房、主機（含虛擬伺服器）或雲端類型服務方案，建議以通過相關資訊安全管理標準，如：ISO 組織的 ISO/IEC 27001、雲端安全聯盟 （Cloud Security Alliance, CSA）的「STAR 驗證（Security, Trust & Assurance Registry）」或「歐洲雲端服務聯盟星級驗證（EuroCloud Star Audit, ECSA）」之服務商為優先考量。

4.2.2. 伺服端安全檢測

行動應用程式所搭配之行動應用平台伺服端，由於其提供之存取介面為行動應用程式，而非使用者直接存取之介面，開發商易忽略伺服端安全的防護措施。行動應用平台伺服端本質為網站及 Web Service 伺服器，若無適當的安全設計與開發，同樣會存在傳統網頁應用程式所具有的弱點。因此，在伺服端的安全檢測，建議開發商可斟酌採用滲透測試方式進行檢測。目前於國際間具公信力及參考價值的滲透測試文件有：

- OWASP （Open Web Application Security Project）的 OWASP 測試指引（OWASP Testing Guide），參考連結為
  https://www.owasp.org/index.php/Category:OWASP_Testing_Project；
- ISECOM （the Institute for Security and Open Methodologies）的開放原始碼安全測試方法手冊（Open Source Security Testing Methodology Manual, OSSTMM），參考連結為
  http://www.isecom.org/research/osstmm.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/。

5. 檢測方式

本檢測基準主要以未取得原始碼情況下進行測試，初級檢測以自動化工具進行檢測，中級、高級檢測以自動化工具及人工方式檢測，並必須進行逆向工程取得程式碼後進行檢測，使用原始碼掃描工具進行掃描後搭配人工分析。因行動應用程式基本安全檢測以黑箱測試方法論為主，本章節提及之檢測方式為概述性質，細項的檢測方法、檢測環境等實作交由各實驗室自行發展，以下針對各級檢測使用之方式進行說明。

5.1. 自動化（Automatic）檢測

初級檢測採用自動化方式進行檢測，檢測方式之類型主要包含：

- 使用者介面導向：以使用者操作介面為主進行自動化測試，包含自動化進行使用者之操作、畫面截圖等功能。在測試中可運用此類工具建構測試個案。
- 資料導向：能夠自動識別測試標的資料欄位或標籤，傳遞或填入不同的資料，並經由追蹤資料流向及回應結果，判斷可能存在之安全問題。

5.2. 人工（Manual）檢測

中級、高級檢測主要以人工方式進行手動檢測，檢測過程中採靜態分析與動態分析混合使用，並可依實際之檢測需求，使用逆向工程或以中間人（man-in-the-middle）攻擊方式進行。

5.2.1. 靜態分析（Static Analysis）

靜態分析透過手動或工具對可執行碼進行逆向工程取得程式碼，藉由欲存取之敏感性資料、行動裝置資源，例如：行動應用程式中的AndroidManifest.xml、iOS Entitlements、WMAppManifest.xml 等檔案，檢查所要求之權限是否如「附錄二、行動應用 App 基本資安檢測資料調查表」所述；檢查測試標的所引用的函式庫版本是否存在常見弱點與漏洞，或是否有引用不當的函式庫，例如：引用存在已知漏洞版本的函式庫之瀏覽器行動應用程式訪問惡意網站時，惡意的網站可能造成敏感性資料外洩；檢查敏感性資料是否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；檢查逆向工程後之程式碼是否出現可識別之敏感性資料檢查是否將敏感性資料儲存於暫存檔或紀錄檔中等方法，確認存在的安全漏洞或

問題。

5.2.2. 動態分析（Dynamic Analysis）

動態分析在測試標的執行階段中引入動態的使用者輸入或資料、參數的傳入等應用程式行為，以分析測試標的執行階段的各項行為或狀態。動態分析可檢測測試標的在模擬器、實體設備及遠端連線、網路存取狀態、資料傳遞等不同的行為，可應用於檢查敏感性資料傳輸與儲存，是否使用適當且有效之金鑰長度與加密演算法進行安全加密，例如使用封包側錄、檢查系統 Log 等方式，於程式執行中，查看是否存在可識別之敏感性資料；檢查是否將敏感性資料應儲存於受作業系統保護之區域，例如：程式執行後，檢查 SD 卡或可共同存取區域是否存在可識別之敏感性資料。

5.3. 程式碼分析（Code Analysis）

中級、高級檢測以逆向工程取得之程式碼進行分析，分析方式可採原始碼掃描工具進行掃描後搭配人工分析掃描結果。

5.4. 執行碼分析（Binary Code Analysis）

除上述檢測方式外，還可搭配其他檢測或分析方法如執行碼分析。執行碼（binary code）可分為中介碼（byte-code）及機器碼（machine code）。依不同類型之可執行碼分析，應採用適當之虛擬機器、實體設備進行手動或自動化工具檢測。

6. 檢測結果與產出

檢測結果產出，應包含在測試過程中的所有紀錄與結果，並應依第 4 節資訊安全技術要求事項所有檢測項目判定標準說明測試標的檢測結果為「符合要求或不符合要求」檢測結果與產出應包含但不限於：

- 檢測標的
- 檢測範圍之宣告
- 檢測時程
- 檢測方式、環境與使用之工具
- 檢測執行人員與負責之項目
- 測試項目為「符合要求或不符合要求」之判定
- 測試過程紀錄及佐證資料，不符合要求之檢測項目應於報告中提供

7. 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 99 年 5 月 26 日

[3] OWASP Mobile Security Project - Top Ten Mobile Risks, OWASP, https://www.owasp.org/index.php/Projects/OWASP_Mobile_Security_Project_-_Top_Ten_Mobile_Risks, 2014

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

[5] Technical Guide to Information Security Testing and Assessment, NIST Special Publication 800-115, http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf, 2008

[6] Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, NIST Special Publication 800-131A, http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf, 2011

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

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

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

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

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

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

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

8. 附錄

附錄一、行動應用 App 基本資安檢測項目表

本表使用符號說明：「★」表示檢測項目；「—」表示參考項目；「△」表示純功能性但納入中級之檢測項目。

資訊安全技術要求面向	資訊安全技術要求事項	各檢測分級必要符合檢測項目			檢測項目
		初級	中級	高級	
4.1.1.行動應用程式發布安全	4.1.1.1.行動應用程式發布	—	—	—	4.1.1.1.1.行動應用程式應於可信任來源之行動應用程式商店發布
		—	★	★	4.1.1.1.2.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
	4.1.1.2.行動應用程式更新	—	—	—	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
		—	—	—	4.1.1.2.2.行動應用程式應提供更新機制
		—	—	—	4.1.1.2.3.行動應用程式應於安全性更新時主動公告
	4.1.1.3.行動應用程式安全性	—	★	★	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

資訊安全技術要求面向	資訊安全技術要求事項	各檢測分級必要符合檢測項目			檢測項目
		初級	中級	高級	
	問題回報	—	—	—	4.1.1.3.2.行動應用程式開發者應於適當之期間內回覆問題並改善
4.1.2.敏感性資料保護	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
		△	★	★	4.1.2.1.2.行動應用程式應提供使用者拒絕蒐集敏感性資料之權利
	4.1.2.2.敏感性資料利用	—	—	—	4.1.2.2.1.行動應用程式應於使用敏感性資料前，取得使用者同意
		—	—	—	4.1.2.2.2.行動應用程式應提供使用者拒絕使用敏感性資料之權利
		—	—	—	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
		—	—	—	4.1.2.2.4.行動應用程式應提醒使用者定期更改通行碼

資訊安全技術要求面向	資訊安全技術要求事項	各檢測分級必要符合檢測項目			檢測項目
		初級	中級	高級	
	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
		△	★	★	4.1.2.3.2.行動應用程式應提供使用者拒絕儲存敏感性資料之權利
		—	—	—	4.1.2.3.3.行動應用程式儲存之敏感性資料，應僅用於其使用聲明之用途
		★	★	★	4.1.2.3.4.行動應用程式應避免將敏感性資料儲存於暫存檔或紀錄檔中
		★	★	★	4.1.2.3.5.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
		★	★	★	4.1.2.3.6.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

資訊安全技術要求面向	資訊安全技術要求事項	各檢測分級必要符合檢測項目			檢測項目
		初級	中級	高級	
		★	★	★	4.1.2.3.7.敏感性資料應避免出現於行動應用程式之程式碼
	4.1.2.4.敏感性資料傳輸	—	★	★	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。
	4.1.2.5.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
		△	★	★	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
		△	★	★	4.1.2.5.3.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
	4.1.2.6.敏感性資料刪除	—	—	—	4.1.2.6.1.行動應用程式如涉及儲存使用者敏感性資料，應提供使用者刪除之功能

資訊安全技術要求面向	資訊安全技術要求事項	各檢測分級必要符合檢測項目			檢測項目
		初級	中級	高級	
4.1.3.付費資源控管安全	4.1.3.1.付費資源使用	—	—	★	4.1.3.1.1.行動應用程式應於使用付費資源前主動通知使用者
		—	—	★	4.1.3.1.2.行動應用程式應提供使用者拒絕使用付費資源之權利
	4.1.3.2.付費資源控管	—	—	★	4.1.3.2.1.行動應用程式應於使用付費資源前進行使用者認證
		—	—	★	4.1.3.2.2.行動應用程式應記錄使用之付費資源與時間
4.1.4.身分認證、授權與連線管理安全	4.1.4.1.使用者身分認證與授權	—	★	★	4.1.4.1.1.行動應用程式應有適當之身分認證機制，確認使用者身分
		—	★	★	4.1.4.1.2.行動應用程式應依使用者身分授權
	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

資訊安全技術要求面向	資訊安全技術要求事項	各檢測分級必要符合檢測項目			檢測項目
		初級	中級	高級	
		—	★	★	4.1.4.2.2.行動應用程式應確認伺服器憑證之有效性
		—	★	★	4.1.4.2.3.行動應用程式應確認伺服器憑證為可信任之憑證機構、政府機關或企業簽發
		—	★	★	4.1.4.2.4.行動應用程式應避免與未具有效憑證之伺服器，進行連線與傳輸資料
4.1.5.行動應用程式碼安全	4.1.5.1.防範惡意程式碼與避免資訊安全漏洞	★	★	★	4.1.5.1.1.行動應用程式應避免含有惡意程式碼
		—	★	★	4.1.5.1.2.行動應用程式應避免資訊安全漏洞
	4.1.5.2.行動應用程式完整性	—	—	—	4.1.5.2.1.行動應用程式應使用適當且有效之完整性驗證機制，以確保其完整性。

資訊安全技術要求面向	資訊安全技術要求事項	各檢測分級必要符合檢測項目			檢測項目
		初級	中級	高級	
	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，應備妥對應之更新版本，更新方式請參酌 4.1.1.行動應用程式發布安全
	4.1.5.4.使用者輸入驗證	★	★	★	4.1.5.4.1.行動應用程式應針對使用者輸入之字串，進行安全檢查
		△	★	★	4.1.5.4.2.行動應用程式應提供相關注入攻擊防護機制

附錄二、行動應用 App 基本資安檢測資料調查表

行動應 App 基本資安檢測資料調查表

※本表填寫內容均需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 簽章憑證指紋	憑證的 MD5、SHA1 或 SHA256 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.		安全分類	請勾選符合之安全分類 □第一類：無連網行為、無身分認證機制，及無網路交易功能 □第二類：具連網行為、具身分認證機制，但無網路交易功能

編號	項目		內容
			□第三類：具網路交易功能
9.		送測級別	第一類須送測初級（含）以上、第二類須送測中級（含）以上，第三類須送測高級之安全檢測 □初級　□中級　□高級
10.	發布狀態		□內部使用，不公開發布
			（內部使用，不公開發布免填） □已發布 □未發布，預計發布日期__________ 已發布或預計發布於： □ 行動作業系統業者提供之行動應用程式商店 □ Apple App Store （URL）： __________ □ Google Play （URL）： __________ □ Microsoft Marketplace （URL）： __________ □ 其他（URL）： __________ □ 行動裝置製造業者提供之行動應用程式商店 （請填寫發布之電信業者及市集名稱） __________ □ 行動通信業者提供之行動應用程式商店 （請填寫發布之電信業者及市集名稱） __________
11.	需要之敏感性資料類型及用途說明		格式：需要< XX 敏感性資料 >，因為< OO 功能 >，< 具體用途描述 > 範例：需要國民身分證統一編號，因為登入功能，作為使用者帳號
12.	需要之行動裝置資源、權限及用途說		格式：需要< XX 權限 >，因為< OO 功能 >，< 具體用途描述 > 範例：需要 android.permission.ACCESS_FINE_LOCATION 權限，因為導航功

編號	項目	內容
	明	能，需要使用 GPS 定位
13.	問題回覆與改善機制之具體聯絡方式	公布於 □行動應用程式內　□應用程式商店內
		□聯絡網頁：________________________ □電子郵件：________________________ □電話：____________________________ □其他：____________________________
14.	引用函式庫名稱、版本、來源（包含作業系統內建及第三方函式庫）	格式：< 函式庫名稱 / 函式庫版本 /函式庫來源 > 範例：webkit / 534.30 / 作業系統內建
15.	連線是否採加密方式（第一類免填）	□ 是，加密協定：______________（如：TLS 1.2） □ 否，原因：__________________
16.	App 是否為免費版	□ 是 □ 否
17.	備註	

單位名稱：

用印

代表人：

用印

統一編號：

單位地址：

中　華　民　國　　　　　　　　年　　　　　　月　　　　　　日

附錄三、行動應用 App 基本資安檢測報告參考格式

報告編號：

○○○○○（機關名稱） ○○○○○（實驗室名稱）

行動應用 App 基本資安檢測報告（首頁參考格式）

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	
	安全分類	
	檢測分級	
檢測結果		
檢測起始日期		
檢測完成日期		
報告日期		
報告版本		

報告核准人（簽章）	報告簽署人（簽章）	檢測人員（簽章）

壹、測試項目及結果

資訊安全技術要求面向	檢測項目	結果（符合要求/不符合要求/參考項目）	備註
4.1.1. 行動應用程式發布安全	4.1.1.1.1.行動應用程式應於可信任來源之行動應用程式商店發布		
	4.1.1.1.2.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		
	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		
・・・	・・・		

貳、編碼格式

（檢測實驗室說明所採用之報告編號編碼格式，檢測項目編號編碼格式）

參、檢測工具

一、檢測軟體工具

（檢測使用之軟硬體工具清單）

二、檢測硬體工具

（檢測使用之硬體工具基本資料，如行動裝置廠牌、型號、裝置序號、作業系統版本...等）

肆、附件

（檢測實驗室檢附行動應用App基本資安檢測資料調查表及相關佐證資料）

附錄四、行動應用 App 基本資安參考項目

本附錄針對不同面向之行動應用程式安全訂定基本資安參考項目，其中包括三大面向，分別詳述於4.1.1.行動應用程式發布安全、4.1.2.敏感性資料保護及4.1.5.行動應用程式碼安全各章節。

針對每一參考項目，訂定其參考編號、依據、技術要求、參考說明、參考來源及備註等欄位並說明如下表參考項目欄位說明。

參考項目欄位說明表

欄位名稱	欄位說明
參考編號	依據「行動應用 App 基本資安規範」之「4.技術要求」編號項次，檢測編號由4碼組成，分別為REF-.x，「REF-.」表示為「附錄四、行動應用 App 基本資安參考項目」，「x」分別為其向下所展開之次編號項目
依據	依據「行動應用 App 基本資安規範」之「4.技術要求」相對應之行動應用程式資訊安全技術要求事項
技術要求	依據「行動應用 App 基本資安規範」之「4.技術要求」相對應之行動應用程式資訊安全技術要求事項「內容」
參考說明	參考原因： 說明：
參考來源	參考依循
備註	其他說明事項

4.1.1. 行動應用程式發布安全

4.1.1.1. 行動應用程式發布

4.1.1.1.1. 行動應用程式應於可信任來源之行動應用程式商店發布

參考編號	REF-1.
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	行動應用程式應於可信任來源之行動應用程式商店發布
參考說明	參考原因：僅供開發者參考，非實際執行檢測之項目。 說明：此參考項目非檢測應用程式本身可以判定之項目，建議行動應用程式發布於行動作業系統業者、行動裝置製造業者及行動通信業者提供之行動應用程式商店。
參考來源	NIST SP 800-163 3.1.6 Testing App Updates
備註	無

4.1.1.2. 行動應用程式更新

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

參考編號	REF-2.
依據	「行動應用 App 基本資安規範」4.1.1.2 行動應用程式更新
技術要求	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
參考說明	參考原因：僅供開發者參考，非實際執行檢測之項目。 說明：此參考項目非檢測應用程式本身可以判定之項目，建議行動應用程式發布更新於行動作業系統業者、行動裝置製造業者及行動通信業者提供之行動應用程式商店。
參考來源	NIST SP 800-163 3.1.6 Testing App Updates
備註	無

4.1.1.2.2 行動應用程式應提供更新機制

參考編號	REF-3.
依據	「行動應用 App 基本資安規範」4.1.1.2.行動應用程式更新
技術要求	行動應用程式應提供更新機制
參考說明	參考原因：僅供開發者參考，非實際執行檢測之項目。 說明：當行動應用程式之程式碼發現有安全性弱點，應提供由可信任來源伺服端進行更新
參考來源	NIST SP 800-163 3.1.5 Securing App Code Dependencies
備註	無

4.1.1.2.3 行動應用程式應於安全性更新時主動公告

參考編號	REF-4.
依據	「行動應用 App 基本資安規範」4.1.1.2.行動應用程式更新
技術要求	行動應用程式應於安全性更新時主動公告
參考說明	參考原因：僅供開發者參考，非實際執行檢測之項目。 說明：此參考項目非檢測應用程式本身可以判定之項目，建議行動應用程式於有安全性更新時於行動作業系統業者、行動裝置製造業者及行動通信業者提供之行動應用程式商店公告。
參考來源	NIST SP 800-64 3.4 SDLC Phase: Operations and Maintenance
備註	無

4.1.1.3. 行動應用程式安全性問題回報

4.1.1.3.2. 行動應用程式開發者應於適當期間內回覆問題並改善

參考編號	REF-5.
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於適當期間內回覆問題並改善
參考說明	參考原因：與品質有關，未直接影響行動應用程式安全性。 說明：此參考項目非檢測應用程式本身可以判定之項目，建議提供問題回覆與改善機制。
參考來源	NIST SP 800-64 3.1.3.5 Ensure Use of Secure Information System
備註	無

4.1.2. 敏感性資料保護

4.1.2.2. 敏感性資料利用

4.1.2.2.1. 行動應用程式應於蒐集敏感性資料前，取得使用者同意

參考編號	REF-6.
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	行動應用程式應於使用敏感性資料前，取得使用者同意
參考說明	參考原因：因檢測所需時間、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：此參考項目非檢測應用程式本身可以判定敏感性資料被利用與否，建議： (1) 行動應用程式使用敏感性資料前，於行動應用程式或行動作業系統業者、行動裝置製造業者及行動通信業者提供之行動應用程式商店聲明。 (2) 行動應用程式使用敏感性資料前，於行動應用程式或行動作業系統業者、行動裝置製造業者及行動通信業者提供之行動應用程式商店取得使用者同意。
參考來源	NIST SP 800-163 3.1.4 Protecting Sensitive Data
備註	無

4.1.2.2.2. 行動應用程式應提供使用者拒絕使用敏感性資料之權利

參考編號	REF-7.
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	行動應用程式應提供使用者拒絕使用敏感性資料之權利
參考說明	參考原因：因檢測所需時間、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：此參考項目非檢測應用程式本身可以判定敏感性資料被利用與否，建議提供使用者拒絕使用敏感性資料之選項。
參考來源	NIST SP 800-163 3.1.4 Protecting Sensitive Data
備註	無

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

參考編號	REF-8.
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
參考說明	參考原因：與品質有關，未直接影響行動應用程式安全性。 說明：此參考項目與使用者體驗相關，建議： (1) 行動應用程式於通行碼設定頁面，提醒使用者通行碼至少 6 個字元。 (2) 行動應用程式於通行碼設定頁面，提醒使用者通行碼包含數字與英文大小寫字母。 (3) 行動應用程式於通行碼設定頁面，提醒使用者避免使用個人相關資料做為通行碼。
參考來源	OWASP M5: Poor Authorization and Authentication
備註	無

4.1.2.2.4. 行動應用程式應提醒使用者定期更改通行碼

參考編號	REF-9.
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
參考說明	參考原因：與品質有關，未直接影響行動應用程式安全性。 說明：此參考項目與使用者體驗相關，建議行動應用程式於通行碼設定頁面，提醒使用者定期更改通行碼（至多不超過 90 天）。
參考來源	OWASP M5: Poor Authorization and Authentication
備註	無

4.1.2.3. 敏感性資料儲存

4.1.2.3.3. 行動應用程式儲存之敏感性資料，應僅用於其使用聲明之用途

參考編號	REF-10.
依據	「行動應用 App 基本資安規範」4.1.2.3.敏感性資料儲存
技術要求	行動應用程式儲存之敏感性資料，應僅用於其使用聲明之用途
參考說明	參考原因：因檢測所需時間、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：此參考項目非檢測應用程式本身可以判定敏感性資料之用途，建議僅在聲明範圍內使用敏感性資料。
參考來源	NIST SP 800-163 3.1.4 Protecting Sensitive Data
備註	無

4.1.2.6. 敏感性資料刪除

4.1.2.6.1. 行動應用程式如涉及儲存使用者敏感性資料，應提供使用者刪除之功能

參考編號	REF-11.
依據	「行動應用 App 基本資安規範」4.1.2.6.敏感性資料刪除
技術要求	行動應用程式如涉及儲存使用者敏感性資料，應提供使用者刪除之功能
參考說明	參考原因：因檢測所需時間、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：此參考項目非檢測應用程式本身可以判定敏感性資料是否刪除，建議行動應用程式敏感性資料刪除介面之功能被執行後，敏感性資料不以任何形式存在於行動裝置。
參考來源	NIST SP 800-163 3.1.4 Protecting Sensitive Data
備註	無

4.1.5. 行動應用程式碼安全

4.1.5.2. 行動應用程式完整性

4.1.5.2.1. 行動應用程式應使用適當且有效之完整性驗證機制，以確保其完整性

參考編號	REF-12.
依據	「行動應用 App 基本資安規範」4.1.5.2.行動應用程式完整性
技術要求	行動應用程式應使用適當且有效之完整性驗證機制，以確保其完整性
參考說明	參考原因：僅供開發者參考，非實際執行檢測之項目。 說明：此參考項目非檢測應用程式本身可以判定應用程式是否完整，驗證程式之完整性需要平台商之配合，建議： (1) 行動應用程式開發者提供應用程式雜湊值（Hash），供使用者驗證行動應用程式之完整性 (2) 採用混淆（Obfuscation）技術，保護行動應用程式商業邏輯
參考來源	OWASP M10: Lack of Binary Protections
備註	無