經濟部工業局

行動應用App基本資安檢測基準

V1.0

經濟部工業局
104 年 7 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。

本次初版優先以「行動應用 App 基本資安規範」安全分類第一類為範疇，訂定其檢測基準，包含「4.1.1 行動應用程式發布安全」3 個子項、「4.1.2 敏感性資料保護」（共 6 個子項）其中 5 個子項及「4.1.5 行動應用程式碼安全」（共 4 個子項）其中 3 個子項，共 11 個子項。後續將持續依據安全分類之第二類及第三類範疇，增訂該類行動應用程式於各安全等級之檢測基準項目，各安全分類所須符合之安全技術要求事項詳見附錄一。

本檢測基準可提供第三方機構依本檢測基準，針對行動應用程式與其所屬安全等級，進行資訊安全檢測、分析檢測結果及評估安全風險，完善行動應用程式安全水準。

2. 適用範圍

本檢測基準為提供行動應用程式，遵循「行動應用 App 基本資安規範」所必要之安全檢測項目與基準。本檢測基準項目適用於非特定領域之行動應用程式，與行動應用程式之共通性功能，以確保受測行動應用程式符合「行動應用 App 基本資安規範」之安全分類對應之安全等級。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對應之安全等級，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

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。

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，建立或儲存於行動裝置及其附屬儲存媒介之資訊，而該資訊之洩漏有對使用者造成損害之虞，包括但不限於個人資料、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、國際行動設備識別碼（International Mobile Equipment Identity, IMEI）、國際行動用戶識別碼（International Mobile Subscriber Identity, IMSI）及其他得以直接或間接方式識別該個人之資料。

3.5. 通行碼（Password）

指能讓使用者完全或有限度之使用系統或取得一組資料之識別使用者身分用之字元串，包括但不限於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（In-App Purchase/Billing）

指透過行動應用程式內建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，包括但不限於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，包括但不限於相機、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 Common Vulnerabilities and Exposures (CVE)編號之加密演算法。

3.19. 已知安全性漏洞（Known Vulnerabilities）

指具 Common Vulnerabilities and Exposures (CVE)編號之漏洞。

3.20. 三重資料加密演算法（Triple DES）

指一種乘積密碼法，使用三個資料加密標準（DES），處理 64 位元的資料區塊。

4. 基本資安檢測基準

本章依據「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，細分為各檢測項目。「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：第一類為僅純功能性，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級：初級為檢測功能相關之安全性，中級為檢測連網安全性(含初級)，高級為檢測交易相關之安全性(含中級)。對行動應用程式類別安全分類，訂定必要符合之安全等級檢測項目，詳見「附錄二、檢測項目表」。行動應用程式通過其所屬安全等級之必要檢測項目，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須通過初級安全檢測、第二類具認證功能與連網行為行動應用程式須通過中級安全檢測，第三類具交易功能行動應用程式須通過高級安全檢測，其行動應用程式分類與檢測基準安全等級之對應關係如下表所示：

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：★為必要通過之檢測等級，V 為可自由選擇通過之檢測等級			

針對每一檢測項目，訂定其檢測編號、安全分類、檢測項目名稱、檢測依據、技術要求、檢測基準及檢測結果判定條件等欄位並說明如表 1。

表1　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
安全分類	依據「行動應用 App 基本資安規範」之「5.安全分類」，不同應用類別之行動應用程式對於安全性有不同之要求，針對不同類型行動應用程式之資訊安全要求事項進行區分，共分為三類，分別為： 第一類、純功能性 第二類、具認證功能與連網行為 第三類、具交易功能（包括認證功能及連網行為）
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」與「不符合」
備註	其他說明事項

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。

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

「行動應用程式發布」之所有檢測項目，檢測結果皆為「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。

4.1.1.1.1. 行動應用程式應於可信任來源之行動應用程式商店發布

檢測編號	4.1.1.1.1
安全分類	「行動應用 App 基本資安規範」第一類、第二類、第三類
檢測項目	行動應用程式發布來源
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	行動應用程式應於可信任來源之行動應用程式商店發布
檢測基準	(1)檢查行動應用程式是否發布於行動作業系統業者提供之行動應用程式商店。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發布於行動裝置製造業者提供之行動應用程式商店。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發布於行動通信業者提供之行動應用程式商店。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：符合任一檢測基準，或行動應用程式尚未發布

	不符合要求：所有檢測基準皆不符合
備註	檢測時機：行動應用程式發布後 如尚未發布，須於「行動應用程式基本資料調查表」(附錄三)自我宣告發布來源

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
安全分類	「行動應用 App 基本資安規範」第一類、第二類、第三類
檢測項目	行動應用程式發布說明
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符合檢測編號 4.1.1.1.1 之所有檢測基準，皆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。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，或行動應用程式尚未發布 不符合要求：不符合檢測基準
備註	檢測時機：行動應用程式發布後 如尚未發布，須於「行動應用程式基本資料調查表」(附錄三)自我宣告發布來源

4.1.1.2. 行動應用程式更新

「行動應用程式更新」之所有檢測項目，除「4.1.1.2.2.行動應用程式應提供更新機制」外，其餘檢測結果皆為「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。

4.1.1.2.1. 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

檢測編號	4.1.1.2.1
安全分類	「行動應用 App 基本資安規範」第一類、第二類、第三類
檢測項目	行動應用程式更新來源
檢測依據	「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
檢測基準	檢查行動應用程式是否於行動應用程式中或符合檢測編號 4.1.1.1.1 之所有檢測基準發布更新。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，或行動應用程式未有更新 不符合要求：不符合檢測基準
備註	檢測時機：行動應用程式發布更新後 如尚未發布更新，須於「行動應用程式基本資料調查表」(附錄三)自我宣告更新方式

4.1.1.2.2. 行動應用程式應提供更新機制

檢測編號	4.1.1.2.2
安全分類	「行動應用 App 基本資安規範」第一類、第二類、第三類
檢測項目	行動應用程式更新機制
檢測依據	「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
檢測基準	檢查行動應用程式是否透過行動應用程式內部更新或符合檢測編號 4.1.1.1.1 之所有檢測基準進行更新。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，或行動應用程式未有更新 不符合要求：不符合檢測基準
備註	檢測時機：行動應用程式發布更新後 如尚未發布更新，須於「行動應用程式基本資料調查表」(附錄三)自我宣告更新方式

4.1.1.2.3. 行動應用程式應於安全性更新時主動公告

檢測編號	4.1.1.2.3
安全分類	「行動應用 App 基本資安規範」第一類、第二類、第三類
檢測項目	行動應用程式更新公告
檢測依據	「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
檢測基準	檢查行動應用程式於有安全性更新時，是否於行動應用程式或符合檢測編號 4.1.1.1.1 之所有檢測基準公告。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：符合檢測基準，或行動應用程式未有更新 不符合要求：不符合檢測基準
備註	檢測時機：行動應用程式發布更新後 如尚未發布更新，須於「行動應用程式基本資料調查表」(附錄三)自我宣告更新方式

4.1.1.3. 行動應用程式安全性問題回報

「行動應用程式安全性問題回報」之檢測項目，除「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」外，其餘檢測結果皆為「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
安全分類	「行動應用 App 基本資安規範」第一類、第二類、第三類
檢測項目	行動應用程式問題回報
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	檢查於行動應用程式或符合檢測編號 4.1.1.1.1 之所有檢測基準，是否提供聯絡網頁、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
備註	無

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

檢測編號	4.1.1.3.2
安全分類	「行動應用 App 基本資安規範」第一類、第二類、第三類
檢測項目	行動應用程式問題回報與改善回覆
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於適當期間內回覆問題並改善
檢測基準	檢查行動應用程式是否提供問題回覆與改善機制。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	須於「行動應用程式基本資料調查表」(附錄三)說明問題回覆與改善機制

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

「敏感性資料蒐集」之所有檢測項目，檢測結果皆為「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
安全分類	「行動應用 App 基本資安規範」第一類、第二類、第三類
檢測項目	行動應用程式敏感性資料蒐集聲明
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	(1)檢查行動應用程式蒐集敏感性資料前，是否於行動應用程式或符合檢測編號 4.1.1.1.1 之所有檢測基準聲明。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準
	(2)檢查行動應用程式蒐集敏感性資料前，是否於行動應用程式或符合檢測編號 4.1.1.1.1 之所有檢測基準，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
	(3)檢查在未聲明或未取得使用者同意敏感性資料蒐集的情況下，是否行動應用程式未搜集敏感性資料。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，或行動應用程式未蒐集敏感性資料 不符合要求：任一檢測基準不符合
備註	無

4.1.2.1.2. 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
安全分類	「行動應用 App 基本資安規範」第一類、第二類、第三類
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搜集敏感性資料。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，或行動應用程式未蒐集敏感性資料 不符合要求：任一檢測基準不符合
備註	無

4.1.2.2. 敏感性資料利用

「敏感性資料利用」之檢測項目，除「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」與「4.1.2.2.4.行動應用程式應提醒使用者定期更改通行碼」外，其餘檢測結果皆為「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。

4.1.2.2.1. 行動應用程式應於使用敏感性資料前，取得使用者同意

檢測編號	4.1.2.2.1
安全分類	「行動應用 App 基本資安規範」第一類、第二類、第三類
檢測項目	行動應用程式敏感性資料使用聲明
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	行動應用程式應於使用敏感性資料前，取得使用者同意
檢測基準	(1)檢查行動應用程式使用敏感性資料前，是否於行動應用程式或符合檢測編號 4.1.1.1.1 之所有檢測基準聲明。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準
	(2)檢查行動應用程式使用敏感性資料前，是否於行動應用程式或符合檢測編號 4.1.1.1.1 之所有檢測基準，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
	(3)檢查在未聲明或未取得使用者同意敏感性資料使用的情況下，行動應用程式是否未使用敏感性資料。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，或行動應用程式未使用敏感性資料 不符合要求：任一檢測基準不符合
備註	無

4.1.2.2.2. 行動應用程式應提供使用者拒絕使用敏感性資料之權利

檢測編號	4.1.2.2.2

安全分類	「行動應用 App 基本資安規範」第一類、第二類、第三類
檢測項目	行動應用程式提供使用者拒絕敏感性資料使用機制
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	行動應用程式應提供使用者拒絕使用敏感性資料之權利
檢測基準	(1)檢查行動應用程式是否提供使用者拒絕使用敏感性資料之選項。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使用的情況下，行動應用程式是否未使用敏感性資料。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，或行動應用程式未使用敏感性資料 不符合要求：任一檢測基準不符合
備註	無

4.1.2.2.3. 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
安全分類	「行動應用 App 基本資安規範」第一類、第二類、第三類
檢測項目	行動應用程式通行碼複雜度
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)檢查行動應用程式於通行碼設定頁面，是否提醒使用者通行碼包含數字與英文大小寫字母。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：所有檢測基準皆通過，或行動應用程式未採用通行碼認證 不符合要求：任一檢測基準不通過
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

檢測編號	4.1.2.2.4
安全分類	「行動應用 App 基本資安規範」第一類、第二類、第三類
檢測項目	行動應用程式通行碼更改
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	行動應用程式如採用通行碼認證，檢查行動應用程式於通行碼設定頁面，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；「否」則不符合檢測基準
檢測結果	符合要求：符合檢測基準，或行動應用程式未採用通行碼認證 不符合要求：不符合檢測基準
備註	無

4.1.2.3. 敏感性資料儲存

「敏感性資料儲存」之所有檢測項目，除「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」外，其餘檢測結果皆為「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
安全分類	「行動應用 App 基本資安規範」第一類、第二類、第三類
檢測項目	行動應用程式敏感性資料儲存聲明
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)檢查行動應用程式儲存敏感性資料前，是否於行動應用程式或符合檢測編號 4.1.1.1.1 之所有檢測基準聲明。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準
	(2)檢查行動應用程式儲存敏感性資料前，是否於行動應用程式或符合檢測編號 4.1.1.1.1 之所有檢測基準，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
	(3)檢查在未聲明或未取得使用者同意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。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	無

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
安全分類	「行動應用 App 基本資安規範」第一類、第二類、第三類
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。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	無

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

檢測編號	4.1.2.3.3
安全分類	「行動應用 App 基本資安規範」第一類、第二類、第三類
檢測項目	行動應用程式敏感性資料使用限制
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	行動應用程式儲存之敏感性資料，應僅用於其使用聲明之用途

檢測基準	檢查行動應用程式儲存之敏感性資料，是否未超出於使用聲明之用途。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，或行動應用程式未儲存敏感性資料 不符合要求：不符合檢測基準
備註	無

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
安全分類	「行動應用 App 基本資安規範」第一類、第二類、第三類
檢測項目	行動應用程式敏感性資料儲存限制
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將敏感性資料儲存於網頁暫存檔或自定義暫存檔。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於系統日誌或自定義日誌。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，或行動應用程式未儲存敏感性資料 不符合要求：任一檢測基準不符合
備註	無

4.1.2.3.5. 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
安全分類	「行動應用 App 基本資安規範」第一類、第二類、第三類
檢測項目	行動應用程式敏感性資料儲存保護
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金鑰有效長度為 112 位元（含以上）之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
備註	無

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
安全分類	「行動應用 App 基本資安規範」第一類、第二類、第三類
檢測項目	行動應用程式敏感性資料儲存控管
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，或行動應用程式未儲存敏感性資料 不符合要求：不符合檢測基準
備註	無

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
安全分類	「行動應用 App 基本資安規範」第一類、第二類、第三類
檢測項目	行動應用程式敏感性資料硬碼(Hard Code)
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或其他封裝之檔案內容，是否未出現可識別之敏感性資料。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 不符合要求：不符合檢測基準
備註	無

4.1.2.4. 敏感性資料傳輸

(待訂)

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

安全分類	「行動應用 App 基本資安規範」第二類、第三類
檢測項目	行動應用程式敏感性資料傳輸
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	(待訂)
檢測結果	(待訂)
備註	(待訂)

4.1.2.5. 敏感性資料分享

「敏感性資料分享」之所有檢測項目，檢測結果皆為「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
安全分類	「行動應用 App 基本資安規範」第一類、第二類、第三類
檢測項目	行動應用程式敏感性資料分享聲明
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或符合檢測編號 4.1.1.1.1 之所有檢測基準聲明。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或符合檢測編號 4.1.1.1.1 之所有檢測基準，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
	(3) 檢查在未聲明或未取得使用者同意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予行動裝置內之不同行動應用程式。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

4.1.2.5.2. 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
安全分類	「行動應用 App 基本資安規範」第一類、第二類、第三類
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
安全分類	「行動應用 App 基本資安規範」第一類、第二類、第三類
檢測項目	行動應用程式敏感性資料分享權限控管
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

「敏感性資料刪除」之所有檢測項目，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」外，其餘檢測結果皆為「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。

4.1.2.6.1. 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

檢測編號	4.1.2.6.1
安全分類	「行動應用 App 基本資安規範」第一類、第二類、第三類
檢測項目	行動應用程式敏感性資料刪除機制
檢測依據	「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
檢測基準	(1)檢查行動應用程式是否提供敏感性資料刪除介面。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準
	(2)檢查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。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，或行動應用程式未涉及儲存使用者敏感性資料 不符合要求：任一檢測基準不符合
備註	無

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

(待訂)

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
安全分類	「行動應用 App 基本資安規範」第三類

檢測項目	行動應用程式付費資源使用聲明
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	(待訂)
檢測結果	(待訂)
備註	(待訂)

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
安全分類	「行動應用 App 基本資安規範」第三類
檢測項目	行動應用程式拒絕付費資源使用機制
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	(待訂)
檢測結果	(待訂)
備註	(待訂)

4.1.3.2. 付費資源控管

(待訂)

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
安全分類	「行動應用 App 基本資安規範」第三類
檢測項目	行動應用程式付費資源使用者認證
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	(待訂)
檢測結果	(待訂)
備註	(待訂)

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
安全分類	「行動應用 App 基本資安規範」第三類
檢測項目	行動應用程式付費資源紀錄
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	(待訂)
檢測結果	(待訂)
備註	(待訂)

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

(待訂)

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
安全分類	「行動應用 App 基本資安規範」第二類、第三類
檢測項目	行動應用程式使用者身分認證機制

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	(待訂)
檢測結果	(待訂)
備註	(待訂)

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
安全分類	「行動應用 App 基本資安規範」第二類、第三類
檢測項目	行動應用程式使用者身分授權
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	(待訂)
檢測結果	(待訂)
備註	(待訂)

4.1.4.2. 連線管理機制

(待訂)

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
安全分類	「行動應用 App 基本資安規範」第二類、第三類
檢測項目	行動應用程式交談識別碼規則性
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	(待訂)
檢測結果	(待訂)
備註	(待訂)

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
安全分類	「行動應用 App 基本資安規範」第二類、第三類
檢測項目	行動應用程式伺服器憑證有效性
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	(待訂)
檢測結果	(待訂)
備註	(待訂)

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
安全分類	「行動應用 App 基本資安規範」第二類、第三類
檢測項目	行動應用程式伺服器憑證簽發來源
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	(待訂)
檢測結果	(待訂)

備註	(待訂)

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
安全分類	「行動應用 App 基本資安規範」第二類、第三類
檢測項目	行動應用程式連線安全
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	(待訂)
檢測結果	(待訂)
備註	(待訂)

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

「防範惡意程式碼與避免資訊安全漏洞」之所有檢測項目，檢測結果皆為「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
安全分類	「行動應用 App 基本資安規範」第一類、第二類、第三類
檢測項目	行動應用程式惡意程式碼

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 4.1.2.2.1 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 4.1.2.3.1 之技術要求。如為「是」則符合檢測基準；「否」則不符合檢測基準
	(4)檢查是否符合檢測編號 4.1.2.3.3 之技術要求。如為「是」則符合檢測基準；「否」則不符合檢測基準
	(5)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
	(6)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
	(7)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
	(8)檢查行動應用程式是否未包括可導致其他行動應用程式或行動作業系統，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
安全分類	「行動應用 App 基本資安規範」第一類、第二類、第三類
檢測項目	行動應用程式資訊安全漏洞
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	無

4.1.5.2. 行動應用程式完整性

(待訂)

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

檢測編號	4.1.5.2.1
安全分類	「行動應用 App 基本資安規範」第三類
檢測項目	行動應用程式完整性驗證機制
檢測依據	「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
檢測基準	(待訂)
檢測結果	(待訂)
備註	(待訂)

4.1.5.3. 函式庫引用安全

「函式庫引用安全」之所有檢測項目，除「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」外，其餘檢測結果皆為「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
安全分類	「行動應用 App 基本資安規範」第一類、第二類、第三類
檢測項目	行動應用程式函式庫引用安全
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」(附錄三)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

「使用者輸入驗證」之所有檢測項目，檢測結果皆為「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
安全分類	「行動應用 App 基本資安規範」第一類、第二類、第三類
檢測項目	行動應用程式使用者輸入檢查

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使用者輸入字串驗證型別。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
安全分類	「行動應用 App 基本資安規範」第一類、第二類、第三類
檢測項目	行動應用程式注入攻擊防護機制
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過濾導致 SQL Injection 之字串。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過濾導致 JavaScript Injection 之字串。如為「是」則符合本項檢測基準;「否」則不符合本項檢測基準
	(3)檢查行動應用程式是否過濾導致 Command Injection 之字串。如為「是」則符合本項檢測基準;「否」則不符合本項檢測基準
	(4)檢查行動應用程式是否過濾導致 Local File Inclusion 之字串。如

	為「是」則符合本項檢測基準；「否」則不符合本項檢測基準
	(5) 檢查行動應用程式是否過濾導致 XML Injection 之字串。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準
	(6) 檢查行動應用程式是否過濾導致 Format String Injection 之字串。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準
	(7) 檢查行動應用程式是否過濾導致 Intent Injection 之字串。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：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。

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。

5. 檢測方式

本檢測基準以黑箱測試方法論為主，主要以未取得原始碼之情況下進行測試，依據本檢測基準測試行動應用程式，是否具有基礎的安全性，後續提供各安全分類所須符合之安全等級。檢測目的在於能夠於開發階段就落實行動應用程式之安全性。因行動應用程式基本安全檢測項目非單一因素控制，本章節提及之檢測方式為基本的軟體檢測流程，與通過檢測基準與否的條件，細項的檢測方法實作交由各實驗室自行發展。

5.1. 執行碼(binary code)分析

可執行碼(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。

5.2. 靜態分析(Static Analysis)或動態(Dynamic Analysis)分析

檢測過程中靜態分析與動態分析可混合使用，並可依實際之檢測需求，進行反編譯、反組譯或中間人(man-in-the-middle)/代理伺服器(Proxy)測試環境檢測第 4 章之基本資安檢測基準。

5.2.1. 靜態分析(Static Analysis)

靜態分析透過手動或工具反組譯可執行碼或檢視原始碼，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三、「行動應用程式基本資料調查表」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；檢查原始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，例如使用封包測錄、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. 手動(Manual)或自動化(Automatic)測試

測試時可依各檢測實驗室之檢測方法、檢測環境等，採用自動化工具或人工手動檢測方法進行相關項目檢測，檢測工具類型可包含：

- 使用者介面導向：此類自動化工具以使用者操作之介面為主，進行自動化測試之工具，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：此類自動化工具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，並經由測試標的回應結果判斷可能存在之安全漏洞。在正確性測試中可運用此類工具建構測試個案。
- 模糊(Fuzzy)測試：此類自動化工具能夠自動產生各項的輸入，以隨機或邊界值測試各項的輸入並經由測試標的回應結果判斷可能存在之安全漏洞。在快速自動化測試情境及正確性測試可使用此類工具。
- 網路層測試：此類自動化工具用以蒐集及檢測測試標的之網路連線或資料傳遞行為。
- 原碼分析工具：此類自動化工具可取代手動工具，快速分析已知及潛在的安全漏洞，可應用在快速靜態及動態測試情境。

5.4. 安全能力分級

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皆於檢測基準中有對應項目。

依據「行動應用 App 基本資安規範」之安全分類，本檢測基準將各類別所需要各自符合之必要安全檢測項目分為三個安全等級，初級為檢測功能相關之安全性，中級為檢測連網安全性(含初級)，高級為檢測交易相關之安全性(含中級)，針對「安全分類」中「第一類」行動應用程式應至少通過「初級」安全等級之所有必要符合檢測項目；「安全分類」中「第二類」行動應用程

式應至少通過「中級」安全等級之所有必要符合檢測項目；「安全分類」中「第三類」行動應用程式應至少通過「高級」安全等級之所有必要符合檢測項目。

考量不同安全分類之行動應用程式，可能面臨之資安風險有所不同，故針對各安全分類，訂定「必要符合」、「非必要符合」、「不適用」等3種樣態之檢測項目，分別說明如下：

1. 必要符合檢測項目：該檢測項目對於行動應用程式本身安全性有直接影響，且目前已有通用技術可檢測，以「★」表示必要符合。
2. 非必要符合檢測項目：

   以「○」表示該檢測項目跟品質有關或無直接影響行動應用程式本身安全性。

   以「Δ」表示因檢測所需時間、複雜度或目前尚無通用檢測方法，造成檢測難以執行或檢測結果不一致。
3. 不適用檢測項目：該檢測項目依行動應用程式分類無此功能，故於檢測基準無對應安全性相關議題，以「—」符號表示不適用。

表2　各安全等級所需之檢測項目

編號	檢測項目	安全等級		
		初級	中級	高級
1	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	★	★	★
2	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	★	★	★
3	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	Δ	Δ	Δ
4	4.1.1.2.2.行動應用程式應提供更新機制	Δ	Δ	★
5	4.1.1.2.3.行動應用程式應於安全性更新時主動公告	Δ	Δ	★
6	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	★	★	★

編號	檢測項目	安全等級		
		初級	中級	高級
7	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	△	△	○
8	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	★	★	★
9	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	★	★	★
10	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	△	△	★
11	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	△	△	★
12	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	○	○	○
13	4.1.2.2.4.行動應用程式應提醒使用者定期更改通行碼	○	○	○
14	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	★	★	★
15	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	★	★	★
16	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	△	△	★
17	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	★	★	★
18	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	△	△	★
19	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	★	★	○
20	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	△	△	★
21	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。	—	★	★
22	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	△	△	★
23	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	△	△	★

編號	檢測項目	安全等級		
		初級	中級	高級
	權利			
24	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	Δ	Δ	★
25	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	○	★	★
26	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	—	—	★
27	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	—	—	★
28	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	—	—	★
29	4.1.3.2.2.行動應用程式應記錄使用之付費資源與時間	—	—	★
30	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	—	★	★
31	4.1.4.1.2.行動應用程式應依使用者身分授權	—	★	★
32	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	—	★	★
33	4.1.4.2.2.行動應用程式應確認伺服器憑證之有效性	—	★	★
34	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	—	★	★
35	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	—	★	★
36	4.1.5.1.1.行動應用程式應避免含有惡意程式碼	Δ	Δ	★
37	4.1.5.1.2.行動應用程式應避免資訊安全漏洞	Δ	Δ	★
38	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。	—	—	★
39	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	Δ	Δ	○
40	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	Δ	Δ	★
41	4.1.5.4.2.行動應用程式應提供相關注入攻擊防護機制	Δ	Δ	★

本表使用符號說明：「—」符號表示不適用；「★」表示必要符合；「○、Δ」表示非必要符合；灰色部分表示「待訂」。

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「符合或不符合」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「符合或不符合」之判定
- 測試過程紀錄及佐證資料

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

8. 附錄

附錄一、各安全分類之資訊安全技術要求事項

編號	資訊安全技術要求事項	安全分類		
		一	二	三
1	4.1.1.1.行動應用程式發布	V	V	V
2	4.1.1.2.行動應用程式更新	V	V	V
3	4.1.1.3.行動應用程式安全性問題回報	V	V	V
4	4.1.2.1.敏感性資料蒐集	V	V	V
5	4.1.2.2.敏感性資料利用	V	V	V
6	4.1.2.3.敏感性資料儲存	V	V	V
7	4.1.2.4.敏感性資料傳輸		V	V
8	4.1.2.5.敏感性資料分享	V	V	V
9	4.1.2.6.敏感性資料刪除	V	V	V
10	4.1.3.1.付費資源使用			V
11	4.1.3.2.付費資源控管			V
12	4.1.4.1.使用者身分認證與授權		V	V
13	4.1.4.2.連線管理機制		V	V
14	4.1.5.1.防範惡意程式碼與避免資訊安全漏洞	V	V	V
15	4.1.5.2.行動應用程式完整性			V
16	4.1.5.3.函式庫引用安全	V	V	V
17	4.1.5.4.使用者輸入驗證	V	V	V

附錄二、行動應用 App 基本資安檢測項目表

本表使用符號說明：「－」符號表示不適用；「★」表示必要符合；「○、Δ」表示非必要符合；灰色部分表示「待訂」。

資訊安全技術要求面向	各安全分類必要符合技術要求事項			資訊安全技術要求事項	各安全等級必要符合檢測項目			檢測項目
	一	二	三		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	Δ	Δ	Δ	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
					Δ	Δ	★	4.1.1.2.2.行動應用程式應提供更新機制

資訊安全技術要求面向	各安全分類必要符合技術要求事項			資訊安全技術要求事項	各安全等級必要符合檢測項目			檢測項目
	一	二	三		初級	中級	高級	
					△	△	★	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
					△	△	○	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

資訊安全技術要求面向	各安全分類必要符合技術要求事項			資訊安全技術要求事項	各安全等級必要符合檢測項目			檢測項目
	一	二	三		初級	中級	高級	
					△	△	★	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
	★	★	★	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

資訊安全技術要求面向	各安全分類必要符合技術要求事項			資訊安全技術要求事項	各安全等級必要符合檢測項目			檢測項目
	一	二	三		初級	中級	高級	
					Δ	Δ	★	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
					Δ	Δ	★	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
					Δ	Δ	★	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

資訊安全技術要求面向	各安全分類必要符合技術要求事項			資訊安全技術要求事項	各安全等級必要符合檢測項目			檢測項目
	一	二	三		初級	中級	高級	
	—	★	★	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	Δ	Δ	★	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
					Δ	Δ	★	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
					Δ	Δ	★	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	各安全分類必要符合技術要求事項			資訊安全技術要求事項	各安全等級必要符合檢測項目			檢測項目
	一	二	三		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	—	★	★	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	各安全分類必要符合技術要求事項			資訊安全技術要求事項	各安全等級必要符合檢測項目			檢測項目
	一	二	三		初級	中級	高級	
				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
					—	★	★	4.1.4.2.3.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	Δ	Δ	★	4.1.5.1.1.行動應用程式應避免含有惡意程式碼
					Δ	Δ	★	4.1.5.1.2.行動應用程式應避免資訊安全漏洞

資訊安全技術要求面向	各安全分類必要符合技術要求事項			資訊安全技術要求事項	各安全等級必要符合檢測項目			檢測項目
	一	二	三		初級	中級	高級	
	—	—	★	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。
	★	★	★	4.1.5.3.函式庫引用安全	Δ	Δ	○	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	Δ	Δ	★	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
					Δ	Δ	★	4.1.5.4.2.行動應用程式應提供相關注入攻擊防護機制

附錄三、行動應用 App 基本資安檢測資料調查表

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		作業系統	☐Andriod ☐iOS ☐Windows ☐其他_____
6		程式版本	
7		安全分類	☐第一類 ☐第二類 ☐第三類
8		安全等級	☐初級 ☐中級 ☐高級
7	發布來源		☐ 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： _____
			☐ 行動裝置製造業者提供之行動應用程式商店： _____
			☐ 行動通信業者提供之行動應用程式商店 ☐ 中華電信 Hami Apps ☐ 遠傳 S 市集

編號	項目	內容
		☐ 台灣大哥大 match Market ☐ 其他：_____
8	更新方式	☐ 行動應用程式發布來源 ☐ 行動應用程式內部更新 ☐ 其他：_____
9	問題回覆與改善機制	
10	引用函式庫名稱及版本資訊	
11	備註	

公司：　　代表人：

統一編號：　　日期：　　年　　月　　日

電話：

地址：

附錄四、行動應用 App 基本資安檢測報告參考格式

○○○○○(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	
	安全等級	
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/不符合/不適用)	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)