行動應用 App 基本資安規範

委託單位：經濟部工業局
執行單位：財團法人資訊工業策進會
公布日期：104 年 4 月 20 日

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，積極研議行動應用 App 基本資安規範。

爰此，經濟部工業局委託財團法人資訊工業策進會，邀集國內資安領域專家成立工作小組，參照國際相關資安規範，歷經多次工作小組會商、專家座談研討等會議，蒐集產官學研先進之建議，並公開徵詢各界意見，完成「行動應用 App 基本資安規範」，供業界開發行動應用 App 自主遵循參考。

本規範係屬非強制性規定，主要目的在於提升我國行動應用 App 基本安全防護能力，從設計初始階段即導入基本資安概念，透過規範之重點要項，提醒 App 開發者強化資訊安全意識，並逐步完善自身 App 安全防護能力。

本規範分從「行動應用程式發布安全」、「敏感性資料保護」、「付費資源控管安全」、「行動應用程式使用者身分認證、授權與連線管理安全」、「行動應用程式碼安全」等五個層面提出資訊安全技術要求，App 開發者可參考規範，自主提升所開發之行動應用 App 安全品質，增進使用者之信賴度與使用意願，創造 App 開發商與使用者雙贏局面。

2. 適用範圍

本規範為提供行動應用程式相關業者之基本資訊安全準則，屬自願性準則，各業者可參酌遵循；本規範適用於非特定領域[1]之行動應用程式，與行動應用程式之共通性功能[2]。特定領域之行動應用程式，其領域功能所需之資訊安全規範，建議應由各目的事業主管機關訂定之。

[1] 特定領域：指歸類於某一專門領域，由特定主管機關及法律加以規範、管制，例如金融、醫療、稅務等。

[2] 共通性功能：指行動應用程式運作所需、具有共同性、相類似之基礎功能，例如資料儲存、傳輸保護機制或使用者身分認證機制等。

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、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。

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（Certificate）

指載有簽章驗證資料，提供伺服器身分鑑別及資料傳輸加密。

3.9. 憑證機構（Certificate 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）、資料隱碼攻擊（SQL Injection）。

4. 技術要求

4.1. 行動應用程式資訊安全技術要求事項

本節針對不同面向之行動應用程式安全訂定技術要求,其中包括五大面向：行動應用程式發布安全、敏感性資料保護、付費資源控管安全、行動應用程式使用者身分認證、授權與連線管理安全及行動應用程式碼安全。

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技術要求，包括發布、更新與問題回報等。

4.1.1.1. 行動應用程式發布

行動應用程式應於可信任來源之行動應用程式商店發布，且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

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。

行動應用程式應提供更新機制，並於有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

行動應用程式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應於適當期間內回覆問題並改善。

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技術要求，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

行動應用程式應於蒐集敏感性資料前，取得使用者同意，並提供使用者拒絕之權利。

4.1.2.2. 敏感性資料利用

行動應用程式應於使用敏感性資料前，取得使用者同意，並提供使用者拒絕之權利。

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。

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

行動應用程式應於儲存敏感性資料前，取得使用者同意，並提供使用者拒絕之權利。

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，並避免將敏感性資料儲存於暫存檔或紀錄檔中。

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。

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。

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

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

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，並提供使用者拒絕之權利。

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

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。

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技術要求，包括付費資源之使用與控管等。

4.1.3.1. 付費資源使用

行動應用程式應於使用付費資源前主動通知使用者，並提供使用者拒絕之權利。

4.1.3.2. 付費資源控管

行動應用程式應於使用付費資源前進行使用者認證，並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

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技術要求，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

行動應用程式應有適當之身分認證機制，確認使用者身分，並依使用者身分授權。

4.1.4.2. 連線管理機制

行動應用程式應避免使用具有規則性之交談識別碼。

行動應用程式應確認伺服器憑證之有效性，且為可信任之憑證機構、政府機關或企業之簽發。

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

本面向主要適用於行動應用程式開發之相關資訊安全技術要求，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

行動應用程式應避免含有惡意程式碼。

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

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

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

行動應用程式應針對使用者輸入之字串，進行安全檢查並提供相關注入攻擊防護機制。

4.2. 伺服端資訊安全技術要求事項

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。

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，本章節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）

針對每一安全分類，定義應符合資訊安全技術要求事項之最小集合，即行動應用程式應符合其所屬分類中之所有資訊安全技術要求事項，非屬上述分類之特殊情況，於檢測標準另行說明。各安全分類之資訊安全技術要求事項詳如表 1。

表1　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

參考資料

Open Web Application Security Project (OWASP)

[1] 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

美國

[2] Vetting the Security of Mobile ApplicationsApp, NIST Special Publication 800-163, http://dx.doi.org/10.6028/NIST.SP.800-163, 2015

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

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

[5] Government Mobile and Wireless Security Baseline, Federal CIO Council, https://cio.gov/wp-content/uploads/downloads/2013/05/Federal-Mobile-Security-Baseline.pdf, 2013

歐洲

[6] Smartphone Secure Development Guidelines for App Developers, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/smartphone-security-1/smartphone-secure-development-guidelines, ENISA, 2011

大陸

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

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

日本

[9] Security Guideline for using Smartphones and Tablets - Advantages for work style innovation - [Version 1], https://www.jssec.org/dl/guidelines2012Enew_v1.0.pdf, JSSEC, 2011

國際標準

[10] ISO/IEC 27001:2013 (Information security management)

[11] ISO/IEC 20000:2011 (Information technology - Service management)

[12] ISO/IEC 19790:2012 (Information technology - Security techniques - Security requirements for cryptographic modules)

[13] ISO/IEC 15408:2009 (Information technology - Security techniques - Evaluation criteria for IT security)

[14] ISO/IEC 14598:2001 (Information technology - Software product evaluation)

[15] ISO/IEC TR 9126-4:2004 (Software engineering - Product quality)

國內法律

[16] 個人資料保護法（民國 99 年 5 月 26 日）

附錄一、技術要求事項與各國規範對照表

技術要求	OWASP 對應項目	美國 NIST [註 1]	歐洲 ENISA [註 2]	大陸 YD/T 2407-2013 [註 3]
4.1.1.1.行動應用程式發布	N/A	Executive Summary	9. Ensure secure distribution/provisioning of mobile Applications	5.5.2 應用軟件安全認證機制要求
4.1.1.2.行動應用程式更新	N/A	Executive Summary	9. Ensure secure distribution/provisioning of mobile Applications	5.5.4 預置應用軟件安全要求
4.1.1.3.行動應用程式安全性問題回報	N/A	Executive Summary	9. Ensure secure distribution/provisioning of mobile Applications	5.5.4 預置應用軟件安全要求
4.1.2.1.敏感性資料蒐集	N/A	4. Mobile App Evaluation - Privacy and Personally Identifiable Information	7. Pay specific attention to the collection and storage of consent for the collection and use of user’s data	5.5.4 預置應用軟件安全要求
4.1.2.2.敏感性資料利用	N/A	4. Mobile App Evaluation - Privacy and Personally Identifiable Information	7. Pay specific attention to the collection and storage of consent for the collection and use of user’s data	5.5.4 預置應用軟件安全要求 5.6.2 文件類用戶數據的授權訪問

技術要求	OWASP 對應項目	美國 NIST [註 1]	歐洲 ENISA [註 2]	大陸 YD/T 2407-2013 [註 3]
4.1.2.3.敏感性資料儲存	M2: Insecure Data Storage M4: Unintended Data Leakage M6: Broken Cryptography	4. Mobile App Evaluation - Protect Sensitive Data	1. Identify and protect sensitive data on the mobile device	5.6.3 用戶數據的加密存儲
4.1.2.4.敏感性資料傳輸	M3: Insufficient Transport Layer Protection	4. Mobile App Evaluation - Protect Sensitive Data	3. Ensure sensitive data is protected in transit	5.5.4 預置應用軟件安全要求 5.6.2 文件類用戶數據的授權訪問
4.1.2.5.敏感性資料分享	M5: Poor Authorization and Authentication	4. Mobile App Evaluation - Preserve Privacy	4. Implement user authentication and authorization and session management correctly	5.6.2 文件類用戶數據的授權訪問
4.1.2.6.敏感性資料刪除	N/A	N/A	1. Identify and protect sensitive data on the mobile device	5.6.4 用戶數據的徹底刪除
4.1.3.1.付費資源使用	N/A	N/A	8. Implement controls to prevent unauthorised access to paid-for resources	5.5.4 預置應用軟件安全要求

技術要求	OWASP 對應項目	美國 NIST [註 1]	歐洲 ENISA [註 2]	大陸 YD/T 2407-2013 [註 3]
4.1.3.2.付費資源控管	M5: Poor Authorization and Authentication	N/A	8. Implement controls to prevent unauthorised access to paid-for resources	5.5.4 預置應用軟件安全要求
4.1.4.1.使用者身分認證與授權	M5: Poor Authorization and Authentication	4. Mobile App Evaluation - Privacy and Personally Identifiable Information	4. Implement user authentication and authorization and session management correctly	5.6.2 文件類用戶數據的授權訪問
4.1.4.2.連線管理機制	M9: Improper Session Handling	4. Mobile App Evaluation – Network Events	4. Implement user authentication and authorization and session management correctly	5.5.4 預置應用軟件安全要求
4.1.5.1.防範惡意程式碼與避免資訊安全漏洞	M7: Client Side Injection M8: Security Decisions Via Untrusted Inputs	4. Mobile App Evaluation: Malicious Functionality Malware Detection Communication with Known Disreputable Sites Libraries Loaded	6. Secure data integration with third party services and Applications 10. Carefully check any runtime interpretation of code for errors	5.5.4 預置應用軟件安全要求
4.1.5.2.行動應用程式	M10: Lack of Binary	4. Mobile App	N/A	5.5.4 預置應用軟件安

技術要求	OWASP 對應項目	美國 NIST [註 1]	歐洲 ENISA [註 2]	大陸 YD/T 2407-2013 [註 3]
完整性	Protections	Evaluation – Classes Loaded		全要求
4.1.5.3.函式庫引用安全	M7: Client Side Injection M8: Security Decisions Via Untrusted Inputs	4. Mobile App Evaluation: Native Methods Libraries Loaded	6. Secure data integration with third party services and Applications	5.5.4 預置應用軟件安全要求
4.1.5.4.使用者輸入驗證	M7: Client Side Injection M8: Security Decisions Via Untrusted Inputs	4. Mobile App Evaluation – Input Validation	10. Carefully check any runtime interpretation of code for errors	5.5.4 預置應用軟件安全要求

[註 1] Vetting the Security of Mobile ApplicationsApp, NIST Special Publication 800-163, http://dx.doi.org/10.6028/NIST.SP.800-163, 2015

[註 2] Smartphone Secure Development Guidelines for App Developers, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/smartphone-security-1/smartphone-secure-development-guidelines, ENISA, 2011

[註 3] 移動智慧終端安全能力技術要求, YD/T 2407-2013, 2013

附錄二、技術要求事項參考檢核表

項次	序號	技術要求
4.1.1.1.行動應用程式發布	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，且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	2	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。
	3	行動應用程式應提供更新機制，並於有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	行動應用程式開發者應提供回報安全性問題之管道。
	5	行動應用程式開發者應於適當之期間內回覆問題並改善。
4.1.2.1.敏感性資料蒐集	6	行動應用程式應於蒐集敏感性資料前，取得使用者同意，並提供使用者拒絕之權利。
4.1.2.2.敏感性資料利用	7	行動應用程式應於使用敏感性資料前，取得使用者同意，並提供使用者拒絕之權利。
	8	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。
	9	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	10	行動應用程式應於儲存敏感性資料前，取得使用者同意，並提供使用者拒絕之權利。
	11	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，並避免將敏感性資料儲存於暫存檔或紀錄檔中。
	12	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。

項次	序號	技術要求
	13	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。
	14	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	15	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	16	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，並提供使用者拒絕之權利。
	17	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	18	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。
4.1.3.1.付費資源使用	19	行動應用程式應於使用付費資源前主動通知使用者，並提供使用者拒絕之權利。
4.1.3.2.付費資源控管	20	行動應用程式應於使用付費資源前進行使用者認證，並記錄使用之付費資源與時間。
4.1.4.1.使用者身分認證與授權	21	行動應用程式應有適當之身分認證機制，確認使用者身分，並依使用者身分授權。
4.1.4.2.連線管理機制	22	行動應用程式應避免使用具有規則性之交談識別碼。
	23	行動應用程式應確認伺服器憑證之有效性，且為可信任之憑證機構、政府機關或企業之簽發。
	24	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

項次	序號	技術要求
		料。
4.1.5.1.防範惡意程式碼與避免資訊安全漏洞	25	行動應用程式應避免含有惡意程式碼。
	26	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	27	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	28	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	29	行動應用程式應針對使用者輸入之字串，進行安全檢查並提供相關注入攻擊防護機制。