經濟部工業局
行動應用App基本資安自主檢測推動制度
V1.0

經濟部工業局

104 年 7 月

目　　次

第一部份：

行動應用App基本資安自主檢測推動制度規章

背景

因應行動裝置之普及、各種類型的行動應用程式與民眾生活已密不可分，然而部分開發者缺乏資安意識，導致使用者面臨資料外洩或財產損害。值此，經濟部工業局依據「行政院國家資通安全會報第 26 次委員會議」決議，規劃制訂資安檢測標準及鼓勵廠商自主驗證等業務。目前已於民國 104 年 4 月公告「行動應用 App 基本資安規範」作為推動行動應用 App 資安檢測機制之基礎。為落實基本資安規範，經濟部工業局續專案計畫委託財團法人資訊工業策進會，制訂本「行動應用 App 基本資安自主檢測推動制度規章」，作為推動我國行動應用 App 自主檢測制度發展之依據。

1. 制度目的

1.1. 落實「行動應用 App 基本資安規範」，制定行動應用 App 資安檢測標準，鼓勵開發商、平台業者遵循。

1.2. 建立行動應用 App 安全標章，使消費者易於識別通過本推動制度檢測之行動應用 App。

1.3. 推動行動應用 APP 資安自主檢測推動制度，建構行動應用 App 安全。

2. 適用範圍

2.1. 本推動制度採自願性參與，依據「行動應用 App 基本資安規

範」，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。

2.2. 本規章設立制度管理委員會，以管理、維護整體制度之運作。認證機構負責認證檢測實驗室之資格。檢測實驗室負責受理行動應用 App 資安檢測，並出具檢測合格報告。行動應用 App 依據檢測合格報告，可向制度管理委員會申請行動應用 App 安全標章之使用。

2.3. 於試辦期內，本規章得隨時依委託機關要求及試辦狀況修訂之。

3. 定義

3.1. 「行動應用 App 基本資安標章」（Mobile Application Security 標章，簡稱 MAS 標章），係表彰行動應用 App 檢測符合「行動應用 App 基本資安檢測基準」之證明。

3.2. 認驗證合格登錄管理網站：簡稱「管理網站」，由制度管理委員會設立之公開網站，登錄公告認證機構、合格檢測實驗室名單及通過檢測、授予檢測合格標章之行動應用 App，並提供檢測合格標章之網路查驗功能。

3.3. 認證：認證機構對特定人或特定機關 (構) 給予正式認可，證明其有能力執行特定工作之程序。

3.4. 驗證：由檢測實驗室出具書面證明特定產品或服務能符合規定要求之程序。

3.5. 行動應用 App：是一種設計給智慧型手機、平板電腦和其他行動裝置使用的應用程式。

3.6. 行動應用程式商店(Application Store)：提供行動裝置使用者下載使用行動應用 App 之平台。

3.7. 試辦期：自民國 104 年 10 月 1 日至民國 105 年 9 月 30 日為期 1 年，經濟部工業局保留變更試辦期之權利。

4. 自主檢測體系

4.1. 制度管理委員會：由經濟部工業局指定成員組成，負責管理、維護及執行本自主檢測推動制度之單位。亦負責行動應用 App 基本資安標章之授權及查核、管理網站之維運。

4.2. 認證機構：符合第 6 條規範，負責認證檢測實驗室是否具備足夠之行動應用 App 資安檢測能力。

4.3. 檢測實驗室：符合第 7 條規範，受理行動應用 App 開發者申請，依據「行動應用 App 基本資安檢測基準」，提供行動應用 App 開發者資安檢測服務之單位。

4.4. 行動應用 App 開發者：係指開發、設計、維護行動應用 App 者。於委託開發時，委託人得視為開發者。

5. 制度管理委員會

5.1. 制度管理委員會之成員，由經濟部工業局指定之。

5.2. 制度管理委員會之任務如下：

a. 制度維運與規範增修

b. 檢測實驗室管理

c. MAS 標章之授權與管理

d. 自主檢測推動制度之教育訓練與宣傳推廣

6. 認證機構

6.1. 資格：經由經濟部工業局指定，為國內合法設立之公益法人或產業公協會，並至少具備下列資格之一，有能力執行檢測實驗室認證服務之單位。

a. 依國際標準組織之標準建立認證制度，並據以實施認證業務。

b. 已簽署國際或區域認證組織相互承認協議者。

c. 具備相當之產業或認證業務經驗者。

7. 檢測實驗室

7.1. 資格認證：檢測實驗室由認證機構依據「檢測實驗室資格認證及管理規範」認證之。<u>於試辦期內，由制度管理委員會選任專家審查之。</u>

7.2. 合格效期：

7.2.1. 於試辦期內取得認可之有效期限至試辦期結束後3個月。檢測實驗室應於前述期間屆至前取得正式資格。

7.2.2. 檢測實驗室之認可有效期限為 3 年,並應經制度管理委員會登錄公告之。

7.2.3. 其他管理事項，依據「檢測實驗室資格認證及管理規範」辦理。

8. 申請程序

8.1. 檢測實驗室資格申請流程，詳參附錄一。

8.2. 行動應用 App 開發者申請認證標章流程，詳參附錄二。

9. 行動應用 App 基本資安標章（MAS 標章）

9.1. 經檢測實驗室依據「行動應用 App 基本資安檢測基準」驗證合格之行動應用 App，開發者可向制度管理委員會申請核發 MAS 標章。於試辦期內，制度管理委員會以發放合格證書替代之。

9.2. MAS 標章依「行動應用 App 基本資安檢測基準」,將檢測安全等級區分為三級：

a. 初級：檢測功能相關之安全性。

b. 中級：檢測連網安全性(含初級)。

c. 高級：檢測交易相關之安全性(含中級)。

9.3. 登載公告：通過檢測並取得標章之行動應用 App，應登錄並公告於管理網站。

9.4. 使用效期：MAS 標章於下列情形之一時，失其效力。

a. 行動應用 App 之名稱或程式版本變更時。

b. 「行動應用 App 基本資安檢測基準」修訂時。

c. 有違反「行動應用 App 基本資安標章使用與管理規範（待擬）」之情事時。

9.5. 其他標章管理事項：依據「行動應用 App 基本資安標章使用與管理規範（待擬）」辦理之。

10. 版本控制

當行動應用 App 開發者變更其 App 版本時，應於上架至行動應用程式商店前，重新送檢測實驗室驗證。

11. 資訊控制

當行動應用 App 之名稱、所有權等資訊有變更時，應即通知制度管理委員會。

12. 追蹤管理

制度管理委員會得定期或不定期以普查或抽測之方式，查驗行動應用 App 通過版本與行動應用程式商店之版本是否相符。

13. 費用

13.1. 自主檢測推動制度之費用包含申請費、認證費、證書費、檢測費、檢測合格標章授權費。

13.2. 檢測實驗室之認證費，由認證機構公告收取之。

13.3. 檢測費由各檢測實驗室公告並收取之。

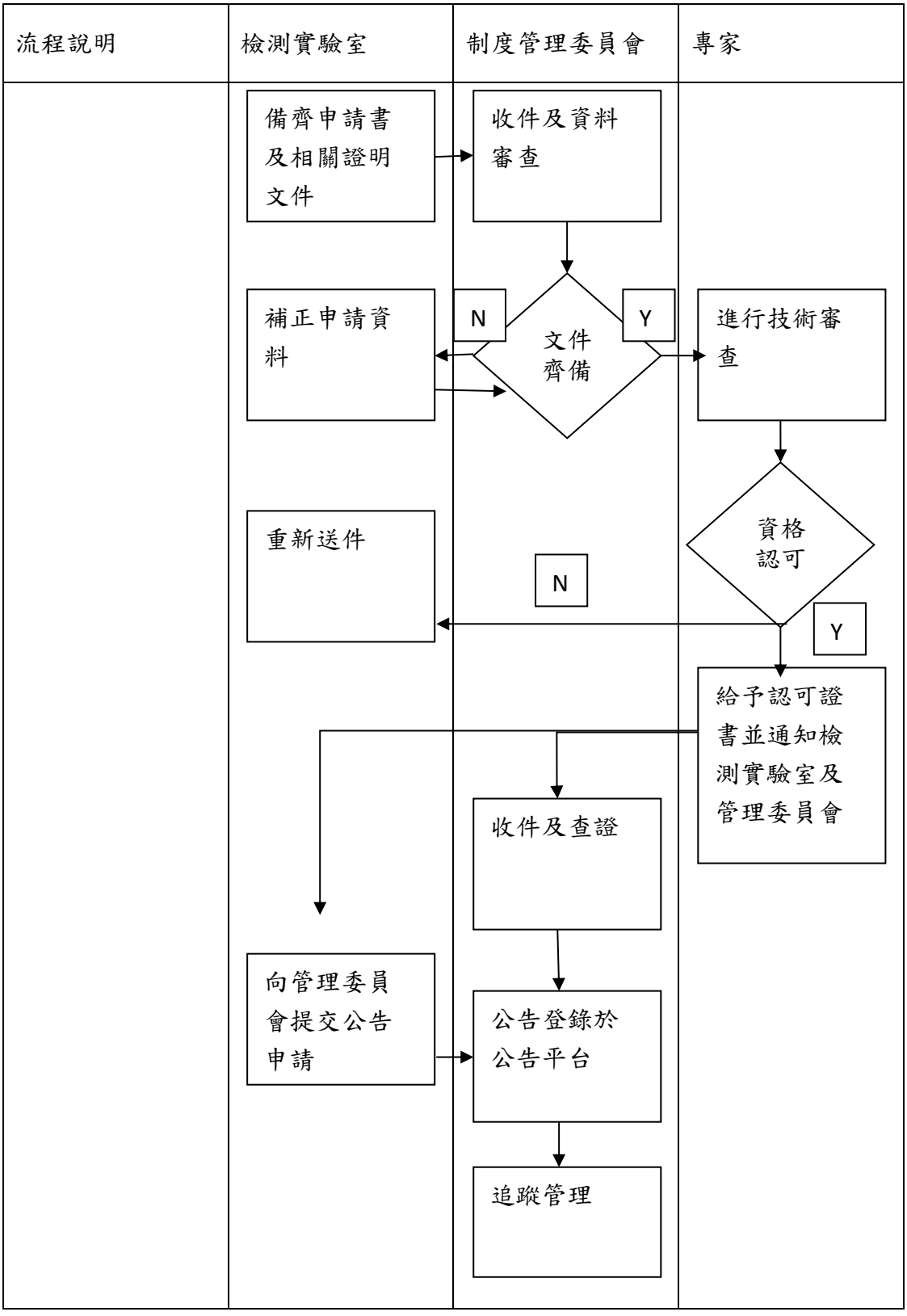
13.4. 其他各種費用由制度管理委員會公告並收取之。

14. 試辦期後之轉換

試辦期結束後，本規章將依委託機關檢討決定修訂之，有關試辦期結束後之認驗證轉換作業，另依委託機關決定並公告之。

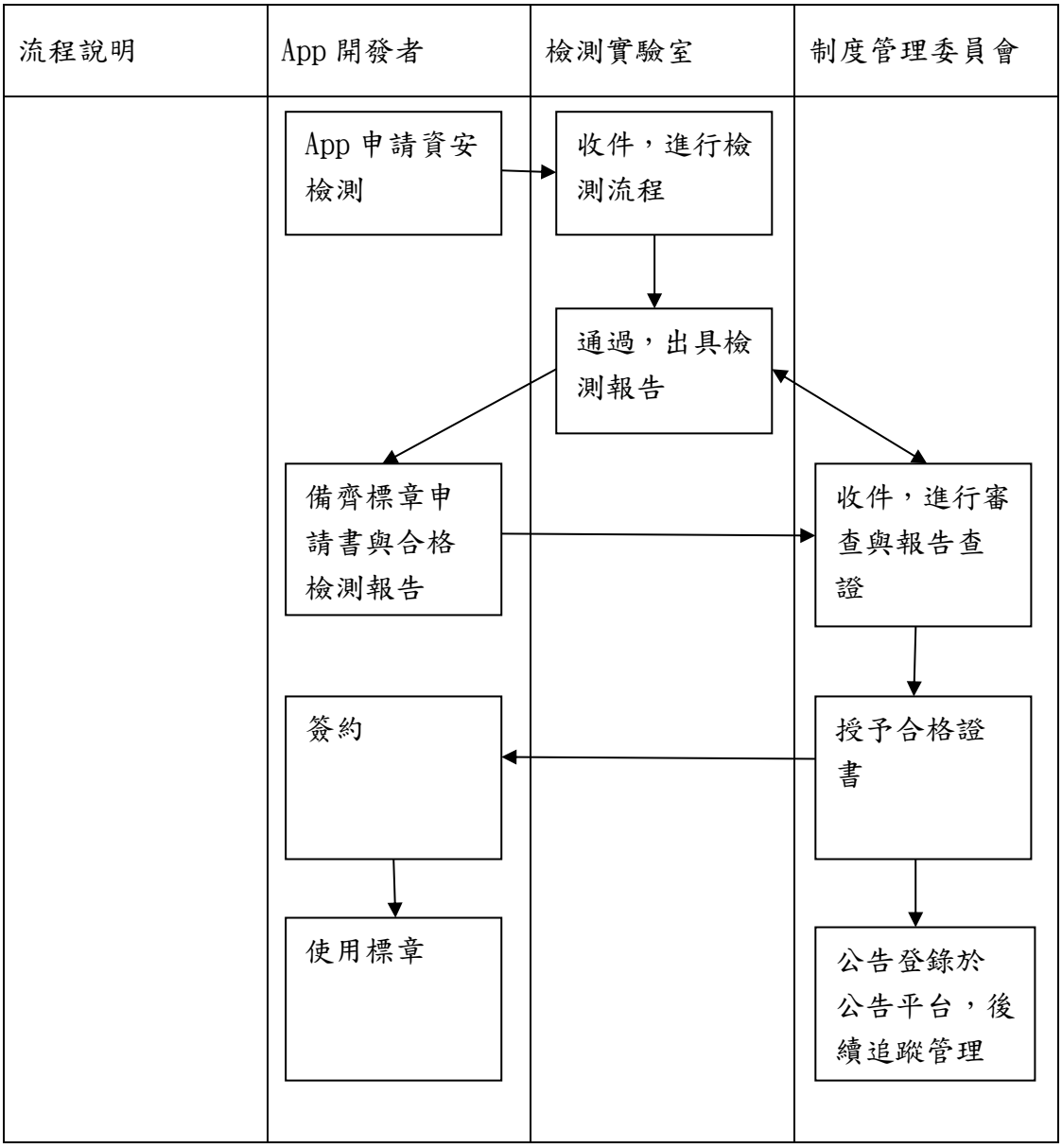
附錄一、檢測實驗室資格認證申請流程

（本流程適用於試辦期，於試辦期後將綜合檢討之。）



附錄二、行動應用 App 開發者申請 MAS 標章流程

（本流程適用於試辦期，於試辦期後將綜合檢討之。）



第二部份：

行動應用 App 檢測實驗室資格認證及管理規範

1. 基本原則

1.1. 依據「行動應用 App 基本資安自主檢測推動制度規章」第 7 條，有關檢測實驗室之資格及管理事宜，依本規範之規定。但認證機構有特別規定時，從其規定。

1.2. 凡國內合法登記之法人或學術研究機構所屬檢測實驗室，具備一定專業條件、依其管理系統從事有關行動應用 App 之測試、檢驗工作，並出具報告者，皆可由法人代表人或機構負責人向認證機構提出申請，由認證機構進行認可程序。

1.3. 試辦期內，應向制度管理委員會提出認可申請，認可程序由制度管理委員會選任專家執行之。

2. 檢測實驗室認可程序審查

檢測實驗室之認可程序，應審查下列各款事項：

2.1. 認證機構之檢測實驗室認證申請書。於試辦期內，採用附錄一之檢測實驗室(試辦期)認證申請書。

2.2. 依法設立之本國法人、機構之證明文件影本。

2.3. 可資證明檢測實驗室能力文件。

2.3.1. 檢測實驗室資格：需具備本國或國際認證組織核發之實驗室認證證明 CNS 17025 或 ISO/IEC 17025。於試辦期得以提出「行動應用 App 基本資安檢測服務計畫書」替代之。前述計畫書內容應載明其具備之實驗室管理程序，包括：

檢測方法及流程、檢測設備及軟體工具、檢測結果品質管理程序等，由制度管理委員選任專家審查。

2.3.2. 人員資格：檢測實驗室基本成員以分權負責原則，應設置有實驗室主管、品質主管及報告簽署人等正式員工至少 3 人。其資格應符合下列要求：

2.3.2.1. 實驗室主管：大學以上且具資訊安全相關管理職經驗 2 年以上，並具備實驗室認證規範 ISO/IEC 17025 或 CNS 17025 訓練合格證書。

2.3.2.2. 品質主管：大學以上且具品質管理或稽核相關工作經驗 2 年以上，並具備品質管理或稽核相關訓練合格證書。

2.3.2.3. 報告簽署人：大學以上且具資訊安全相關工作經驗 3 年以上，並依以下條件具備資訊安全相關專業證照：

a. 具備道德駭客認證(Certified Ethical Hacker, CEH) 或安全基礎認證(GIACSecurity Essentials, GSEC)。

b. 具備下列證照之一：資訊系統安全專家認證(Certified Information Systems Security Professional, CISSP)、或資安分析專家認證(EC-Council Certified Security Analyst, ECSA)、或資安鑑識調查專家認證(EC-Council Computer Hacking Forensic Investigator, CHFI)、或滲透測試專家認證(GIAC Penetration Tester,GPEN)、或行動裝置安全性分析專家認證

(GIAC Mobile Device Security Analyst,GMOB)或行動審驗專職認證(Certificate of Application Vetting Professional,CAVP)。

c. 其他經制度管理委員會公告認可之證照。

2.3.2.4. 試辦期內之人員資格：檢測實驗室成員以分權負責原則，應設置實驗室主管、品質主管及報告簽署人等正式員工至少 3 人。檢測實驗室成員之資訊安全及管理相關專業資格，需符合以下條件，不限是否為同一人：

a. 應至少有一人具備實驗室認證規範 ISO/IEC 17025 或 CNS 17025 訓練合格證書。

b. 應至少有一人具備道德駭客認證(Certified Ethical Hacker, CEH)。

c. 應至少有一人具備以下認證資格之一：資訊系統安全專家認證 (Certified Information Systems Security Professional, CISSP)、或資安分析專家認證(EC-Council Certified Security Analyst, ECSA)、或資安鑑識調查專家認證(EC-Council Computer Hacking Forensic Investigator, CHFI)、或行動審驗專職認證(Certificate of Application Vetting Professional, CAVP)。

2.3.3. 執行實績：於 3 年內有 2 件（含）以上，檢測行動應用

App 資安之實際經驗，需具備證明文件備查（如客戶端合約或訂單、檢測報告等）。

3. 補正期間

第 2 條各款文件有不全或記載不完備者，認證機構應通知限期補正，屆期未補正或補正不完備者，不予受理其申請。補正期間以 1 個月為限。

4. 檢測實驗室認證證書

檢測實驗室經認證機構審查符合資格者，由認證機構核發「檢測實驗室認證證書」（以下簡稱認證證書）。於試辦期內，檢測實驗室經管理委員會選任專家認可後，由制度管理委員會核發認證證書（格式如附錄二），認證證書應記載事項如下：

a. 法人/機構名稱。

b. 代表人/負責人。

c. 實驗室名稱。

d. 實驗室地址。

e. 有效期間。

5. 檢測實驗室人員守密原則

檢測實驗室或其服務人員對於申請者及檢測相關資料，應嚴守秘密，退職人員亦同。

6. 檢測實驗室費用原則

檢測實驗室所報之檢測費用，應符合透明、公平之原則。

6.1. 檢測費用應依行動應用 App 開發者申請標章之類別至少分為 3 個等級。

6.2. 檢測實驗室通知行動應用 App 開發者未符合規定時，應列舉不符合事項並通知開發者改善，通知改善方式及收費機制由檢測實驗室自訂。

7. 檢測實驗室之權利義務

檢測實驗室通過認證後，應遵守下列義務：

7.1. 檢測實驗室，應維持檢測品質及技術能力，以符合第 2 條各項條件之要求。

7.2. 檢測實驗室出具之資安檢測報告不得有虛偽不實，或經制度管理委員會抽驗認定不合格。

7.3. 檢測實驗室受理檢測申請案件，應秉持公平、公正、獨立之立場，無正當理由不得拒絕受理、給予差別待遇或有違反公正性、公平性之行為。

7.4. 檢測實驗室與其受理測試之行動應用 App 開發者間，不得有妨害檢測制度公正性之關係。

7.5. 有違反 7.1~7.4 之情況時，制度管理委員會得公告於管理網站，並通知認證機構撤銷認證證書。於試辦期內，由管理委員會撤銷之。

7.6. 檢測實驗室應接受及配合認證機構安排之定期或不定期之監督評定、查訪、訪談、重新評鑑等作業，提供作業順利完成所需之必要協助。對前述作業，制度管理委員會得定期或不定期抽查複核之。

7.7. 檢測實驗室下列相關資訊之異動，應通知認證機構，並於異動發生日起 15 日內通知管理委員會。

a. 所有權、名稱或地址之異動

b. 機構負責人之異動

c. 認證證書內記載事項之變動

d. 業務終止或停業

7.8. 前項異動，如檢測實驗室未依期限告知管理委員會，管理委員會必要時得通知認證機構撤銷認證證書。

7.9. 當行動應用 App 開發者以其開發程式之原始碼送測時，檢測實驗室應將原始碼檔案內容妥善封存，確保送測行動應用 App 版本之正確性與一致性，不受竄改與損壞。

8. 試辦期

試辦期自民國 104 年 10 月 1 日至民國 105 年 9 月 30 日為期 1 年，經濟部工業局保留變更試辦期之權利，規範內容將依試辦情況與委託機關之要求檢討修訂之。

附錄一、檢測實驗室(試辦期)認證申請書

行動應用 App 資安檢測實驗室認證申請書

申請日期：____年____月____日　　受理編號：___

法人/機構名稱					
代表人/負責人					
實驗室名稱					
實驗室地址					
本國實驗室認證組織之認證證書	證書證號		有效期間		
相關檢測實績描述					
具備之檢測環境					
管理及檢測人員資格					
聯絡人		地址			
電話		傳真		電子信箱	

檢附文件：

☐ 1.法人/機構之登記證明文件影本。

☐ 2.本國實驗室認證組織之認證證明文件影本。

☐ 3.向本國實驗室認證組織申請檢測實驗室認證時，所檢附相關資料之光碟片。

☐ 4.其他經管理委員會指定者。

本實驗室如因提供資訊不實造成損害，願依相關法律負起責任。

謹　此

法人/機構印鑑章：_____ 代表人/負責人簽章：_____

附錄二、檢測實驗室認證證書

行動應用 App 資安檢測實驗室認證證書

證書號碼：

一、 法人/機 構名稱：

二、 代表人/負責人：

三、 實驗室名稱：

四、 實驗室地址：

五、 有效期間：自 年 月 日至 年 月 日止

認證機構（試辦期為行動應用 App 自主檢測推動制度管理委員會）

中 華 民 國 年 月 日