行動應用App基本資安自主檢測推動制度

V4.2

經濟部工業局

中華民國 109 年 08 月

行動應用 App 基本資安自主檢測推動制度版本沿革

日期	行動應用 App 基本資安自主檢測推動制度版本沿革
104 年 8 月	行動應用 App 基本資安自主檢測推動制度 V1.0
105 年 2 月	行動應用 App 基本資安自主檢測推動制度 V2.0
106 年 3 月	行動應用 App 基本資安自主檢測推動制度 V3.0
107 年 8 月	行動應用 App 基本資安自主檢測推動制度 V4.0
108 年 9 月	行動應用 App 基本資安自主檢測推動制度 V4.1
109 年 8 月	行動應用 App 基本資安自主檢測推動制度 V4.2

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 App 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 109 年 8 月將「行動應用 App 基本資安規範」之版本更新至 V1.3，以作為推動行動應用 App 資安檢測機制之基礎。民國 108 年 9 月，為落實基本資安規範，經濟部工業局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，修訂本「行動應用 App 基本資安自主檢測推動制度規章」至 V4.1，並於民國 109 年 8 月更新修訂至 V4.2，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 基本資安檢測標準，鼓勵開發商、平台業者遵循。

   1.2. 建立「行動應用 App 基本資安標章」（Mobile Application Basic Security 標章，簡稱 MAS 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 基本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」，適用於非特定領域及「行動應用 App 基本資安規範」中所有類別之行動應用程式。

   2.2. 本規章設立制度推動委員會，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 基本資安檢測，出具檢測合格報告，可向制度推動委員會或其授權機構申請檢測合格證明或 MAS 標章之使用。

3. 定義

3.1. 行動應用 App 基本資安標章：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. 合格登錄管理網站：簡稱「管理網站」，由制度推動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程式。

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：由合格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. 行動應用程式：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」。

3.6. 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。

4. 自主檢測體系

4.1. 行動應用資安聯盟：使得資安自主檢測機制更加完善，提升國內行動應用 App 資訊安全。

4.2. 行動應用資安制度推動委員會：負責管理、維護及執行本自主檢測推動制度之單位。亦負責 MAS 標章之授權及查核、管理網站之維運。

4.3. 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 基本資安檢測能力。

4.4. 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。

4.5. 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. 行動應用資安聯盟

負責推動我國行動應用 App 相關產業發展，使得資安自主檢測機制更加完善，培育行動應用資安產業人才，提升國內行動應用 App 資訊安全，拓展國內外商機。

6. 行動應用資安制度推動委員會

6.1. 行動應用資安制度推動委員會以下簡稱制度推動委員會。

6.2. 制度推動委員會隸屬於行動應用資安聯盟，其成員由行動應用資安聯盟選任之。

6.3. 制度推動委員會之任務如下：

a. 推動行動應用 App 基本資安規範及驗證制度。

b. 協助政府推廣行動應用 App 之產業政策，並辦理制度維運與規範增修、合格檢測實驗室管理及檢測報告審查、合格證明及 MAS 標章之授權與管理、教育訓練、國際合作、推廣活動等事項。

7. 認證機構

本制度之認證機構為財團法人全國認證基金會（Taiwan Accreditation Foundation，簡稱 TAF）。

8. 檢測實驗室

8.1. 資格認證：檢測實驗室應由認證機構依據「行動應用 App 基本資安檢測實驗室資格認證及管理規範」認證合格，認可有效期限為 3 年。

8.2. 檢測實驗室之權利義務：

8.2.1. 檢測實驗室應向制度推動委員會申請登錄，經制度推動委員會審查認可後登錄公告之，申請流程詳參附錄一，相關登錄申請書與權利義務規章詳參附錄二與附錄三。

8.2.2. 其他管理事項，依據「行動應用 App 基本資安檢測實驗室資格認證及管理規範」辦理。

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」檢測合格之行動應用 App，開發者可向制度推動委員會或經制度推動委員會授權之檢測實驗室申請核發 MAS 標章，申請流程詳參附錄四，相關標章使用申請書與標章使用權利義務規章詳參附錄五與附錄六。於 MAS 標章未通過證明標章申請前，得發放合格證明替代之。

9.2. MAS 標章依「行動應用 App 基本資安檢測基準」，將行動應用程式區分為三類：

a. 「L1」行動應用程式：無需使用者身分鑑別之應用程式。

b. 「L2」行動應用程式：需使用者身分鑑別之應用程式。

c. 「L3」行動應用程式：含有交易行為之應用程式。

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 標章使用效期為 1 年，並於下列情形之一時，制度推動委員會得停止或終止其效力：

a. 有違反「行動應用 App 基本資安標章使用與管理規範」之情事時。

b. 違反標章使用權利義務規章之規定時。

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」辦理之。

10. 資訊控制

當行動應用 App 之名稱、所有權等資訊有變更時，行動應用 App 開發者應即通知制度推動委員會。

11. 追蹤管理

制度推動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。

12. 費用

12.1.自主檢測推動制度之費用包含認證費、檢測費、合格證明申請費等各項行政管理費用。

12.2.檢測實驗室之認證費，由認證機構公告收取之。

12.3.檢測費由各檢測實驗室收取之。

12.4.合格證明申請費及其他各種費用由制度推動委員會公告並收取之。

第二部份：

行動應用App基本資安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。

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。

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。

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：大專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：大專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：大專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（GIAC Security 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）、或資安軟體開發專家認證（Certified Secure Software Lifecycle Professional，CSSLP）、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）。

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。補正期間以認證機構通知為準。

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）。

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 App 開發者申請之行動應用程式所屬之類別至少分為 3 個類別。

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。

6.3. 檢測實驗室應依制度推動委員會所公告之合格證明費等各項行政管理費用，並代制度推動委員會收取之。

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，或經制度推動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，制度推動委員會得公告於管理網站，並通知認證機構撤銷認證證書。

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，制度推動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 日內通知制度推動委員會。

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制度推動委員會，制度推動委員會必要時得通知認證機構撤銷認證證書。

7.9. 檢測實驗室應將送測之行動應用 App 檔案封存，並至少保存 1 年，確保送測行動應用 App 版本之正確性，不受竄改與損壞。於有抽測之必要時，制度推動委員會得請檢測實驗室提供檢測實驗室封存之 App 原始檔案資料。

7.10.如有實驗室主管、品質主管、報告簽署人之人事異動，檢測實驗室應主動告知行動應用資安聯盟秘書組。

8. 檢測實驗室訪視原則

8.1. 新進檢測實驗室於取得 20 件（含）以上之申請案件並取得標章後，會於 3 個月內進行訪視。

8.2. 若檢測實驗室於 6 個月內無受理任何申請案件，行動應用資安聯盟秘書組須於接下來 1 個月內進行實地訪視以了解實驗室狀況。

8.3. 其餘相關狀況依 TAF 規定，由行動應用資安聯盟秘書組配合辦理。

9. 檢測實驗室績效評核辦法

確保檢測實驗室對 App 檢測品質之一致性，以及鼓勵檢測實驗室積極參與聯盟活動，透過「績效評核」計點方式，評核出優質之檢測實驗室，預計每年第二、三季執行，視抽測之 App 總量而定。相關辦法詳餐附錄七。

第三部份：

行動應用App基本資安標章使用與管理規範

1. 基本原則

1.1. 依據「行動應用 App 自主檢測推動制度規章：9.行動應用 App 基本資安標章」，有關標章之管理事項，依本規範之規定。

1.2. 為明確「行動應用 App 基本資安標章」之申請核發與管理事宜，特訂定本規範。

2. 名詞定義

2.1. 本規範未特別規定者，均依「行動應用 App 自主檢測推動制度規章」及「行動應用 App 基本資安規範」之規定為準。

2.2. 「行動應用 App 基本資安標章」（Mobile Application Basic 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. 標章之核發與使用

3.1. 標章核發

3.1.1. 通過認證之檢測實驗室負責行動應用 App 基本資安驗證，對於通過驗證之行動應用 App 出具合格檢測報告與證明，並通報制度推動委員會。行動應用 App 之開發者通過驗證後，得填寫 MAS 標章使用申請書與權利義務規章，向制度推動委員會申請 MAS 標章之使用。

3.1.2. 制度推動委員會應就 3.1.1 之申請進行審核，如有審核不通過或需補正者，另應通知申請人。

3.2. 標章使用

3.2.1. 開發者應依制度推動委員會所規定之樣式，於行動應用程式商店之網站頁面上使用 MAS 標章，不得改變形狀、顏色或加註字樣，如需為其他使用方式，應另以例外需求使用申請書向制度推動委員會申請。

3.2.2. 不得將 MAS 標章用於證明標章以外之用途。

3.2.3. 制度推動委員會應將授予 MAS 標章之行動應用 App，公

告於管理網站供查詢。

4. 標章之更新與資訊通知

4.1. 使用效期：MAS標章使用效期為1年，並於下列情形之一時，制度推動委員會得停止或終止其效力：

a. 違反本規範關於標章使用、更新與追蹤管理之規定時。

b. 違反標章使用權利義務規章之規定時。

4.2. 行動應用 App 之名稱或程式版本變更時，該更名或版本變更之行動應用 App 如欲使用標章，應重新依本規範申請之。

4.3. 當行動應用 App 之名稱、所有權等資訊有變更時，應即通知制度推動委員會。

5. 標章之追蹤管理

5.1. 制度推動委員會得自行或委託檢測實驗室，定期或不定期以普查或抽查之方式，確認行動應用 App 通過檢測之版本與使用標章之版本是否相符，如未相符，則應停止標章使用權。

5.2. 行動應用 App 之開發者如知悉其取得 MAS 標章之行動應用App，可能導致行動裝置遭受不當存取，或個人資料之外洩、竄改、毀損或滅失之風險時，應通知制度推動委員會。

5.3. 制度推動委員會知有 5.2 之情形，應對該行動應用 App 進行複檢，如該行動應用 App 確有可能導致行動裝置遭受不當存取，或個人資料之外洩、竄改、毀損或滅失之風險時，應停止標章使用權，並命行動應用 App 之開發者限期改善，若屆期未改善者，應終止標章使用權。

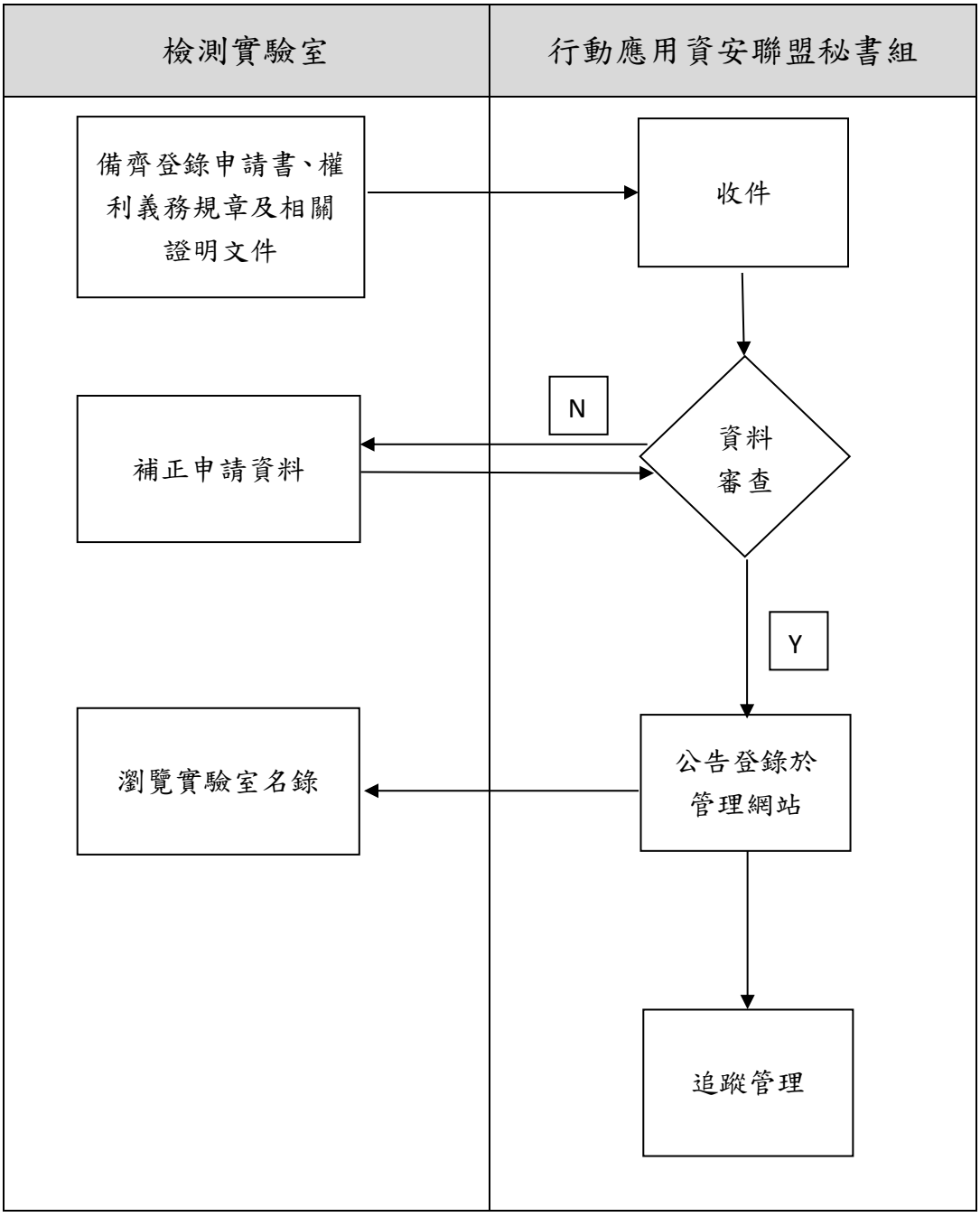
6. 費用

6.1. 檢測費由各檢測實驗室公告並收取之，並應參照「行動應用 App 檢測實驗室資格認證及管理規範」「6.檢測實驗室費用原則」收取。

6.2. 各項行政管理費用，由制度推動委員會公告並收取之。

附錄

附錄一、檢測實驗室資格認證申請流程



附錄二、「行動應用 App 基本資安檢測實驗室」登錄申請書

本公司（以下稱申請機構）茲向「行動應用資安聯盟秘書組）申請登錄為「行動應用 App 基本資安檢測實驗室」，同意接受條款如下：

一、申請機構之基本資訊：

機構全名	
機構負責人	
機構地址	
實驗室名稱	
實驗室主管	
實驗室地址	
TAF 認證編號	
對外連絡窗口	姓名： 電話：　　分機 傳真： e-mail：

二、申請機構同意並知悉「行動應用 App 基本資安檢測實驗室權利義務規章」（如附件）構成雙方權利義務規範。

三、申請機構授權本申請書第一條所載之檢測實驗室主管，代表申請機構及檢測實驗室，並負監督檢測實驗室遵守委員會所訂規章之責。

四、申請機構同意本申請書第一條所載之資訊可供委員會各項對外公告、通知服務、相關訊息寄送等用途，申請機構確認前述所載之實驗室主管及聯絡人已獲知且瞭解上述事項，並同意前述所列蒐集目的範圍內，合理蒐集、處理及利用前述資料。本申請書第一條所載之資訊有異動時，將於異動發生日起 15 日內通知委員會。

此致

行動應用資安聯盟 秘書組

申請機構印鑑	申請機構負責人簽名或蓋章

申請日期：民國　　年　　月　　日

「行動應用 App 基本資安檢測實驗室」權利義務規章為本申請書之一部份，請併同本申請書用印

附錄三、「行動應用 App 基本資安檢測實驗室」權利義務規章

申請機構（以下或稱檢測實驗室）茲向「行動應用資安制度推動委員會」（以下簡稱制度推動委員會）申請登錄為「行動應用 App 基本資安自主檢測推動制度」（以下簡稱本推動制度）之「行動應用 App 基本資安檢測實驗室」（以下簡稱檢測實驗室），同意遵守以下條款：

1. 檢測實驗室之意義

本規章所稱之檢測實驗室，係指向「財團法人全國認證基金會」（以下簡稱 TAF）申請「行動應用 App 基本資安檢測實驗室認證服務計畫」且獲得 TAF 認可之「行動應用 App 基本資安檢測實驗室」。

2. 制度推動委員會之權利義務

2.1. 制度推動委員會因主管機關或制度推動委員會公告之規範或要求得隨時變更本規章，因此而直接涉及申請機構之部分，應於合理期間內告知申請機構。申請機構於收到通知後，不即為反對表示者，視為同意該項變更。

2.2. 制度推動委員會應將合格證書所登載資訊，公告於制度推動委員會網站或以其他方式對外公告之。

3. 申請機構之權利義務

3.1. 申請機構應據實提出相關認證或其他相類似作業所需文件，並配合制度推動委員會定期或不定期之監督、查訪、訪談、抽驗等作業要求提供相關資訊，如經發現申請機構所提供之資訊不實或不足，制度推動委員會得通知認證機構撤銷合格證書，如因陳述不實或疏漏而造成損害，應負賠償責任。

3.2. 制度推動委員會因提供申請機構登錄而遭任何第三人求償時，申請機構應就該等求償負責。

3.3. 申請機構下列相關資訊之異動，應於異動發生日起 15 日內通知制度推動委員會。

a. 機構名稱或地址之異動

b. 機構負責人之異動

c. 實驗室名稱或地址之異動

d. 實驗室主管之異動

e. 合格證書內記載事項之變動

f. 業務終止或停業

3.4. 前項異動，如申請機構未依期限告知制度推動委員會，制度推動委員會必要時得通知認證機構撤銷合格證書。

4. 檢測實驗室之權利義務

4.1. 檢測實驗室應維持品質系統及技術能力，以符合制度推動委員會所訂

之規範與要求。

4.2. 檢測實驗室應接受制度推動委員會之定期或不定期之監督、查訪、訪談、抽驗等作業，並配合制度推動委員會要求提供所需相關資訊、場地、人員及完成作業所需之必要協助。

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

4.4. 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。

4.5. 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。

4.6. 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。

4.7. 有違反 4.1~4.6 之情況時，制度推動委員會得公告並通知認證機構撤銷合格證書。

4.8. 檢測實驗室應將送測之行動應用 App 檔案封存，並至少保存 1 年，確保送測行動應用 App 版本之正確性，不受竄改與損壞。於有抽測之必要時，制度推動委員會得請檢測實驗室提供檢測實驗室封存之 App 原始檔案資料。

5. 檢測實驗室費用原則

5.1. 檢測實驗室所報之檢測費用，應符合透明、公平之原則。

5.2. 檢測費用依公告最新版「行動應用 App 基本資安檢測基準」所定義之 3 個行動應用程式類別及其對應檢測項目，由各檢測實驗室公告並收取之。

5.3. 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。

5.4. 檢測實驗室應依制度推動委員會所公告之各項行政管理費用，並得經制度推動委員會授權代制度推動委員會收取之。

6. 檢測合格證明與標章

6.1. 檢測實驗室須依據本推動制度或制度推動委員會所公告之「行動應用 App 基本資安檢測合格證明」與標章管理規定辦理。

6.2. 檢測實驗室須依據通過「行動應用 App 基本資安檢測基準」所定義該行動應用程式類別應檢測所有項目之檢測報告，發放「行動應用 App 基本資安檢測合格證明」。

6.3. 檢測合格證明之應記載事項如下，證明書格式由制度推動委員會設計印製：

a. 證書編號（依制度推動委員會規定之編碼原則，如：實驗室之 TAF 認證編號、民國年與流水號）

b. 申請單位名稱

c. App 名稱、App 版本

d. 行動應用 App 基本資安檢測基準版本、行動應用程式類別

e. 證書效期（發證日起一年）

f. 檢測實驗室名稱

g. 檢測日期（檢測實驗室出具檢測報告日期）

6.4. 由制度推動委員會發放之檢測合格證明（正本乙份），收取相關審查費用。

7. 智慧財產歸屬

7.1. 申請機構授權制度推動委員會得因於認證、抽驗或其他相類似作業之需要，無償使用該申請機構所交付之文件或物品。

7.2. 除非雙方另有書面約定，凡在申請機構於申請之前即已存在的智慧財產不受本文件的影響。

8. 違約處理

8.1. 除本規章有特別規定外，申請機構若有違約情事時，情節輕微者，制度推動委員會得以書面通知其於一個月內改善完成，若有特殊原因，得延長一個月。

8.2. 前條違反情事若屆期仍未改善，且屬情節重大者，制度推動委員會得通知認證機構撤銷其合格證書。

8.3. 申請機構有下列情事之一者，制度推動委員會得通知認證機構撤銷其合格證書：

a. 填報申請資料虛偽不實者。

b. 運作違反相關法令規定者。

c. 出具不實證書或相同用途之文件。

d. 作不當聲明或使用致制度推動委員會陷於爭議者。

e. 逾越合格證書內容，或其他違反制度推動委員會之規定，情節重大者。

9. 保密義務

9.1. 申請機構對 App 開發者提供之資料及相關資訊應提供合理之保密措施。除執行業務人員因提供或辦理 App 資安檢測服務，而有必要知悉者外，申請機構均不得使用、披露或複製機密資料，且均不得將機密資料移做他用。

9.2. 前條所稱機密資料不包括以下情形之任何資訊：

a. App 開發者所提供當時已公開或之後非因申請機構之過失而公開者。

b. 申請機構合法自不須對 App 開發者負任何保密義務之第三者取得者。

c. App 開發者提供之前，已為申請機構所持有，並有書面紀錄證明者。

d. 申請機構之員工獨立發展，未以任何方式參考機密資料，並有書面紀錄證明者。

e. 因法令或政府機關要求而提供者。

9.3. 本文件之任何一方對於下列資訊得自由決定是否告知他方：

a. 由第三人處得知之他方保密資訊。

b. 認證適用之法令、技術規則或技術標準。

c. 法令所規定認證機構應公開之資訊。

10. 責任

10.1. 申請機構如有濫用認證機構所發認證之情事，致制度推動委員會遭受損害時，應對制度推動委員會負損害賠償責任。

10.2. 雙方對可歸責於己之事由所致任何第三人之損害應自行負擔全部責任。

10.3. 本文件之任何一方得知有任何事件可能造成上述賠償請求時應立即通知他方，並應以任何可能之方法防止損害之發生及擴大。

11. 其他

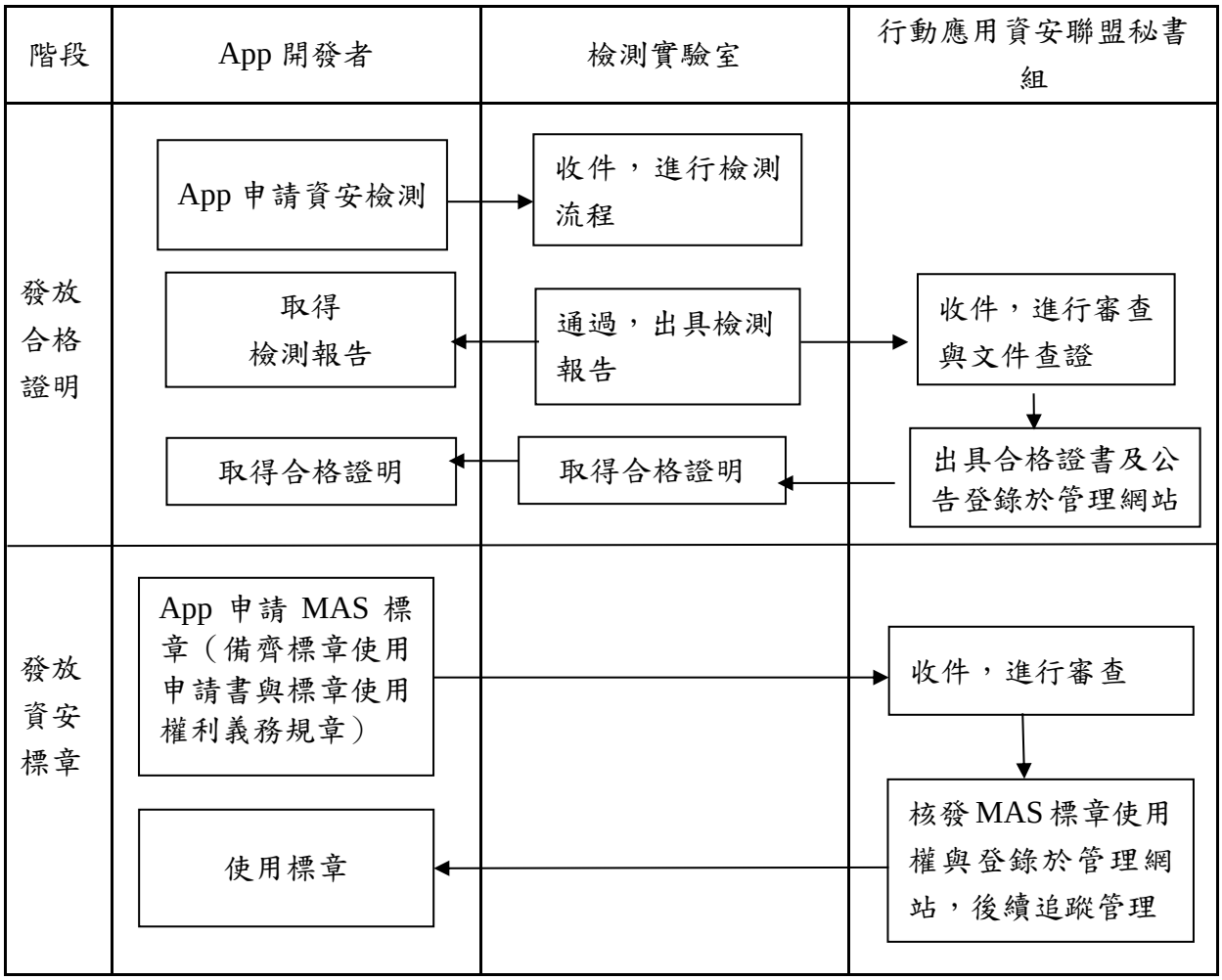
11.1. 因本規章發生爭議、糾紛、歧見或違反時，依中華民國仲裁法申請仲裁，以台北市為仲裁地。

11.2. 如仍有未盡事宜，得由雙方另行協議補充訂定之。

（以下空白）

附錄四、行動應用 App 開發者申請檢測與 MAS 標章流程

經檢測實驗室檢測合格之行動應用 App，檢測實驗室須依據通過「行動應用 App 基本資安檢測基準」所定義該行動應用程式類別應檢測所有項目之檢測報告，發放「行動應用 App 基本資安檢測合格證明」與資安標章。



附錄五、「行動應用 App 基本資安標章」使用申請書

本公司（以下稱申請機構）茲向「行動應用資安聯盟」（以下簡稱本聯盟）申請使用行動應用 App 基本資安標章（Mobile Application Basic Security 標章，以下簡稱 MAS 標章），同意遵守以下條款：

一、申請機構之基本資訊：

行動應用程式基本資料	申請日期	中華民國　　年　　月　　日		
	申請 App 名稱			
	App 安全類別	□L1 □L2 □L3		
	作業系統	□Android □iOS		
	App 版本		基準版本	
	App 分類（單選主要功能）	□金融(銀行、保險) □購物(商城) □政府 □醫療 □通訊(通話、訊息、社交) □工具/應用程式 □教育□其他＿＿＿＿＿＿＿＿		
	App 送測意願	□自願送測 □配合政策(主管機關要求)		
檢測機構	檢測機構名稱			
	檢測實驗室名稱			
	申請檢測日期	中華民國　　年　　月　　日		
	檢測完成日期	中華民國　　年　　月　　日		
	檢測報告編號			
行動應用廠商資料	申請證書之單位名稱	□受測單位(APP 所有者) □開發單位(APP 開發者)		
	受測單位名稱	(必填)		
	統一編號	(必填)		
	受測單位地址	(必填)		
	聯絡人姓名	(必填)		
	聯絡人電話	(必填)		
	聯絡人電子信箱	(必填)		
	開發單位名稱	(必填)		

	統　一　編　號	(必填)
	開發單位地址	(必填)
	聯絡人姓名	(必填)
	聯絡人電話	(必填)
	聯絡人電子信箱	(必填)
公告	公告於 MAS 網站	□公告　□不公告
	發　佈　狀　態	□已發佈 □預計發佈 □內部使用
	行動應用程式商店網址	
申請英文證書	是否申請英文證書	□是(請填寫以下表格)　□否
	App 名稱(英文)	
	單位名稱(英文)	(※請依照申請證書之單位名稱填寫)
	檢測機構名稱(英文)	
	檢測實驗室名稱(英文)	

二、申請機構同意並知悉「行動應用 App 基本資安標章使用權利義務規章」構成雙方權利義務規範。

三、申請人如因提供資訊不實造成損害，願依相關法律負起責任，其並應保證具有將行動應用 App 上架至行動應用程式商店之權利。

此致

行動應用資安聯盟

檢測實驗室主管簽名或蓋章
受測單位承辦人簽名或蓋章
開發單位承辦人簽名或蓋章

(若為開發單位送測則必填)

「行動應用 App 基本資安標章」使用權利義務規章為本申請書之一部份，請併同本申請書用印

附錄六、「行動應用 App 基本資安標章」使用權利義務規章

申請機構（以下或稱行動應用 App 開發者）茲向「行動應用資安制度推動委員會」(以下簡稱制度推動委員會）申請使用行動應用 App 基本資安標章（Mobile Application Basic Security 標章，以下簡稱 MAS 標章)，同意遵守以下條款：

1. 標章之使用期限

   MAS 標章有效期間為一年，制度推動委員會同意申請機構以申請書上之 App 名稱使用 MAS 標章。

2. 標章之使用方式

   2.1 申請機構應依制度推動委員會所規定之樣式，於行動應用程式商店之網站頁面上使用 MAS 標章，不得改變形狀、顏色或加註字樣，如需為其他使用方式，應另以 MAS 標章例外規定使用方式申請書向制度推動委員會申請。

   2.2 申請機構不得將 MAS 標章用於證明標章以外之用途。

3. 標章之使用依據

   申請機構使用 MAS 標章應確實遵守「行動應用 App 基本資安自主檢測推動制度規章」及「行動應用 App 基本資安標章使用與管理規範」等相關規定。

4. 制度推動委員會之權利義務

   4.1 制度推動委員會因主管機關或制度推動委員會公告之規範或要求得隨時變更本規章，因此而直接涉及申請機構之部分，應於合理期間內告知申請機構。申請機構於收到通知後，不即為反對表示者，視為同意該項變更。

   4.2 制度推動委員會應將 MAS 標章之證號，公告於制度推動委員會網站或以其他方式對外公告之。

5. 行動應用App開發者之權利義務

   5.1 申請機構同意隨時接受制度推動委員會不定期抽查，不得以任何理由拒絕。制度推動委員會如發現申請機構之未符合本規章之規定或行動應用 App 基本資安檢測基準之要求，制度推動委員會得立即通知申請機構停止使用 MAS 標章，並得公告之。

   5.2 自制度推動委員會發出通知或公告後，申請機構應立即停止使用 MAS 標章，並將相關廣告文宣回收。經制度推動委員會以書面通知限期改善，並於期滿後實施複查，複查仍未符合規定時，制度推動委員會得終止標章之使用。

   5.3 MAS 標章有效期間內，制度推動委員會發現申請機構以詐欺、脅迫或偽造、變造等不正方法獲准使用 MAS 標章者，制度推動委員會得終止標章之使用。申請機構應負責回收廣告文宣，並賠償制度推動委員會因此所生之損害。

   5.4 申請機構同意於行動應用 App 之名稱、所有權等資訊有變更時，應檢具相關證明文件向制度推動委員會報備。

   5.5 MAS 標章有效期間內，若申請機構有下列情事之一者，制度推動委

員會應終止申請機構 MAS 標章之使用權，申請機構不得異議：

a. 申請機構申請終止使用。
b. 申請機構解散或歇業。
c. 申請機構之營利事業登記證經主管機關依法註銷。
d. 申請機構違反本規章第2點。
e. 申請機構違反本規章第6點。
f. 申請機構違反本規章第7.1點及第7.2點，未通知或屆期未改善。
g. 申請機構規避、妨礙或拒絕制度推動委員會所進行之不定期抽驗。
h. 申請機構獲證App經抽驗複查，未符行動應用App基本資安檢測基準之要求。
i. 申請機構獲證App之MAS標章依「行動應用App基本資安自主檢測推動制度規章」8.4之規定已失其效力者。經制度推動委員會終止申請機構之MAS標章使用權者，制度推動委員會應以書面通知申請機構停止使用MAS標章並限期自行動應用程式商店取下相關標示。申請機構逾期不取下者，應負賠償經濟部工業局或制度推動委員會因此所生之一切損害。

6. 違約處理

6.1 申請機構保證僅將本標章使用於本規章第1點所載之行動應用 App，其他行動應用 App 均不得使用本標章。

6.2 申請機構依本規章所取得之 MAS 標章使用權不得轉讓、買賣或移轉與任何第三者。申請機構違反本條約者，應賠償經濟部工業局或制度推動委員會因此所生之一切損害。

7. 責任

7.1 申請機構如知悉其取得 MAS 標章之行動應用 App，可能導致行動裝置遭受不當存取，或個人資料之外洩、竄改、毀損或滅失之風險時，應通知制度推動委員會。

7.2 制度推動委員會知有前款之情形，應對該行動應用 App 進行複檢，如該行動應用 App 確有可能導致行動裝置遭受不當存取，或個人資料之外洩、竄改、毀損或滅失之風險時，應暫停標章效力，並命申請機構限期改善。

7.3 申請機構同意如因違反本文件而損害經濟部工業局或制度推動委員會兩方之權益時，申請機構願負完全賠償責任。

7.4 申請機構於通過使用 MAS 標章審查並簽訂本規章後，應積極配合經濟部工業局及制度推動委員會兩方推行 MAS 標章之宗旨所辦理之各項技術研討、訓練講習及推廣宣導活動。

8. 其它

8.1 對於 MAS 標章之申請、檢測、使用、停止或終止所產生之爭議，應於收到相關通知之日起一個月內，以書面方式明確說明理由與訴求，向制度推動委員會提出申訴，制度推動委員會自收到申訴書之日起一個月內應將申訴結果函覆申訴人。

8.2 對於 MAS 標章之申請、檢測、使用、停止或終止所產生之爭議，得

聲請調解或依民事訴訟程序處理，並以臺北地方法院為第一審管轄法院。

8.3 本文件後續補充修訂之換文，均視為本文件之一部份，與本文件具有同等之效力。

（以下空白）

附錄七、行動應用 App 基本資安檢測實驗室績效評核辦法

一、目的

確保行動應用 App 基本資安檢測實驗室（以下簡稱檢測實驗室）對 App 檢測品質之一致性，以及鼓勵檢測實驗室積極參與聯盟活動，透過「績效評核」計點方式，評核出優質之檢測實驗室。

二、對象

經行動應用資安聯盟（以下簡稱聯盟）公告之檢測實驗室（以下簡稱實驗室）。

三、抽測時程

預計每年第二、三季執行，視抽測之 App 總量而定。

四、抽測 App 方式

1. 每年至少一次，採抽測方式，抽測期間以聯盟公告為準。
2. 聯盟應於抽測舉辦日前兩周通知實驗室。
3. 由聯盟委託第三方具有 App 檢測能量之單位執行抽測作業，抽測各實驗室一年內通過 MAS 標章申請之 App 品質。
4. 每家實驗室之抽測數量基準，以該年度通過 MAS 標章之 App 總數之一定比例為抽測數量，其比例由聯盟視每年情況而制定之，不足 1 支者以 1 計算。

五、計點原則

1. 該實驗室年度抽測之 App 通過比率達 80%以上，本次抽測則列為”通過”。
2. 該實驗室年度抽測之 App 通過比率低於 80%，經申請複審後仍不通過者，本次抽測則列為”不通過”。
3. 計點以每年統計一次為主,於隔年度 1 月 1 日起點數歸零從新計算，不予累計。

4. 抽測計點方式，請詳見十、計點表。

六、抽測結果

1. 抽測結果不公布，由聯盟通知各實驗室。

2. 實驗室得於聯盟公布結果起七個工作天內提出複審，如逾期視同實驗室針對抽測結果無異議。

3. 複審作業以二次為限，第一次複審由聯盟召開技術專家委員會與第三方檢測實驗室進行審核，如不通過，實驗室得於聯盟公布結果起七個工作天內提出第二次複審；第二次複審由實驗室、第三方檢測單位以及技術專家共同決議之，實驗室針對複審結果不得異議。

4. 經決議或複審結果為不通過之實驗室，須於 30 工作天內提出改善報告，並於聯盟技術專家委員會審核，審核不通過即列本次抽測結果為”不通過”，實驗室針對審核結果不得異議。

七、停權及復權

1. 該年度抽測不通過之實驗室，取消參與獎勵頒獎及主管機關推薦資格。

2. 連續兩年抽測不通過者，將停權半年，並公告於聯盟網站。

3. 停權之實驗室半年後可於停權期限內提出復權申請，申請人至遲應於停權終止期限屆滿日的三個月前提出恢復申請與改善資料，若須補正改善資料，應於暫時終止期限屆滿日的一個月前完成改善資料之補正。

4. 申請復權者須通過聯盟審查，由聯盟技術專家委員會核定通過後允予復權，申請復權仍不通過者，聯盟另將兩年不通過之檢測相關報告函送經濟部工業局及財團法人全國認證基金會，並列為財團法人全國認證基金會各評鑑活動之參考，比照「團法人全國認證基金會權利義務規章、認證規範及特定服務計畫」辦理。

八、獎勵及推薦

1. 每年 12 月聯盟統計各實驗室該年度計點結果，經聯盟討論核可後由經濟部工業局或聯盟予以頒獎，並公告於聯盟網站上。

2. 受獎之實驗室如未通過該年度抽測稽核，則取消獲獎資格。

3. 獎勵計點原則，請參閱附件計點表。

4. 榮獲該年度獎勵資格者，由聯盟核定後，聯盟將發函予各主管機關（金管會、教育部等）推薦其優良專業檢測能力。

九、注意事項

1. 若市場上可下載之 App 版本與檢測實驗室出具檢測報告時之版本不符時，實驗室須於抽測日期前，提供聯盟當時檢測之 App 檔案。請各實驗室保留檢測之 App 檔案至少一年。

2. 聯盟保留本評核辦法變更之權利，並以聯盟網站公告為依據。

3. 本辦法均依「行動應用 App 基本資安自主檢測推動制度」及「行動應用 App 基本資安規範」之規定為準。

十、記點表

項目	子項目	計點方式	統計時間
1. App 檢測	1-1 該年度取得 MAS 標章之 App 總數	每通過 1 支 App，計 1 點	每年12月統計結算一次
		每通過 1 支 App，並上架聯盟網站者，加計 3 點	
2. 抽測	2-1 抽測通過數	抽測之 App 每通過 1 支，計 2 點	每年至少一次
		抽測之 App 全數通過者，計 30 點	
	2-2 抽測不通過數	抽測之 App 不通過者，每支 App 扣 5 點	
3. 聯盟活動	3-1 App 檢測基準推廣活動及其他聯盟相關活動	每場次擔任主講者，每位計 1 點	每年至少三場次
4. 聯盟會議	4-1 一致性會議	參與會議出席者，每公司計 2 點	每年至少三場次
	4-2 高階主管會議	參與會議出席者，每公司計 5 點	每年至少一場次
	4-3 其他臨時會議	參與會議出席者，每公司計 1 點	不定期
5. 聯盟其他交辦事項	5-1 每月 App 統計數量	如期交付者，每公司計 5 點	每月一次
	5-2 其他事項，視工作緊急性及重要性	如期交付者，每公司計 1~5 點（由聯盟秘書組依情狀緊急及重要性認定為準）	不定期

＊實驗室所有參與聯盟活動及會議者，必須為執行 App 檢測相關之主管、技術或執行人員，除外人員聯盟將不予以記點。

＊行動應用資安聯盟保有點數調整之權利。

附錄八、「行動應用 App 基本資安標章」例外需求使用申請書

申請日期：　　年　　月　　日

申請人名稱	
申請 App 名稱	（中文） （英文）
例外需求說明	（請列點提出需要例外標示或張貼資安標章之方式及其位置之需求說明）