

### **附錄三、「行動應用 App 基本資安檢測實驗室」權利義務規章**

檢測實驗室茲向「行動應用資安聯盟」(以下簡稱本聯盟)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)申請特定服務計畫「智慧連網服務系統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. 行動應用資安聯盟之權利義務**

- 2.1. 本聯盟因主管機關或本聯盟公告之規範或要求得隨時變更本規章，因此而直接涉及之部分，應於合理期間內告知。於收到通知後，不即為反對表示者，視為同意該項變更。
- 2.2. 本聯盟應將合格證明所登載資訊，公告於本聯盟網站或以其他方式對外公告之。

#### **3. 檢測實驗室之權利義務**

- 3.1. 檢測實驗室應據實提出相關認證或其他相類似作業所需文件，並配合本聯盟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，本聯盟得通知認證機構撤銷認證證書，如因陳述不實或疏漏而造成損害，應負賠償責任。
- 3.2. 本聯盟因提供檢測實驗室登錄而遭任何第三人求償時，檢測實驗室應就該等求償負責。
- 3.3. 檢測實驗室下列相關資訊之異動，應於異動發生日起 15 日內通知本聯盟。
  - 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、品質主管及報告簽署人之異動。
  - e. 認證證書內記載事項之變動。
  - f. 業務終止或停業。
- 3.4. 前項異動，如檢測實驗室未依期限告知本聯盟，本聯盟必要時得通知認證機構撤銷認證證書。

#### **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，以符合本聯盟所訂之

規範與要求。

- 4.2. 檢測實驗室應接受本聯盟之定期或不定期之監督、查訪、訪談、抽驗等作業，並配合本聯盟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，或經本聯盟抽驗認定不合格。
- 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，本聯盟得公告並通知認證機構撤銷認證證書。
- 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，本聯盟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」所定義之行動應用程式安全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行動應用 App 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. 檢測實驗室應依本聯盟所公告之各項行政管理費用，由本聯盟收取之；並得經本聯盟授權，可由檢測實驗室代本聯盟向檢測申請者收取之。

## 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本聯盟所公告之「行動應用 App 基本資安標章使用與管理規範」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<sup>+</sup> 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<sup>+</sup> 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，證明書格式由本聯盟設計印製：

- a. 證書編號（依本聯盟規定之編碼原則，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、行動應用程式安全類別。
- e. 證書效期（發證日起一年）。
- f. 檢測實驗室名稱。

6.4. 由本聯盟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. 檢測實驗室授權本聯盟得因於認證、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，檢測實驗室若有違約情事時，情節輕微者，本聯盟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，本聯盟得通知認證機構撤銷其認證證書。
- 8.3. 檢測實驗室有下列情事之一者，本聯盟得通知認證機構撤銷其認證證書：
  - 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本聯盟陷於爭議者。
  - e. 逾越認證證書內容，或其他違反本聯盟之規定，情節重大者。

## 9. 保密義務

- 9.1. 檢測實驗室對行動應用 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，檢測實驗室均不得使用、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. 行動應用 App 開發者所提供之資料，為當時已公開或之後非因檢測實驗室之過失而公開者。

- b. 檢測實驗室合法自不須對行動應用 App 開發者負任何保密義務之第三者取得者。
- c. 行動應用 App 開發者提供之前，已為檢測實驗室所持有，並有書面紀錄證明者。
- d. 檢測實驗室之員工獨立發展，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. 檢測實驗室如有濫用認證機構所發認證之情事，致本聯盟遭受損害時，應對本聯盟負損害賠償責任。

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。

| 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

(以下空白)