附件二、保險業提供行動應用程式（App）作業原則

一、保險業有提供行動應用程式者，會員公司可依不同應用類別之行動應用程式對於安全性有不同之要求，除符合經濟部工業局「行動應用 App 基本資安規範」外，應遵循本作業原則。

二、會員公司應依個人資料保護法於行動應用程式下載前，明確告知消費者對於個人資料蒐集處理利用之法定事項及消費者得要求刪除資料之權利等事項，以保護消費者權益。

三、應用程式發布程序，應符合權責分工原則。

四、應於發布前檢視應用程式所需權限應與提供服務相當，首次發布或權限變動應經資安、法遵及風控等單位同意，以利綜合評估是否符合「個人資料保護法」之告知義務。

五、行動應用程式資安檢測作業：

(一)檢測範圍：

1. 委託專業機構辦理資安檢測時，參考經濟部工業局「行動應用 APP 基本資安檢測基準」及 OWASP 公布之 Mobile Top 10 項目。
2. 自行辦理檢測時，應對行動應用程式進行程式碼掃描或黑箱測試，並修正中、 高風險漏洞（如屬可承擔風險者除外）。

(二)依行動應用程式之重要性，定期委由專業機構完成資安檢測：

類別	定義	評估週期
第一類	對外部提供服務或直接提供客戶自動化服務之行動應用程式	每年委由專業機構完成資安檢測
第二類	對內部員工（含其他通路）提供服務，其經員工介入以提供客戶服務之行動應用程式（如:行動投保、行動保全、行動理賠等）	每二年委由專業機構完成資安檢測
第三類	對內部員工（含其他通路）提供服務，其未接觸客戶資訊或服務之行動應用程式（如:行動差勤、行動電子書等）	每五年委由專業機構完成資安檢測

(三)會員公司應建立行動應用程式上架前資安檢測程序：

1. 初次上架前，屬第一、二類者，應委由專業機構完成資安檢測；屬第三類者，應通過資安檢測程序。

2. 更新上架前，應通過資安檢測程序；若涉有重大變更作業或行動應用程式版本大幅更新時，應委由專業機構完成資安檢測。

3. 重大變更作業包括但不限於保單投保交易、涉及資金轉移、身分辨識及客戶權益等有重大相關項目。

4. 如因故需緊急變更過版時，應於兩個月內完成上述檢測。

六、保險業委託專業機構辦理 APP 資安檢測，應訂定內部程序，其至少包含下列項目：

(一)專業機構之遴選方法。

(二)專業機構之評鑑機制。

(三)就專業機構檢測報告建立檢核機制，其應辦理形式檢核項目，至少包含下列內容：

1. 檢測標的。

2. 檢測範圍之宣告。

3. 檢測時程。

4. 檢測方式、環境與使用之工具。

5. 檢測執行人員與負責之項目。

6. 測試項目為「符合要求或不符合要求」之判定。

7. 測試過程紀錄及佐證資料，不符合要求之檢測項目應於報告中提出。

七、啟動應用程式時，如偵測行動裝置疑似遭破解，應提示使用者注意風險，且與行 動裝置有關之安全設計（如設備指定、生物識別、敏感資料保護等），應評估其有效性。

八、行動應用程式屬第一類，對外部提供服務或直接提供客戶自動化服務者，應於官 網上提供應用程式之名稱、版本與下載位置。

九、行動應用程式屬第一類，應建立偽冒應用程式偵測機制，以維客戶權益。

十、採用憑證技術進行傳輸加密時，應用程式應建立可信任憑證清單並驗證完整憑證 鏈及其憑證有效性。

十一、應進行身分驗證相關資訊不以明文傳輸並具備帳戶鎖定機制，以防範自動化程式 之登入或密碼更換嘗試。

附錄：用語及定義

一、行動裝置：係指包含但不限於智慧型手機、平板電腦等具通信及連網功能之設備。

二、專業機構：係指非會員公司之法人機構，其應具備經濟部工業局「行動應用 APP 基本資安自主檢測推動制度」列示之合格檢測實驗室資格。

三、遭破解之行動裝置：係指透過系統程序取得手機最高權限，藉以突破手機作

業系 統之基本防護，可能導致遭植入惡意程式。

四、完成資安檢測：係指辦理資安檢測，並針對相關漏洞規劃修補作業，於一定時間 內完成修補。

五、黑箱測試：動態分析或動態程式碼安全性檢測，主要用於受測主機資訊不足的情 況下進行測試。

六、憑證：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。