保險業辦理資訊安全防護自律規範

金管會 102 年 12 月 26 日金管保綜字第 10200145480 號函准備查訂定
金管會 104 年 2 月 16 日金管保綜字第 10402562872 號函准備查修正
金管會 106 年 12 月 28 日金管保壽字第 10600961080 號函准備查修正
金管會 109 年 5 月 26 日金管保綜字第 1090419516 號函准備查修正

第一條

中華民國人壽保險商業同業公會與中華民國產物保險商業同業公會為督促會員公司資訊業務與相關資訊資產之安全，發揚自律精神，防範資訊處理作業過程發生影響資訊及系統機密性、完整性及可用性之安全事件，確保各會員公司資訊處理作業能安全有效地運作，特訂定本自律規範。

第二條

本自律規範用詞定義如下：

一、 資訊資產：包含軟體、硬體、環境、文件、通訊、資料、人員等。

二、 自攜裝置：係指非屬公司資產、透過該裝置以無線或有線通訊方式連接至會員公司內部網路，存取作業系統或檔案服務。

三、 雲端服務：係指服務提供者以租借方式提供個人或企業得承租其網路、伺服器、儲存空間、基礎設施、資安設備、系統軟體、應用程式、分析與計算等資源，以達資源共享之服務。

第三條

各會員公司辦理資訊安全規範除應依據各該公司訂立之資安處理程序及其應注意事項外，並應符合依本自律規範辦理。

第四條

各會員公司辦理資訊安全規範，應至少遵循下列規定：

一、 應要求所聘任之員工簽署資訊安全保密切結書、雇佣契約、工作手冊，明訂員工應遵守資訊安全保密協定。

二、 有委外業務者，應於委外契約中明訂資訊安全保密協定。

三、 應透過每年定期、適當之教育訓練或宣導，告知內部員工應遵循之資訊安全規範。

四、 管理階層應督導員工遵循公司既定之資訊安全規範。

五、 員工職務異動時，應依既定程序辦理資訊資產退回與存取權限之變更或取消。

第五條

各會員公司應視資訊系統規模與架構，訂定核心資訊系統之範圍與相關作業規範：

一、 核心資訊系統應包括但不限於核保出單、保全（批改）、理賠、保費系統。

二、 訂定核心資訊系統開發及程式修改作業程序。

三、 訂定核心資訊系統置換作業程序，其至少應包括成本效益分析、風險評估、需求分析、設計規劃、功能測試驗證(含完整性、正確性與穩定性)、轉換決策評估及平行測試等項目。

第六條

各會員公司若有建置管理系統及有關個資之資安資料，應建立資安防禦機制，並依據保險業辦理電腦系統資訊安全評估作業原則(如附件一)辦理各項資訊安全評估作業，以改善並提升網路與資訊系統安全防護能力。

第七條

各會員公司若有開發並提供行動裝置應用程式，應依據保險業提供行動裝置應用程式作業原則(如附件二)辦理，以確保行動應用程式(App)安全防護能力，並保障消費者權益。

第八條

各會員公司若有運用新興科技(包含雲端服務、社群媒體、生物特徵資料及自攜裝置等)，需依據保險業運用新興科技作業原則（如附件三）辦理，以建立完善之控管機制，降低新興科技之運用風險。

第九條

各會員公司若有運用物聯網設備，需依據保險業物聯網設備作業準則(如附件四)辦理，以強化物聯網設備之安全。

第十條

各會員公司若有辦理電子商務，需依據保險業經營電子商務自律規範及保險業網路投保註冊會員密碼之設計安全作業準則（如附件五）辦理，以確保電子商務之資訊安全，降低遭破解之風險。

第十一條

各會員公司應訂定設備報廢作業程序，報廢前應將機密性、敏感性資料及授權軟體予以移除、實施安全性覆寫或實體破壞，應確保報廢之電腦硬碟及儲存媒體儲存之資料不可還原，並留存報廢紀錄，若委託第三者銷毀時，應簽訂保密合約。

第十二條

各會員公司於非公司職場實施異地辦公或遠端工作時，應評估相關作業風險，以強化遠端作業之安全：

一、 針對營運環境調整、資料傳輸及加密機制、機敏資料防護、稽核軌跡留存、異常行為監控及對外遠端存取設備進行評估及強化，系統及設備如有重大漏洞應立即處理及因應，降低業務運作風險，確保整體保險系統穩定及安全。

二、 針對使用之視訊會議系統、VPN 及 VDI 等設備，應訂定相關使用規範並落實各項安全管控作業。

第十三條

各會員公司應加強資訊安全事故管理。

各會員公司應依資訊安全事件通報應變作業實施原則，若發生資訊安全事件時，應儘速回報各所屬公會及主管機關，並採取適當處理措施，以控制資安事件影響範圍之擴大。

第十四條

各會員公司應將本自律規範內容，納入內稽內控制度中，並定期辦理查核。

第十五條

各會員公司如有違反本自律規範之情事，經查證屬實者且違反情節較輕者，得先予書面糾正；如情節較重大者，提報經各所屬公會理事會通過後，處以新台幣伍萬元以上，貳拾萬元以下之罰款；前述處理情形並應於一個月內報主管機關。

第十六條

本規範由中華民國人壽保險商業同業公會與中華民國產物保險商業同業公會共同訂定，經各該公會理事會決議通過報主管機關備查後施行，修正時亦同。

附件一

保險業電腦系統資訊安全評估作業原則

壹、前言

為確保保險業提供電腦系統具有一致性基本系統安全防護能力，擬透過各項資訊安全評估作業，發現資安威脅與弱點，藉以實施技術面與管理面相關控制措施，以改善並提升網路與資訊系統安全防護能力，訂定本辦法。

貳、評估範圍

一、 保險業應就整體電腦系統（含自建與委外維運）依據本作業原則建構一套評估計畫，基於持續營運及保障客戶權益，依資訊資產之重要性及影響程度進行分類，定期或分階段辦理資訊安全評估作業，並提交「電腦系統資訊安全評估報告」，辦理矯正預防措施，並定期追蹤檢討。

二、 評估計畫應報董（理）事會或經其授權之經理部門核定，但外國保險業在台分公司，得授權由在中華民國負責人為之。評估計畫至少每三年重新審視一次。

參、電腦系統分類及評估週期

一、 電腦系統依其重要性分為三類：

電腦系統類別	定義	評估週期
第一類	直接提供客戶自動化服務之系統（如網路投保、網路要保等系統）及核心資訊系統	每年至少辦理一次資訊安全評估作業
第二類	存放大量客戶資料之系統 （如檔案伺服器、資料倉儲、客服及行銷等系統）	每三年至少辦理一次資訊安全評估作業
第三類	非核心資訊系統 （如人資、總務等系統）	每五年至少辦理一次資訊安全評估作業

二、 單一系統而為數眾多且財產權歸屬於公司之設備得以抽測方式辦理，抽測比例每次至少應占該系統全部設備之 10%或 100 台以上。

三、 單一系統發生重大資訊安全事件，應於三個月內重新完成資訊安全評估作業。

肆、資訊安全評估作業

一、 資訊安全評估作業項目：

（一）資訊架構檢視

1. 檢視網路架構之配置、資訊設備安全管理規則之妥適性等，以評估可能之風險，採取必要因應措施。
2. 檢視單點故障最大衝擊與風險承擔能力。
3. 檢視對於持續營運所採取相關措施之妥適性。
4. 適時參考金融資安資訊分享與分析中心(F-ISAC)所發布之資安威脅情資及資安防護建議，並採取相關措施。

（二）網路活動檢視

1. 檢視網路設備、伺服器及物聯網設備之存取紀錄及帳號權限，識別異常紀錄與確認警示機制。
2. 檢視資安設備（如：防火牆、入侵偵測或防禦、惡意軟體防護、資料外洩防護、垃圾郵件過濾、網路釣魚偵測、網頁防護等）之監控紀錄，識別異常紀錄與確認警示機制。
3. 檢視網路是否存在異常連線或異常網域名稱解析伺服器(Domain Name System Server，DNS Server)查詢，並比對是否為已知惡意 IP、中繼站或有符合網路惡意行為的特徵。

（三）網路設備、伺服器、終端設備及物聯網設備等設備檢測

1. 辦理網路設備、伺服器、終端設備及物聯網設備等設備的弱點掃描與修補作業。
2. 檢測終端機及伺服器是否存在惡意程式。
3. 檢測系統帳號登入密碼複雜度；檢視外部連接密碼（如檔案傳輸（File Transfer Protocol, FTP）連線、資料庫連線等）之儲存保護機制與存取控制。

（四）網路設備、伺服器及物聯網等設備且連線至 Internet 者應辦理下列事項

1. 進行滲透測試。
2. 進行伺服器應用系統之程式原始碼掃描或黑箱測試。
3. 檢視伺服器目錄及網頁之存取權限。
4. 檢視系統是否有異常的授權連線、CPU 資源異常耗用及異常之資料庫存取行為等情況。

（五）客戶端應用程式檢測

針對保險業交付給客戶之應用程式進行下列檢測：

1. 提供 http, https, FTP 者應進行弱點掃描。
2. 程式原始碼掃描或滲透測試。
3. 敏感性資料保護檢測（如記憶體、儲存媒體）。
4. 金鑰保護檢測。

（六）安全設定檢視

1. 檢視伺服器(如網域服務 Active Directory)有關「密碼設定原則」與「帳號鎖定原則」設定。
2. 檢視防火牆是否開啟具有安全性風險的通訊埠或非必要通訊埠，連線設定是否有安全性弱點。
3. 檢視系統存取限制(如存取控制清單 Access Control List)及特權帳號管理。
4. 檢視作業系統、防毒軟體、辦公軟體及應用軟體等之更新設定及更新狀態。
5. 檢視金鑰之儲存保護機制與存取控制。

（七）資訊系統可靠性與安全性侵害之對策

1. 會員公司應就提升資訊系統可靠性研擬相關對策，其內容包括：

（1） 提升硬體設備之可靠性：包含預防硬體設備故障與備用硬體設備設置之對策。

（2） 提昇軟體系統之可靠性：包含提升軟體開發品質與提升軟體維護品質對策。
（3） 提升營運可靠性之對策。
（4） 故障之早期發現與早期復原對策。
（5） 災變對策。

2. 會員公司應就資訊安全性侵害，研擬相關對策，其內容包括：
（1） 資料保護：包含防止洩漏、防止破壞篡改與相對應檢測之對策。
（2） 防止非法使用：包含存取權限確認、應用範圍限制、防止非法偽造、限制外部網路存取及偵測與因應之對策。
（3） 防止非法程式：包含防禦、偵測與復原對策。

3. 檢視電腦系統是否符合「保險業辦理資訊安全防護自律規範」、「保險業經營電子商務自律規範」、「保險業辦理電子保單簽發作業自律規範」、「保險業經營行動投保業務自律規範」及主管機關相關函文之要求。

4. 如有使用 SWIFT 系統者，需檢視電腦系統之 SWIFT 系統是否符合 SWIFT 公布之 Customer Security Programme 規範及公會相關函文之要求，若與本作業原則衝突，依 SWIFT 公布為主。

二、 第一類電腦系統應依前項辦理資訊安全評估作業，第二類及第三類電腦系統辦理資訊安全評估作業則依系統特性選擇前項必要之評估作業項目。

伍、分散式阻斷服務攻擊(DDoS)演練

辦理電子商務業務者，應訂定分散式阻斷服務攻擊(DDoS)防禦與應變作業程序，並定期辦理 DDoS 實地演練。

陸、社交工程演練

每年應至少一次針對使用電腦系統人員，於安全監控範圍內，寄發演練郵件，加強資通安全教育，以期防範惡意程式透過社交方式入侵。

柒、評估單位資格與責任

一、 評估單位可委由外部專業機構或由會員公司內部單位進行。如為外部專業機構，該機構應與資安評估標的無利害關係，若為內部單位，應獨立於原電腦系統開發與維護等相關單位。

二、 辦理第一類電腦系統資訊安全評估作業之評估單位應具備下列各款資格條件；辦理第二類及第三類電腦系統資訊安全評估作業者，依評估作業項目需要，具備下列相關資格條件之一：

（一）具備資訊安全管理知識，如持有國際資訊安全經理人(Certified Information Security Manager, CISM）證書或通過國際資安管理系統主導稽核員（Information Security Management System Lead Auditor, ISO 27001 LA）考試合格等。

（二）具備資訊安全技術能力，如國際資訊安全系統專家（Certified Information Systems Security Professional, CISSP）證書等。

（三）具備模擬駭客攻擊能力，如滲透專家（Certified Ethical Hacking, CEH）證書或事件處理專家（Certified Incident Handler, CIH）證書等。

（四）熟悉金融領域載具應用、系統開發或稽核經驗。

三、相關檢視文件、檢測紀錄檔、組態參數、程式原始碼、側錄封包資料等與本案相關之全部資料，評估單位應簽立保密切結書並提供適當保護措施，以防止資料外洩。

四、評估單位及人員不得隱瞞缺失、不實陳述、洩露資料及不當利用等情事。

捌、評估報告

一、「電腦系統資訊安全評估報告」內容應至少包含評估人員資格、評估範圍、評估作業項目與標的、評估紀錄、評估時所發現之缺失項目、缺失嚴重程度、缺失類別、風險說明、具體改善建議及社交演練結果。

二、會員公司應依據評估報告內容缺失程度區分風險等級，並擬定各風險對應之控管措施及處理時限，送稽核單位進行缺失改善事項之追蹤覆查。

三、評估報告缺失覆查應提報董（理）事會或經其授權之經理部門，但外國保險業在台分公司，得由總公司授權之人員為之，以落實由高階管理階層督導缺失改善。

四、評估報告應併同缺失改善等相關文件至少保存五年。

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	資安檢測頻率
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. 檢測項目是否有缺漏。

2. 檢測項目是否與佐證資料不符。

3. 檢測結果是否與說明矛盾。

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。

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。

附件三

保險業運用新興科技作業原則

壹、 為協助保險業適當管理運用新興科技之風險，並保障消費者權益，特訂定本作業原則。

貳、 雲端服務安全控管

一、 雲端服務係指服務提供者以租借方式提供個人或企業得承租其網路、伺服器、儲存空間、基礎設施、資安設備、系統軟體、應用程式、分析與計算等資源，以達資源共享之服務。

二、 本安全控管範圍不包含僅提供會員公司內部使用且不涉及客戶資料處理之服務。

三、 應制定雲端服務管理政策，至少每年檢視一次。

四、 應評估雲端服務提供者之合格條件、服務水準、復原時間、備援機制、權責歸屬及資訊安全防護等項目。

五、 應評估雲端服務提供之平台、協定、介面、檔案格式等，以確保互通性與可移植性。

六、 應確保雲端服務提供者提供之資源與其他承租人所使用之資源各自獨立，互不影響(如防火牆區隔)。

七、 應與雲端服務提供者簽訂服務協議，維持所需之服務水準並定期提出報告與操作紀錄(如服務水準報告、系統變更紀錄、作業系統映像檔 存取紀錄等)。

八、 應針對所傳輸或儲存之客戶資料或敏感資料，建置適當之保護設備或技術，採取適當之存取管制(如資料加密)。採用加密演算法者，應能妥善保護加密金鑰(如使用硬體安全模組)。

九、 應監控並建立資通安全事件通報程序。遇事件發生時，相關單位及人員應依循前述通報程序辦理。

十、 應於服務合約終止或轉移時，將使用之作業系統映像檔、儲存空間、快取空間、備份媒體、客戶資料或敏感資料等全數刪除或銷毀，並留存刪除或銷毀之紀錄，以供事後確認。

十一、 提供電子商務服務者，應符合「保險業經營電子商務自律規範」及「保險業網路投保註冊會員密碼之設計安全作業準則」規定。

參、 社群媒體控管程序

一、 社群媒體係指一交流平台，參與者透過與其他單一或多位參與者單向分享或雙向互動，進行內容產出、知識分享、討論共創之平台。

二、 本控管程序不包含會員公司內部使用或與個別客戶溝通使用之平台。

三、 應制定社群媒體管理政策，至少每年檢視一次。

四、 應制定社群媒體使用守則，明確列出可接受使用之社群媒體、功能及使用規則。

五、 應制定會員公司發言規範，明確定義各角色被授予之發言權責，並避免非授權之公務言論發表。

六、 應制定內容過濾與監視政策，其監視內容應至少包含防止客戶隱私及會員公司機密外洩、非授權或偽冒身分發言及不可有攻擊或詆毀同業之情事。
七、 應制定不當發言之緊急應變程序。
八、 應制定社群媒體異常事件通報程序。
九、 如有不當發言，應留存通聯紀錄，以供日後調查使用。

肆、 自攜裝置安全控管
一、 自攜裝置係指非屬公司資產、透過該裝置以無線或有線通訊方式連接至會員公司內部網路，存取作業系統或檔案服務。
二、 應制定自攜裝置管理政策，至少每年檢視一次。
三、 應列出允許使用之自攜裝置類型、作業系統、應用系統或服務。
四、 對自攜裝置所採取之相關措施，應先取得裝置持有者同意，以避免爭議。
五、 應列冊管理使用人員與裝置，至少每年審閱一次。
六、 應建置使用人員身分與裝置識別機制(如帳號密碼識別、裝置識別碼)。
七、 應制定自攜裝置連網環境標準，如未符合標準(如作業系統疑似遭破解或提權、未安裝病毒防護、重大漏洞未修復)，應限制其連網功能。
八、 應建置自攜裝置資料保護措施(如資料加密或遮罩)，並採取適當之存取管制。
九、 應制定自攜裝置遺失處理程序。

伍、 生物特徵資料安全控管
一、 用詞定義如下:
(一) 原始生物特徵資料:是指透過感應器(如掃描器、照相機)所擷取的原始資料。
(二) 假名標識符:是指用於生物特徵比對之資料,其內容不為原始生物特徵資料之一部份。
(三) 輔助資料:是指一演算法或機制,用來將原始生物特徵資料分離產生假名標識符。
(四) 生物特徵資料:指包含原始生物特徵資料、假名標識符及輔助資料。
(五) 身分識別資料:為非生物特徵資料之個人資料(如身分證字號、出生日期等)。
(六) 錯誤拒絕率:是指同一人卻因比對其留存之生物特徵資料誤認為不同特徵而拒絕的機率。
(七) 錯誤接受率:是指不同人卻因比對其留存之生物特徵資料誤認為相同特徵而接受的機率。
二、 運用生物特徵資料做為識別客戶身分時，其蒐集、處理及利用之行為，應納入個資管理機制。
三、 應針對生物識別機制，建立其錯誤接受率及錯誤拒絕率之標準，並每年定期檢視。若不符合會員公司要求時，應建立補償措施。
四、 應於蒐集生物特徵資料時，取得客戶同意，並讓客戶充份了解所蒐集之目的及方式。
五、 生物特徵資料儲存於會員公司內部系統時，應將原始生物特徵資料去識別化使其難以還原、將原始生物特徵資料及假名標識符進行加密儲存、 將生物特徵資

料分別儲存於不同之儲存媒體(如資料庫);儲存於會員公司提供之終端設備時，應儲存於符合FIPS 140-2 Level 3標準含以上之設備。

六、 應考量現行業務情況，必要時更新客戶之生物特徵資料，以確保生物特徵資料不會隨時間而失效(如人臉辨識、聲紋辨識等)。

七、 當會員公司無法以生物特徵資料識別客戶時，應提供重新蒐集生物特徵資料之管道。

八、 應確保生物特徵資料於傳輸過程中之訊息隱密性、完整性、不可重複性及來源辨識性，相關控管應符合「保險業經營電子商務自律規範」及「保險業網路投保註冊會員密碼之設計安全作業準則」。

九、 應於首次使用生物辨識技術或技術有重大變更時(如輔助資料、技術提供商)，經資訊部門檢視該技術足以有效識別客戶身分，其評估範圍包含但不限於模擬偽冒生物特徵資料、確認符合相關法規要求、確認生物辨識機制、作業流程及補償措施之風險控管。

附件四

保險業使用物聯網設備作業準則

一、 為確保保險業使用物聯網(Internet of Things, IoT)設備之安全性，以確保適當管理運用物聯網設備之風險，並保障消費者。

二、 本作業準則所稱物聯網設備係指具網路連線功能之嵌入式系統(具有小型作業系統）設備（以下簡稱設備），包含自動化辦公(OA)設備（如數位錄影機、電話交換機、傳真機、錄音設備、影印機等）及不具備遠端操控介面功能之感測器。

三、 應建立物聯網設備管理清冊並至少每年更新一次，以識別設備用途、網段、存放位置與管理人員，評估適當之實體環境控管措施及存取權限管制。

四、 設備應具備安全性更新機制，以維持設備之整體安全性。

五、 為確保經授權之使用者使得進行資料存取、設備管理及安全性更新等操作，設備應具備身分驗證機制，並應進行初始密碼變更，密碼長度不應少於六位，建議採英數字混合使用，且宜包含大小寫英文字母或符號，並以最小權限原則針對不同的使用者身分進行授權。

六、 設備以無線連接網路者，應採用具加密協定之無線存取點連接網路，並以網路卡卡號白名單等機制進行設備綁定。

七、 設備應關閉不必要之網路連線及服務，並避免使用對外公開之網際網路位置，如設備採用公開的網際網路位置，應於設備前端設置防火牆以防護，並採用白名單方式進行存取過濾。

八、 應與設備供應商簽訂資訊安全相關協議，以明確約定相關責任。

九、 設備存在已知弱點且無法修補或更新，無法落實前述安全控管規範，應限制網際網路連線能力，加強存取控制或進行網路連線行為監控；並視需要訂定汰換期程。

十、 採購物聯網設備時，應優先採購經濟部與國家通訊傳播委員會共同發布物聯網資安標章認驗證制度之具有安全標章之物聯網設備。

十一、 應每年對物聯網設備使用及管理人員安排適當之資訊安全教育訓練。

十二、 針對不具備遠端操控介面功能之感測器，仍應遵循本作業準則三、七、八、九之要求辦理。

附件五

保險業網路投保註冊會員密碼之設計安全作業準則

會員公司若辦理網路投保業務，則網路投保註冊會員時應以靜態密碼或使用一次性密碼(OTP)自行設定，使用規則如下：

一、 靜態密碼:

1. 應至少 8 位數。
2. 建議採英數字混合使用，且宜包含大小寫英文字母或符號。
3. 不得使用客戶之統一編號及身分證字號等顯性資料作為密碼。
4. 不應訂為相同的英數字、連續英文字或連號數字，預設密碼不在此限。
5. 密碼與代號/帳號不應相同。
6. 密碼連續錯誤達五次，各公司應做妥善處理。
7. 變更密碼不得與前一次相同。
8. 首次登入時，應強制變更預設密碼。
9. 密碼超過一年未變更，各公司應做妥善處理。
10. 應採用下列一項密碼儲存管控機制：
    (1)密碼於儲存時應先進行不可逆運算（如雜湊演算法），雜湊值應進行加密保護或加入不可得知的資料運算。
    (2)採用加密演算法者，其金鑰應儲存於經第三方認證（如 FIPS 140-2 Level 3 以上）之硬體安全模組內並限制明文匯出功能等。

二、 一次性密碼(OTP)：

1. 應至少 6 位數。
2. 密碼與帳號不應相同。
3. 輸入密碼連續錯誤達五次，該密碼即失效。
4. 每次密碼有效性不得超過 5 分鐘，超過時即需重新申請發給新密碼。