保險業辦理資訊安全防護自律規範

金融監督管理委員會 109 年 5 月 26 日金管保綜字第 1090419516 號同意備查
金融監督管理委員會 110 年 12 月 30 日金管保綜字第 1100495362 號函同意備查
金融監督管理委員會 111 年 12 月 20 日金管保綜字第 1110466806 號函同意備查
金融監督管理委員會 112 年 9 月 7 日金管保綜字第 1120493120 號函同意備查

第 1 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 2 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 3 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 4 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 5 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（收費）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之項目：

(一)系統轉換前之準備工作：

1. 應建立架構審查機制，從應用程式、資料庫、資安、網路、平台、營運等面向進行評估，並評估一次過版或平行運轉可行性。
2. 應檢視相關設備容量，評估營運及業務需求所需備載容量。應建置擬真測試環境（如 UAT），測試新系統或功能相容於既有營運環境之架構、設備及參數。
3. 應訂定測試計劃與產出標準，依計劃以及影響範圍進行各項測試。測試應含功能測試 （如單元、整合、迴歸等），及非功能性測試（如相容性、尖峰量壓力測試及複合情境等）項目，並進行整體性演練。
4. 應進行上線變更審查及風險評估，辨識複雜度及影響範圍，並檢視測試個案及上線復原計畫之完整性，與建立多個檢核點及啟動復原之決策條件。
5. 應預留復原作業及上線驗證時間。
6. 應要求設備提供廠商與委外開發廠商於上線支援時，能緊急提供備品、問題查找及修改人力。
7. 應召開上線協調會議，安排工作項目並確保各項準備到位。
8. 應提前公告並進行教育訓練（含異常話術）。

(二)系統轉換作業：

1. 依上線計畫逐步執行，檢視每一個檢核點，必要時召開復原決策會議。
2. 執行系統及資料備份，以因應復原時所需。
3. 驗證各項變更作業，確保如預期結果。
4. 驗證各項資料內容，確保資料完整性。
5. 逐步啟動各項作業並監控網路及系統，確保提供足夠資源。

(三)系統轉換後之事件管理：

1. 持續系統監控，確保資料正確、功能正常、系統穩定。
2. 落實事故應變，以消費者權益及持續營運優先處理。
3. 集中管理問題並適時調配各單位資源。
4. 追蹤問題原因，提出短中長期改善方案並持續追蹤。

第 6 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 7 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 8 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 9 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 10 條

各會員公司辦理電子商務，應遵循下列事項：依據保險業經營電子商務自律規範及保險業電子商務身分驗證之資訊安全作業準則（如附件五）辦理，並建立安全有效之驗證機制，減少身分冒用及詐騙情事發生，以確保電子商務之資訊安全。

第 11 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 12 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。

三、應使用會員公司配發之裝置或設備，或使用資料不落地之機制，方得辦理遠端作業。

第 13 條

各會員公司應加強資訊安全事故管理。

各會員公司若發生重大資訊安全事故時，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 14 條

各會員公司若有建置可由外部 Internet 直接連線之網際網路應用系統及核心資訊系統，應定期辦理相關安全性檢測，相關資訊安全說明如下：

一、網際網路應用系統：

(一)應至少每季進行一次作業系統之弱點掃描，會員公司依掃描結果應進行風險評估，評估為高風險以上之弱點應於 2 個月內修補或完成補償性控制措施，評估為中、低風險應訂定適當措施及完成時間，執行矯正、紀錄處理情形並追蹤改善。

(二)新系統或系統功能首次上線前及至少每半年應針對異動程式進行程式碼掃描或黑箱測試，並針對其掃描或測試結果進行風險評估，及針對不同風險訂定適當措施及完成時間，執行矯正、記錄處理情形並追蹤改善；如無異動者則不在此限，但仍應參照「保險業電腦系統資訊安全評估作業原則」辦理電腦系統分類及評估週期相關作業。

二、核心資訊系統：

(一)應至少每半年進行一次作業系統之弱點掃描，會員公司依掃描結果應進行風險評估，評估為高風險以上之弱點應於 3 個月內修補或完成補償性控制措施，評估為中、低風險應訂定適當措施及完成時間，執行矯正、紀錄處理情形並追蹤改善。

(二)如為開放式系統，新系統或系統功能首次上線前及至少每半年應針對異動程式進行程式碼掃描或黑箱測試，並針對其掃描或測試結果進行風險評估，及針對不同風險訂定適當措施及完成時間，執行矯正、記錄處理情形並追蹤改善；如無異動者則不在此限，但仍應參照「保險業電腦系統資訊安全評估作業原則」辦理電腦系統分類及評估週期相關作業。

第 15 條

各會員公司辦理資訊系統維運時，應注意相關控制措施如下：

一、系統發展生命週期之維運（包含開發、測試）時，須注意版本控制與變更管理。

二、應定期審核資訊系統帳號之建立、修改及刪除。

三、應建立帳號管理機制，包含帳號之申請及刪除之程序。

四、應定期檢視防火牆規則，以確保現行控制之有效性。

第 16 條

各會員公司依保險業作業委託他人處理應注意事項辦理資訊系統作業委外，應於規劃及遴選階段，將資訊安全相關內容納入評估項目，以強化資訊安全。並遵循下列事項：

一、服務提供廠商應具備資訊安全相關認證或已有資通安全維護之相關措施。

二、審核作業委外廠商資格：

(一)各會員公司應制定有關審核廠商資格之內控機制，並就作業委外提供廠商進行評選審查作業。

(二)將資訊安全相關認證納入遴選項目，且應訂定內部程序，其至少包含作業委外廠商遴選機制、合約或協議簽訂、作業委外廠商管理要項、產品交付和驗收或維運等項目。

(三)各會員公司應將資訊安全或個人資料隱私管理相關認證納入資訊系統之作業委外廠商評估項目。

(四)各會員公司之資訊系統委外時，應依據委外廠商規模或作業特性，評估進行委外廠商監督。

三、作業委外廠商管理要項：

(一)應建立作業委外廠商管理規範，其內容應含作業委外廠商之人員管控，並建立適當檢驗機制，以確保管理機制有效落實。

(二)各會員公司之資訊系統委外廠商管理時，其管理項目應納入對委外廠商存取資訊之控管機制、對委外廠商服務之資訊安全管理措施查核機制、發生資安事故時委外廠商通知機制與應處時效要求、與委外廠商關係終止管理機制等項目。

(三)作業委外廠商進行軟、硬體維運時，應具備資通安全維護之措施。

(四)若作業委外內容有重大變更或重大事件時，應審查是否影響相關資訊安全管理制度或依循標準之要求並評估其風險，採取適當控制措施。

(五)作業委外廠商簽訂合約或協議，應遵循相關安全管理措施，其內容包含：

1. 服務供應廠商履行合約或協議時所提供軟體（或交付標的物）為交付產品，需具備合法性且不得違反智慧財產權之規定或侵害第三人合法權益。

2. 作業委外廠商進行資訊系統開發或維運時，若涉及客戶、員工個人資料，需考量具個人資料安全防範措施。

3. 應約定資安檢測與弱點修補之責任與時效要求。

4. 應訂定相關資訊安全管理責任。

5. 委外廠商交付之系統或程式，應確保無惡意程式及後門程式，或提供相關掃描報告。

(六)資訊系統作業委外終止或結束時，委外廠商應提供移轉服務，將留存資料移回至各會員公司自行處理，並應刪除或銷毀全數資料，且提供刪除或銷毀之佐證資訊與紀錄。

四、委外稽核：

(一)定期進行查核作業。

(二)辦理作業委外稽核時，於簽訂之合約應載明保留相關之稽核權利，得自行或委託獨立單位對委外廠商監督及查核之權責行為。

(三)執行委外稽核作業後，應對稽核紀錄之文件進行複審及保存並由需求單位進行存查。

(四)提供委外稽核服務的廠商須通過政府資通安全建議的相關證照或可參照「保險業電腦系統資訊安全評估作業原則」之第柒點要求。

各會員公司辦理資訊系統委外作業項目，有涉及核心資訊系統者，除應依前項各款規定辦理外，應併同遵循「保險業核心資通系統作業委外資安注意事項」(如附件六)。

第 17 條

第一類、第二類電腦系統應加強日誌紀錄管理，並遵循下列事項：

一、系統產生之事件日誌紀錄(內容包含但不限於事件類型、發生時間、發生位置、使用者身分識別等資訊)應有保留機制，除相關法令規定外，日誌紀錄至少需保留 180 天。如涉及個人資料之日誌紀錄者，保留期限應依個人資料保護法等相關規定辦理。

二、事件日誌應設有存取限制，並應用適當方式確保完整性；另應依據事件日誌紀錄之儲存需求配置容量，且定期備份日誌紀錄至原系統外之其他系統；或建置日誌伺服器等相關方案滿足以上需求。

三、應定期審查系統管理者活動以識別異常或潛在資安事件並保留紀錄；或將相關事件日誌納入資訊安全事件之監控管理機制範圍。

四、應訂定日誌處理失效之告警及應處機制。

五、系統內部時間應定期進行基準時間源進行同步。

第 18 條

各會員公司應強化對跨機構合作夥伴(含保險經紀人、代理人等合作關係)之資訊安全風險評估與措施，並遵循下列事項：

一、就保險業與跨機構合作夥伴共同使用之網際網路應用系統(如網路投保、網路要保等直接提供客戶自動化服務之系統)，其系統管控機制應包括資料傳輸之保密方式、系統使用權限之區隔及系統帳號權限控管等相關資訊安全機制。

二、與跨機構合作夥伴合約簽訂時，應進行風險評估並規劃風險處置措施，並於雙方簽訂備忘錄或契約中載明相關要求，其內容需包含資訊安全及保戶個人資料保護相關條款、禁止多人共用同一帳號，以及相關業務往來之查核機制或控管措施，以確保資訊安全維護能力與水準。

三、提供跨機構合作夥伴資訊服務者，應採用雙因子驗證或相關身分驗證方式，並應定期辦理帳號密碼變更及帳號清查。

第 19 條

辦理網路安全管理時，應注意下列控制措施：

一、保險業對外提供之網站服務應建立 https 安全連線，以確保連線之機密性與完整性。

二、內部網路應依正式營運、測試、辦公室等使用目的區隔網段，網路區域間連接應進行控管，如以防火牆、虛擬區域網路 VLAN 或實體線路加以區隔；正式營運內應再依電腦系統分類或系統功能或服務特性進行網段區隔。

三、人員使用外部網路連線內部電腦系統時，應使用虛擬私有網路（VPN）或虛擬桌面（Virtual Desktop）之方式連線，並採多因子驗證，且須進行異常連線管理。

四、保險業網際網路應用系統，須建立防火牆（Firewall）、網站應用程式防火牆（WAF）防護機制、入侵偵測及防禦機制，並定期檢視其防護規則及參數設定。

五、員工電腦應建立上網行為管理措施，並啟用偵測惡意連線機制，確保阻斷外部惡意連線。

六、為強化正式伺服器主機的安全控管機制，於使用特權帳號進行正式伺服器主機管理作業時，應經主管審核後，透過特權帳號管理（PAM）或跳板機等管理系統或獨立的管制網段才可連線正式伺服器主機，並留存稽核軌跡，以確保正式伺服器網段的連線安全性。

七、應關閉非必要之網路服務，限制對網際網路非必要之連線。

第 20 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 21 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 22 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	可由外部 Internet 直接連線之網際網路應用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。
5. 檢視伺服器應依電腦系統分類或系統功能或服務特性進行網段區隔。
6. 檢視邊界防護設備(包含閘道器、路由器、防火牆、防護裝置等設備)與外部網路連接之網點，是否設立防火牆控管內外部網路資料傳輸及資源存取，並限制非必要之連線對象與服務。

(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)查詢或監控進出之通訊流量，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。
4. 檢視是否訂定偵測偽冒網站之處理措施。

(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。
4. 辦理物聯網設備檢測作業時，依據「保險業使用物聯網設備作業準則」第四、五、六、七條之安全控管規範進行評估。

(四)可由外部 Internet 直接連線之網路設備、伺服器及物聯網等設備，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建立對外網站網頁防竄改機制。
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

保險業與客戶端之應用程式應採加密連線，並針對保險業交付給客戶之應用程式進行下列檢測：

1. 提供 https、SFTP 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。
5. 採最小權限原則，僅允許使用者依任務及業務功能所需完成指派之授權存取控管。

(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等安全措施。
6. 檢視從外部網路連回內部時需確認使用者身分。

(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) 提升軟體系統之可靠性：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。
   (6) 備份之系統備份媒體，須擬定驗證計畫，並驗證備份媒體之可靠性及資訊之完整性。
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」、「保險業經營行動服務自律規範」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、第二類及第三類電腦系統應依前項評估項目全部納入資訊安全評估作業以確保評估作業之有效性。

伍、強化系統運作可用性之資安措施

辦理電子商務業務者，應強化系統運作可用性之資安措施【如導入分散式阻斷服務攻擊（DDoS）流量清洗、線路流量監控與備援及訂定 DDoS 防禦與應變作業程序等】，並定期辦理 DDoS 實際演練。

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 InformationSystems 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	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。

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、雲端服務安全名詞定義

(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)軟體即服務(SaaS)：雲端服務業者提供軟體使用，承租人能使用軟體，但並不掌控軟體、作業系統、硬體。

(三)平台即服務（PaaS)：雲端服務業者提供作業系統使用，承租人能於此作業系統操作其軟體，可掌控運作軟體的環境也擁有作業系統部分掌控權，但並不掌控作業系統、硬體。

(四)基礎設施即服務（IaaS)：雲端服務業者提供基礎運算資源（如處理能力、儲存空間、網路元件或中介軟體)，承租人能掌控作業系統、儲存空間、已部署的應用程式及網路元件（如防火牆、負載平衡器等)，但並不掌控雲端基礎運算資源。

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、若使用雲端服務涉及保險業作業委託他人處理應注意事項之範疇，應依據其規定辦理監督與查核、境外規定要求、緊急應變及營運持續計畫等機制。

五、採用 IaaS 或 Paas 雲端服務模式者，應符合下列規定：

(一)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。

(二)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。

(三)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)。

(四)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)。

(五)保險業應確保資料之刪除、銷毀或不可復原，並留存必要之佐證紀錄以供查驗。

六、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）；另應明訂客戶資料保存期限及應留存之相關重要軌跡紀錄。

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

八、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。

九、應遵循「個人資料保護法」，資料當事人如申請行使其權利，要求停止處理或利用其資料，應確保其資料皆從雲端刪除或提供相關佐證。

十、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「保險業電子商務身分驗證之資訊安全作業準則」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)。

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。

九、應於首次使用生物辨識技術、每年定期及技術有重大變更時(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實際連線於 Internet 或 Intranet 之辦公公用設備（包括但不限於事務機、網路電話機、傳真機及印表機）、門禁監控（包括但不限於門禁、DVR 等）、環境管控（包括但不限於環境感測器、網路攝影機）等實體裝置或設備。

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、設備 IP、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始得進行資料存取、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，密碼長度不應少於八位，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，若設備現階段未能符合本條所要求之控管措施，則依本作業準則第九條規定辦理。

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，限制其對網際網路不必要之網路連線；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或該物聯網設備不與公司內部網路介接。

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、汰換物聯網設備時，應訂定汰除作業程序以避免儲存於物聯網設備資料外洩。

十三、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、十二之要求辦理。

附件五、保險業網路電子商務身分驗證之資訊安全作業準則

一、為協助保險業使用網路身分驗證時，可建立有效的安全驗證機制，以確保減少身分冒用及詐騙情事發生，降低保戶與各公司之機敏資料外洩之風險，特訂定本作業準則。

二、用詞定義及說明：

(一)網路身分驗證：係指於網路應用系統通過特定的身分驗證機制，以確認是否為客戶本人。

(二)多因子驗證(Multi-Factor Authentication,MFA)：係指為強化帳號密碼管理，降低系統相關帳號密碼遭假冒或竊用之風險，提高系統整體安全性並使用二種以上因子驗證方式。

三、各會員公司電子商務系統辦理採用與用戶約定之靜態密碼方式進行身分驗證，相關規則如下:

(一)應至少 8 位數。

(二)應採英數字混合使用，且宜包含大小寫英文字母或符號。

(三)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。

(四)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。

(五)密碼與代號/帳號不應相同。

(六)密碼連續錯誤達五次，各公司應做妥善處理。

(七)變更密碼不得與前一次相同。

(八)首次登入時，應強制變更預設密碼。

(九)密碼超過一年未變更，各公司應妥善提醒客戶密碼變更事宜。

(十)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，其金鑰應儲存於軟體式金鑰管理器並與原資料庫區隔，或搭配經第三方認證（如 FIPS 140-2 Level 3 以上）之硬體安全模組並限制明文匯出功能等。

四、各會員公司電子商務系統辦理採用與用戶約定之一次性密碼(One Time Password)方式進行身分驗證，相關規則如下:

(一)應至少 6 位數。

(二)密碼與帳號不應相同。

(三)輸入密碼連續錯誤達五次，該密碼即失效。

(四)每次密碼有效性不得逾 5 分鐘，逾時即需重新申請發給新密碼。

五、各會員公司提供消費者或保戶辦理身分驗證作業，得依主管機關核准或與保戶線上約定之身分驗證程序或數位憑證辦理；有關主管機關核准之第三方認證方式如下:

(一)內政部核發之自然人憑證與行動自然人憑證。

(二)金融機構核發之金融憑證。

(三)金融行動身分識別聯盟之「金融機構辦理快速身分識別機制」(金融 FIDO) 。

(四)Mobile ID 行動身分識別服務應由提供手機門號之電信業者進行身分驗證。

(五)除第一款至第四款規定之認證方式外，於其他法令或相關函釋另有規定者，從其規定。

六、各會員公司電子商務應用系統得依風險考量採用多因子驗證，其安全設計具有下列三項之任兩項以上技術，其說明如下：

(一)用戶與保險業所約定之資訊，且無第三人知悉（如密碼、圖形鎖、手勢等）。

(二)用戶所持有之設備，保險業應確認該設備為用戶與保險業所約定持有之實體設備（如密碼產生器、密碼卡、晶片卡、電腦、行動裝置、憑證載具等）。

(三)用戶提供給保險業其所擁有之生物特徵（如指紋、臉部、虹膜、聲音、掌紋、靜脈、簽名等），保險業應直接或間接驗證該生物特徵。間接驗證係指由用戶端設備（如行動裝置）驗證或委由第三方驗證，僅讀取驗證結果，必要時應增加驗證來源辨識。

七、各會員公司電子商務應用系統得採用國際組織FIDO聯盟之身分驗證機制。

八、會員公司辦理網路身分驗證，則系統或環境存取需建立身分驗證控管機制，相關規則如下：

(一)建立身份驗證機制應防範自動化程式之登入或密碼更換嘗試。

(二)當進行密碼重設機制(如忘記密碼)時，應針對使用者重新身分確認，並發送一次性及具有時效性符記。

(三)供應商或合作廠商之網路身分驗證，應依合作性質建立適當控管機制，如限制登入IP及加強進行登入身分核實。

九、會員公司當運用網路身分驗證時，應符合各會員公司所訂定之情境下採用適當身分驗證，相關說明如下：

(一)當進行網路投保及網路保險服務時，應符合保險業辦理電子商務應注意事項規範之規定辦理網路投保業務需進行身分驗證作業。

(二)當進行保全/理賠聯盟鏈契約變更及理賠申請時，應符合保全/理賠聯盟鏈業務應遵循事項規範推播通知業務進行註冊及身分驗證作業，同時也應符合保險業辦理電子商務應注意事項之網路保險服務之身分驗證作業之規範以及所屬可執行事項。

附件六、保險業核心資通系統作業委外資安注意事項

一、本注意事項目的

為協助保險業於辦理核心資通系統作業委外過程，於各階段(包括「計畫作業」、「招標」、「決標」、「履約管理」、「驗收」及「保固作業」等)考量相關資訊安全需求，以適當管理供應鏈風險，提升相關系統作業委外安全，特訂定本注意事項。

二、本注意事項所稱核心資通系統，係指核心資訊系統與涉及核心業務持續運作之重要資訊系統。

三、計畫作業階段

(一)核心資通系統作業委外可行性分析：

1. 篩選適合委託辦理之業務項目，確定該項業務委外之資訊安全可行性。
2. 將資安列入成本估算項目，進行效益分析。
3. 評估資訊系統作業委外資安風險與對策。

(二)核心資通系統作業委外開發案，專案成員中應有資安人員參與。

(三)識別核心資通系統作業委外資安需求：

1. 委外業務涉及敏感性或含資安疑慮時，應識別委外廠商之限制。
2. 宜邀請廠商提出資安對應措施方案。

四、招標作業階段

(一)招標文件之制定與發布包含以下項目：

1. 採購產品或服務之資安要求事項。
2. 明定資安要求事項之服務水準（如：系統可用率、安全管控機制、稽核作業、資安檢測與弱點修補之責任與義務等）。
3. 未符合資安要求事項或服務水準時，應訂定罰責標準，依損害程度向委外廠商進行求償或罰款。

(二)準備保密協議書。

(三)委外廠商遴選準則之定義與實作：

1. 委外廠商之資安能量，評估核心系統是否承接過多會員公司之專案及其因應措施。
2. 要求委外廠商允許經授權之第三方稽核，以確認所定義資安要求事項之遵循性。
3. 委外廠商對其提供產品或服務之資安管理機制。

(四)評估委外位置與提供產品或服務之位置，對資安是否有不利影響，並納入評估項目。

五、決標作業階段

與委外廠商簽訂合約或協議時，遵循相關安全管理措施，其內容包含：

(一)應訂定相關資訊安全管理責任，載明與委外廠商雙方之資安角色與責任，若有分包，需一併確認分包計畫可能產生之資安風險。

(二)資訊安全事件之通報流程及處理程序。

(三)委外廠商履行合約或協議時所提供軟體(或交付標的物)為交付產品，需具備合法性且不得違反智慧財產權之規定或侵害第三人合法權益，確認軟體(含元件)之使用版權及安全性。

(四)委外廠商進行資訊系統開發或維運時，若涉及客戶、員工個人資料，需考量具個人資料安全防範措施。

(五)委外廠商提供之優規產品或服務，仍需確認可能產生之資安風險。

六、履約管理階段

(一)建立委外廠商管理規範，其內容應含委外廠商之人員管控，雙方皆應指定專案負責人，負責督導及辦理各項資安要求事項。

(二)持續識別資訊系統作業委外風險，並採取適當管控措施。

(三)監督廠商於人員、實體環境及委外管理等資安要求事項是否落實執行，並建立適當檢驗機制，以確保管理機制有效落實。

(四)委外廠商對相關作業人員進行資訊安全教育訓練，使其充分了解資安政策及責任。

七、驗收作業階段

委外作業於驗收程序，注意事項如下：

(一)顧問訓練類:確認使用檢測工具的安全性和教育訓練時安裝軟體的安全性。

(二)系統發展類：

1. 要求委外廠商揭露第三方程式元件之來源與授權。

2. 要求委外廠商提供資訊系統之安全性檢測證明，如：源碼檢測、弱點掃描或滲透測試等。

(三)維運管理類：每半年執行系統弱點掃描。

(四)雲端服務類：確認雲端服務供應商宣稱之資安認證範圍（含功能）。

委外關係終止或結束時，應依本自律規範第十六條第一項之規定辦理。

八、保固作業階段

(一)保固服務：系統異常造成運作中斷或部分無法正常運作時，如可歸責於廠商時，廠商應依契約規定，履行保固服務或進行異常管理。

(二)異常管理：系統若有重大資安問題，應有變更計畫，評估潛在資安衝擊

及提供變更及復原程序。

九、其他應注意事項

(一)於籌獲套裝軟體時，應確認可能產生之資安風險。

(二)核心資通系統作業委外服務案中，委外廠商有須結合第三方服務提供者(Third-party Service Provider, TSP)方能提供完整服務之情形，應將TSP可能產生之資安風險納入評估。