保險代理人公司資訊安全作業控管自律規範

遵奉金融監督管理委員會102年7月19日金管保綜字第10202075951號函示辦理
103年1月24日第5屆第12次理事會議決議訂定
103年1月28日金管保綜字第10202163713號函准予備查
遵奉金融監督管理委員會保險局103年12月2日保局(綜)字第10302572750號書函暨
保險局103年11月19日召開資安自律規範檢視會議決議辦理修訂
104年1月22日第6屆第5次理監事聯席會議決議暨105年1月28日第6屆第9次理監事聯席會議決議修訂
遵奉金融監督管理委員會105年4月8日保局(綜)字第10510906620號函示辦理
105年7月29日第6屆第11次理監事聯席會議決議
遵奉金融監督管理委員會保險局105年11月2日保局(綜)字第10502105320號函示辦理
105年11月10日第6屆第12次理監事聯席會議決議
106年3月7日金管保綜字第10602000460號准予備查
遵奉金融監督管理委員會保險局107年10月3日保局(綜)字第10704188522號函示辦理
107年11月28日第7屆第8次理監事聯席會議決議
遵奉金融監督管理委員會108年2月1日金管保綜字第10704228870號准予備查
108年2月26日第7屆第9次理監事聯席會議追認修訂
遵奉金融監督管理委員會保險局112年10月31日保局(綜)字第1120434468號准予備查
112年11月2日第9屆第3次理監事聯席會議追認修訂

第一條

中華民國保險代理人商業同業公會（以下簡稱本公會）為促進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，確保本公會所屬會員公司資訊處理作業能安全有效地運作，特訂定本自律規範以為遵循。

第二條

前條所稱資訊資產係包含軟體、硬體、環境、文件、通訊、資料及人員。

本自律規範所指資訊設備係指具備處理、傳輸、儲存電子形式資訊功能之電子產品，包括但不限於下列設備：

一、各等級伺服主機；

二、個人電腦（PC）、筆記型電腦（NB）、平板電腦（tablet PC）與行動裝置（mobile device）等設備。

第三條

各會員公司應視實際使用之資訊資產確實依據各公司訂立之資安處理程序規定及其應注意事項辦理外，並應依本自律規範辦理。但因受限於營運規模，無獨立資安單位及專職資安人員配置之公司，本自律規範第五條、第十一條至第十六條資訊安全管理規定，得視公司營運規模、使用之資訊系統類別、業務營業需求參酌辦理即可，惟仍須遵循相關法令要求。

第四條

各會員公司應確實遵循下列規定：

一、延攬人員時，應依據相關法令合約、產業文化及業務需求，進行相當的人員背景查驗。

二、各公司成員應要求首聘任之人員簽署「資訊安全保密切結書」或於雇用契約、工作手冊明訂成員應遵守資訊安全保密協定。

三、各會員公司所委外業務之公司或自然人，應於委外契約中明訂資訊安全保密，以保障公司資訊安全。

四、所有公司成員應透過定期、適當的教育訓練，告知內部人員應遵循的資訊安全政策規範。

五、管理階層須要求人員遵循公司既定之資訊安全規範。

六、所屬人員職務異動時，應依既定程序辦理資訊業務與相關資訊資產退回與存取權限的變更或取消。

第四條之一

前條所指教育訓練依其所任職務分為二類標準：

一、資訊人員：每人每年至少接受三小時以上之資訊安全相關教育訓練（如資通安全通識教育訓練、資通安全專業課程訓練等）。

二、一般使用者及主管：每年應安排至少一次定期、適當的教育訓練。

保險代理人公司使用之電腦系統如為直接提供客戶自動化服務、對營運有重大影響、或經人工介入直接或間接提供客戶服務，應要求合作廠商對其專案執行人員辦理資訊安全教育訓練。

保險代理人公司得視公司營運規模、使用之資訊系統類別、業務營業需求聘用資通安全專責人員，該人員每年應至少接受十二小時以上之資通安全專業課程訓練。

第五條

各會員公司應參考國際資安管理標準(ISMS)訂定使用資訊設備（含自攜資訊設備（BYOD））之相關規範，其內容應至少包含下列項目：

一、使用資訊設備透過公司內部網路連至外網或有（無）線通訊方式連接至公司內部網路及存取資料管理。

二、資訊設備的外接式存取裝置之使用管理。

三、資訊設備使用之安全控管程序。

四、物聯網（IOT）設備管理之安全控管程序。

第六條

各會員公司應訂定使用社群媒體及電子郵件之相關規範，其內容應至少包含下列項目：

一、訂定使用社群媒體之管理辦法。

二、不得使用社群媒體討論公司機密訊息。

三、嚴禁使用他人的帳號來傳送、存取電子郵件。

四、公司機密性或專有資訊，透過電子郵件傳送之規定。

五、公司應加強人員資安宣導社群媒體及電子郵件之網路安全教育。

第七條

各會員公司應訂定使用雲端(含私有雲)服務之相關規範,其內容應至少包含下列項目:

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、避免因使用雲端服務導致共享環境所造成的資安問題。

三、於雲端服務進行存取時,應防止資料遺失或外洩,並予以適當之備份。

四、雲端服務的資安教育宣導。

五、不得使用不安全的介接介面。

六、規劃雲端運算解決方案的安全和隱私性。

七、謹慎處理公司置放於雲端資料之管理。

第八條

各會員公司若有建置或提供行動裝置應用程式給消費者或內部人員使用,應遵循保險代理人公司行動裝置應用程式作業原則(如附件),以強化行動裝置之安全性。

第九條

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「保險代理人公司辦理電腦系統資訊安全評估作業原則(如附件)」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。

各會員公司欲建置資通系統之資通服務,若有個人資料檔案,應遵循資通系統防護基準;且針對勒索軟體之威脅,應採取勒索軟體之應處及防護。

第十條

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。

第十一條

各會員公司應制定嚴謹之使用者電腦帳號、密碼及權限管理規範,並依循下列管理原則:

一、電腦帳號之建立、修改、啟用、停用及刪除之作業,並定期審核帳號與權限的合宜性。

二、應制定嚴謹之使用者電腦帳號的密碼管理原則,包含密碼長度、複雜性、預設密碼變更、變更周期、幾代密碼不應相同、連續輸入錯誤鎖定、保管方式與密碼須經編碼後以暗碼形式傳輸及儲存等要求,並明確告知使用者對於密碼保護的責任,且應禁止共用使用者電腦帳號。

三、應訂定資訊系統存取控制規定，負責重要資訊系統作業之管理及操作人員，應以足能遂行業務運作需求之最小權限（least privilege）為原則劃分其權責，並納入權責分工（segregation of duty）與監督牽制（maker-checker control）機制，以建立分項負責之制度，並分別配賦相關人員必要的安全責任。如可能，應實施人員輪調，以強化內部控制之機制。

第十二條

各會員公司應制定遠端登入存取管理規範，並依循下列管理原則：

一、進行遠端登入使用之資訊設備，其資訊安全管制與防護措施，不應低於連結於內部資訊網路所應有之安全管制與防護等級；如因特殊需要無法達成（例如：使用自攜資訊設備），應研擬安全管制與防護補強措施。

二、應針對遠端登入之需求進行管制，除採用加密機制建立傳輸安全管道，並應預先定義存取權限並加以管理。

三、應保存遠端登入連線紀錄，包含遠端登入、登出時間與登入帳號等，並研擬適當的連線紀錄審查機制。

第十三條

各會員公司應針對客戶權益相關之保險代理業務資訊系統之存取留存特定事件日誌，並依循下列管理原則：

一、日誌紀錄內容應包含事件類型、發生時間、發生位置及任何與事件相關之使用者身分或設備識別等資訊，並規範日誌留存週期，留存期限至少應六個月。

二、確保完整保存、無遭竄改之虞並應限縮存取權限，並確保日誌產生之時戳（time stamp）同步校時，以利後續關聯性分析與追蹤。

三、應監控前述日誌儲存系統之容量充足性與系統之可用性，於異常發生即時通知管理人員於規定時限內有效復原，避免造成日誌保存之漏失。

第十四條

各會員公司應針對客戶權益相關之保險代理業務資訊系統研擬營運持續對策，並依循下列管理原則：

一、為確保資訊系統與資料之完整性，並降低遭遇勒索惡意軟體攻擊所可能造成的傷害，應制定重要資料（包含但不限於系統源碼）備份程序並定期或不定期執行，以確保資料的安全性（safety）與客戶權益相關之保險代理業務資訊系統之可用性（availability），建議遵循下列「3-2-1 備份原則」並定期測試驗證備份資料之可用性，以確保備份的有效性：

（一）至少製作三份備份；

（二）將備份分別存放在二種不同儲存媒體（例如：離線儲存或使用一寫多讀(WORM)之設備等）；

（三）至少一份放在異地保存。

二、應綜合考量客戶權益相關之保險代理業務資訊系統重要性與可容許中斷時間（Maximum Tolerable Downtime：MTD 或 MTPD），研擬符合成本效益之客戶權益相關之保險代理業務資訊系統備援、災難復原（disaster recovery）環境與復原順序，訂定災難復原計畫並定期演練，以確保業務持續運作。

三、資訊系統下線時，應評估歷史資料之保存期限，並依法令、主管機關、國際組織（例如：VISA、MasterCard）規定辦理。資料備份如必須使用其他備份軟體進行資料備份情況下，應確定保留回存（restore）之系統環境及所需軟體及版權，確保合法使用。

第十五條

各會員公司客戶權益相關之保險代理業務資訊系統之開發與維運，應依循下列管理原則：

一、開發新資訊系統或變更現有資訊系統，應依據該資訊系統之重要性，在開發規劃階段，即應將符合機密性、完整性與可用性及與資訊系統重要度相符的適當資訊安全管控措施納入功能(例如：使用者輸入資料之合法性檢查(如字元集、長度、數值範圍為可接受值等、或使用者成功登入後之 Session ID 管理等)，並應將此資訊安全管控措施延續至營運維護階段，且留存資訊系統發展生命週期之必要文件。

二、資訊系統開發如委外辦理，應將資訊系統資訊安全防護基準與檢核納入需求規格，並應於委外合約中明定著作權之歸屬與使用權的範圍，且清楚約定委外廠商於資訊安全維護之責任與違反時之罰則。

三、應酌衡資訊系統之資安風險進行適切的網路網段區隔（例如：區隔營運網段與測試網段），以避免具不同資安風險等級之資訊設備在同一網路網段內產生未知資安威脅。存在於同一安全風險環境之資訊資產，應以同一標準之資訊安全管控。

四、除依循「保險代理人公司辦理電腦系統資訊安全評估作業原則（如附件）」制定資訊安全弱點掃描管理原則，定期或不定期執行安全性檢測(弱點掃描、滲透測試)，並適時修補安全漏洞。資訊系統開發上線前，應視變更範圍評估進行弱點掃描之必要性。

第十六條

各會員公司資訊系統之脆弱性管理，應依循下列管理原則：

一、應充分運用「金融資安資訊分享與分析中心（F-ISAC）」，及外部資安專業廠商提供之資安威脅情資分享，即時檢視資訊架構、資訊系統受威脅情形，修補資訊安全弱點風險或提出風險減緩之補強措施，並適時調整資訊架構或增加資訊安全防護措施。

二、應依循「保險代理人公司辦理電腦系統資訊安全評估作業原則（如附件）」制定資訊安全弱點掃描管理原則，定期或不定期執行安全性檢測(弱點掃描、滲透測試)，並適時修補安全漏洞。

三、應建立資訊系統監控機制，充分運用「金融資安資訊分享與分析中心（F-ISAC）」研析攻擊者入侵過程的特徵行為，進而提供獵捕該特徵行為之事件（event）監控規則，並視需要將規則設定於資安事件監控機制內，藉由觸發之告警，可即時掌握整體資訊環境之安全狀況。另應針對資安防護管制相關之資訊系統進行容量、效能與可用性監控，避免失效而產生資訊安全防護空窗期。

四、應建立資訊安全通報與緊急應變管理機制，如發現資訊系統有異常狀況潛在原因時，應進行通報與應變改善相關程序，相關通報與應變程序應定期演練。

五、應掌握資訊系統軟硬體產品之生命週期（end of support）並預作因應，以降低資安風險。

第十七條

各會員公司若有辦理網路投保及網路保險服務業務，應建立偽冒網站與行動裝置 APP 偵測、封鎖、下架或告警機制，以防制如釣魚網站攻擊、偽冒行動裝置 APP 詐欺或竊取客戶個人機敏資訊等偽冒事件威脅，並應提供客戶安全教育宣導以提醒客戶注意。

第十八條

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，若發生資訊安全事故或是個人資料外洩時，應儘速回報本公會及主管機關，並採取其他處理措施以控制資安事件影響範圍之擴大。

第十九條

各會員公司應將本自律規範內容納入內部資訊安全業務及資安處理制度及程序。另已實施內稽內控制度之會員公司，應納入內稽內控制度，並定期辦理查核。

第二十條

各會員公司違反本自律規範經查核屬實者，提報本會理事會依章程規定處置，前述處理情形並應於 1 個月內報主管機關。

第二十一條

本規範由中華民國保險代理人商業同業公會訂定，經理事會決議通過報主管機關備查後施行，修正時亦同。

本自律規範除於中華民國一一二年十月三十一日修正發布之第五條、第十一條至第十六條資訊安全管理規定，應於修正發布日後一年內完成調整外，自發布日施行。