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次理監事聯席會議決議修訂

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

前項所稱資訊資產係包含軟體，硬體，環境，文件，通訊，資料，人員。

第三條

各會員公司應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。

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。

第五條

各會員公司應訂定使用行動裝置（含BYOD）之相關規範，其內容應至少包含下列項目：

一、使用行動裝置透過公司內部網路連至外網或有線通訊方式連接至公司內部網路及存取資料管理。

二、外接式存取裝置之使用管理。

三、使用行動裝置之安全控管程序。

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。

第十條

各會員公司若有辦理網路投保及網路保險服務業務,應建置偵測釣魚網站機制，提醒客戶防範網路釣魚，並應提供客戶安全教育宣導。

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。

第十三條

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。

第十四條

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。

第十五條

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。