附件一

「壽險業辦理資訊安全防護自律規範」建議修正條文

建議修正內容	現行條文	說明
第一條 中華民國人壽保險商業同業公會（以下簡稱本公會）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。	第一條 中華民國人壽保險商業同業公會（以下簡稱本公會）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。	未修正。
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、行動裝置（Mobile device）：亦稱為移動設備、流動裝置或手持裝置（handheld device）等，係指一種可攜帶的計算裝置。典型的行動裝置如智慧型手機、行動電話、攜帶型遊樂器與平板電腦、筆記型電腦等。 三、員工攜帶自有設備上班BYOD（BringYour Own Device）：指公司政策允許員工可以在公司內使用自己的筆電、手機、平板等行動裝置來連接到公司網路取用資料，或進行公務處理。	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、行動裝置（Mobile device）：亦稱為移動設備、流動裝置或手持裝置（handheld device）等，係指一種可攜帶的計算裝置。典型的行動裝置如智慧型手機、行動電話、攜帶型遊樂器與平板電腦、筆記型電腦等。 三、員工攜帶自有設備上班BYOD（BringYour Own Device）：指公司政策允許員工可以在公司內使用自己的筆電、手機、平板等行動裝置來連接到公司網路取用資料，或進行公務處理。	未修正。
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	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	未修正。

建議修正內容	現行條文	說明
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。	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、延攬員工時，應依據相關法令、合約、產業文化及業務需求，瞭解該員之背景、學經歷。 二、應要求所聘任之員工簽署資訊安全保密切結書、雇佣契約、工作手冊或相當文件，明訂員工應遵守資訊安全保密協定。 三、有委外業務者，應於委外契約中明訂資訊安全保密協定。 四、應透過定期、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。 五、管理階層應督導員工遵循公司既定之資訊安全規範。 六、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、延攬員工時，應依據相關法令、合約、產業文化及業務需求，瞭解該員之背景、學經歷。 二、應要求所聘任之員工簽署資訊安全保密切結書、雇佣契約、工作手冊或相當文件，明訂員工應遵守資訊安全保密協定。 三、有委外業務者，應於委外契約中明訂資訊安全保密協定。 四、應透過定期、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。 五、管理階層應督導員工遵循公司既定之資訊安全規範。 六、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。	未修正。
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、訂定行動裝置管理規範。 二、使用行動裝置使用人員管理規範。 三、使用行動裝置之安全控管規範。	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、訂定行動裝置管理規範。 二、使用行動裝置使用人員管理規範。 三、使用行動裝置之安全控管規範。	未修正。
第六條 各會員公司應訂定使用社群媒體相關規範，其內容應至少	第六條 各會員公司應訂定使用社群媒體相關規範，其內容應至少	未修正。

建議修正內容	現行條文	說明
包含下列項目： 一、訂定使用社群媒體管理與監督機制。 二、若屬該公司之社群媒體者，應揭露相關資訊，至少包含下列事項： (1) 公司名稱。 (2) 主營業場所地址、通訊連絡方式。 三、制定申訴處理機制。	包含下列項目： 一、訂定使用社群媒體管理與監督機制。 二、若屬該公司之社群媒體者，應揭露相關資訊，至少包含下列事項： (1) 公司名稱。 (2) 主營業場所地址、通訊連絡方式。 三、制定申訴處理機制。	
第七條 各會員公司應訂定使用雲端服務（含私有雲）之相關規範，其內容應至少包含下列項目： 一、訂定雲端服務安全管理規範。 二、訂定雲端服務提供者遴選機制。 三、訂定雲端服務持續營運管理規範。	第七條 各會員公司應訂定使用雲端服務（含私有雲）之相關規範，其內容應至少包含下列項目： 一、訂定雲端服務安全管理規範。 二、訂定雲端服務提供者遴選機制。 三、訂定雲端服務持續營運管理規範。	未修正。
第八條 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，並依據壽險業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。	第八條 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，其內容應至少包含下列項目： 一、需定期評估其有效性。 二、定期使用弱點掃描。 宜有適度加密機密資料內容及加強防護工具。	為改善並提升網路與資訊系統安全防護能力，參考銀行業「金融機構辦理電腦系統資訊安全評估辦法」，訂定「壽險業辦理電腦系統資訊安全評估作業原則」，各會員公司若有建置管理系統及有關個資之資安資料，應依前揭評估作業原則辦理各項資訊安全評估作業。

建議修正內容	現行條文	說明
第九條 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，應儘速回報本公會及主管機關，並採取適當處理措施，以控制資安事件影響範圍之擴大。	第九條 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，應儘速回報本公會及主管機關，並採取適當處理措施，以控制資安事件影響範圍之擴大。	未修正。
第十條 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。	未修正。
第十一條 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，提報經本會理監事會通過後，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。	第十一條 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，提報經本會理監事會通過後，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。	未修正。
第十二條 本規範由中華民國人壽保險商業同業公會訂定，經理監事會決議通過報主管機關備查後施行，修正時亦同。	第十二條 本規範由中華民國人壽保險商業同業公會訂定，經理監事會決議通過報主管機關備查後施行，修正時亦同。	未修正。

附件二

「壽險業辦理電腦系統資訊安全評估作業原則」

<table>
<tr><th>現行條文</th><th>說明</th></tr>
<tr><td>壹、前言
為確保壽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。</td><td>本評估作業原則係依「壽險業辦理資訊安全防護自律規範」第 8 條內容辦理，爰修正相關文字以資明確。</td></tr>
<tr><td>貳、評估範圍
一、壽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。</td><td>參考銀行業「金融機構辦理電腦系統資訊安全評估辦法」之「貳、評估範圍」條文一及二，爰修正相關文字以配合行業特性。</td></tr>
<tr><td>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：
<table><tr><th>電腦系統類別</th><th>定義</th><th>評估週期</th></tr><tr><td>第一類</td><td>直接提供客戶自動化服務或對營運有重大影響之系統(如網路投保、線上保單交易系統、保單貸款 ATM 系統等系統）</td><td>每年至少辦理一次資訊安全評估作業</td></tr><tr><td>第二類</td><td>經人工介入以直接或間接提供客戶服務之系統(如作業中心、客戶服務、新契約受理、契約變更受理、保單行政系統等系統）</td><td>每三年至少辦理一次資訊安全評估作業</td></tr><tr><td>第三類</td><td>未接觸客戶資訊或服務且對營運無影響之系統(如人資、財會、總務等系統）</td><td>每五年至少辦理一次資訊安全評估作業</td></tr></table></td><td>1. 參考銀行業「金融機構辦理電腦系統資訊安全評估辦法」之「參、電腦系統分類及評估週期」條文一至三，爰修正相關文字以配合行業特性。</td></tr>
</table>

現行條文	說明
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。	2.明確定義需抽測之設備僅限定於財產權屬於公司者。
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。 (二)網路活動檢視 1.檢視網路設備、伺服器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、防毒軟體、資料防護等）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，並比對是否有符合網路惡意行為的特徵。 (三)網路設備、伺服器等設備檢測 1.辦理網路設備、伺服器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)網站安全檢測 1.針對網站進行滲透測試。 2.針對網站進行弱點掃描、程式原始碼掃描或黑箱測試。 3.檢視網站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)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)	1. 參考銀行業「金融機構辦理電腦系統資訊安全評估辦法」之「肆、資訊安全評估作業」條文一及二，爰修正相關文字以配合行業特性。

現行條文	說明
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。 (六)合規檢視 檢視整體電腦系統是否符合本作業原則「伍、資訊系統可靠性與安全性侵害之對策」之規範。 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。	2.參考銀行業「金融機構資訊系統安全基準」，將符合壽險業性質之規範納入其中，惟考量本章節篇幅過鉅，有關「資訊系統可靠性與安全性侵害之對策」之內容，將另闢章節說明。
伍、資訊系統可靠性與安全性侵害之對策 一、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： （一）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。 （二）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。 （三）提升營運可靠性之對策。 （四）故障之早期發現與早期復原對策。 （五）災變對策 二、會員公司應就資訊安全性侵害研擬相關對策，其內容包括： （一）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。 （二）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。 （三）防止非法程式：包含防禦、偵測與復原對策。	參考銀行業「金融機構資訊系統安全基準」之「貳、基準」條文，並擷取其「(參)、技術基準」內「大項目」與「中項目」之內容訂定本業「提升系統可靠性對策」與「安全性侵害對策」之參考標準。
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。	參考銀行業「金融機構辦理電腦系統資訊安全評估辦法」之「伍、社交工程演練」條文，爰修正相關文字以配合行業特性。
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。	1. 參考銀行業「金融機構辦理電腦系統資訊安全評估辦法」之「陸、評估單位資格與責任」條文一至四，爰修正相關

現行條文	說明
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，其資格應符合下列條件之一： 1.通過國內外學術機構或團體所舉辦有關資訊安全管理知識考試及格取得證書者。 2.參加國內外學術機構或團體所舉辦有關資訊安全管理知識教育訓練達一定時數並取得教育訓練合格證明文件者。 3.具相關工作經驗且於金融業工作達一定年資者。 （二）具備資訊安全技術能力，其資格應符合下列條件之一： 1.通過國內外學術機構或團體所舉辦有關資訊安全技術能力考試及格取得證書者。 2.參加國內外學術機構或團體所舉辦有關資訊安全技術能力教育訓練達一定時數並取得教育訓練合格證明文件者。 3.具相關工作經驗且於金融業工作達一定年資者。 （三）具備模擬駭客攻擊能力，其資格應符合下列條件之一： 1.通過國內外學術機構或團體所舉辦有關模擬駭客攻擊能力考試及格取得證書者。 2.參加國內外學術機構或團體所舉辦有關模擬駭客攻擊能力教育訓練達一定時數並取得教育訓練合格證明文件者。 3.具相關工作經驗且於金融業工作達一定年資者。 （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。	文字以配合行業特性。 2.訂定壽險業辦理第一類至第三類電腦系統資訊安全評估作業者應具備條件。
捌、評估報告 「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，且應送稽核單位進行缺失改善事項之追蹤覆查。該報告應併同缺失改善等相關文件至少保存五年。	參考銀行業「金融機構辦理電腦系統資訊安全評估辦法」之「柒、評估報告」條文，爰修正相關文字以配合行業特性。