「保險業辦理資訊安全防護自律規範」部分條文修正對照表

113.04.23

修正條文	現行條文 （金管會 112 年 9 月 7 日金管保綜字第 1120493120 號函准備查）	修正說明
第 3 條 各會員公司辦理資訊安全作業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 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。	因應第 4 條修正，一併修正相關文字。
第 4 條 各會員公司辦理資訊安全作業，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。 六、應每年檢討資訊安全政策及資訊作業相關管理與操作規範，並於發生重大變更（如新頒布法令法規）時審查，以持續確保其合宜性、適切性及有效性。 七、應依據作業流程，識別人員、表單、設備、軟體、系統等資產，建立資產清冊、網路架構圖、組織架構圖及負責人，並定期清點以維持其正確性。 八、應定義人員角色及責任並區隔相互衝突的角色。	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。	一、有鑑於辦理資訊安全「作業」一詞，較貼近各會員公司辦理資訊安全相關業務用語，爰修正第 1 項文字。 二、會員公司應每年檢討資訊作業相關規範，並明訂識別資訊資產及人員分工牽制之角色，爰參酌「金融機構資通安全防護基準」第 3 條之規範內容，增訂本條第 1 項第 6 至 8 款。

修正條文	現行條文 (金管會 112 年 9 月 7 日金管保綜字第 1120493120 號函准備查)	修正說明
第 4 條之 1 各會員公司之營運環境管理人員應遵循下列事項： 一、應建立人員之註冊、異動及撤銷註冊程序，用以配置適當之存取權限；人員離調職時應儘速移除權限。 二、應列管硬體設備、應用軟體、系統軟體之最高權限帳號及具程式異動、參數變更權限之帳號。 三、應確認人員之身分及存取權限，必要時得限定其使用之機器或網路位置（IP）。 四、人員超過一定時間未操作個人電腦時，應設定密碼啟動螢幕保護程式或登出系統。 五、登入作業系統進行系統異動或資料庫存取時，應留存操作紀錄，除利用系統代登外，應於使用後儘速變更密碼；但因故無法變更密碼者，應建立監控機制，避免未授權變更，並於使用後覆核其操作紀錄。 六、帳號應採一人一號管理，避免多人共用同一個帳號為原則，如有共用需求，申請及使用須有其他補強管控方式(如使用後更換密碼、代登入機制、密碼拆分保管等)，並留存操作紀錄且應能區分人員身分。 七、採用固定密碼進行身分確認者應符合下列要求： (一)訂定密碼檢核邏輯。	（無）	一、本條新增。 二、為訂定營運環境管理人員規範，以確保依最小權限及僅知原則配發權限予人員使用，爰參酌「金融機構資通安全防護基準」第 4 條之規範內容，增訂本條。 三、惟如個人電腦係用於特定用途者(如監控)，則無須依本條第 4 款辦理設定密碼啟動螢幕保護程式或或登出系統。 四、因於利用系統代登之情形，該系統將於登出後自動變更密碼，毋須另行變更，故於第 5 款中段予以排除。

修正條文	現行條文 (金管會 112 年 9 月 7 日金管保綜字第 1120493120 號函准備查)	修正說明
(二)提供給人員使用之帳號於使用後三個月內應變更密碼。 (三)提供給系統使用之帳號應採取適當之管控措施(如限制人工登入、監控告警)。 八、加解密程式或具變更權限之公用程式(如資料庫工具程式)應列管並限制使用,防止未經授權存取並保留稽核軌跡。 九、最高權限帳號使用時應先取得權責主管或授權人員同意並保留稽核軌跡。 十、具最高權限帳號、特殊功能(如程式或軟體異動、參數或組態變更權限等)權限帳號應和日常維運用帳號區隔,並每月抽查使用結果,以防範未經授權使用;如為核心資通系統,應於該等帳號被使用後,覆核使用結果。 十一、提供網際網路服務之伺服器及AD(網域服務)主機,對於最高權限 帳號及特殊功能權限帳號,應採雙因子認證或納入特權帳號管理系統強化授權及監控。 十二、應針對第一類及第二類電腦系統依最小權限(least privilege)及僅知原則(need-to-know)配發權限予人員使用並定期審 查帳號、		

修正條文	現行條文 (金管會 112 年 9 月 7 日金管保綜字第 1120493120 號函准備查)	修正說明
權限之合理性及異常存取紀錄，以符合職務分工及牽制原則。		
第 5 條 各會員公司應視資訊系統規模與架構，訂定資訊系統之範圍與相關作業規範： 一、訂定資訊系統開發及程式修改作業程序。 二、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。 三、訂定核心資訊系統與第一類電腦系統中遠距服務、行動服務及電子商務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	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	一、為擴大本條適用範圍至全資訊系統，爰修正本條第 1 項及同項第 2 款。 二、原同款第 1 項第 1 款與第 2 款之款次對調。 三、考量同屬第一類電腦系統之遠距投保、行動服務、電子商務資訊系統，其等置換作業程序應比照核心資訊系統，爰修訂本條第 1 項第 3 款，將前揭系統納入適用範圍。

修正條文	現行條文 (金管會 112 年 9 月 7 日金管保綜字第 1120493120 號函准備查)	修正說明
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	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。	

修正條文	現行條文 (金管會 112 年 9 月 7 日金管保綜字第 1120493120 號函准備查)	修正說明
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。	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。	有鑑於產、壽險公司均已採電腦化作業，原條文所定「若有建置管理系統及有關個資之資安資料」等語已屬贅文，爰予刪除。
第 13 條 各會員公司應加強資訊安全事故管理。 各會員公司若發生資通安全事件，足以影響保險業信譽、或危及保險業正常營運、或金融秩序情事者，應依「保險業通報重大偶發事件之範圍申報程序及其他應遵循事項」規定辦理通報及回報各所屬公會,並採取適當處理措施,以控制資安事件影響範圍之擴大。	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。	會員公司如發生重大資通安全事件，應遵循「保險業通報重大偶發事件之範圍申報程序及其他應遵循事項」辦理，修正第 2 項文字，以資明確。
第17條 各會員公司電腦系統應加強日誌紀錄管理，並遵循下列事項： 一、應評估各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）之保留機制。	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	一、為將系統事件日誌紀錄保留機制之適用系統,擴大為全資訊系統,爰修正第 1 項第 1 款。 二、增訂第一、二類電腦系統日誌紀錄送至原系統外之其他系統進行集中管理之相關規定,並調整條文文字架構,及修正第 1 項第 2 款及

修正條文	現行條文 （金管會 112 年 9 月 7 日金管保綜字第 1120493120 號函准備查）	修正說明
二、第一類、第二類電腦系統日誌應至少遵循下列規定辦理： (一)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，且定期將日誌紀錄送至原系統外之其他系統進行集中管理，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，設定合適告警指標並定期檢討修訂；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。	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。	同款第 1、2 目。 三、確保可對資安事件迅速回應，乃增訂日誌異常分析告警機制，而修正第 2 款第 3 目。