「保險業辦理資訊安全防護自律規範」修正條文對照表

修正條文	現行條文 （金管會110年12月30日金管保綜字第1100495362號函准備查）	修正說明
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~~、其至少應包括成本效益分析、風險評估、需求分析、設計規劃、功能測試驗證(含完整性、正確性與穩定性)、轉換決策評估及平行測試等~~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)	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。	一、依金管會110.12.30金管保綜字第1100495362號函說明三、(二)、1，參考金融機構資通安全防護基準第15條規定，就第5條第3款之核心系統作業規範，增訂核心系統轉換之前、中、後作業程序。 二、修正前之第3款僅列舉核心系統置換程序之大項目。爰參酌金融機構資通安全防護基準第15條規定，就核心系統轉換之前、中、後作業程序，應依資訊作業內容調整。 三、依保險局111年12月6日保局(綜)字第1110495063號函所附會議記錄決議(一)、1修正第3款第1目第3子目規定。

修正條文	現行條文 （金管會110年12月30日金管保綜字第1100495362號函准備查）	修正說明
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		

修正條文	現行條文 （金管會110年12月30日金管保綜字第1100495362號函准備查）	修正說明
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：。 ~~一、應依據保險業經營電子商務自律規範及保險業網路投保註冊會員密碼之設計安全作業準則（如附件五）辦理，以確保電子商務之資訊安全，降低遭破解之風險。~~ ~~二、運用網路身分驗證技術，依據保險業網路身分驗證之資訊安全作業準則(如附件六)辦理，以建立安全有效之驗證機制，減少身分冒用及詐騙情事發生，並降低保戶及會員公司之機敏資料外洩風險。~~	第10條 各會員公司辦理電子商務，應遵循下列事項，以確保電子商務之資訊安全： 一、應依據保險業經營電子商務自律規範及保險業網路投保註冊會員密碼之設計安全作業準則（如附件五）辦理，以確保電子商務之資訊安全，降低遭破解之風險。 二、運用網路身分驗證技術，依據保險業網路身分驗證之資訊安全作業準則(如附件六)辦理，以建立安全有效之驗證機制，減少身分冒用及詐騙情事發生，並降低保戶及會員公司之機敏資料外洩風險。	依金管會110.12.30金管保綜字第1100495362號說明三、(二)、2，第10條電子商務應遵循事項，整併修正前之附件五及附件六，並刪除本條第1、2款文字。
第13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，~~若發生重大資訊安全事故件時，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13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。	一、依據「保險業內部控制及稽核制度實施辦法」第6條第2項規定，請定期檢討保險業辦理資訊安全防護自律規範，俾因應保險業務發展之資訊安全防護需要，修正本條文字。 二、因「資訊安全事件通報應變作業實施原

修正條文	現行條文 （金管會110年12月30日金管保綜字第1100495362號函准備查）	修正說明
		則」尚未訂定，各公司於原則訂定前應先回歸「保險業通報重大偶發事件之範圍與適用對象」及各公司內規進行相關資安事件通報。
第14條 各會員公司若有建置網際網路應用系統（如網路投保、網路要保等直接提供客戶自動化服務之系統）及核心資訊系統，應定期辦理相關安全性檢測，~~以確保網際網路應用系統之~~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	第14條 各會員公司若有建置網際網路應用系統（如網路投保、網路要保等直接提供客戶自動化服務之系統），應定期辦理相關安全性檢測，以確保網際網路應用系統之資訊安全： (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，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。	一、依金管會110.12.30金管保綜字第1100495362號說明三、(二)、3.第14條網際網路應用系統安全性檢測，增訂核心系統之相關安全性檢測機制。 二、依保險局111年12月6日保局(綜)字第1110495063號函所附會議記錄決議(一)、2、(1)修正第1款第2目規定。 三、統一開放外網使用之系統於程式碼掃描或黑箱測試相關執行之作業週期頻率，同步修正為應至少每半年執行。 四、依保險局111年12月6日保局(綜)字第1110495063號函所附會議記錄決議(一)、2、(2)修正第2款第2目規定。

修正條文	現行條文 （金管會110年12月30日金管保綜字第1100495362號函准備查）	修正說明
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~~核心~~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	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核心資訊系統作業委外，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	一、依金管會110.12.30金管保綜字第1100495362號說明三、(二)、4.本規範第16條核心系統作業委外應遵循事項： (一)增訂合作結束時之資料處理機制。

修正條文	現行條文 （金管會110年12月30日金管保綜字第1100495362號函准備查）	修正說明
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~~核心~~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。	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核心資訊系統之作業委外廠商評估項目。 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)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。 (三)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。 (四)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	(二)作業委外廠商管理納入「資通安全管理法施行細則」第4條第1項第5及6款規定。 (三)軟硬體供應與維運商管理機制參考「政府資訊作業委外資安參考指引」，列入重要監督項目。 (四)訂定非核心系統委外管理機制。 二、就本條第1項刪除核心二字，並依金管會來函說明就訂定非核心系統委外管理機制也納入本條。 三、依保險局111年12月6日保局(綜)字第1110495063號函所附會議記錄決議(一)、3、(1)修正本條第1項第2款第3目文字。 四、就本條第2款增訂第4目納入資訊系統委外依廠商規模或作業特性進行評估。 五、就本條第3款新增訂第2目之軟硬體供應與維運商管理機制參考「政府資訊作業委外資安參考指引」

修正條文	現行條文 (金管會110年12月30日金管保綜字第1100495362號函准備查)	修正說明
(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~~核心~~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	(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.作業委外廠商進行核心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.應訂定相關資訊安全管理責任。	，列入重要監督項目。並依保險局111年12月6日保局(綜)字第1110495063號函所附會議記錄決議(一)、3、(2)修正文字。 六、就本條第3款各目次調整。 七、就本條第3款第5目第2、3子目，參酌「資通安全管理法施行細則」第4條第1項第5及6款規定，修訂部分文字，並調整子目號次。 八、依保險局111年12月6日保局(綜)字第1110495063號函所附會議記錄決議(一)、3、(3)修訂第3款第5目第3子目文字。 九、依保險局111年12月6日保局(綜)字第1110495063號函所附會議記錄決議(一)、3、(3)增訂第3款第5目第5子目規定。 十、就本條第3款新增第6目增訂合作結束時之資料處理機制。並依保險局111年12月6日保局(綜)字第1110495063號函所附會議記錄決議(一)、3、(4)修正文字。

修正條文	現行條文 (金管會110年12月30日金管保綜字第1100495362號函准備查)	修正說明
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)~~若核心系統作業為委外之業務項目，需符合保險業作業委託他人處理應注意事項之規定，並~~定期進行~~實地~~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「保險業核心資訊系統作業委外資安注意事項」(如附件六)。		十一、 就本條第4款，針對資訊系統委外稽核時訂定更明確範圍及明確需進行查核作業之情況，爰作文字修正。 十二、依111.7.1保局(綜)字第1110433192號函意旨，爰將金管會擬訂之「金融機構資訊委外之資安應注意事項」納入本自律規範，併考量「資訊系統作業委外」、「資訊系統委外作業」內涵範圍不同，皆宜併同遵循「保險業核心資訊系統作業委外資安注意事項」(如修正後之附件六)。遂增訂第16條第2項。並依保險局111年12月6日保局(綜)字第1110495063號函所附會議記錄決議(一)、3、(5)修正該項文字。
第17條 核心資訊系統及直接提供客戶自動化服務系統應加強~~稽核~~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	第17條 核心資訊系統及直接提供客戶自動化服務系統應加強稽核紀錄管理，並遵循下列事項： 一、系統產生之稽核紀錄(內容包	一、依金管會110.12.30金管保綜字第1100495362號說明三、(二)、5，修正本規範第17條核心

修正條文	現行條文 （金管會110年12月30日金管保綜字第1100495362號函准備查）	修正說明
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。 二、事件日誌應設有存取限制，並應用適當方式確保完整性；另應依據事件日誌稽核紀錄之儲存需求~~，應~~配置~~稽核紀錄所需之儲存~~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、系統內部時間應定期進行基準時間源進行同步。	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)應有保留機制及存取管理。	系統及自動化服務系統之稽核紀錄應遵循事項： (一)研議訂定非核心系統之處理機制。 (二)增訂日誌保留時間、定期審查機制、定期備份及保留紀錄完整性。 二、依保險局來函指示，針對核心系統及自動化服務系統之稽核紀錄應遵循事項加以增定，惟有鑑於保險業者產業規模差距甚大，且就日誌管理要求保險業者要求不一，爰不予訂定非核心系統之相關處理，仍回歸至各保險業者內控制度管理。 三、於本條第1款增訂日誌紀錄保留期限。 四、於本條第2款增訂日誌紀錄定期備份及日誌保存紀錄完整性之規定。 五、考量資安監控系統係用以蒐集與資訊安全事件相關之日誌，於本條第3款增訂日誌定期審查機制。
第18條	第十八條	依保險局111年12月6日

修正條文	現行條文 （金管會110年12月30日金管保綜字第1100495362號函准備查）	修正說明
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，且並應定期辦理帳號密碼變更及帳號清查。	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，應採用雙因子認證或相關身分驗證方式且帳號密碼應定期變更。	保局（綜）字第1110495063號函所附會議記錄決議(一)、4修正本條第3款文字。
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		一、本條新增。 二、就本條第1款就增加網路連線機密性與完整性提出保險業對外提供之網站服務事項。 三、就本條第2款就增加內部網段隔離及分行網路依需求分隔並控管橫向連線要求。 四、就本條第3款依前揭函文說明增列跨場

修正條文	現行條文 （金管會110年12月30日金管保綜字第1100495362號函准備查）	修正說明
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。		域連線防護與監控。 五、就本條第4款依前揭函文說明增列對外服務網站需有WAF等防護機制。並依保險局111年12月6日保局（綜）字第1110495063號函所附會議記錄決議(一)、5、(1)修正該項文字。 六、就本條第5款依前揭函文說明增列員工上網行為隔離或監控規劃。 七、就本條第6款依前揭函文說明增列正式環境之管理需於獨立網路連線管理。 八、依保險局111年12月6日保局(綜)字第1110495063號函所附會議記錄決議(一)、5、(2)增訂第七款。 九、就金管會所提網路邊界定義與防護原保險業電腦系統資訊安全評估作業原則之資訊安全評估中資訊架構檢視檢視邊界防護已有包含，爰不另作文字修正。 十、就金管會所提設備識別原保險業電腦系統資訊安全評估

修正條文	現行條文 （金管會110年12月30日金管保綜字第1100495362號函准備查）	修正說明
		作業原則之資訊安全評估中網路活動檢視已有包含，爰不另作文字修正。 十一、就金管會所提外部網路(分點、雲端、Mobile/Home)之內容原保險業電腦系統資訊安全評估作業原則之資訊安全評估中資訊架構檢視檢視及安全設定檢視已包含分點，就雲端、Mobile/Home)議題原保險業運用新興科技作業原則之雲端服務安全控管已包含在內，爰不另作文字修正。
第~~19~~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19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。	條號調整。
第~~20~~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20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。	條號調整。
第~~21~~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	第21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	條號調整。

修正條文	現行條文 （金管會110年12月30日金管保綜字第1100495362號函准備查）	修正說明
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。	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。	

「保險業辦理資訊安全防護自律規範」
附件一、保險業電腦系統資訊安全評估作業原則修正條文對照表

<table>
<tr><th>修正條文</th><th>現行條文
（金管會110年12月30日金管保綜字第1100495362號函准備查）</th><th>修正說明</th></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之系統（如網路投保、網路要保等系統）及核心資訊系統</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>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)</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>非核心資訊系統（如人資、總務等系統，及提供員工外部連線使用之資訊系統）</td><td>每五年至少辦理一次資訊安全評估作業</td></tr></table>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。</td><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之系統（如網路投保、網路要保等系統）及核心資訊系統</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>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)</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>非核心資訊系統（如人資、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>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。</td><td>依據金管會保險局於111年7月7日保局(綜)字第1110429198號函說明二，就「提供員工外部連線使用之資訊系統」維持歸屬為第三類，並依依保險局111年12月6日保局(綜)字第1110495063號函所附會議記錄決議(一)、6、(1)修正本條文字。</td></tr>
<tr><td>肆、資訊安全評估作業</td><td>肆、資訊安全評估作業</td><td>一、參酌「保險業電腦系</td></tr>
</table>

修正條文	現行條文 (金管會110年12月30日金管保綜字第1100495362號函准備查)	修正說明
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。	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	統資訊安全評估作業原則」七大評估之物聯網設備，並為求統一性，新增本條第1項第3款第4目，以進行評估項目以利遵循。 二、依金管會保險局於111年7月7日保局(綜)字第1110429198號函說明二，就「提供員工於外部連線使用之系統」強化相關防護措施。並依保險局111年12月6日保局(綜)字第11104 95063號函所附會議記錄決議(一)、6、(2)修正本條第1項第4款第3目文字。 三、依保險局111年12月6日保局(綜)字第11110495063號函所附會議記錄決議(一)、6、(3)修正本條第1項第5款文字。 四、依保險局 111 年 12 月 6 日保局(綜)字第 1110495063 號函所附會議記錄決議(一)、6、(4)修正本條第 1 項第 5 款第 1 目文字。 五、修正本條第 1 項第 7 款第 1 目第 2 子目文字。 六、新增本條第 3 項，規

修正條文	現行條文 （金管會110年12月30日金管保綜字第1100495362號函准備查）	修正說明
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。 (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	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。 (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。 (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。	定保險業對提供員工外部連線使用之資訊系統。並依保險局111年12月6日保局（綜）字第1110495063號函所附會議記錄決議(一)、6、(5)修正文字。

修正條文	現行條文 （金管會110年12月30日金管保綜字第1100495362號函准備查）	修正說明
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，並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 ~~針對~~保險業~~交付給與~~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 ~~http,~~ https~~,~~ ~~FTP~~、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	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。 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 針對保險業交付給客戶之應用程式進行下列檢測： 1. 提供 http, https, FTP 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	

修正條文	現行條文 (金管會110年12月30日金管保綜字第1100495362號函准備查)	修正說明
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~~昇~~軟體系統之	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。 (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。	

修正條文	現行條文 （金管會110年12月30日金管保綜字第1100495362號函准備查）	修正說明
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	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	

修正條文	現行條文 （金管會110年12月30日金管保綜字第1100495362號函准備查）	修正說明
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。 三、保險業提供員工外部連線使用之資訊系統，應依前項評估項目並定期執行相關作業，包括但不限於弱點掃描、滲透測試、原始碼掃描、強化網頁防竄改機制並納入監控範圍，並於保險業指定時間內完成弱點修補。	入資訊安全評估作業以確保評估作業之有效性。	

「保險業辦理資訊安全防護自律規範」

附件二、保險業提供行動應用程式(App)作業原則修正條文對照表

修正條文	現行條文 (金管會110年12月30日金管保綜字第1100495362號函准備查)	修正說明
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~~形式~~檢核項目，至少包含下列內容： 1. ~~檢測項目是否有缺漏~~檢測標的。 2. ~~檢測項目是否佐證資料不符~~檢測範圍之宣告。 3. ~~檢測結果是否與說明矛盾~~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。		一、依金管會110.12.30金管保綜字第1100495362號說明三、(二)、6.附件二、保險業委託專業機構辦理APP資安檢測中第6條建議增訂實質檢視機制，以確認檢測報告之完整性，落實辦理安全檢測，爰新增該款7目規定，並刪除原條文第1至3目。 二、並依保險局111年12月6日保局(綜)字第1110495063號函所附會議記錄決議(一)、7修正本條第1項第3款文字。

「保險業辦理資訊安全防護自律規範」

附件三、保險業運用新興科技作業原則修正條文對照表

修正條文	現行條文 （金管會110年12月30日金管保綜字第1100495362號函准備查）	修正說明
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	貳、雲端服務安全控管 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、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、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。 五、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。 六、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)。 七、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)。	一、依金管會110.12.30金管保綜字第1100495362號說明三、(二)、7.附件三、保險業運用新興科技作業原則：參考「金融機構運用新興科技作業規範」(109.4.17版)，增加監督及查核機制、境外處理原則、緊急應變計畫、設備更換之資料處理機制等議題。 二、就雲端服務之定義，修正第1項、同項第1款。 三、參酌「金融機構運用新興科技作業規範」(109.4.17版)，就軟體即服務、平台即服務及基礎設施即服務定義，增訂本條第1項第1至3款。 四、參酌「金融機構運用新興科技作業規範」，增訂雲端服務之監督及查核機制、境外處理原則及

修正條文	現行條文 (金管會110年12月30日金管保綜字第1100495362號函准備查)	修正說明
(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)~~四、~~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)~~五、~~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)~~六、~~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)~~七、~~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	八、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)。 九、應監控並建立資通安全事件通報程序。遇事件發生時，相關單位及人員應依循前述通報程序辦理。 十、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。 十一、應制定雲端資料管理程序，並明訂資料保存期限及應留存之相關重要軌跡紀錄。 十二、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。 十三、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「保險業網路投保註冊會員密碼之設計安全作業準則」規定。	緊急應變計畫，並說明依保險業作業委託他人處理應注意事項十七之一(二)、(三)、(四)、(七)及(八)之規定，增訂本條第1項第4款。 五、參酌「金融機構運用新興科技作業規範」第2條第13項，將原附件三、「保險業運用新興科技作業原則」第貳條第4項至第7項修正為第5項第1至4款。 六、參考「金融機構運用新興科技作業規範」第2條第13款第5目，納入設備更換之資料處理(對應金融機構運用新興科技作業規範-設備更換之資料處理(§2第13項之5)，爰增訂本條第第5項第5款。 七、就設備更換資料處理中之維護更換之管理機制於使用Iaas或Paas時，因定期更換設備並不能確保資料之刪除、銷毀或不可復原」行為，因與服務提供者訂定服務水準合約維持可用性及可行

修正條文	現行條文 （金管會110年12月30日金管保綜字第1100495362號函准備查）	修正說明
除、銷毀或不可復原，並留存必要之佐證紀錄以供查驗。 六、~~八、~~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、~~九、~~應監控並建立資訊~~通~~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、~~十、~~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。 ~~十一、應制定雲端資料管理程序，並明訂客戶資料保存期限及應留存之相關重要軌跡紀錄。~~ 九、~~十二、~~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、~~十三、~~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。		性，確保資料之刪除、銷毀或不可復原行為。 八、本條第3、11項所定程序重複，遂將後半段客戶資料留存期限整併入第6項，明確範圍為涉及客戶資料或敏感資料。 九、配合本條第6項修正，將第11項刪除。 十、原附件五「保險業網路投保註冊會員密碼之設計安全作業準則」與原附件六中整併，爰修正第10項規範名稱。 十一、調整本條項次。

修正條文	現行條文 (金管會110年12月30日金管保綜字第1100495362號函准備查)	修正說明
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。		依保險局111年12月6日保局(綜)字第1110495063號函所附會議記錄決議(一)、8修正本條第8項文字。

修正條文	現行條文 （金管會110年12月30日金管保綜字第1100495362號函准備查）	修正說明
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，~~相關控管應符合「保險業經營電子商務自律規範」及「保險業網路投保註冊會員密碼之設計安全作業準則」~~。 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。		

「保險業辦理資訊安全防護自律規範」
附件四、保險業使用物聯網設備作業準則修正條文對照表

修正條文	現行條文 （金管會110年12月30日金管保綜字第1100495362號函准備查）	修正說明
二、本作業準則所稱物聯網設備係指具實際~~網路~~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~~功能之嵌入式系統（具有小型作業系統）設備（以下簡稱設備），包含自動化辦公(OA)設備（如數位錄影機、電話交換機、傳真機、錄音設備、影印機等）及不具備遠端操控介面功能之感測器~~。	二、本作業準則所稱物聯網設備係指具網路連線功能之嵌入式系統（具有小型作業系統）設備（以下簡稱設備），包含自動化辦公(OA)設備（如數位錄影機、電話交換機、傳真機、錄音設備、影印機等）及不具備遠端操控介面功能之感測器。	依金管會110.12.30金管保綜字第1100495362號說明三、(二)、8.附件四、保險業使用物聯網設備作業準則：參考「金融機構使用物聯網設備安全控管規範」（依110.4.30版），修正第2條。
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~~網段~~、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。	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、網段、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。	依金管會110.12.30金管保綜字第1100495362號說明三、(二)、8.附件四、保險業使用物聯網設備作業準則：參考「金融機構使用物聯網設備安全控管規範」（依110.4.30版），修正第3條。
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	七、設備應關閉不必要之網路連線及服務，並避免使用對外公開之網際網路位置，如設備採用	依金管會110.12.30金管保綜字第1100495362號說明三、(二)8.附件四、

修正條文	現行條文 （金管會110年12月30日金管保綜字第1100495362號函准備查）	修正說明
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。	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。	保險業使用物聯網設備作業準則：參考「金融機構使用物聯網設備安全控管規範」（依110.4.30版），修正第7條。

「保險業辦理資訊安全防護自律規範」
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（原名稱：保險業網路投保註冊會員密碼之設計安全作業準則）
修正條文對照表

修正名稱	現行名稱 （金管會110年12月30日金管保綜字第1100495362號函准備查）	修正說明
附件五 ~~保險業網路投保註冊會員密碼之設計安全作業準則~~ 保險業網路電子商務身分驗證之資訊安全作業準則	附件五 保險業網路投保註冊會員密碼之設計安全作業準則	依金管會110.12.30金管保綜字第1100495362號整併原附件五及附件六，修正整併後之附件五名稱。
修正條文	現行條文 （金管會110年12月30日金管保綜字第1100495362號函准備查）	修正說明
~~會員公司若辦理網路投保業務，則網路投保註冊會員時應以靜態密碼或使用一次性密碼(OTP)自行設定，使用規則如下：~~	會員公司若辦理網路投保業務，則網路投保註冊會員時應以靜態密碼或使用一次性密碼(OTP)自行設定，使用規則如下：	原附件五條文全數刪除並於修正後之附件五第3條進行相關說明。
~~一、靜態密碼:~~ ~~1. 應至少8位數。~~ ~~2. 應採英數字混合使用，且宜包含大小寫英文字母或符號。~~ ~~3. 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。~~ ~~4. 不應訂為相同的英數字、連續英文字或連號數字，預設~~	一、靜態密碼: 1. 應至少8位數。 2. 應採英數字混合使用，且宜包含大小寫英文字母或符號。 3. 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。 4. 不應訂為相同的英數字、連續英文字或連號數字，預設	

修正條文	現行條文 （金管會110年12月30日金管保綜字第1100495362號函准備查）	修正說明
~~密碼不在此限。~~ ~~5. 密碼與代號/帳號不應相同。~~ ~~6. 密碼連續錯誤達五次，各公司應做妥善處理。~~ ~~7. 變更密碼不得與前一次相同。~~ ~~8. 首次登入時，應強制變更預設密碼。~~ ~~9. 密碼超過一年未變更，各公司應做妥善處理。~~ ~~10. 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，其金鑰應儲存於經第三方認證（如FIPS 140-2 Level 3以上）之硬體安全模組內並限制明文匯出功能等。~~	密碼不在此限。 5. 密碼與代號/帳號不應相同。 6. 密碼連續錯誤達五次，各公司應做妥善處理。 7. 變更密碼不得與前一次相同。 8. 首次登入時，應強制變更預設密碼。 9. 密碼超過一年未變更，各公司應做妥善處理。 10. 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，其金鑰應儲存於經第三方認證（如FIPS 140-2 Level 3以上）之硬體安全模組內並限制明文匯出功能等。	
~~二、一次性密碼(OTP)：~~ ~~1. 應至少6位數。~~ ~~2. 密碼與帳號不應相同。~~ ~~3. 輸入密碼連續錯誤達五次，該密碼即失效。~~ ~~4. 每次密碼有效性不得超過5分鐘，超過時即需重新申請發給新密碼。~~	二、一次性密碼(OTP)： 1. 應至少6位數。 2. 密碼與帳號不應相同。 3. 輸入密碼連續錯誤達五次，該密碼即失效。 4. 每次密碼有效性不得超過5分鐘，超過時即需重新申請發給新密碼。	
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。	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。	一、本條新增。 二、將修正前之附件六第1條，列為修正後之附件五第1條。
二、用詞定義及說明： (一)網路身分~~認驗~~證：係指於網路應用~~程序~~系統通過特定的身分驗證機制，以確認是否為~~保~~客戶本人。	二、用詞定義及說明： (一)網路身分認證：係指於網路應用程序系統通過特定的身分驗證機制，以確認是否為保戶本人。	一、修正前之附件六第2條未修正，僅改列為修正後之附件第2條。

修正條文	現行條文 （金管會110年12月30日金管保綜字第1100495362號函准備查）	修正說明
(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。	(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。	二、就網路身分認證定義中網路應用程序系統之程序為贅詞，故刪除。 三、辦理網路身分驗證時，因客戶身分未必為保戶，爰作文字修正。
三、~~多因子驗證可運用的因子包含帳號及密碼、一次性密碼(OTP)、智慧卡、憑證、生物特徵辯識、或符合FIDO標準的驗證方式（Fast Identity Online）及Mobile ID行動身分識別服務等，其相關說明如下~~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：	三、多因子驗證可運用的因子包含帳號及密碼、一次性密碼(OTP)、智慧卡、憑證、生物特徵辯識、或符合FIDO標準的驗證方式（Fast Identity Online）及Mobile ID行動身分識別服務等，其相關說明如下： (一)帳號及密碼、一次性密碼(OTP)安全性設計，應參考「保險業網路投保註冊會員密碼之設計安全作業準則」執行。 (二)智慧卡應設有密碼功能(Pin Code)，於晶片進行密碼驗證，晶片應符合共通準則(Common Criteria) EAL 4+以上或其他相同安全強度之認證。 (三)憑證應由憑證機構依經濟部核定之憑證實務作業基準簽發，憑證應具有時效性，過期應立即失效，須重新簽發或展延期限。 (四)生物特徵辯識應符合「保險業運用新興科技作業原則」之(伍、生物特徵資料安全控管)規範。 (五)FIDO應遵循國際FIDO聯盟所訂定之產業技術標準，並符合我國金融行動身分識別聯盟所制訂之相關標準及規範。 (六)Mobile ID行動身分識別	一、原附件六第3條包含帳號及密碼、一次性密碼、智慧卡、憑證、生物特徵及符合FIDO標準相關身分認證方式，並依金管會110.12.30金管保綜字第1100495362號說明三、(二)、2.應用情境於附件五及附件六整併時補充修正。 二、就修正前之附件五靜態密碼中採用與用戶約定方式相關驗證之規定，納為修正後之附件五第3條

修正條文	現行條文 （金管會110年12月30日金管保綜字第1100495362號函准備查）	修正說明
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。 ~~(一)帳號及密碼、一次性密碼(OTP)安全性設計，應參考「保險業網路投保註冊會員密碼之設計安全作業準則」執行。~~ ~~(二)智慧卡應設有密碼功能(Pin Code)，於晶片進行密碼驗證，晶片應符合共通準則(Common Criteria) EAL 4+以上或其他相同安全強度之認證。~~ ~~(三)憑證應由憑證機構依經濟部核定之憑證實務作業基準簽發，憑證應具有時效性，過期應立即失效，須重新簽發或展延期限。~~ ~~(四)生物特徵辯識應符合「保險業運用新興科技作業原則」之(伍、生物特徵資料安全控管)規範。~~ ~~(五)FIDO應遵循國際FIDO聯盟所訂定之產業技術標準，並符合我國金融行動身分識別聯盟所制訂之相關標準及規範。~~ ~~(六)Mobile ID行動身分識別服務應由提供手機門號之~~	服務應由提供手機門號之電信業者進行身分驗證。	

修正條文	現行條文 （金管會110年12月30日金管保綜字第1100495362號函准備查）	修正說明
~~電信業者進行身分驗證。~~		
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。		一、本條新增。 二、增訂電子商務使用一次性密碼(OTP)之規定。
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。		一、本條新增。 二、增訂各會員公司電子商務實際運作主管機關認可之第三方認證之規定。
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		一、本條新增。 二、增訂第6條使用電子商務應用系統採兩項以上技術使用之規定。

修正條文	現行條文 （金管會110年12月30日金管保綜字第1100495362號函准備查）	修正說明
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。		一、本條新增。 二、增訂電子商務應用系統使用國際組織 FIDO 聯盟之身分驗證機制之規定。
八、~~四、~~會員公司辦理網路身分~~認~~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。	四、會員公司辦理網路身分認證，則系統或環境存取需建立身分驗證機制，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。	一、修正前之附件六第 4 條列為修正後之附件第 8 條，並作部份文字修正。 二、第 2 款中情境補充使用者忘記密碼之相關啟動密碼重設機制確認，並發送一次性及具有時效性符記，以利法令解釋及業務配合執行正確。
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		一、本條新增。 二、依金管會 110.12.30 金管保綜字第 1100495362 號說明三、(二)、2，增訂電子商務應用情境。

修正條文	現行條文 （金管會110年12月30日金管保綜字第1100495362號函准備查）	修正說明
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。		

「保險業辦理資訊安全防護自律規範」

附件六、保險業核心資訊系統作業委外資安注意事項修正條文對照表

修正條文	現行條文 （金管會110年12月30日金管保綜字第1100495362號函准備查）	修正說明
一、本注意事項目的 為協助保險業於辦理核心資訊系統作業委外過程，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。 保險業宜參照本注意事項辦理。		參酌「金融機構資訊委外之資安應注意事項」前言，新增本注意事項第1條。
二、計畫作業階段 (一)核心資訊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)核心資訊系統作業委外開發案，專案成員中應有資		依「金融機構資訊委外之資安應注意事項」第1條，新增本注意事項第2條。

修正條文	現行條文 （金管會110年12月30日金管保綜字第1100495362號函准備查）	修正說明
安人員參與。 (三)識別核心資訊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。		
三、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		依「金融機構資訊委外之資安應注意事項」第2條，新增本注意事項第3條。

修正條文	現行條文 （金管會110年12月30日金管保綜字第1100495362號函准備查）	修正說明
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。		
四、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。		依「金融機構資訊委外之資安應注意事項」第3條，新增本注意事項第4條。
五、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		依「金融機構資訊委外之資安應注意事項」第4條，新增本注意事項第5條。

修正條文	現行條文 （金管會110年12月30日金管保綜字第1100495362號函准備查）	修正說明
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。		
六、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		依「金融機構資訊委外之資安應注意事項」第5條，新增本注意事項第6條。並依保險局111年12月6日保局(綜)字第1110495063號函所附會議記錄決議(一)、9修正本條第1項第3款文字。

修正條文	現行條文 （金管會110年12月30日金管保綜字第1100495362號函准備查）	修正說明
本自律規範第十六條第一項之規定辦理。		
七、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。		依「金融機構資訊委外之資安應注意事項」第6條，新增本注意事項第7條。
八、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)資訊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。		依「金融機構資訊委外之資安應注意事項」第7條，新增本注意事項第8條。