「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111年12月20日金管保綜字第 1100495362 號函准備查）	修正說明
第 12 條 各會員公司於非公司職場實施異地辦公或遠端工作時，應評估相關作業風險，以強化遠端作業之安全： 一、針對營運環境調整、資料傳輸及加密機制、機敏資料防護、稽核軌跡留存、異常行為監控及對外遠端存取設備進行評估及強化，系統及設備如有重大漏洞應立即處理及因應，降低業務運作風險，確保整體保險系統穩定及安全。 二、針對使用之視訊會議系統、VPN 及 VDI 等設備，應訂定相關使用規範並落實各項安全管控作業。 三、應使用會員公司配發之裝置或設備，或使用資料不落地之機制，方得辦理遠端作業。	第 12 條 各會員公司於非公司職場實施異地辦公或遠端工作時，應評估相關作業風險，以強化遠端作業之安全： 一、針對營運環境調整、資料傳輸及加密機制、機敏資料防護、稽核軌跡留存、異常行為監控及對外遠端存取設備進行評估及強化，系統及設備如有重大漏洞應立即處理及因應，降低業務運作風險，確保整體保險系統穩定及安全。 二、針對使用之視訊會議系統、VPN 及 VDI 等設備，應訂定相關使用規範並落實各項安全管控作業。	為增進會員公司於非公司職場實施異地辦公或遠端工作之資訊安全防護，乃限制使用公司配發之裝置或設備，或使用資料不落地之機制；並依保險局112年1月7日保局(綜)字第11110465709號函（下稱保險局112年1月7日函）說明一之意旨，增訂第3款。
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~~可由外部Internet直接連線之網際網路應用系統~~）~~及核心資訊系統，應定期辦理相關安全性檢測，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	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，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	為使「可由外部 Internet 直接連線之網際網路應用系統」與核心資訊系統一併適用同等級之安全控管及檢測要求，乃配合擴大本自律規範原附件一第參條第 1 項所定之第一類電腦系統適用範圍，修正本條第 1 項文字。

修正條文	現行條文 (金管會111年12月20日金管保綜字第 1100495362 號函准備查)	修正說明
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	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	

修正條文	現行條文 (金管會111年12月20日金管保綜字第 1100495362 號函准備查)	修正說明
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。	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	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	一、有鑑現行查核方式並非限於實地查核一種，實務上以線上、書面等其他方式進行查核作業亦在多有，爰修正第1項第4款第1目之文字。 二、因應附件六名稱之修訂，併同修正第2項文字。

修正條文	現行條文 (金管會111年12月20日金管保綜字第 1100495362 號函准備查)	修正說明
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。 (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	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。 (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	

修正條文	現行條文 (金管會111年12月20日金管保綜字第 1100495362 號函准備查)	修正說明
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,將留存資料移回至各會員公司自行處理,並應刪除或	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	

修正條文	現行條文 (金管會111年12月20日金管保綜字第 1100495362 號函准備查)	修正說明
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)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「保險業核心資通~~訊~~系統作業委外資安注意事項」（如附件六）。	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)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	

修正條文	現行條文 （金管會111年12月20日金管保綜字第 1100495362 號函准備查）	修正說明
	心資訊系統作業委外資安注意事項」（如附件六）。	
第 17 條 ~~核心資訊系統及~~第一類、第二類電腦系統~~直接提供客戶自動化服務系統~~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。	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、系統內部時間應定期進行基準時間源進行同步。	一、原核心資訊系統及直接提供客戶自動化服務系統之日誌紀錄等應遵循事項，擴大適用範圍至第一、二類電腦系統，爰修訂第1項文字。 二、為使涉及個人資料之日誌紀錄之保留期限符合個人資料保護法等法令規範，爰增訂第17條第1項第1款後段。 三、於日誌處理失效時應有告警及應處機制，爰參考資通安全責任等級分級辦法附表十之「日誌處理失效之回應」所定內容，增訂第4款，並調整款次。

<table>
<tr><th>修正條文</th><th>現行條文
（金管會111年12月20日金管保綜字第1100495362號函准備查）</th><th>修正說明</th></tr>
<tr>
<td>附件一、保險業電腦系統資訊安全評估作業原則：
壹、前言
為確保保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。
貳、評估範圍
一、保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。
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</td><td><s>直接提供客戶自動化服</s></td><td>每年至少辦理一次資訊</td></tr>
</table>
</td>
<td>附件一、保險業電腦系統資訊安全評估作業原則：
壹、前言
為確保保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。
貳、評估範圍
一、保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。
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</td><td>每年至少辦理一次資訊安全評估作業</td></tr>
</table>
</td>
<td>一、為使「可由外部Internet直接連線之網際網路應用系統」與核心資訊系統一併適用同等級之安全控管及檢測要求，乃藉由擴大本自律規範原附件一第參條第1項所定之第一類電腦系統適用範圍，以增加資訊安全評估作業頻率以提升防護能量，遂修正本附件第參條第1項文字。
二、又因「提供員工外部連線使用之資訊系統」已併入第一類，爰併同刪除第肆條第3項文字。
三、為打擊金融詐騙犯罪、防止個人資料外洩、保障民眾權益，應納入「偵測偽冒網站」之資安措施，並依保險局112年1月7日函說明二之意旨，增訂第肆條第1項第2款第4目。
四、為強化系統運作可用性之資安措施（如導入DDoS流量清洗、線路流量監控與備援等），並依保險局112年1月7日函說明二之意</td>
</tr>
</table>

修正條文			現行條文 （金管會111年12月20日金管保綜字第1100495362號函准備查）			修正說明
類	~~務之系統網際網路應用系統（如網路投保、網路要保等直接提供客戶自動化服務之系統~~可由外部Internet直接連線之網際網路應用系統~~）~~及核心資訊系統。	安全評估作業		保、網路要保等系統）及核心資訊系統		旨，爰修正第伍條文字。
第二類	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）	每三年至少辦理一次資訊安全評估作業	第二類	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）	每三年至少辦理一次資訊安全評估作業	
第三類	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~~）	每五年至少辦理一次資訊安全評估作業	第三類	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）	每五年至少辦理一次資訊安全評估作業	
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。 肆、資訊安全評估作業 一、資訊安全評估作業項目：			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。 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，			

修正條文	現行條文 (金管會111年12月20日金管保綜字第1100495362號函准備查)	修正說明
(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：	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	

修正條文	現行條文 （金管會111年12月20日金管保綜字第1100495362號函准備查）	修正說明
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。 4. 檢視是否訂定偵測偽冒網站之處理措施。 (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	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	

修正條文	現行條文 （金管會111年12月20日金管保綜字第1100495362號函准備查）	修正說明
作業時，依據「保險業使用物聯網設備作業準則」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 保險業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 https、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	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 保險業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 https、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。	

修正條文	現行條文 (金管會111年12月20日金管保綜字第1100495362號函准備查)	修正說明
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 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) 提升軟體系統之	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	

修正條文	現行條文 （金管會111年12月20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	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	

修正條文	現行條文 （金管會111年12月20日金管保綜字第1100495362號函准備查）	修正說明
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~~。 伍、~~分散式阻斷服務攻擊（DDoS）演練~~ 強化系統運作可用性之資安措施 辦理電子商務業務者，應強化系統運作可用性之資安措施【如導入分散式阻斷服務攻擊(DDoS)流量清洗、線路流量監控與備援及訂定DDoS防禦與應變作業程序等】~~應訂定分散式阻斷服務攻擊（DDoS）防禦與應~~	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。 伍、分散式阻斷服務攻擊（DDoS）演練 辦理電子商務業務者，應訂定分散式阻斷服務攻擊（DDoS）防禦與應變作業程序，並定期辦理 DDoS 實地演練。 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。 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	

修正條文	現行條文 （金管會111年12月20日金管保綜字第1100495362號函准備查）	修正說明
~~變作業程序~~，並定期辦理DDoS實~~地~~際演練。 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。 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。 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，如持有國際資訊安全經理人（Certified Information Security Manager,CISM）證書或通過國際資安管理系統主導 稽核員（Information Security Management System Lead Auditor,ISO 27001 LA）考試合格等。 (二)具備資訊安全技術能力，如國際資訊安全系統專家（Certified InformationSystems Security Professional,CISSP）證書	位。 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，如持有國際資訊安全經理人（Certified Information Security Manager,CISM）證書或通過國際資安管理系統主導 稽核員（Information Security Management System Lead Auditor,ISO 27001 LA）考試合格等。 (二)具備資訊安全技術能力，如國際資訊安全系統專家（Certified InformationSystems Security Professional,CISSP）證書等。 (三)具備模擬駭客攻擊能力，如滲透專家（Certified Ethical Hacking, CEH）證書或事件處理專家（Certified Incident Handler,CIH）證書等。 (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。	

修正條文	現行條文 （金管會111年12月20日金管保綜字第1100495362號函准備查）	修正說明
等。 (三)具備模擬駭客攻擊能力，如滲透專家（Certified Ethical Hacking, CEH）證書或事件處理專家（Certified Incident Handler,CIH）證書等。 (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。 捌、評估報告 一、「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、評估作業項目與標的、評估紀錄、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。 二、會員公司應依據評估報告內容缺失程度區分風險等級，並擬定各風險對應之控管措施及處理時限，送稽核單位進行缺失改善事項之追蹤覆查。 三、評估報告缺失覆查應提報董（理）事會或經其授權之經理部門，但外國保險業在台分公司，得由總公司授權之人員為之，以落實由高階管理階層督導缺失改善。	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。 捌、評估報告 一、「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、評估作業項目與標的、評估紀錄、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。 二、會員公司應依據評估報告內容缺失程度區分風險等級，並擬定各風險對應之控管措施及處理時限，送稽核單位進行缺失改善事項之追蹤覆查。 三、評估報告缺失覆查應提報董（理）事會或經其授權之經理部門，但外國保險業在台分公司，得由總公司授權之人員為之，以落實由高階管理階層督導缺失改善。 四、評估報告應併同缺失改善等相關文件至少保存五年。	

修正條文	現行條文 (金管會111年12月20日金管保綜字第1100495362號函准備查)	修正說明
四、評估報告應併同缺失改善等相關文件至少保存五年。		

修正條文	現行條文 (金管會 111 年 12 月 20 日金管保綜字第 1100495362 號函准備查)	修正說明
附件二、保險業提供行動應用程式（App）作業原則： 一、保險業有提供行動應用程式者，會員公司可依不同應用類別之行動應用程式對於安全性有不同之要求，除符合經濟部工業局「行動應用 App 基本資安規範」外，應遵循本作業原則。 二、會員公司應依個人資料保護法於行動應用程式下載前，明確告知消費者對於個人資料蒐集處理利用之法定事項及消費者得要求刪除資料之權利等事項，以保護消費者權益。 三、應用程式發布程序，應符合權責分工原則。 四、應於發布前檢視應用程式所需權限應與提供服務相當，首次發布或權限變動應經資安、法遵及風控等單位同意，以利綜合評估是否符合「個人資料保護法」之告知義務。 五、行動應用程式資安檢測作業： (一)檢測範圍： 1. 委託專業機構辦理資安檢測時，參考經濟部工業局「行動應用 APP 基本資安檢測基準」及 OWASP 公布之Mobile Top 10 項目。 2. 自行辦理檢測	附件二、保險業提供行動應用程式（App）作業原則： 一、保險業有提供行動應用程式者，會員公司可依不同應用類別之行動應用程式對於安全性有不同之要求，除符合經濟部工業局「行動應用 App 基本資安規範」外，應遵循本作業原則。 二、會員公司應依個人資料保護法於行動應用程式下載前，明確告知消費者對於個人資料蒐集處理利用之法定事項及消費者得要求刪除資料之權利等事項，以保護消費者權益。 三、應用程式發布程序，應符合權責分工原則。 四、應於發布前檢視應用程式所需權限應與提供服務相當，首次發布或權限變動應經資安、法遵及風控等單位同意，以利綜合評估是否符合「個人資料保護法」之告知義務。 五、行動應用程式資安檢測作業： (一)檢測範圍： 1. 委託專業機構辦理資安檢測時，參考經濟部工業局「行動應用 APP 基本資安檢測基準」及 OWASP 公布之Mobile Top 10 項目。 2. 自行辦理檢測	為明確規範辦理「實質」性檢視機制，以確認檢測報告之完整性，落實辦理安全檢測，爰修正第 6 條第 1 項第 3 款文字。

<table>
<tr><th>修正條文</th><th>現行條文
(金管會 111 年 12 月 20 日金管保綜字第 1100495362 號函准備查)</th><th>修正說明</th></tr>
<tr>
<td>時,應對行動應用程式進行程式碼掃描或黑箱測試,並修正中、高風險漏洞(如屬可承擔風險者除外)。
(二)依行動應用程式之重要性,定期委由專業機構完成資安檢測:
<table>
<tr><th>類別</th><th>定義</th><th>評估週期</th></tr>
<tr><td>第一類</td><td>對外部提供服務或直接提供客戶自動化服務之行動應用程式</td><td>每年委由專業機構完成資安檢測</td></tr>
<tr><td>第二類</td><td>對內部員工(含其他通路)提供服務,其經員工介入以提供客戶服務之行動應用程式(如:行動投保、行動保全、行動理賠</td><td>每二年委由專業機構完成資安檢測</td></tr>
</table>
</td>
<td>時,應對行動應用程式進行程式碼掃描或黑箱測試,並修正中、高風險漏洞(如屬可承擔風險者除外)。
(二)依行動應用程式之重要性,定期委由專業機構完成資安檢測:
<table>
<tr><th>類別</th><th>定義</th><th>評估週期</th></tr>
<tr><td>第一類</td><td>對外部提供服務或直接提供客戶自動化服務之行動應用程式</td><td>每年委由專業機構完成資安檢測</td></tr>
<tr><td>第二類</td><td>對內部員工(含其他通路)提供服務,其經員工介入以提供客戶服務之行動應用程式(如:行動投保、行動保全、行動理賠</td><td>每二年委由專業機構完成資安檢測</td></tr>
</table>
</td>
<td></td>
</tr>
</table>

修正條文			現行條文 (金管會 111 年 12 月 20 日金管保綜字第 1100495362 號函准備查)			修正說明
	等)			等)		
第三類	對內部員工(含其他通路)提供服務,其未接觸客戶資訊或服務之行動應用程式(如:行動差勤、行動電子書等)	每五年委由專業機構完成資安檢測	第三類	對內部員工(含其他通路)提供服務,其未接觸客戶資訊或服務之行動應用程式(如:行動差勤、行動電子書等)	每五年委由專業機構完成資安檢測	
(三)會員公司應建立行動應用程式上架前資安檢測程序: 1. 初次上架前,屬第一、二類者,應委由專業機構完成資安檢測;屬第三類者,應通過資安檢測程序。 2. 更新上架前,應通過資安檢測程序;若涉有重大變更作業或行動應用程式版本大幅更新時,應委由專業機構完成資安檢測。 3. 重大變更作業包括但不限於保單投保交易、涉及資			(三)會員公司應建立行動應用程式上架前資安檢測程序: 1. 初次上架前,屬第一、二類者,應委由專業機構完成資安檢測;屬第三類者,應通過資安檢測程序。 2. 更新上架前,應通過資安檢測程序;若涉有重大變更作業或行動應用程式版本大幅更新時,應委由專業機構完成資安檢測。 3. 重大變更作業包括但不限於保單投保交易、涉及資			

修正條文	現行條文 (金管會 111 年 12 月 20 日金管保綜字第 1100495362 號函准備查)	修正說明
金轉移、身分辨識及客戶權益等有重大相關項目。 4. 如因故需緊急變更過版時，應於兩個月內完成上述檢測。 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. 檢測標的。 2. 檢測範圍之宣告。 3. 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。 七、啟動應用程式時，如偵測行動裝置疑似遭破解，應提示使用者注意風險，且與行動裝置有關之安全設計(如設備指定、生物識別、敏感資料保護等)，應評估其有	金轉移、身分辨識及客戶權益等有重大相關項目。 4. 如因故需緊急變更過版時，應於兩個月內完成上述檢測。 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. 檢測標的。 2. 檢測範圍之宣告。 3. 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。 七、啟動應用程式時，如偵測行動裝置疑似遭破解，應提示使用者注意風險，且與行動裝置有關之安全設計(如設備指定、生物識別、敏感資料保護等)，應評估其有	

修正條文	現行條文 (金管會 111 年 12 月 20 日金管保綜字第 1100495362 號函准備查)	修正說明
效性。 八、行動應用程式屬第一類，對外部提供服務或直接提供客戶自動化服務者，應於官網上提供應用程式之名稱、版本與下載位置。 九、行動應用程式屬第一類，應建立偽冒應用程式偵測機制，以維客戶權益。 十、採用憑證技術進行傳輸加密時，應用程式應建立可信任憑證清單並驗證完整憑證鏈及其憑證有效性。 十一、 應進行身分驗證相關資訊不以明文傳輸並具備帳戶鎖定機制，以防範自動化程式之登入或密碼更換嘗試。 附錄：用語及定義 一、行動裝置：係指包含但不限於智慧型手機、平板電腦等具通信及連網功能之設備。 二、專業機構：係指非會員公司之法人機構，其應具備經濟部工業局「行動應用 APP 基本資安自主檢測推動制度」列示之合格檢測實驗室資格。 三、遭破解之行動裝置：係指透過系統程序取得手機最高權限，藉以突破手機作業系統之基本防護，可能導致遭植入惡意程式。 四、完成資安檢測：係指辦理資安檢測，並針對相關漏洞規劃修補作業，於一定時間內完成修補。	效性。 八、行動應用程式屬第一類，對外部提供服務或直接提供客戶自動化服務者，應於官網上提供應用程式之名稱、版本與下載位置。 九、行動應用程式屬第一類，應建立偽冒應用程式偵測機制，以維客戶權益。 十、採用憑證技術進行傳輸加密時，應用程式應建立可信任憑證清單並驗證完整憑證鏈及其憑證有效性。 十一、 應進行身分驗證相關資訊不以明文傳輸並具備帳戶鎖定機制，以防範自動化程式之登入或密碼更換嘗試。 附錄：用語及定義 一、行動裝置：係指包含但不限於智慧型手機、平板電腦等具通信及連網功能之設備。 二、專業機構：係指非會員公司之法人機構，其應具備經濟部工業局「行動應用 APP 基本資安自主檢測推動制度」列示之合格檢測實驗室資格。 三、遭破解之行動裝置：係指透過系統程序取得手機最高權限，藉以突破手機作業系統之基本防護，可能導致遭植入惡意程式。 四、完成資安檢測：係指辦理資安檢測，並針對相關漏洞規劃修補作業，於一定時間內完成修補。	

修正條文	現行條文 (金管會 111 年 12 月 20 日金管保綜字第 1100495362 號函准備查)	修正說明
五、黑箱測試:動態分析或動態程式碼安全性檢測,主要用於受測主機資訊不足的情況下進行測試。 六、憑證:指載有簽章驗證資料,提供行動應用程式鑑別伺服器身分及資料傳輸加密使用。	五、黑箱測試:動態分析或動態程式碼安全性檢測,主要用於受測主機資訊不足的情況下進行測試。 六、憑證:指載有簽章驗證資料,提供行動應用程式鑑別伺服器身分及資料傳輸加密使用。	

修正條文	現行條文 (金管會 111 年 12 月 20 日金管保綜字第 1100495362 號函准備查)	修正說明
附件四、保險業使用物聯網設備作業準則 一、為確保保險業使用物聯網(Internet of Things, IoT)設備之安全性,以確保適當管理運用物聯網設備之風險,並保障消費者。 二、本作業準則所稱物聯網設備係指具實際連線於 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。 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、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。 四、設備應具備安全性更新機	附件四、保險業使用物聯網設備作業準則 一、為確保保險業使用物聯網(Internet of Things, IoT)設備之安全性,以確保適當管理運用物聯網設備之風險,並保障消費者。 二、本作業準則所稱物聯網設備係指具實際連線於 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。 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、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。 四、設備應具備安全性更新機	一、為增加密碼保護強度,密碼長度應加長為至少 8 碼,並增訂替代性措施,爰修正第 5 條文字。

修正條文	現行條文 （金管會 111 年 12 月 20 日金管保綜字第 1100495362 號函准備查）	修正說明
制，以維持設備之整體安全性。 五、為確保經授權之使用者始得進行資料存取、設備管理及安全性更新等操作，設備應具備身分驗證機制，並應進行初始密碼變更，密碼長度不應少於六八位，建議採英數字混合使用，且宜包含大小寫英文字母或符號，並以最小權限原則針對不同的使用者身分進行授權，若設備現階段未能符合本條所要求之控管措施，則依本作業準則第九條規定辦理。 六、設備以無線連接網路者，應採用具加密協定之無線存取點連接網路，並以網路卡卡號白名單等機制進行設備綁定。 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。 八、應與設備供應商簽訂資訊安全相關協議，以明確約定相關責任。 九、設備存在已知弱點且無法修補或更新，無法落實前述安全控管規範，應限制網際網路連線能力，加強存取控	制，以維持設備之整體安全性。 五、為確保經授權之使用者始得進行資料存取、設備管理及安全性更新等操作，設備應具備身分驗證機制，並應進行初始密碼變更，密碼長度不應少於六位，建議採英數字混合使用，且宜包含大小寫英文字母或符號，並以最小權限原則針對不同的使用者身分進行授權。 六、設備以無線連接網路者，應採用具加密協定之無線存取點連接網路，並以網路卡卡號白名單等機制進行設備綁定。 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。 八、應與設備供應商簽訂資訊安全相關協議，以明確約定相關責任。 九、設備存在已知弱點且無法修補或更新，無法落實前述安全控管規範，應限制網際網路連線能力，加強存取控制或進行網路連線行為監控；並視需要訂定汰換期程。	

修正條文	現行條文 (金管會 111 年 12 月 20 日金管保綜字第 1100495362 號函准備查)	修正說明
制或進行網路連線行為監控；並視需要訂定汰換期程。 十、採購物聯網設備時，應優先採購經濟部與國家通訊傳播委員會共同發布物聯網資安標章認驗證制度之具有安全標章之物聯網設備。 十一、應每年對物聯網設備使用及管理人員安排適當之資訊安全教育訓練。 十二、汰換物聯網設備時，應訂定汰除作業程序以避免儲存於物聯網設備資料外洩。 十三、針對不具備遠端操控介面功能之感測器，仍應遵循本作業準則三、七、八、九、十二之要求辦理。	十、採購物聯網設備時，應優先採購經濟部與國家通訊傳播委員會共同發布物聯網資安標章認驗證制度之具有安全標章之物聯網設備。 十一、應每年對物聯網設備使用及管理人員安排適當之資訊安全教育訓練。 十二、汰換物聯網設備時，應訂定汰除作業程序以避免儲存於物聯網設備資料外洩。 十三、針對不具備遠端操控介面功能之感測器，仍應遵循本作業準則三、七、八、九、十二之要求辦理。	

修正條文	現行條文 (金管會 111 年 12 月 20 日金管保綜字第 1100495362 號函准備查)	修正說明
附件六、保險業核心資通訊~~訊~~系統作業委外資安注意事項 一、本注意事項目的 為協助保險業於辦理核心資通訊~~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	附件六、保險業核心資訊系統作業委外資安注意事項 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	一、為擴張本附件之適用範圍，併參考「保險業資訊作業韌性參考原則」第 2 點第 1 項第 2 款核心資通系統之定義，修訂本注意事項名稱、第 1 條第 1 項、第 3 條第 1 至 3 項、第 9 條第 2 項，並新增第 2 條文字，及依序調整條號。 二、依保險業內部控制及稽核制度實施辦法第 6 條規定，保險業使用電腦化資訊系

修正條文	現行條文 (金管會 111 年 12 月 20 日金管保綜字第 1100495362 號函准備查)	修正說明
意事項。 ~~保險業宜參照本注意事項辦理。~~ 二、本注意事項所稱核心資通系統，係指核心資訊系統與涉及核心業務持續運作之重要資訊系統。 三、計畫作業階段 (一)核心資~~通訊~~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~~通訊~~系統作業委外開發案，專案成員中應有資安人員參與。 (三)識別核心資~~通訊~~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。 四、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	項。 保險業宜參照本注意事項辦理。 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	統處理者，其內部控制制度應包含核心業務委外處理之控制，並應依所屬商業同業公會訂定之自律規範辦理。是會員公司應遵循本注意事項辦理，爰刪除第一點第二項文字。

修正條文	現行條文 (金管會 111 年 12 月 20 日金管保綜字第 1100495362 號函准備查)	修正說明
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。 五、決標作業階段 與委外廠商簽訂合約或協	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	

修正條文	現行條文 (金管會 111 年 12 月 20 日金管保綜字第 1100495362 號函准備查)	修正說明
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。 六、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。	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。 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	

修正條文	現行條文 (金管會 111 年 12 月 20 日金管保綜字第 1100495362 號函准備查)	修正說明
(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。 七、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,應依本自律規範第十六條第一項之規定辦理。 八、保固作業階段	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	

修正條文	現行條文 (金管會 111 年 12 月 20 日金管保綜字第 1100495362 號函准備查)	修正說明
(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。 九、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)核心資通~~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。	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。 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。	