「壽險業辦理資訊安全防護自律規範」部分條文修正對照表

中華民國人壽保險商業同業公會 106 年 11 月 16 日第 7 屆第 7 次理監事聯席會議決議通過

修正條文	現行條文	說明
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、應透過至少每年、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。	一、本次修正。 二、考量資訊安全風險較高，明確定義教育訓練頻率，應至少每年對內部人員進行訓練，以強化員工之資安觀念。
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。	一、本次未修正。 二、本修正條文業以 105 年 6 月 30 日壽會貴字第 1050607836 號函報鈞會保險局在案。
第九條 各會員公司若有開發並提供行動裝置應用程式給消費者或員工使用者，應依據壽險業提供行動裝置應用程式作業原則如附		一、本次未修正。 二、配合鈞會保險局 105 年 4 月 18 日保局 10510915370 號函指示，為加強行動 App

修正條文	現行條文	說明
件二建立行動App資訊安全控管機制，以強化行動裝置應用之安全。		之資訊安全控管機制，參考經濟部所訂「行動應用App基本資安規範」，訂定「壽險業提供行動裝置應用程式作業原則」。 三、本修正條文業以105年6月30日壽會貴字第1050607836號函報鈞會保險局在案。
第十條 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。		一、本次未修正。 二、配合鈞會保險局105年4月8日保局(綜)字第10510906620號函，為建構完善資通安全管理機制，參考「證券商資通安全內部控制制度標準規範」第二條第六項設備報廢作業程序，爰增訂此條文。 三、本修正條文業以105年6月30日壽會貴字第1050607836號函報鈞會保險局在案。
第十一條 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。	一、本次未修正。 二、本修正條文業以105年6月30日壽會貴字第1050607836號函報鈞會保險局在案。
第十二條 各會員公司應將本自律規範內	第十條 各會員公司應將本自律規範內	一、本次未修正。 二、本修正條文業以105

修正條文	現行條文	說明
容，納入內稽內控制度中，並定期辦理查核。	容，納入內稽內控制度中，並定期辦理查核。	年6月30日壽會貴字第1050607836號函報鈞會保險局在案。
第十三條 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。	一、本次未修正。 二、本修正條文業以105年6月30日壽會貴字第1050607836號函報鈞會保險局在案。
第十四條 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。	一、本次未修正。 二、本修正條文業以105年6月30日壽會貴字第1050607836號函報鈞會保險局在案。

附件一

壽險業辦理電腦系統資訊安全評估作業原則

<table>
<tr><th>條文內容</th><th>條文內容</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>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>本次未修正。</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>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>本次未修正。</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</td><td>每三年至少辦</td></tr></table></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</td><td>每三年至少辦</td></tr></table></td><td>本次未修正。</td></tr>
</table>

條文內容			條文內容			說明
	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）	理一次資訊安全評估作業		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）	理一次資訊安全評估作業	
第三類	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）	每五年至少辦理一次資訊安全評估作業	**第三類**	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）	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。			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，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			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		本次未修正。

條文內容	條文內容	說明
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)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。	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)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。	

條文內容	條文內容	說明
(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。	(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。	
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。	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。	本次未修正。
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。	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。	本次未修正。

條文內容	條文內容	說明
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，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	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，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	本次未修正。

條文內容	條文內容	說明
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、 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。	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、 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 「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。	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。	本次未修正。

「壽險業提供行動裝置應用程式作業原則」條文修正對照表

中華民國人壽保險商業同業公會 106 年 11 月 16 日第 7 屆第 7 次理監事聯席會議決議通過

修正條文	105.12.29 函報條文	說　明
壹、前言 為提升我國壽險業行動應用 App 基本安全防護能力，透過本作業原則之重點要項，強化資訊安全意識，並逐步完善所提供之行動 App 安全防護能力。	壹、前言 為提升我國壽險業行動應用 App 基本安全防護能力，透過本作業原則之重點要項，強化資訊安全意識，並逐步完善所提供之行動 App 安全防護能力。	1. 本次未修正。 2. 本作業原則依「壽險業辦理資訊安全防護自律規範」第 9 條內容辦理。 3. 依 鈞會保險局 105 年 8 月 29 日保局(壽)字第第 10502083110 號函(下稱 105.8.29 函)指示，增列說明文字： (1) 本作業原則係參考工業局版本，該版本已符合各產業 APP 基本安全要求，爰本作業原則亦符合壽險業各類功能 APP 基本安全需求。 (2) 本作業原則已涵括多面向之安控要求：App 之上架前安控檢測、於可信任來源之行動應用商店或網站發布、使用者下載前之告知事項與資安宣導、敏感性資料保護措施、身分認證、連線管理安全、程式碼安全等，並將具交易功能之 App 納入獨立第三方單位定期評估範疇，此符合壽險業所需。

修正條文	105.12.29 函報條文	說　明
貳、範圍 本作業原則為壽險業提供行動應用程式之基本資訊安全準則。	貳、範圍 本作業原則為壽險業提供行動應用程式之基本資訊安全準則。	1. 本次未修正。 2. 參考經濟部工業局「行動應用 App 基本資安規範」之「2. 評估範圍」條文，訂定本作業原則之適用範圍。
參、用語及定義 一、行動應用程式（Mobile Application）：指一種設計給智慧型手機、平板電腦和其他行動裝置使用之應用程式。 二、行動應用程式商店(Application Store)：指行動裝置使用者透過內建在裝置中之行動應用程式商店或透過網站對應用程式、音樂、雜誌、書籍、電影、電視節目進行瀏覽、下載或購買。 三、敏感性資料(Sensitive Data)：指依使用者行為或行動應用程式之運作，建立或儲存於行動裝置及其附屬儲存媒介之資訊，而該資訊之洩漏有對使用者造成損害之虞，包括但不限於個人資料、通行碼、即時通訊訊息、筆記、備忘錄、通訊錄、地理位置、行事曆、通話紀錄及簡訊。 四、個人資料(Personal Data)：指主要依「個人資料保護法」上定義之所有得以直接或間接方式識別該個人之資料，包括自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動、國際行動設備識別碼（International Mobile Equipment Identity,	參、用語及定義 一、行動應用程式（Mobile Application）：指一種設計給智慧型手機、平板電腦和其他行動裝置使用之應用程式。 二、行動應用程式商店(Application Store)：指行動裝置使用者透過內建在裝置中之行動應用程式商店或透過網站對應用程式、音樂、雜誌、書籍、電影、電視節目進行瀏覽、下載或購買。 三、敏感性資料(Sensitive Data)：指依使用者行為或行動應用程式之運作，建立或儲存於行動裝置及其附屬儲存媒介之資訊，而該資訊之洩漏有對使用者造成損害之虞，包括但不限於個人資料、通行碼、即時通訊訊息、筆記、備忘錄、通訊錄、地理位置、行事曆、通話紀錄及簡訊。 四、個人資料(Personal Data)：指主要依「個人資料保護法」上定義之所有得以直接或間接方式識別該個人之資料，包括自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動、國際行動設備識別碼（International Mobile Equipment Identity,	1. 參考經濟部工業局「行動應用 App 基本資安規範」之「3. 用語及定義」條文，訂定本作業原則之用語及定義。

修正條文	105.12.29 函報條文	說　明
IMEI）、國際行動用戶識別碼（International Mobile Subscriber Identity, IMSI）及其他得以直接或間接方式識別該個人之資料。	IMEI）、國際行動用戶識別碼（International Mobile Subscriber Identity, IMSI）及其他得以直接或間接方式識別該個人之資料。	2. 配合工業局 106 年 3 月公告「行動應用 App 基本資安規範」更新(V1.1)，調整相關用語與定義之敘述。
五、通行碼（Password）：指一組能讓使用者使用系統或用以識別使用者身分之字元串。	五、通行碼（Password）：指能讓使用者完全或有限度之使用系統或取得一組資料之識別使用者身分用之字元串。	
六、付費資源(Payment Resource)：指透過行動應用程式內建購買功能取得之額外功能、內容及訂閱項目。	六、付費資源（In-App Purchase/Billing）：指透過行動應用程式內建購買功能取得之額外功能、內容及訂閱項目。	
七、交談識別碼（Session Identification, Session ID）：指在建立連線時，指派給該連線之識別碼，並做為連線期間之唯一識別碼；當連線結束時，該識別碼可釋出並重新指派給新之連線。	七、交談識別碼（Session Identification, Session ID）：指在建立連線時，指派給該連線之識別碼，並做為連線期間之唯一識別碼；當連線結束時，該識別碼可釋出並重新指派給新之連線。	
八、伺服器憑證(Certificate)：指載有簽章驗證資料，提供伺服器身分鑑別及資料傳輸加密。	八、伺服器憑證(Certificate)：指載有簽章驗證資料，提供伺服器身分鑑別及資料傳輸加密。	
九、憑證機構（Certificate Authority）：指簽發憑證之機關、法人。	九、憑證機構（Certificate Authority）：指簽發憑證之機關、法人。	
十、惡意程式碼(Malicious Code)：指在未經使用者同意之情況下，侵害使用者權益，包括但不限於任何具有惡意特徵或行為之程式碼。	十、惡意程式碼(Malicious Code)：指在未經使用者同意之情況下，侵害使用者權益，包括但不限於任何具有惡意特徵或行為之程式碼。	
十一、資訊安全漏洞（Vulnerability）:指行動應用程式安全方面之缺陷，使得系統或行動應用程式資料之保密性、完整性、可用性面臨威脅。	十一、資訊安全漏洞（Vulnerability）:指行動應用程式安全方面之缺陷，使得系統或行動應用程式資料之保密性、完整性、可用性面臨威脅。	
十二、函式庫(Library)：指將一些繁複或者牽涉到硬體層面之程	十二、函式庫(Library)：指將一些繁複或者牽涉到硬體層面之程	

修正條文	105.12.29 函報條文	說　明
式包裝成函式（Function）或物件（Object）收集在一起，編譯成二進位碼提供程式設計者使用。 十三、注入攻擊（Code Injection）：指因行動應用程式設計缺陷而執行使用者所輸入之惡意指令，包括但不限於命令注入（Command Injection）、資料隱碼攻擊（SQL Injection）。	式包裝成函式（Function）或物件（Object）收集在一起，編譯成二進位碼提供程式設計者使用。 十三、注入攻擊（Code Injection）：指因行動應用程式設計缺陷而執行使用者所輸入之惡意指令，包括但不限於命令注入（Command Injection）、資料隱碼攻擊（SQL Injection）。	
肆、技術要求 一、行動應用程式資訊安全技術要求事項 （一）行動應用程式發布安全 1. 行動應用程式發布： (1) 行動應用程式應於可信任來源之行動應用程式商店或網站發布，且應於發布時說明欲存取之敏感性資料、行動裝置資源及宣告之權限用途。 (2) 應於發布前檢視行動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負責個人資料保護相關單位同意，以利綜合評估是否符合「個人資料保護法」之告知義務。 2. 行動應用程式更新 (1) 行動應用程式應於可信任來源之行動應用程式商店或網站發布更新。 (2) 行動應用程式應提供更新機制，並於有安全性更新時主動公告。 3. 行動應用程式安全性問題回報 (1) 行動應用程式開發者應提供回報安全性問題之管道。 (2) 行動應用程式開發者應於適當期間內回覆問題並改善。 4. 行動應用程式上架資安檢測與評估	肆、技術要求 一、行動應用程式資訊安全技術要求事項 （一）行動應用程式發布安全 1. 行動應用程式發布：行動應用程式應於可信任來源之行動應用程式商店或網站發布，且應於發布時說明欲存取之敏感性資料、行動裝置資源及宣告之權限用途。 2. 行動應用程式更新 (1) 行動應用程式應於可信任來源之行動應用程式商店或網站發布更新。 (2) 行動應用程式應提供更新機制，並於有安全性更新時主動公告。 3. 行動應用程式安全性問題回報 (1) 行動應用程式開發者應提供回報安全性問題之管道。 (2) 行動應用程式開發者應於適當期間內回覆問題並改善。 4. 行動應用程式上架資安檢測與評估	1. 參考經濟部工業局「行動應用 App 基本資安規範」之「4. 技術要求」條文，訂定 App 各項資訊安全技術要求。 2. 依鈞會保險局 105 年 4 月 18 日保局(綜)字第 10510915370 號函、105.8.29 函、106 年 3 月 1 日保局（壽）字第 10500969550 號函（下稱 106.3.1 函）示，參考銀行業「金融機構提供行動裝置應用程式作業規範」，訂定壽險業 APP 上架相關作業： (1) 參考銀行業「金融機構提供行動裝置應用程式作業規範」第二條，於 APP 發布前需評估利用之權限，並考量個資保護之告知義務，訂定肆、一、(一)、1、(2)條文。 (2) 參考銀行業「金融機構提供行動裝置應

修正條文	105.12.29 函報條文	說　明
(1) 應建立行動應用程式資安檢測程序，行動應用程式上架前，應通過資安檢測程序，並針對檢測發現可能影響敏感性資料被竊取或竄改之弱點完成改善。 (2) 行動應用程式之資安評估：行動應用程式依本作業原則伍、安全分類，其屬第三類、具交易功能者，應納入本自律規範附件一壽險業辦理電腦系統資訊安全評估作業原則之第一類電腦系統，定期辦理評估作業。 5.行動應用程式下載、安裝與首次啟動 (1) 行動應用程式如有涉及敏感性資料蒐集、利用，應於下載、安裝或首次啟動應用程式時告知使用者所涉敏感性資料的使用目的、資料類別、使用方式及刪除方式，並加強資安風險意識之宣導。 (2) 行動應用程式所要求使用者對其個人敏感性資料蒐集、利用之授權，應與所提供之服務相當。 (二)　敏感性資料保護 1. 敏感性資料存取同意：行動應用程式於敏感性資料蒐集、利用、儲存及分享前，應取得使用者同意，並提供使用者拒絕之權利。 2. 敏感性資料利用 (1) 行動應用程式如採用通行碼認證，應主動提醒使用者設定較複雜之通行碼。 (2) 行動應用程式應提醒使用者定期更改通行碼。 3. 敏感性資料儲存 (1) 行動應用程式儲存之敏感性資料，應僅用於其使用聲明之用途，並避免將敏感性資料儲存於暫存檔或紀錄檔中。	(1) 應建立行動應用程式資安檢測程序，行動應用程式上架前，應通過資安檢測程序，並針對檢測發現可能影響敏感資料被竊取或竄改之弱點完成改善。 (2) 行動應用程式之資安評估：行動應用程式依本作業原則伍、安全分類，其屬第三類、具交易功能者，應納入本自律規範附件一壽險業辦理電腦系統資訊安全評估作業原則之第一類電腦系統，定期辦理評估作業。 5.行動應用程式下載、安裝與首次啟動 (1) 行動應用程式如有涉及敏感性資料蒐集、利用，應於下載、安裝或首次啟動應用程式時明確告知使用者，並加強資安風險意識之宣導。 (2) 行動應用程式所要求使用者對其個人敏感性資料蒐集、利用之授權，應與所提供之服務相當。 (二)　敏感性資料保護 1. 敏感性資料存取同意：行動應用程式於敏感性資料蒐集、利用、儲存及分享前，應取得使用者同意，並提供使用者拒絕之權利。 2. 敏感性資料利用 (1) 行動應用程式如採用通行碼認證，應主動提醒使用者設定較複雜之通行碼。 (2) 行動應用程式應提醒使用者定期更改通行碼。 3. 敏感性資料儲存 (1) 行動應用程式儲存之敏感性資料，應僅用於其使用聲明之用途，並避免將敏感性資料儲存於暫存檔或紀錄檔中。	用程式作業規範」第一條，建立 APP 上架資安檢測程序，訂定肆、一、(一)、4、(1)條文。 (3) 參考銀行業「金融機構提供行動裝置應用程式作業規範」第三條，針對屬第三類之 App（具交易功能與客戶個人資料處理），每年定期由獨立第三方單位進行資訊安全評估作業，訂定肆、一、(一)、4、(2)條文。 3. 依　鈞會保險局 106.3.1 函示，全面檢視並一致修正為「敏感性資料」。 4. 依　鈞會保險局 105.8.29 函、106.3.1 函指示，為建立 App 下載規範，並訂定使用者可要求刪除及詳列明確告知使用者之權利內容，修訂肆、一、(一)、5 條文。

修正條文	105.12.29 函報條文	說　明
(2) 敏感性資料應採用適當且有效之金鑰長度與加密演算法，進行加密處理再儲存。 (3) 敏感性資料應儲存於受作業系統保護之區域，以防止其他應用程式未經授權之存取。 (4) 敏感性資料應避免出現於行動應用程式之程式碼。 4. 敏感性資料傳輸：行動應用程式透過網路傳輸敏感性資料，應使用適當且有效之金鑰長度與加密演算法進行安全加密。 5. 敏感性資料分享：行動裝置內之不同行動應用程式間，於分享敏感性資料時，應避免未授權之行動應用程式存取。 6. 敏感性資料刪除：行動應用程式如涉及儲存使用者敏感性資料，應提供使用者刪除之功能。 (三) 付費資源控管安全 1. 付費資源使用：行動應用程式應於使用付費資源前主動通知使用者，並提供使用者拒絕之權利。 2. 付費資源控管：行動應用程式應於使用付費資源前進行使用者認證，並記錄使用之付費資源與時間。 (四) 身分認證、授權與連線管理安全 1. 使用者身分認證與授權：行動應用程式應有適當之身分認證機制，確認使用者身分，並依使用者身分授權。 2. 連線管理機制 (1)行動應用程式應避免使用具有規則性之交談識別碼。 (2)行動應用程式應確認伺服器憑證之有效性，且為可信任之憑證機構、政府機關或企業之簽發。	(2) 敏感性資料應採用適當且有效之金鑰長度與加密演算法，進行加密處理再儲存。 (3) 敏感性資料應儲存於受作業系統保護之區域，以防止其他應用程式未經授權之存取。 (4) 敏感性資料應避免出現於行動應用程式之程式碼。 4. 敏感性資料傳輸：行動應用程式透過網路傳輸敏感性資料，應使用適當且有效之金鑰長度與加密演算法進行安全加密。 5. 敏感性資料分享：行動裝置內之不同行動應用程式間，於分享敏感性資料時，應避免未授權之行動應用程式存取。 6. 敏感性資料刪除：行動應用程式如涉及儲存使用者敏感性資料，應提供使用者刪除之功能。 (三) 付費資源控管安全 1. 付費資源使用：行動應用程式應於使用付費資源前主動通知使用者，並提供使用者拒絕之權利。 2. 付費資源控管：行動應用程式應於使用付費資源前進行使用者認證，並記錄使用之付費資源與時間。 (四) 身分認證、授權與連線管理安全 1. 使用者身分認證與授權：行動應用程式應有適當之身分認證機制，確認使用者身分，並依使用者身分授權。 2. 連線管理機制 (1)行動應用程式應避免使用具有規則性之交談識別碼。 (2)行動應用程式應確認伺服器憑證之有效性，且為可信任之憑證機構、政府機關或企業之簽發。	

<table>
<tr><th>修正條文</th><th>105.12.29 函報條文</th><th>說　明</th></tr>
<tr><td>(3)行動應用程式應避免與未具有效憑證之伺服器，進行連線與傳輸資料。
（五） 行動應用程式碼安全

1. 防範惡意程式碼與避免資訊安全漏洞
(1)行動應用程式應避免含有惡意程式碼。
(2)行動應用程式應避免資訊安全漏洞。
2. 行動應用程式完整性：行動應用程式應使用適當且有效之完整性驗證機制，以確保其完整性。
3. 函式庫引用安全：行動應用程式於引用之函式庫有更新時，應備妥對應之更新版本。
4. 使用者輸入驗證：行動應用程式應針對使用者輸入之字串，進行安全檢查並提供相關注入攻擊防護機制。
二、 伺服端資訊安全技術要求事項
各會員公司針對行動應用程式涉及伺服端之資訊安全需求，其伺服端服務之資訊安全防護與管理，應依據附件一壽險業辦理電腦系統資訊安全評估作業原則肆、一、(三)網路設備、伺服器等設備檢測辦理。</td><td>(3)行動應用程式應避免與未具有效憑證之伺服器，進行連線與傳輸資料。
（五） 行動應用程式碼安全

1. 防範惡意程式碼與避免資訊安全漏洞
(1)行動應用程式應避免含有惡意程式碼。
(2)行動應用程式應避免資訊安全漏洞。
2. 行動應用程式完整性：行動應用程式應使用適當且有效之完整性驗證機制，以確保其完整性。
3. 函式庫引用安全：行動應用程式於引用之函式庫有更新時，應備妥對應之更新版本。
4. 使用者輸入驗證：行動應用程式應針對使用者輸入之字串，進行安全檢查並提供相關注入攻擊防護機制。
二、 伺服端資訊安全技術要求事項
各會員公司針對行動應用程式涉及伺服端之資訊安全需求，其伺服端服務之資訊安全防護與管理，應依據附件一壽險業辦理電腦系統資訊安全評估作業原則肆、一、(三)網路設備、伺服器等設備檢測辦理。</td><td></td></tr>
<tr><td>伍、安全分類
不同應用類別之行動應用程式對於安全性有不同之要求，針對不同類型行動應用程式之資訊安全要求事項進行區分，共分為三類，分別為：
<table><tr><th>分類</th><th>定義</th></tr><tr><td>第一類、純功能性</td><td>僅提供離線公開資訊檢視功能。</td></tr><tr><td>第二類、具認證功能與</td><td>具認證功能與連網行為，能夠執行本機端或</td></tr></table></td><td>伍、安全分類
不同應用類別之行動應用程式對於安全性有不同之要求，針對不同類型行動應用程式之資訊安全要求事項進行區分，共分為三類，分別為：
<table><tr><th>分類</th><th>定義</th></tr><tr><td>第一類、純功能性</td><td>僅提供離線公開資訊檢視功能。</td></tr><tr><td>第二類、具認證功能與</td><td>具認證功能與連網行為，能夠執行本機端或</td></tr></table></td><td>1. 本次未修正。
2. 參考經濟部工業局「行動應用 App 基本資安規範」之「5. 安全分類」條文，訂定各 App 分類之定義，以明確區分各類別 App 應符合之技術要求。</td></tr>
</table>

修正條文		105.12.29 函報條文		說　明
連網行為	伺服器端資料之查詢、新增、修改與刪除。	連網行為	伺服器端資料之查詢、新增、修改與刪除。	
第三類、具交易功能與客戶個人資料處理（包含認證功能與連網行為）	具認證功能與連網行為，能夠執行交易、將個人資料下載至行動設備端或執行伺服器端客戶資料之查詢、新增、修改與刪除。	第三類、具交易功能與客戶個人資料處理（包含認證功能與連網行為）	具認證功能與連網行為，能夠執行交易、將個人資料下載至行動設備端或執行伺服器端客戶資料之查詢、新增、修改與刪除。	

針對每一安全分類，定義應符合資訊安全技術要求事項之最小集合，即行動應用程式應符合其所屬分類中之所有資訊安全技術要求事項。各安全分類之資訊安全技術要求事項詳如表1。

表1 各安全分類之資訊安全技術要求事項

編號	資訊安全技術要求事項	安全分類 一	二	三
1	行動應用程式發布	V	V	V
2	行動應用程式更新	V	V	V
3	行動應用程式安全性問題回報	V	V	V
4	行動應用程式上架資安檢測與評估	V	V	V
5	行動應用程式下載、安裝與首次啟動	V	V	V
6	敏感性資料存取同意		V	V
7	敏感性資料利用		V	V
8	敏感性資料儲存		V	V
9	敏感性資料傳輸		V	V
10	敏感性資料分享		V	V
11	敏感性資料刪除		V	V
12	付費資源使用			V
13	付費資源控管			V
14	使用者身分認證與授權		V	V
15	連線管理機制		V	V
16	防範惡意程式碼與避免資訊安全漏洞	V	V	V

針對每一安全分類，定義應符合資訊安全技術要求事項之最小集合，即行動應用程式應符合其所屬分類中之所有資訊安全技術要求事項。各安全分類之資訊安全技術要求事項詳如表1。

表1 各安全分類之資訊安全技術要求事項

編號	資訊安全技術要求事項	安全分類 一	二	三
1	行動應用程式發布	V	V	V
2	行動應用程式更新	V	V	V
3	行動應用程式安全性問題回報	V	V	V
4	行動應用程式上架資安檢測與評估	V	V	V
5	行動應用程式下載、安裝與首次啟動	V	V	V
6	敏感性資料存取同意		V	V
7	敏感性資料利用		V	V
8	敏感性資料儲存		V	V
9	敏感性資料傳輸		V	V
10	敏感性資料分享		V	V
11	敏感性資料刪除		V	V
12	付費資源使用			V
13	付費資源控管			V
14	使用者身分認證與授權		V	V
15	連線管理機制		V	V
16	防範惡意程式碼與避免資訊安全漏洞	V	V	V

修正條文					105.12.29 函報條文					說　明
17	行動應用程式完整性			V	17	行動應用程式完整性			V	
18	函式庫引用安全	V	V	V	18	函式庫引用安全	V	V	V	
19	使用者輸入驗證		V	V	19	使用者輸入驗證		V	V	