保險經紀人資訊安全作業控管自律規範

112.9.13保局(綜)字第1120431623號函備查

第一條

中華民國保險經紀人商業同業公會(以下簡稱本公會)為促進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，確保本公會所屬會員公司資訊處理作業能安全有效地運作，特訂定本自律規範以為遵循。

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、自攜裝置：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。

第三條

各會員公司應確實依據各公司訂立之資安處理程序規定及其應注意事項辦理外，並應依本自律規範辦理。

第四條

各會員公司應確實遵循下列規定：

一、延攬人員時，應依據相關法令合約、產業文化及業務需求，進行相當的人員背景查驗。

二、各公司成員應要求首聘任之人員簽署 「資訊安全保密切結書」或於雇用契約、工作手冊明訂成員應遵守資訊安全 保密協定。

三、各會員公司所委外業務之公司或自然人，應於委外契約中明訂資訊安全保密，以保障公司資訊安全。

四、已實施內稽內控制度之會員公司，應配置至少一名資安專責人員，並定期辦理查核。

五、應透過定期、適當的教育訓練，告知內部人員應遵循的資訊安全政策規範。資通安全專責人員每人每年至少接受十二小時以上之資通安全專業課程訓練，資訊人員每人每年至少接受三小時以上之資訊安全通識教育訓練，一般使用者及主管每人每年接受三小時以上之資通安全通識教育訓練。

六、管理階層須要求人員遵循公司既定之資訊安全規範。

七、所屬人員職務異動時，應依既定程序辦理資訊業務與相關資訊資產退回與存取權限的變更或取消。

第五條

各會員公司應訂定使用行動裝置（含自攜裝置）之相關規範，其內容應至少包含下列項目：

一、使用行動裝置透過公司內部網路連至外網及存取資料管理。

二、外接式存取裝置之使用管理。

三、使用行動裝置之安全控管程序。

第六條

各會員公司應訂定使用社群媒體及電子郵件之相關規範，其內容應至少包含下列項目：

一、訂定使用社群媒體之管理辦法

二、不得使用社群媒體討論公司機密訊息。

三、嚴禁使用他人的帳號來傳送、存取電子郵件。

四、公司機密性或專有資訊，透過電子郵件傳送之規定。

五、公司應加強人員資安宣導社群媒體及電子郵件之網路安全教育。

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、 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、避免因使用雲端服務導致共享環境所造成的資安問題。

三、於雲端服務進行存取時，應防止資料遺失或外洩，並予以適當之備份。

四、雲端服務的資安教育宣導。

五、不得使用不安全的介接介面。

六、規劃雲端運算解決方案的安全和隱私性。

七、謹慎處理公司置放於雲端資料之管理。

第八條

各會員公司若有建置或提供行動裝置應用程式給消費者或內部人員使用，應依據保險經紀人行動裝置應用程式作業原則(如附件一)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性。

第九條

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，強化事件日誌與可歸責性、營運持續計畫、識別與鑑別及系統與服務，並依據保險經紀人辦理電腦系統資訊安全評估作業原則(如附件二)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。

第十條

各會員公司應建立存取控制機制，包含帳號管理、最小權限、遠端存取。

第十一條

各會員公司應建立事件日誌機制，包含紀錄事件、日誌紀錄內容、日誌儲存容量、時戳及校時、日誌資訊之保護。已實施內稽內控制度之會員公司應增加日誌處理失效之回應。

第十二條

各會員公司應建置系統備份機制，已實施內稽內控制度之會員公司應增加系統備援，以維持公司持續營運。

第十三條

各會員公司應訂定勒索軟體攻擊之防護、處理、應變及通報之相關規範，並依據保險經紀人公司辦理勒索軟體應變處理及防護作業原則(如附件三)，以強化資訊系統安全及資料防護能力。

第十四條

各會員公司辦理網路投保及網路保險服務業務，應偵測釣魚網站，提醒客戶防範網路釣魚，並提供客戶安全教育宣導。

第十五條

各會員公司應建立漏洞修復機制，已實施內稽內控制度之會員公司應增加資通系統監控及系統與資訊完整性。

第十六條

各會員公司應部署防毒軟體、網路防火牆，具有郵件伺服器者，應備電子郵件過濾機制，並持續更新病毒碼、惡意郵件特徵等，適時進行軟、硬體之必要更新或升級等資通安全防護。

第十七條

各會員公司應訂定設備（含行動裝置）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。

第十八條

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，確保整體系統穩定及安全。

二、針對使用之視訊會議系統、VPN（虛擬專用網路）及 VDI（虛擬桌面基礎結構）等設備，應訂定相關使用規範並落實各項安全管控作業。

第十九條

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，若發生資訊安全事故或是個人資料外洩時，應儘速回報本公會及主管機關，並採取其他處理措施以控制資安事件影響範圍之擴大。

第二十條

各會員公司應將本自律規範內容納入內部資訊安全業務及資安處理制度及程序。另已實施內稽內控制度之會員公司，應納入內稽內控制度，並定期辦理查核。

第二十一條

各會員公司違反本自律規範經查核屬實者，提報本會理事會依章程規定處置，前述處理情形並應於1個月內報主管機關。

第二十二條

本規範由中華民國保險經紀人商業同業公會訂定，經理事會決議通過報主管機關備查後施行，修正時亦同。

附件一

保險經紀人行動裝置應用程式作業原則

107 年 10 月 24 日金管保綜字第 10704943750 號函備查

壹、前言

為提升我國保險經紀人公司行動裝置應用程式基本安全防護能力，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裝置應用程式安全防護能力。

貳、適用範圍

一、本作業原則為保險經紀人公司提供行動應用程式之基本資訊安全準則。

二、消費者或內部人員在首次使用行動裝置應用程式前，若有個人資料蒐集處理及利用應依法告知。

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,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。

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。

七、 交談識別碼（Session Identification, SessionID）: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。

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:

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公司內部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。

3. 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。

4. 行動應用程式安全性問題回報：

行動應用程式開發者應提供回報安全性問題之管道，並應於適當期間內回覆問題並改善。

5. 行動應用程式上架資安檢測與評估

(1)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保險經紀人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。

6. 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，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：行動應用程式應於蒐集、利用、儲存、傳輸、分享敏感性資料前，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: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並提醒使用者定期更改通行碼。

3. 敏感性資料儲存:

(1)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。

(2)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。

(3)應避免出現於行動應用程式之程式碼。

4. 敏感性資料傳輸: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：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. 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. 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. 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. 應避免使用具有規則性之交談識別碼。

3. 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，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應依據本會所訂「保險經紀人辦理電腦系統資訊安全評估作業原則」肆、一、(三)、網路設備、伺服器及終端機等設備檢測辦理。

伍、安全分類

一、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：

第一類、純功能性:僅提供離線公開資訊檢視功能。

第二類、具認證功能與連網行為:具認證功能與連網行為，能夠執行本機端或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(包括認證功能及連網行為):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。

二、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
5	行動應用程式下載、安裝與首次啟動		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
17	行動應用程式完整性			V
18	函式庫引用安全	V	V	V
19	使用者輸入驗證		V	V

附件二

保險經紀人辦理電腦系統資訊安全評估作業原則

112.9.13 保局(綜)字第 1120431623 號函備查

壹、前言

為確保保險經紀人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、保險經紀人應就整體電腦系統（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，但外國保險經紀人公司在台分公司，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：

電腦系統類別	定義	評估週期
第一類	直接提供客戶自動化服務或對營運有重大影響之系統	每年至少辦理一次資訊安全評估作業
第二類	經人工介入以直接或間接提供客戶服務之系統（如客戶服務、保單行政系統等系統）	每三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。

四、保險經紀人如有第一類電腦系統，全部核心資通系統至少每二年辦理一次業務持續運作演練。

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。

4.適時參考金融資安資訊分享與分析中心(F-ISAC)或其他資安廠商所發布之資安威脅情資及資安防護建議，並採取相關措施。

(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、入侵偵測或防禦、防毒軟體、資料外洩防護、垃圾郵件過濾、網路釣魚偵測、網頁防護）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、伺服器及終端機等設備檢測

1.檢視網路設備、伺服器及終端機的弱點與修補。

2.檢視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或針對網站及客戶端軟體進行弱點掃描、程式原始碼掃描或黑箱測試。

2.檢視網站目錄及網頁之存取權限。

3.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。

（六）存取機制檢視

1.檢視帳號管理:

(1)帳號管理機制，包含帳號之申請、建立、修改、啟用、停用及刪除之程序。

(2)已逾期之臨時或緊急帳號應刪除或禁用。

(3)資通系統閒置帳號應禁用。

(4)定期審核資通系統帳號之申請、建立、修改、啟用、停用及刪除。

2.檢視最小權限：採最小權限原則，僅允許使用者（或代表使用者行為之系統程序）依業務需求取得所需之存取權限。

3.檢視遠端存取:

(1)通過授權檢查後始可放行，並建立相關使用限制、組態需求及連線需求，包含使用者身分類型、來源位址、連線人數上限、網路連線類型、開放時段、允許存取的功能資源及任何先備條件等限制。

(2)於伺服器端完成使用者之權限檢查作業。
(3)監控遠端存取公司內部網段或資通系統後臺之連線。
(4)採用加密機制建立安全通道。
(5)遠端存取之來源應為公司已預先定義及管理之存取控制點。
（七）事件日誌機制檢視
1.檢視紀錄事件:
(1)訂定日誌之記錄時間週期及留存政策，並保留日誌至少六個月。
(2)確保資通系統有記錄特定事件之功能，並決定應記錄之特定資通系統事件。
(3)記錄資通系統管理者帳號所執行之各項功能。
(4)定期審查公司所保留資通系統產生之日誌掌握期間是否曾發生重要資安事件 。
2.檢視日誌紀錄內容應包含事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別等資訊。
3.檢視日誌儲存容量：依據日誌儲存需求，配置充足之儲存容量。
4.檢視日誌處理失效之回應
(1)資通系統於日誌處理失效致無法順利產生或留存時，應採取適當之行動。
(2)日誌處理失效事件發生時，資通系統於規定時效內，對特定人員提出告警。
5.檢視時戳及校時
(1)資通系統應使用系統內部時鐘產生日誌所需時戳，並可以對應到世界協調時間(UTC)或格林威治標準時間(GMT)。
(2)系統內部時鐘應定期與基準時間源進行同步。
6.檢視日誌資訊之保護:
(1)對日誌之存取管理，僅限於有權限之特定人員。
(2)應運用雜湊或其他適當方式確保日誌未遭竄改。
（八）系統備份檢視:
1.訂定可容忍資料損失之時間要求。
2.定期執行系統源碼 含原始程式碼、目的程式等與資料備份。
3.應在與運作系統不同地點之安全處所，儲存備份資料，並定期測試備份資料為可用。
（九）系統備援檢視：
1.訂定資通系統從中斷後至重新恢復服務之可容忍時間要求。
2.應規劃適當的備援機制，於原服務中斷時，由備援設備或其他方式取代並提供服務。
(十)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管理對策」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管理對策
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。

三、會員公司應就系統與資訊完整性研擬相關對策，其內容包括：

(一)漏洞修復：

1.應定期進行軟體元件漏洞修復與更新，包含作業系統、資通系統伺服器、開發框架，以及第三方函式庫等軟體元件。並於更新前評估可能風險，避免對系統服務造成預期外的影響。

2.應注意安全漏洞訊息(如 F-ISAC 情資或其他資安廠商、CVE 相關網站、廠商安全通告等)，如有資通系統相關漏洞應儘快修復。

(二)資通系統監控：

1.應建立資通安全通報機制，如有發現資通系統有被入侵跡象時，應通報公司特定人員。

2.應建立資通監控機制(如 Web 應用程式防火牆、入侵偵測系統、入侵防禦系統、惡意程式碼防護軟體、掃描工具，日誌監控軟體、網路監控軟體等)，以偵測惡意攻擊與未授權之連線，並發現未經授權之使用行為。

(三)軟體及資訊完整性：

1.應使用適當工具，檢查重要軟體及資訊內容是否被惡意竄改。

2.使用者輸入資料之合法性檢查(如字元集、長度、數值範圍及可接受值等)，應置於應用系統伺服器端 。

3.發現違反完整性時，應進行事件通報、緊急應處及復原等安全保護措施。

四、會員公司應就識別與鑑別研擬相關對策，其內容包括：

（一）資通系統應具有身分驗證機制識別及鑑別公司使用者或代表公司使用者行為之程序之功能，採帳號密碼者，應禁止使用共用帳號。

（二）身分驗證管理：

1.使用預設密碼登入系統時，應於登入後要求立即變更。

2.身分驗證相關資訊不以明文傳輸。

3.具備帳戶鎖定機制，帳號登入進行身分驗證失敗達五次後，至少十五分鐘內不允許該帳號繼續嘗試登入或使用公司自建之失敗驗證機制。

4.使用密碼進行驗證時，應強制最低密碼複雜度；強制
密碼最短及最長之效期限制。

5.密碼變更時，至少不可以與前三次使用過之密碼相同。

6.身分驗證機制應防範自動化程式之登入或密碼更換 。

7.密碼重設機制 除 對使用者重新身分確認外應發送一次性及具有時效性符記 Token 。

（三）資通系統應遮蔽輸入過程之鑑別資訊如密碼以*取代 。

（四）資通系統密碼應經加密或雜湊處理後儲存。

五、會員公司應就營運持續研擬相關對策，其內容包括：

（一）系統備份：

1.訂定可容忍資料損失之時間要求 。

2.定期執行系統源碼（含原始程式碼、目的程式等）與資料備份。

3.應在與運作系統不同地點之安全處所，儲存備份資料，並定期測試備份資料為可用。

（二）系統備援：

1.訂定資通系統從中斷後至重新恢復服務之可容忍時訂間要求。

2.應規劃適當的備援機制，於原服務中斷時，由備援設備或其他方式取代並提供服務。

六、會員公司應就系統與服務獲得研擬相關對策，其內容包括：

（一）系統發展前，應先依機密性、完整性、可用性評定所需安全控制措施需求 。
（二）系統開發應避免產生具安全弱點之程式碼 。
（三）定期執行系統主機作業系統及應用程式執行「弱點掃描」安全檢測、「滲透測試」安全檢測，並進行漏洞修補 。
（四）系統相關軟體元件應進行版本更新與漏洞修補並關閉不必要服務及埠口。
（五）資通系統不使用預設密碼。
（六）資通系統開發如委外辦理，應將系統發展生命週期各階段依 系統安全等級所需之防護基準納入委外契約。
（七）開發、測試及正式作業環境應為區隔。
（八）應儲存與管理系統發展生命週期之相關文件。

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，應與提供、維護資安評估標的之機構無利害關係，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或可採用獨立電腦系統（弱點掃描工具、原碼掃描平臺、滲透測試工具、原碼掃、社交工具平臺、惡意程式或防毒軟體檢測平臺…等）輔助進行評估。

二、辦理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：

（一)參加相關資訊安全管理課程訓練達一定時數並取得教育訓練合格證明文件者或具備相關證照者。

（二）熟悉金融領域作業流程或具備相關經驗者。

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

「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。

附件三

保險經紀人公司辦理勒索軟體應變處理及防護作業原則

一、 定義：

勒索軟體(Ransomware)是一種透過破壞受駭者存取權限，並向受駭者要求贖金的惡意程式，目前可分類為「非加密型勒索軟體」(鎖資訊設備)與「加密型勒索軟體」(加密檔案)。

二、 勒索軟體類型

勒索軟體可以進行無差別的攻擊(Indiscriminate Attack)，即駭客大規模且不加選擇地散布勒索軟體進行攻擊，亦或是針對性的目標式攻擊(Targeted Attack)，鎖定金融行業組織、醫療組織、工業企業和運輸等行業，以取得更高的贖金，目標式攻擊使用更複雜的魚叉式網路釣魚(Spear Phishing)或利用進階持續性滲透攻擊(Advanced Persistent Threat, APT)及系統漏洞進行攻擊，以避開日益精進的垃圾郵件過濾系統及資安防護機制。

三、 勒索軟體造成的威脅損害類型：

(一)、 資料可用性：是最主要的威脅傷害型態，加密受害電腦中的檔案，要求受害者支付贖金換取解密金鑰，然而即使受害者願意支付贖金，也未必能確保資料完整的恢復。

(二)、 系統可用性：特徵是阻止受害者存取受感染的電腦或行動裝置，鎖住電腦螢幕與瀏覽器導致無法使用，藉以達到威脅的目標。

(三)、 隱私挾持(Doxware)：主要是對資料的機密性造成傷害，駭客將受害者電腦中的資料大量加密和上傳，以洩漏該隱私或機敏資料作為要脅，迫使受害者支付贖金換取資料不外洩。

四、 攻擊跡象：

常見的勒索軟體會連線到C&C伺服器下載加密金鑰，並開始加密電腦中的檔案，然後在電腦上放置支付贖金的說明檔案(RansomNote)，多於文中威脅受駭者若不支付贖金將無法解密檔案或將公開電腦中的機敏資料，當出現下列跡象出現時，就有可能就是遭到勒索軟體感染：

- 勒索留言通常是.txt檔或是.html檔。
- 發現文件被加密無法開啟。
- 發現各目錄下開始出現奇怪副檔名的檔案，例如：.crypt、.VVV、.CCC、.ZZZ、.AAA、.ABC、.XXX、.TTT等。
- 瀏覽器遭鎖定或瀏覽器工具列發現奇怪的捷徑。
- 畫面遭鎖定。
- 電腦出現藍色當機畫面，在電腦重新開機時顯示勒索訊息。

五、 勒索軟體感染途徑：

(一)、 網站瀏覽：

- 瀏覽網站時，倘若使用者電腦存在Java/Flash/Adobe/瀏覽器等軟體漏洞，當輪播到惡意廣告，便可能遭受勒索軟體入侵。
- 點選到網站內的惡意連結(如：廣告、新聞)。
- 誘騙使用者連到看似真正銀行或政府機關網站的假網站(山寨網站)。

(二)、 電子郵件感染：當使用者點選或開啟電子郵件中的惡意網站或內嵌惡意程式的附件檔案，便可能遭受勒索軟體入侵。

(三)、 非法軟體感染：網路上非法軟體或小工具可能含有惡意程式，若使用者下載安裝這類非法軟體或小工具，惡意程式可能在安裝過程中讓使用者授權以存取機密資料或加密資料。

(四)、 被已遭受勒索軟體攻擊的電腦或裝置感染。

六、 感染勒索軟體的緊急處理：

(一)、 立即中斷受駭主機網路連線並隔離，避免災情擴大，若發現主機中的檔案正在被惡意程式加密，應立即關機讓被加密的檔案降低到最少，關機時請持續按壓電源鍵強迫電腦進行關機動作，切勿重新開啟主機以免加密程式繼續進行。

(二)、 監控網路流量並執行防毒掃描以確定是否仍有感染，並盤點可能受影響設備及執行防毒軟體掃描。

(三)、 可嘗試使用信任來源的解密工具解密，並保存受駭主機以提供分析環境，請求專家協助或報警處理。

(四)、 系統重灌及備份還原，讓主機回復成乾淨的原始狀態，重灌及還原前確認受駭當時主機本身的風險與狀態，以避免重灌及還原後因同樣漏洞再感染，並安裝、更新及執行防毒軟體。

(五)、 依受駭原因，規劃改善措施並執行。

(六)、 不建議支付贖金，因支付贖金並不能保證取回存取權限，且將助長勒索軟體更加猖獗。

七、 勒索軟體預防措施：

(一)、 使用防毒軟體，並及時更新系統、軟體和應用程序：攻擊者通常利用未修補的漏洞來訪問未經授權的系統和網路，以執行後續惡意活動。

(二)、 強化具派送功能伺服器安全：防毒軟體中控、AD 伺服器、資產管理系統等因具有軟體派送功能，更需注意安全更新，並密切觀察其群組原則或工作排程不正常異動狀況。

(三)、 最小化開放埠的設置:勒索軟體可能會利用對外曝露的服務和開放埠(例如 RDP 埠 3389 和 SMB 埠 445)在網路中傳播，除了確認其開放的必要性外，還應確認使用這些服務的對象為可信任。

(四)、 實施網路分段區隔並監控流量

i. 在實施網路分段區隔後，如果某一區段受到威脅，至少可限制勒索軟體在網路中的傳播。

ii. 監控任何可疑連接的網路流量，並阻止任何與已知惡意 IP、URL 的網路連線行為。

(五)、 實施應用程序控制：應考慮安裝可控制應用程序、目錄白名單的軟體，僅允許執行已批准的程序，以防止惡意軟體程序被執行。

(六)、 人員的最小使用權限：為了減少攻擊者獲得管理權限的機會，應該：

i. 控制和限制存取權限，僅限於需要完整存取權限才能執行工作的人員獲得授權。

ii. 為管理者以外的使用者提供工作所需的最低權限。

iii. 查看和管理所有使用戶帳戶的使用情況，並禁用非活動帳戶 。

(七)、 監控可疑活動：監控可疑掃描活動和未經授權的登錄嘗試，對防止遭到攻擊具有極大幫助。

(八)、 僅在需要時啟用 Microsoft Office 巨集：勒索軟體可能透過惡意 Microsoft Office 檔案感染，誘使受害者啟用巨集以查看檔案內容。

(九)、 提高資安意識：建立良好資安意識及網路使用習慣，例如識別可疑電子郵件，不要隨意點擊連結，不打開未知或不受信任來源的電子郵件的附件。並進行社交工程演練，提高訓練

成效。

(十)、 加密重要或敏感資料：應對重要或敏感資料進行加密，如果資料被竊取，可以使攻擊者難以處理這些資料，另外，某些勒索軟體僅對常用文件類型（例如圖檔和文檔）起作用，則加密還可以防止它們檢測到文件。

(十一)、 維護更新的備份並保持離線：定期執行資料備份有助於在發生勒索軟體攻擊時恢復資料，而備份資料必須離線儲存且不能連接到既有企業網路中，可防止勒索軟體透過網路影響備份資料。備份原則：3 份備份、2 種儲存媒體、1 個不同的存放地點。

(十二)、 定期維護關鍵系統的映像檔：虛擬機或服務器的映像檔包括預先配置的作業系統和相關的應用軟體，當發生攻擊，而需要重建系統，可以利用這些映像檔達到快速部署恢復。

(十三)、 啟用 Windows 受控制資料夾存取功能。其功能是限制只有安全的應用程式才能存取特定資料夾，防止勒索軟體對資料進行加密或竊取。

(十四)、 在事件發生之前，制定事件應變計劃並進行演練，以測試計劃是否可行是非常重要的。在受到攻擊時難以即時判斷正確作法，透過已制定好的計劃並實施，將有助於員工了解要採取的行動，並確定各項系統與環境的恢復優先等級。

(十五)、 預先備妥資安事件發生時可協助之外部資安單位、警調清單與連絡方式。