公勝保險經紀人股份有限公司

文件編號	CG-1-016-00-03	資通安全檢查控制作業	制／修訂日期	2022.05.10
編訂單位	資訊部		版次：3	等級：一般

制／修訂日期	版本	制／修訂內容	制／修訂者
2017.11.28	1	制訂「資通安全檢查控制作業」	資訊部
2018.08.16	2	配合公開發行、相關法令規則修訂與公司組織異動，修訂相關條文	資訊部
2022.05.10	3	因管理辦法整併，酌作文件編號修訂	資訊部

公勝保險經紀人股份有限公司

文件編號	CG-1-016-00-03	資通安全檢查控制作業	制／修訂日期	2022.05.10
編訂單位	資訊部		版次：3	等級：一般

一、目的：

建立本公司防火牆建置、網路服務、電子郵件、網路入侵之安全指導原則，以有效強化資訊安全。

二、適用範圍：

本作業程序適用於資通安全作業之建立、實施與控制等作業。

三、定義：

進出規則(ACL)：

(一)防火牆規則正面表列：依允許進入的方式作存取控制，其內定設定為禁止。

(二)防火牆規則負面表列：依禁止進入的方式作存取控制，其內定設定為開放。

四、權責單位：

(一)網路使用者：

提出網路存取使用需求。

(二)系統負責人：

1.分析系統與應用程式之網路存取行為，提供防火牆設定之參考資訊。

2.負責提供網路存取行為相關流量數據，提供防火牆配置之參考資訊。

(三)資訊部主管：

1.審核防火牆開放與限制之申請。

2.監督防火牆管理作業。

3.使用防火牆產品之審核。

(四)防火牆系統負責人：

1.防火牆之建置、管理與維護。

2.產品評估建議。

五、處理程序：

(一)依「QT-3-001-00電腦病毒防範管理作業說明書」辦理。

(二)軟體使用控制：

1.禁止網路使用者使用非法軟體。

2.區域網路內各檔案伺服器安裝防毒軟體，防止病毒在網路上擴散。

3.網路使用者應定期以電腦病毒掃描工具執行病毒掃描（目前均定期進行全面掃毒），採行防範措施。

4.網路使用者如偵測到電腦病毒或其他惡意軟體入侵，應立即通知網管人員；網管人員需將已遭感染之資料與程式隔離掃毒，以免病毒擴散。

5.電腦設備如遭病毒感染，應立即將網路離線，直到網管人員確認病毒已掃除後，方可連線。

(三)網路服務之管理控制：

1. 系統最高權限，應經權責主管審慎評估後，交付可信賴的人員管理。
2. 網管人員應負責執行網路管理工具之設定操作，確保系統與資料的安全與完整性。
3. 網管人員負責核發帳號，提供取得授權的人員使用；除非有特殊情況，不得核發匿名或多人共享帳號。
4. 提供給內部人員或開放有關人員遠端登入的網路系統，應使用防火牆或其他代理程式進行安全控管。
5. 若使用者已非合法授權之使用者，網管人員應立即撤銷其使用帳號;離（休）職人員應依其離職程序，取消其存取網路之權力。
6. 網管人員不得閱覽使用者私人檔案，但有發現可疑的網路安全情事，網路系統管理員得依安全規定，使用自動搜尋工具檢查檔案或呈報資訊單位主管，經核准後始可檢查檔案。
7. 網管人員未經使用者同意，不得增加、刪除及修改私人檔案。如有特殊緊急狀況，需刪除私人檔案，應以電子郵件或其他方式事先知會檔案擁有者。
8. 對任何網路安全事件，網管人員應立即向機關內部或其他電腦安全事件緊急處理人員反應。
9. 網管人員不得新增、刪除及修改稽核資料檔案，以避免違反安全事件發生時，造成追蹤查詢的困擾。

(四)網路使用者之管理控制：

1. 被授權的網路使用者（以下簡稱網路使用者），只能在授權範圍內存取網路資源。
2. 網路使用者應遵守安全規定，並確實了解其應負之責任；如有違反網路安全情事，應依資訊安全規定，限制或撤銷其網路資源存取權利。
3. 網路使用者不得將自己的登入身分識別與密碼交付他人使用，並禁止網路使用者以任何方法竊取他人的登入身分識別與密碼。
4. 禁止及防範網路使用者以任何儀器設備或軟體工具竊聽網路上的通訊。
5. 禁止網路使用者在網路上取用未經授權的檔案。
6. 網路使用者不得將色情檔案建置在公司網路，亦不得在網路上散播色情文字、圖片、影像、聲音等不法或不當的資訊。
7. 禁止網路使用者使用電子郵件騷擾、猥褻、恐嚇他人，導致其他使用者之不安與不便。
8. 禁止網路使用者發送匿名信，或偽造他人名義發送電子郵件。
9. 網路使用者不得以任何手段蓄意干擾或防害網路系統之正常運作。

10.公司外部取得授權的電腦主機或網路設備，與公司內部網路連線作業時，應確實遵守網路安全規定及連線作業程序。

(五)防火牆之安全管理控制：

依「QT-3-005-00 防火牆管理作業說明書」辦理。

(六)電子郵件之安全管理控制：

依「QT-2-007-00 電子郵件管理作業程序」辦理。

(七)全球資訊網之安全管理控制：

1.內部使用的瀏覽器，應開啟作業系統所提供之防火牆或安裝額外防火牆軟體。

2.內部使用的瀏覽器，應設定對下載的每一檔案作電腦病毒或內容掃描。

3.需考量網際網路新技術（如 Java、ActiveX 等）的可能安全性弱點，並採防護措施以確保內部網路安全。

4.公司內部各分公司間敏感性資料應經由虛擬專用網路（VPN）處理，以確保資料安全的隱密性。

(八)網路線路備援與系統備援機制控制：

1.網路硬體設備應加設不斷電系統，以防止不正常斷電狀況。

2.為確保內部網路與外界服務持續暢通，內部網路與外界網路的介接，應增加一個以上替代路徑(如 ISDN、ADSL 線路備援)。

3.網路系統中之防火牆與各主機應定期作系統備份，包括完整系統備份、系統架構設定備份以及稽核資料備份。

(九)網路入侵之處理控制：

1.網路如有發現被入侵或疑似被侵入情形，應依事前訂定的處理程序，採取必要的行動。

2.網路遭入侵處理步驟如下:

(1)立即拒絕入侵者任何存取動作（及時更改 Administrator 密碼），防止災害繼續擴大，當防護網被突破時，系統應設定拒絕任何存取動作，或入侵者已被嚴密監控，在不危害內部網路安全前提下，得適度允許入侵者存取不相關檔案資料，以利追查入侵者。

(2)切斷入侵者的連接，如無法切斷，則必須關閉防火牆，或為達到追查入侵者之目的，可考慮入侵者作有條件之連接，一旦入侵者危害內部網路安全，則必須切斷入侵者的連接。

(3)全面檢討網路安全措施及修正防火牆的設定與病毒防護，以防禦類似的入侵攻擊。

(4)正式紀錄入侵情形及評估影響的層面。

(5)立即向權責主管報告入侵情形，並加以檢討。

(6)向公司內部或外部的電腦安全緊急處理人員反應，以獲取必要的外部協助。

3.對入侵者的追查，除利用稽核檔案提供之資料外，得使用系統指令執行反向查詢，並聯合相關服務單位（資訊網路服務公司）追蹤入侵者。

4.入侵者之行為若觸犯法律規定，構成現行法令之犯罪事實，應立即告知檢警憲調單位，請其處理入侵者之犯罪事實調查。

六、控制要點：

(一)公司對外網路是否裝設防火牆及伺服器是否安裝防毒軟體以隔絕外來侵害？

(二)資訊人員是否定期檢視伺服器上郵件收發情形，若有異常狀況應呈報權責主管處理？

(三)是否訂定資訊安全相關政策並透過公告或訓練傳達給員工，並定期執行檢查？

(四)資通安全檢查作業相關報告是否呈核主管，並對缺失做追蹤改善？

七、相關法規：

略。

八、使用表單：

略。