智新資通股份有限公司

文件名稱：網路安全管理程序			
文件編號：ISMS-2-020	版本：C	頁次：1/6	發行日期：2024/11/15

版本修訂紀錄表

文件版本	制/修訂日期	修訂重點內容	修訂人員
A	2023/01/07	初稿	Pake
B	2023/03/10	修訂5.7.3、5.7.4與7.1	潘彣昕
C	2024/11/15	新增項次5.8.網路過濾與其內容。	Judy

智新資通股份有限公司

文件名稱：網路安全管理程序			
文件編號：ISMS-2-020	版本：C	頁次：2/6	發行日期：2024/11/15

1. 目的：

為辦理本公司網路安全之協調、規劃、稽核等事項，皆由網路管理員負責處理網路安全相關事宜。

2. 範圍：

2.1.

2.2. 網路作業使用之相關設備與資產，例如各項設備及網路服務作業流程中之書面文件及電子紀錄等。

2.3. 本公司之所有同仁、工讀生以及承包本公司各項作業之廠商。

3. 權責：

3.1. 管理代表

3.1.1. 賦予/收回系統最高權限給所指定之網路管理員。

3.1.2. 依據網路作業相關規範，監督網路管理員執行工作。

3.1.3. 接受同仁通報網路安全事件，並決定回應機制。

3.1.4. 指派網路管理相關人員執行網路管理任務。

3.2. 網路管理員

3.2.1. 負責本公司同仁網路安全之維護。

3.2.2. 負責同仁之職務異動、離職及申請等權限的管理。

3.2.3. 負責相關網路設備之操作與管理，以確保本公司內部網路與外部網路之連線暢通。

3.2.4. 負責網路安全之維護，利用各項網路安全工具，以保護本公司網路之安全。

4. 名詞釋義：無。

5. 作業內容：

5.1. 網路服務之安全控管

智新資通股份有限公司

文件名稱：網路安全管理程序			
文件編號：ISMS-2-020	版本：C	頁次：3/6	發行日期：2024/11/15

5.1.1. 同仁在使用網路傳送機密等級以上的資料時，應注意資料的完整性及機密性，並留意作業系統操作的安全性。

5.1.2. 當網路使用者為逾期授權或非合法授權的使用時，網路管理員應立即撤銷其使用權限；離（休）職人員也應立即取消其使用網路之權限。

5.1.3. 網路管理人員除有緊急狀況外，未經使用者同意，不得增加、刪除及修改私人檔案。

5.1.4. 網路設備服務之管控須留存紀錄備查。

5.1.5. 網路設備事件紀錄需保留6個月以上。

5.2. 網路使用者之管理

5.2.1. 網路使用者經授權後，只能在授權範圍內存取網路資源。

5.2.2. 網路使用者應遵守本程序，並確實瞭解其使用之權利與義務；如有違反本程序應依規定，限制或撤銷其網路權限。

5.2.3. 網路使用者不得將自己登入之身分識別與密碼交付他人使用。

5.2.4. 網路使用者禁止以任何方法竊取他人之登入身分與網路通行碼。

5.2.5. 網路使用者禁止以任何儀器設備或軟體工具進行非受權截取網路上的資訊。

5.2.6. 網路使用者禁止在網路上取用未經授權之檔案。

5.2.7. 網路使用者不得將色情檔案建置在網路，亦不得在網路上散播色情文字、圖片、影像、聲音等不法或不當之資訊。

5.2.8. 網路使用者禁止發送電子郵件騷擾他人，導致其他使用者之不安與不便；或以任何手段蓄意干擾或妨害網路系統之正常運作。

5.3. 網路資訊之管理

5.3.1. 如具有內部、機密等級及極機密等級之業務資料或文件不得存放於對外開放之資訊系統中，若因特殊業務功能之需求，必須採取加強之安全管控機制，如：資料加密或密碼防護等措施。

智新資通股份有限公司

文件名稱：網路安全管理程序			
文件編號：ISMS-2-020	版本：C	頁次：4/6	發行日期：2024/11/15

5.3.2. 對外開放或存放重要資訊的資訊系統，其傳輸時應以加密方式或密碼防護處理，以防止被竊取或移作他途之用。

5.3.3. 針對加密使用之憑證由網路管理員進行取得、安裝及展延等管理事宜。

5.3.4. 偵測到資訊系統異常狀況或駭客入侵之警示訊息時，應立即通報，並採取緊急應變處理措施，及留存系統異常處理紀錄。

5.4. 網路入侵之處理

5.4.1. 若發現入侵者之行為已觸犯法律規定，構成犯罪事實，應立即通報管理代表，請其派人協助處理入侵者之犯罪事實調查。

5.4.2. 應查詢最新資安訊息，如國家資通安全會報技術服務公司網站、相關資安論壇等，以掌握最新網路安全訊息及防範措施。

5.5. 網路安全事件之處理

5.5.1. 一經發現或接獲通報發生網路安全事件，應立即通資訊安全管理委員會管理代表，並採取緊急應變措施處理。

5.6. 強制性通道：

5.6.1. 對使用網路系統的電腦連接線路，應適當加以控制，以減少未經授權之系統存取或電腦設施的風險。

5.6.2. 應建立強制的通道並建立控制措施、設定網路存取規則。

5.6.3. 設定網路區隔之規劃，應遵循內外網路實體區隔規定，並應禁止個人無線網路裝置破壞內外網路實體區隔之安全機制。

5.7. 網路安全管理作業

5.7.1. 防火牆安全管理作業

5.7.2. 本公司內部網路與訪客網際網路之間以不同網段作為分隔。

5.7.3. 如防火牆政策有新增或異動需求時，需求單位填寫「防火牆進出規則申請表」，描述連線目的、用途及連線起/訖日期，經管理代表核准後，交由網路管理員設定防火牆。

5.7.4. 網路管理員應於申請日期結束當日，重新設定關閉防火牆，以防止未經授權之連線，並針對申請開放期間之連線作業進行檢視，是否有異常之形式，並將關閉及檢視作業記錄於「防火牆進出規則申請表」。

5.7.5. 防火牆開放或防護政策審查：

5.7.5.1. 網路管理員於每年將防火牆設定檔輸出，交管理代表審查、確認。

5.7.5.2. 網路管理員依審查確認結果進行必要之調整。

5.7.6. 防火牆管理包含地端及雲端。

5.8. 網路過濾

5.8.1. 本公司管理對外部網站之存取，以降低暴露於惡意內容，保護系統免受惡意軟體之危害，並防止存取未經授權的網頁資源。

5.8.2. 本公司封鎖存取下列型式之網站：

5.8.2.1. 色情、暴力、賭博、股市、遊戲。

5.8.2.2. 已知或可疑之惡意網站(例:散布惡意軟體或網路釣魚內容的網站)。

5.8.2.3. 指揮控制(C&C)伺服器。

5.8.2.4. 由威脅情資中獲取之惡意網站

5.8.2.5. 分享非法內容之網站。

5.9. 網路分隔控制：規劃適當網路區隔之管理機制，以防止不當網路存取行為與流量散佈。

5.9.1. 內部網路之使用，應對使用狀況與條件區分不同網路區段，以便進行網路存取控管，各區段應以特定的安全設施加以保護，以降低可能的安全風險。

5.9.2. 內部網路之使用，應鑑別主機與使用者之工作內容，並賦予適當網路區段之IP位址，以供網路存取控制管理考量。

5.9.3. 對外網際網路服務與內部網路使用需求應設定適當存取控制機制，防止機密性資訊外洩。

5.9.4. 非經授權嚴禁使用無線網路及私有有線設備與網路介接。

5.10.網路路由控制：本公司以防火牆進行網路邊界與網路路由之管理。

6.相關文件：無。

7.使用表單：

7.1.防火牆進出規則申請表(ISMS-2-020-01)。