雲林縣西螺鎮公所

網路安全管理程序

文件編號： XLTG-02-016

版　　次： V1.0

文件日期： 110 年 11 月 24 日

機密等級： 普通

文件制/修訂履歷

制/修訂 版次	制/修訂 日期	制/修訂 說明	作 者	備 註
V1.0	110.11.24	初版發行	ISMS 執行小組	

目　　錄

壹、 目的

雲林縣西螺鎮公所(以下簡稱本所)為確保網路安全防護之合理性、有效性，特訂定本「網路安全管理程序」(以下簡稱本程序)。

貳、 適用範圍

本程序適用於本所提供服務內、外部使用者之網路管理相關作業。

參、 權責

一、 資安長或其授權人核定、發布本程序。

二、 ISMS 執行小組組長審查本程序，並督導本程序之執行。

三、 ISMS 執行小組研擬、評估及檢討本程序。

四、 ISMS 承辦人協調及彙總本程序之執行。

五、 主機房管理相關人員負責網路安全相關防護工具之適當設定、更新、稽核軌跡分析。

肆、 定義

一、 安全防護工具:指提供網路安全防護之相關工具,包含防毒軟體、防毒牆、防火牆、入侵偵測系統等軟硬體設施。

二、 資訊安全事故：單一或一連串有顯著機率可能危害營運作業與威脅資訊安全之非所欲或非預期的資訊安全事件。

三、 通訊資料：於網路通訊中傳輸的資料。

四、 對外網路服務區(DMZ 區)：指位於內部網路與外部網路間，受到防火牆保護的一個特殊網路區域，用以放置對外服務的伺服器如 Web、FTP 等。

五、 外部網路：本所對外防火牆以外的網際網路。

六、 內部網路(Trusted 區)：本所防火牆以內的網路，本網路區域內的使用者通常是被視為可信賴的使用者。

七、 服務提供商：本所資訊相關業務委外時，提供服務的廠商。

八、 備援：建置一套與目前運作系統、網路或資料庫完全相同或類似的環境，以預防目前作業環境因故無法作業時，可及時取代，以避免作業停頓。備援可視需要採取同地備援或異地備援等方式。

九、 存取：指授權使用者、群組及電腦存取網路上物件的程序。

十、 系統設定文件：記錄安全防護工具之組態設定參數的文件。

十一、密碼複雜性原則：密碼設定內含 1 個大寫英文字母、1 個小寫英文字母、1 個阿拉伯數字、1 個特殊字元，至少符合 3 項上述原則。

伍、 管理項目

本所電腦網路規劃為內部網路(Trusted 區)及對外網路服務區(DMZ 區)，內、外部網路間以防火牆區隔，內部網路應與外部網路隔絕，外部網路不得直接存取內部網路。

DMZ 區網路需明確限定允許之通訊協定(如 HTTP、SMTP)對 Internet 開放，並做適當安全防護。有關網路整體安全防護措施，請參考下頁圖 5-1 及後續各節說明。

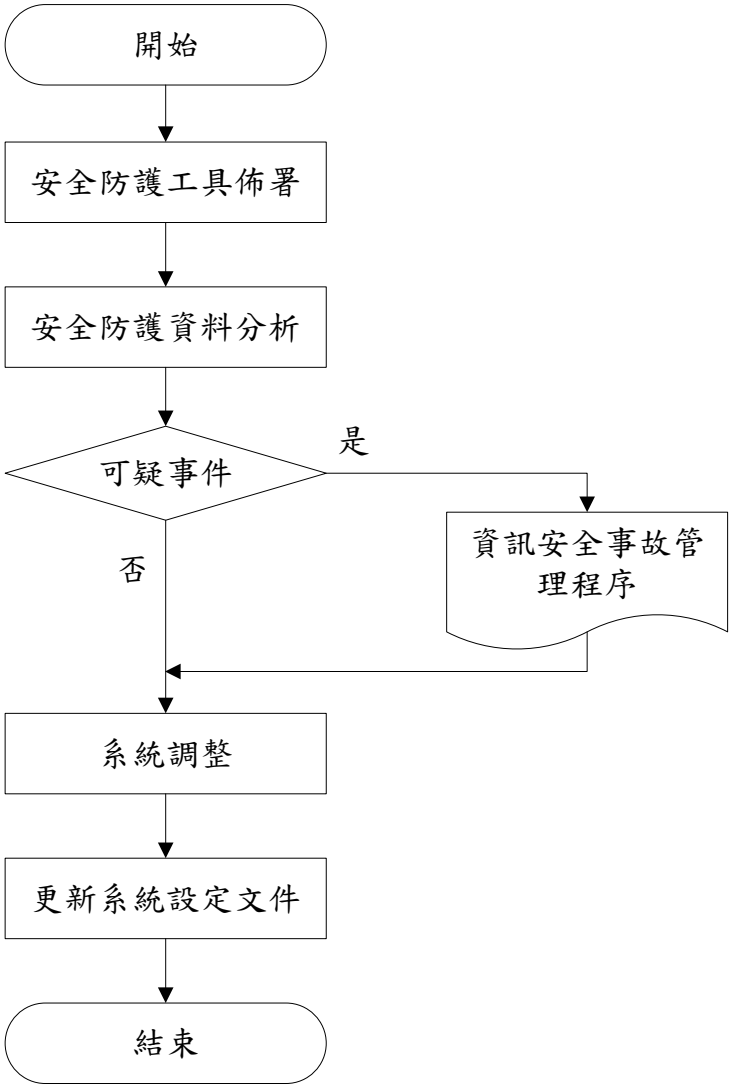

圖 5-1：網路安全管理流程圖

一、 安全防護工具佈署

（一）機房管理相關人員應依據存取控制基準及要求(參見「存取控制管理程序」)，適當設定各項安全防護工具參數。

（二）機房管理相關人員應記錄各安全防護工具之設定參數，以作為後續微調之依據。

（三）重要網路設備(如核心交換器(Core Switch)、防火牆(Firewall)、防毒牆(Virus Wall)、入侵偵測系統(IDS)等)之組態檔案(Configuration files)應於異動後，將檔案備份至其他伺服器或儲

存媒體中。

二、 安全防護資訊分析

（一）主機房管理相關人員應每日由監控終端機(Console)或授權可遠端桌面連線之個人電腦檢視安全防護工具，確認無可疑之安全事件。

（二）主機房管理相關人員應定期彙整相關安全防護工具之稽核軌跡（Audit Trail），提具分析報告，分析報告之內容應包含下列項目：

1. 可疑之活動。
2. 來源位址。
3. 網路流量。
4. 可疑事件之服務類別。
5. 可疑事件之人員處理作業。

（三）主機房管理相關人員應依據分析報告，適當進行安全防護工具之微調，以發揮工具之最大防護效果。

（四）主機房管理相關人員應定期評估，適當更新安全防護工具之引擎、病毒碼、版本等，以確保安全防護工具之辨識能力。

（五）內部網路(Trusted 區)安全管理

1. 應依「存取控制管理程序」之網路存取控制規定辦理。
2. 電腦設備如遭病毒感染，宜立即停止網路連線功能，按「資訊安全事故管理程序」之應變處理，直到病毒已消除後，才可重新連線。
3. 被授權的網路使用者，只能在授權範圍內存取網路資源。
4. 未經許可，不得使用任何儀器設備或軟體工具竊取網路上的通訊

資料。

5. 未經許可,不得使用任何儀器設備或軟體工具進行網路偵測與攻擊。

6. 禁止網路使用者在網路上取用未經授權的檔案。

7. 網路使用者不得將色情檔案建置在公共網路,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。

8. 網路使用者不得以任何手段蓄意干擾或妨害本所網路系統的正常運作。

9. 應關閉不必要的網路資源分享,如需網路資源分享時,應設定適當存取權限及密碼。

10. 未經許可,不得攜入私人資訊設備連接本所區域網路。

11. 廠商或其他機關人員攜入電腦設備,非經申請許可,不得私自連接本所區域網路。

12. 連接本所區域網路之資訊設備,未經許可,不得私設固接、撥接、無線網路等可對外連線之設備。

(六) 對外網路服務區(DMZ 區)安全管理

1. 本所電腦機房網路的連接及管理,得由服務提供商負責維運,並由權責單位監督,各單位或個人均不得私自以固接、撥接、無線網路連接,而形成網路的後門。

2. 對外開放的資訊系統,應置於本所對外網路服務區(DMZ 區),以防火牆與內部網路區隔(Trusted 區),以提高內部網路的安全性。

3. 具機密性及敏感性的資料或文件,不得存放在對外開放的資訊系統中。

4. 主機房管理相關人員應負責監督網路資料使用情形,檢查有無違

反資訊安全規定之事件發生。

5. 對外開放的資訊系統所提供之網路服務(FTP、HTTP 等)，應做適當的存取控管，以維護系統正常運作。

6. 對外開放的資訊系統，如存放個人資料檔案，應以加密方式處理，並妥善保管，以防止被竊取或移作他途之用，保護其個人隱私。

7. 對外開放的資訊系統應只開放所需之服務及通訊埠，關閉不必要的服務及通訊埠。

8. 敏感性資料如透過網路傳送，應經過妥善之加密處理，以確保資料的隱密與安全。

9. 使用瀏覽器，應使用瀏覽器軟體所提供之建議(預設)安全性層級以上，並對下載的每一檔案做電腦病毒或惡意內容的掃描。

10. 相關使用者應正確使用網際網路資源，遵循資訊使用相關規定，保障資通安全。

11. 為維持網路的持續正常運作，各重要網路設備應有備援，或於採購(維護)合約中明訂由承包廠商提供替代品。

12. 網路硬體設備之電源應使用不斷電系統，以防止異常的斷電狀況。

13. 應不定期分析、預防、檢討及公告資訊安全事件，提高人員安全意識。

三、 安全防護工具管理

（一）防火牆管理

1. 本所對外網路之連接點，應加裝防火牆，以控管外部與內部網路

(及外部與 DMZ 區)之間的資料傳輸與資源存取之安全。

2. 防火牆應放置於主機房並限制人員存取。

3. 防火牆應由主機房管理相關人員執行控管設定，並依 ISMS 政策，建立適當安全機制，以規範資源被讀取、更改、刪除、下載或上傳等行為，以及系統存取權限等資訊。

4. 機房管理相關人員應由監控終端機（Console）或授權可遠端桌面連線之個人電腦登入防火牆主機，宜採取加密連線遠端登入方式，以避免登入資料遭竊取，危害網路安全。

5. 防火牆的出入管制規則（Access Control Rules）應儘量減少，以避免混淆，如需變更時，需求人員應將需變動規則於「防火牆異動說明表」中敘明，並作為「資訊服務申請表」之附件，經申請核可後始得變更。

6. 防火牆之系統組態資料(Configuration)及出入管制規則應於每次變更後進行備份。

7. 防火牆應開啟稽核軌跡（Audit Trail），並應每日複製至其他伺服器與執行備份。

8. 防火牆帳號應設定 8 碼以上的密碼，須符合密碼複雜性原則，並至少每年變更 1 次。

9. 防火牆操作畫面於完成相關操作或將暫停操作一段時間時，應即登出，避免不當存取。

（二）防毒牆（Virus Wall）管理

1. 本所檔案伺服器前應加裝防毒牆，掃瞄 http 上傳及下載之檔案，避免使用者電腦中毒。

2. 防毒牆應放置於電腦機房並限制人員存取。

3. 防毒牆應由機房管理相關人員建立適當防毒原則，以偵測可能的病毒檔案型態。

4. 機房管理相關人員應由監控終端機（Console）或授權可遠端桌面連線之個人電腦登入防毒牆主機，宜採取加密連線遠端登入方式(如 HTTPS)，以避免登入資料遭竊取，危害網路安全。

5. 防毒牆的防毒原則如需變更時，需求人員應事先填寫「資訊服務申請表」，經過申請核可後始得變更。

6. 防毒牆應每日與原廠保持即時更新（Real-time Live update)。

7. 防毒牆應啟動防護日誌紀錄，並應每日複製至其他儲存裝置與執行備份。

8. 防毒牆之帳號應設定 8 碼以上的密碼，須符合密碼複雜性原則，並至少每年變更 1 次。

9. 防毒牆操作畫面於完成相關操作或將暫停操作一段時間時，應即登出，避免不當存取。

四、 系統調整

（一）安全防護工具設置完成時，應測試安全防護工具是否依設定的功能正常及安全地運作。如有缺失，應立即調整系統設定，直到符合既定的安全目標。

（二）機房管理相關人員應配合資訊安全政策及規定的更新，以及網路設備的變動，每年至少 1 次檢討及調整安全防護工具的設定，調整系統存取權限，以反應最新的狀況。

（三）應至少每半年檢核及評估安全防護工具之適用性，修補可能漏洞，調整相關管理規則與設定條件。

五、 更新系統設定文件

安全防護工具之相關組態設定參數如有微調或變更，應於變更後將變後之參數內容，更新紀錄於系統設定文件，以供日後參考依據

陸、 參考文件

一、 通訊與操作管理程序。

二、 存取控制管理程序。

三、 資訊安全事故管理程序。

四、 電腦機房管理作業。

五、 職務說明書。

六、 資產清冊。

柒、 使用表單

一、 防火牆異動說明表。

二、 資訊服務申請表。