雲林縣西螺鎮公所

通訊與操作管理程序

文件編號： XLTG-02-010

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)為確保資訊傳輸通訊及處理設施被正確與安全地操作，以防止資料被未經授權的揭露、修改、移除或破壞，以及營運活動的中斷，特訂定本「通訊與操作管理程序」(以下簡稱本程序)。

貳、 適用範圍

本程序適用於本所內任何形式的資訊傳輸通訊及處理設施操作活動。

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：執行本程序相關作業。

肆、 定義

一、 資訊處理設施：係指伺服器、個人電腦、作業系統、應用系統、資料庫等。

二、 網路通訊設備：指數據機、路由器、交換器、集線器、頻寬管理

器、無線基地台等。

三、 可攜式媒體：指可隨身攜帶之儲存媒體，如隨身碟、記憶卡、外接式硬碟、磁帶、磁片、光碟片（CD/DVD）等。

四、 可攜式設備：指可隨身攜帶之設備，如筆記型電腦、平板電腦、掌上型電腦、個人數位助理(PDA)、智慧型行動電話(Smart phone)等。

五、 帳戶鎖定原則：在指定期間內鍵入了指定的錯誤密碼次數，帳戶鎖定原則就會停用使用者帳戶，以防止他人透過猜使用者密碼來進行攻擊，並降低成功攻擊網路的可能性。

六、 SSL(Secure Sockets Layer)：為網頁伺服器和瀏覽器之間以加解密方式溝通的安全技術標準，以確保所有在伺服器與瀏覽器之間通過資料的私密性與完整性。

七、 TLS(Transport Layer Security)：其前身安全通訊協定（Secure Sockets Layer，縮寫：SSL）是一種安全協定，目的是為網際網路通訊，提供安全及資料完整性保障。

八、 SSH(Secure Shell)：是一套安全的網路連線程式，可在編碼的保護下，透過網路連線至其他電腦，在其他電腦上執行程式或在電腦之間拷貝檔案。

伍、 管理項目

為確保正確與安全地操作資訊傳輸通訊及處理設施，透過資訊處理設施管理、網路通訊設備管理、可攜式設備及媒體管理、與資訊交換管理等措施，以防止資料被未經授權的揭露、修改、移除或破壞，以及營運活動的中斷，相關管理程序如下頁圖 5-1 所示。

一、 資訊處理設施管理

（一）伺服器應固定於機架上，並依「網路安全管理程序」部署安全防護工具。

（二）資訊處理設施應賦予每一使用者專用的唯一帳號，並啟用帳戶鎖定原則及暫用密碼，使用者於第一次登錄使用時，應即更改暫用密碼。

（三）帳戶鎖定原則設定如下：登入失敗最多 5 次即鎖定帳號，至少 20 分鐘後才可解除；登入 15 分鐘未動作即自動登出。

（四）使用者應依據密碼設定原則(請參照存取控制管理程序)設定密碼。

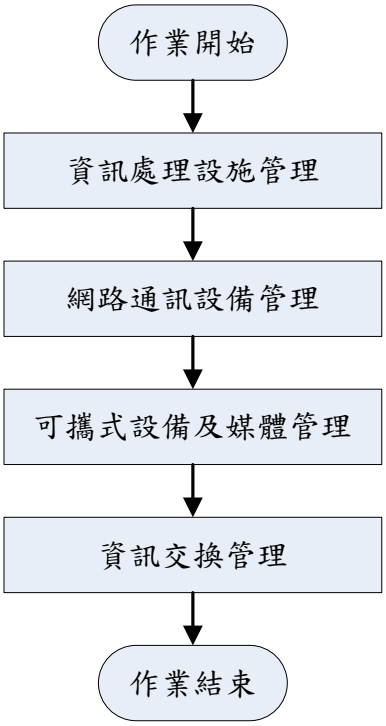

圖 5-1：通訊與操作管理程序

（五）資訊處理設施及共用資料夾應依使用者權責賦予適當的權限，如儲存之資料含有敏感資訊或重要資訊則需應用加密技術以保護資料(如使用檔案加密軟體 7-zip)。

（六）資訊處理設施應啟動螢幕保護與密碼保護機制，啟動時間不得超過

15 分鐘。

（七） 資訊系統變更及維護，依「資訊系統開發與維護管理程序」辦理。

（八） 資訊處理設施變更及維護，依「資訊系統開發與維護管理程序」辦理。

（九） 測試及正式作業應予區隔，以降低正式作業資訊系統因意外造成損害或中斷之機率。

(一〇)資訊處理設施應依「資料備份與回復管理程序」，定期執行備份與回復測試。

(一一)資訊處理設施與具有系統紀錄（log）的網路通訊設備應設定時間同步機制。

(一二)資訊處理設施之系統紀錄（log）應每週查看，如發現異常，應記錄於「主機房工作日誌」持續監控，並應執行備份。

(一三)資訊處理設施之資源使用情形，應依「主機房管理作業」規定巡查與記錄，以適時因應，確保系統效能。

(一四)資訊處理設施汰除時，其儲存媒體應依「資料備份與回復管理程序」之儲存媒體管理規定辦理。

(一五)資訊處理設施如需與外單位進行資料交換，需應用加密技術及身份識別，以保護資料安全，並應妥尚保管其金鑰及憑證。

(一六)核心系統與重要伺服器重大變更(如系統升級、韌體升級)應進行評估並留存紀錄，且保留原始環境與資料以利緊急復原。

(一七)核心系統每年應進行技術脆弱性管理，如:弱點掃描或安全測試，

高風險應予以修正處理或修補、或封閉於內部網路中。

(一八)伺服器與電腦應安裝防毒軟體，並定期更新病毒碼保持 7 天內最新之病毒碼狀態 。

二、 網路通訊設備管理

（一） 網路通訊設備安裝完成後，授權之管理人員應立即刪除系統預設帳號或修改預設密碼。

（二） 如需遠端登入網路通訊設備進行維護或系統設定變更時，除本所授權人員或經行政室同意之網路設備維護廠商外，其餘一律禁止。

（三） 除因網路通訊設備未能提供加解密功能外，應使用其加解密方式作業，以防止網路監聽竊取帳號密碼。

（四） 網路通訊設備應啟動系統紀錄（log），至少應記錄登入、登出之成功或失敗紀錄並每週查看。如發現異常，應記錄於「主機房工作日誌」持續監控，且應執行備份。

（五） 網路通訊設備之系統組態資料(Configuration)應於每次變更後進行備份。

（六） 網路通訊設備帳號及密碼須依「存取控制管理程序」進行管理。

（七） 網路通訊設備汰除時，應先清除系統組態資料(Configuration)。

三、 可攜式設備及媒體管理

（一） 欲攜入可攜式設備或媒體至主機房內使用，應先註記於「資訊服務申請表」，經核可後方得使用。

（二）可攜式設備或媒體使用前，應先離線進行掃毒，以防止病毒感染。

（三）機敏性資料如利用可攜式設備或媒體處理或儲存時，應設密碼(password)保護，並於使用完畢後立即刪除，以避免資料外洩。

（四）主機房內使用可攜式設備或媒體儲存、複製或傳遞資料時，應經主機房管理人員確認，作業結束後，應由電腦機房管理人員確認刪除。

四、 資訊交換管理

（一）若需與本所以外之機關或個人進行資訊交換，應先簽報核准後方能進行。

（二）傳遞資訊須依「資產分類與管理程序」，按資訊機密等級採取適當地安全防護措施。

（三）須告知外部機關或個人有關所交換資訊之機密等級與建議安全防護措施。

陸、 參考文件

一、 網路安全管理程序。

二、 存取控制管理程序。

三、 資訊系統開發與維護管理程序。

四、 主機房管理作業。

五、 資料備份與回復管理程序。

六、 資產分類與管理程序。

柒、 使用表單

一、　資訊服務申請表。

二、　主機房工作日誌。