雲林縣西螺鎮公所

存取控制管理程序

文件編號： XLTG-02-011

版　　次： V1.0

文件日期： 110 年 06 月 10 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)為確保資訊系統軟硬體設備之存取控制，以避免遭受未經授權之存取、破壞或竊取，特訂定本「存取控制管理程序」(以下簡稱本程序)。

貳、 適用範圍

本程序適用於本所資訊系統軟硬體設備之存取作業。

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、 機房或網路管理相關人員管控相關存取作業。

肆、 定義

一、 資訊系統：提供網路資訊作業有關的軟硬體設備，包括網路基礎設備(如網路連線設備、安全防護工具、網管軟體及伺服器等)、作業系統及應用系統等。

二、 網路存取控制：本程序中所界定之「網路存取控制」，係指對本所網路之存取行為進行控制。

三、 作業系統存取控制：本程序中所界定之「作業系統」，係指適用於電腦機房內設備所搭配、安裝之各類資訊硬體，為使用者與硬體間之界面軟體系統。例如 Windows XP、Windows 2000/2003、Linux、Unix 等。

四、 應用系統存取控制：本程序中所界定之「應用系統」，係指除了網路及作業系統外，自行開發或委外採購之應用系統。

五、 資料庫存取控制：本程序中所界定之「資料庫」，係指應用系統或設備廠商所提供之「資料庫應用系統」，如 Microsoft SQL Server、Oracle database、IBM DB2、Sybase 與 Informix 等。

六、 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。

七、 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。

八、 密碼設定原則：密碼設定不可與帳號相同，且避免使用與個人有關資料（如生日、身份證字號、單位簡稱、電話號碼等）作為通行碼，最少要有 8 個字元以上，並符合密碼複雜性原則。

九、 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

為確保資訊系統軟硬體設備之存取安全，相關維運人員應實施適當之職務區隔，將系統管理、系統操作與應用系統維護等職務由不同的人

員擔任，並就網路、作業系統、應用系統及資料庫之存取予以管控，以避免遭受未經授權之存取、破壞或竊取，相關存取控制程序如下圖 5-1 所示：

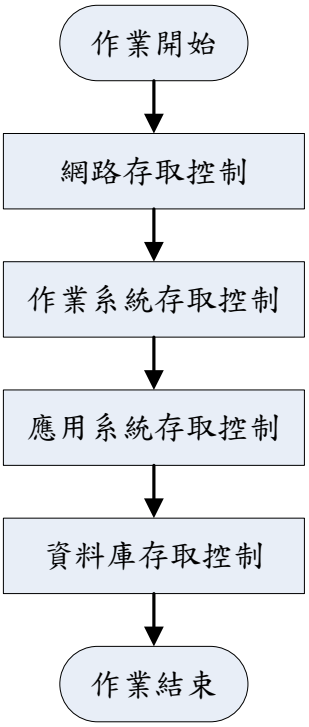

圖 5-1：存取控制管理程序

一、 網路存取控制

（一）網路設備管理

1. 網路連線設備須置於機房或安全場所，如需移動設備或更改設定時，應填寫「資訊服務申請表」，經核准後始得辦理。

（二）網路區隔

1. 機房或網路管理相關人員應於實體網路上做實體分割，可藉由路由器、防火牆等設備，連接內部使用者端網路（Internal）、外部服務伺服器區網路（DMZ）、內部服務伺服器區網路（Trusted）及網際網路（Internet）等。

2. 使用者端網路（Internal）應於網段或 V-LAN 設定上予以邏輯分割。

（三）網路連線控制

機房或網路管理相關人員應於路由器或防火牆設備上，定義以下網路區之存取規則：

1. 內部使用者端網路（Internal）對內部服務伺服器區網路（Trusted）及外部服務伺服器區網路（DMZ）之連線相關存取規則，除必要服務 Port 之外，均須予以封鎖。

2. 使用者端網路（Internal）對網際網路（Internet）之連線相關存取規則，連線需求之電腦、網段、服務等均須加以規範。

3. 外部伺服器區網路（DMZ）對網際網路（Internet）之連線相關存取規則，應僅需開啟必要服務 Port 予以連入。

4. 網路設備管理連接通訊埠限制

(1)經授權的機房或網路管理相關人員，可透過 SSH、SSL 或其他方式使用遠端管理，連接通訊埠來管理網路設備，

(2)應限制來源端連線位址。

(3)機房或網路管理相關人員應使用其個人帳號，以明責任。

（四）遠端連線申請流程

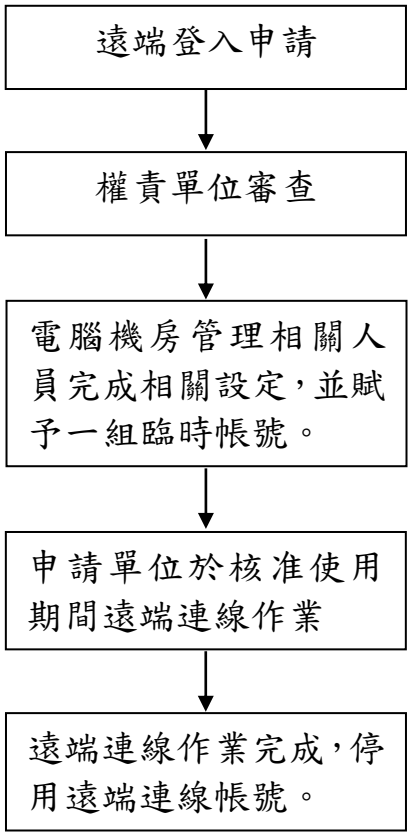

圖 5-2：遠端連線申請流程圖

二、 作業系統存取控制

（一）使用者註冊管理

1. 非授權人員如需登入伺服器進行必要作業時，應填寫「資訊服務申請表」進行註冊申請，並說明使用目的及使用起迄時間。
2. 機房或網路管理相關人員於接獲非授權人員註冊申請時，應審查其目的及申請權限是否適當。
3. 機房或網路管理相關人員同意其申請後，方可進行臨時帳號註冊

及權限配賦，並於申請期限到期時關閉該帳號。

4. 非授權人員所申請之帳號權限若屬特殊帳號權限者，須經權責單位主管同意後方可賦予。

（二）使用者密碼管理

密碼設定長度至少 8 碼以上，並符合密碼複雜度原則，每 1 年須變更一次。

（三）使用者權限定期審查

核心系統負責人每年應審查伺服器所設定之帳號權限是否適當，並留存紀錄於「資訊系統使用權限授權說明表」或其它紀錄佐證。

（四）遠距工作

使用者登入作業系統不得記憶記憶，管理人員離座時應鎖定電腦。

（五）系統公用程式使用

對於隨作業系統所附之重要公用程式，須進行以下管理：

1. 限制使用系統工具之權限。

2. 記錄系統工具的各種使用情況。

3. 考量移除非必要的公用程式及系統軟體。

（六）連線作業時間控制

1. 有高風險的應用系統，應限制使用者的連線作業時間（如限定僅能內部 IP 連線時使用，外部 IP 連線需申請核准）。

2. 對處理機密及敏感性系統的終端設備，應限定連線作業及網址連線時間，以減少未經授權存取系統的機會。

三、 應用系統存取控制

（一）資訊存取限制

應用系統之選單，應依據使用者權限的不同，只顯示有權限的選項。

（二）敏感性系統隔離

具有機密性或敏感性資料的應用系統，必要時應以網路隔離或實體隔離的方式進行區隔。

四、 資料庫存取控制

（一）資料庫系統帳號密碼管理

1. 資料庫系統管理員帳號應限制保管人數為 3 人，可依需求指定另一人為其代理人。
2. 至少每 1 年變更一次密碼(若為應用系統程式使用之密碼可不予變更)。
3. 密碼長度至少應為 8 碼。

（二）資料庫檔案之目錄存取權限

須限制對資料庫檔案所在目錄之存取，僅有資料庫管理人員、應用系統程式可進行存取。

（三）帳號管理控管

1. 在資料庫系統完成安裝作業後，應立即更改廠商預設的使用者帳號及密碼。
2. 資料庫使用帳號之申請，應填寫「資訊服務申請表」並說明原因，經權責單位主管核可後，由機房或網路管理相關人員(或其授權

人員)配賦帳號及權限。

（四） 資料庫公用程式及工具使用權限

限制僅有經授權之人員方可使用資料庫公用程式及工具。

（五） 資料庫資料表存取權限

1. 對於資料庫資料表，應限制僅有應用系統程式可進行存取。
2. 若需直接對資料庫資料表進行存取時,應填寫「資訊服務申請表」敘明原因，並取得權責單位主管之核可後，由機房或網路管理相關人員(或其授權人員)進行。

（六） 事件紀錄

應啟動資料庫系統事件記錄功能，記錄項目至少包含：

1. 登入使用者帳號。
2. 系統存取失敗之歷史紀錄。

（七） 稽核工具安全管理

未經申請核准，不得使用稽核工具（例如資料庫弱點掃描軟體或程式)，以防止被誤用。

陸、 參考文件

一、 網路安全管理程序。

二、 資產分類與管理程序

柒、 使用表單

一、 資訊服務申請表。

二、 防火牆異動說明表。

三、 遠端登入使用申請表

四、 資訊系統使用權限授權說明表