雲林縣西螺鎮公所

資產分類與管理程序

文件編號： XLTG-02-007

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)為識別資訊安全管理系統(以下簡稱 ISMS)實施範圍內相關資產，釐清資產管理方式與責任，應用資產分類、分級控管方式，以達到保護各項資產機密性、完整性與可用性的資訊安全要求，特訂定本「資產分類與管理程序」(以下簡稱本程序)。

貳、 適用範圍

本程序適用於本所 ISMS 實施範圍內與資訊業務營運相關之各項資產管理。

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，並建立及維護資產清冊。

五、 資產保管人員配合 ISMS 承辦人提供並清查相關資產資料。

六、 資產權責單位管理人員：

（一） 配合 ISMS 承辦人進行資產盤點、識別、分類及價值評估。

（二） 依據分級管制措施進行資產使用控管。

肆、 定義

一、 資產：對組織有價值的任何事物。

二、 資產的型式：依其性質不同，可區分為資訊類資產、軟體類資產、實體類資產、人員類資產、服務類資產等。

三、 資產的格式：指完成資產功能及用途所需具備的規格，如人員類之資格、技能及經驗。

四、 權責單位：指對資產具有管轄權及所有權之單位。

五、 權責單位管理人員：指對資產具有管轄權及所有權之人員，或對應聯絡之人員。

六、 保管人員：指由本所授權或委託協助資產操作或代管之人員或單位。

七、 資產價值：依資產的機密性(Confidentiality)、完整性(Integrity)、可用性(Availability)及法規/合約(Legal)遵循性等級的演算結果，用以衡量資產對業務營運的重要性。

八、 存取依賴程度：須同時考量以下 2 者：

(一)使用者於正常上班時間對資產的存取時間百分比。

(二)資產服務中斷到恢復運作之可容忍時間。

伍、 管理項目

透過對資產的識別與分類，釐清安全管理方式及責任，評估其對營運之影響程度，以決定該資產之價值，並建立資產清冊予以適當的控管，達成保護資產之機密性、完整性與可用性的資訊安全要求。相關作業流程如圖 5-1 所示。

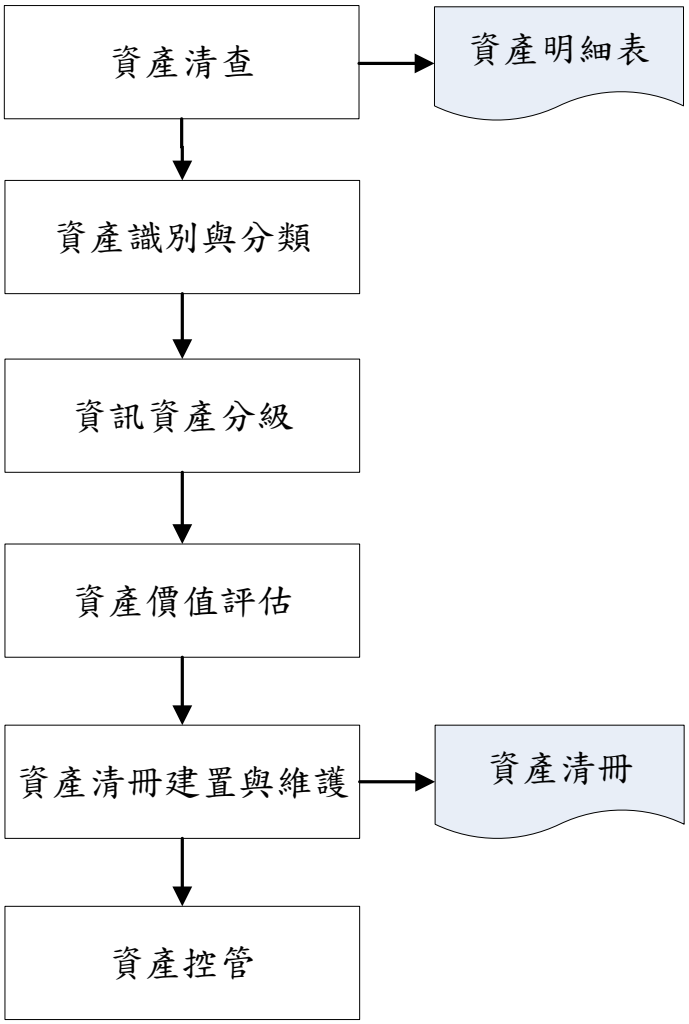

圖 5-1：資產管理流程

一、 資產清查

由 ISMS 承辦人會同各資產之保管人員，就各項資產逐一盤點，將資產名稱、功能及用途、權責單位、權責單位管理人員、識別方式或存放位置等，記錄於「資產清冊」。

二、 資產識別與分類

（一）資產識別

1. 所有資產均須界定權責單位、權責單位管理人員及保管人員。
2. 經由資產價值評估，找出涉及關鍵營運過程的所有資產，確定災害復原時所需資訊，如資產的型式、格式、位置、維護廠商、或其他相關資訊等，記錄於「資產清冊」中。
3. 可運用識別標籤、示意圖或對照表等方式，來區分資產個體、位置或性質，以利需要時能迅速找出正確之資產。

（二）資產分類

資產依其型式不同，分為五類：資訊資產、軟體資產、實體資產、人員資產及服務資產。

1. 資訊資產(Information Assets, IA)

   諸如資料庫與資料檔案、系統規劃文件、需求規格與設計文件、程式及測試相關文件、使用與操作手冊、研究資訊、契約與協議、訓練教材、制度文件、運作或支援程序、營運持續計畫、後撤（fallback)安排、稽核底搞、已歸檔資訊及各式紀錄等均屬之。

2. 軟體資產(Software Assets, SA)

   諸如各類作業系統(OS)、應用軟體、系統軟體、開發工具及公用程式等均屬之。

3. 實體資產(Hardware Assets, HW)

   包含具管轄權及所有權之實體空間、各式主機、工作站、伺服器、電腦設備、通信設備、可移除式媒體及其他設備、一般公用設施(如照明設備、電源、空調、消防設施等)等均屬之。

4. 人員資產(People Assets, PE)

包含正式人員、約聘雇人員、臨時人員、使用機關資源之委外廠商人員等均屬之，並需連帶考量人員之資格、技能及經驗。

5. 服務資產(Services Assets, SE)

具管轄權或使用權，但無所有權之設施，包含辦公室實體、數據通訊服務(電信公司)、一般公用設施(如中央空調、照明設備、電力供應及中央控制型消防設備)等均屬之。

三、 資訊資產分級

資訊資產分級分為下列三級，應隨時或定期查核，若須變更機密等級或解密者，應依規定辦理變更或解密手續。

(一) 普通等級：此資產無包含敏感且無特殊機密性要求之資訊。

(二) 限閱等級：依法令或合約有保密義務，或其外洩可能造成個人、各單位與本所困擾或有助外界取得不當利益之資產。

(三) 機密等級：凡洩露後足以使國家安全、公共利益或個人權益遭受損害資產均屬之。

四、 資產價值評估

ISMS 承辦人應會同資產保管人員或權責單位管理人員，對所有已識別之資產依照 ISO27001/CNS27001 有關資訊安全的要求及政府資訊作業安全之需求，就機密性(Confidentiality)、完整性(Integrity)、可用性(Availability)及法規/合約(Legal)遵循性等進行資產價值評估，並將評估之結果記錄於「資產清冊」中。

(一) 機密性等級(C)

參照「國家機密保護法」、行政院訂頒之「文書處理手冊」或依法令、合約等，對所持有或保管之資產有保密義務者，按其機密性需求評定價值等級，如下表 1 所示。

表 1：資產機密性價值等級評估準則

價值	等級	說　明
0	NA	資產無此特性。
1	普通	此資產無包含敏感且無特殊機密性要求之資訊。
2	限閱	依法令或合約有保密義務，或其外洩可能造成個人、單位、機關之困擾，致外界取得不當利益之資產。
3	機密	凡洩露後足以使國家安全、公共利益或個人權益遭受損害資產均屬之。

（二）完整性（I）

依據資產在運作過程中，如有未經授權的破壞或修改，對資產效能或業務所造成衝擊的影響程度，評定其完整性價值等級，如下頁表 2 所示。

表 2：資產完整性價值等級評估準則

價值	等級	說　明
0	NA	資產無此特性。
1	低	未經授權的破壞或修改不會對資訊系統造成重大影響且(或)對業務衝擊輕微。
2	中	未經授權的破壞或修改已對資訊系統造成影響且(或)對業務有明顯衝擊。
3	高	未經授權的破壞或修改對資訊系統造成重大影響且可能導致暫時性業務中斷。

（三）可用性(A)

依據合法使用者對資產的存取依賴程度，評定其可用性價值等級。評估時，須依據資產特性及所提供服務性質，同時考量使用者每日對資產的存取時間與資產之可容許中斷時間，取其大者(如下表 3 所示)。

價值	等級	說　明
0	NA	資產無此特性。
1	低	資訊資產不可用時衝擊單位同仁。
2	中	資訊資產不可用時衝擊單位跨單位同仁。
3	高	資訊資產不可用時衝擊單位全組織單位且有法律責任。

（四）法規或合約(L)遵循性

依據資產須遵循法令、法規的層級或合約要求，評定其遵循性價值等級，如下表 4 所示。

表 4：資產法規或合約遵循性價值等級評量準則

價值	等級	說　明
0	NA	無法規與合約之遵循性需求規定
1	低	一般性的合約要求及本所內部規章
2	高	行政法規要求
3	極高	國家法律層面的規範

（五）資產總價值與資產價值等級

資產總價值依據下列方式計算，資產價值等級依資產總價值區分為 5

個等級，如下表 5 所示。

資產總價值＝
機密性價值＋完整性價值＋可用性價值＋法規或合約遵循性價值

五、 資產清冊建置與維護

（一）建立資產清冊

1. ISMS 承辦人會同資產保管人員或權責單位管理人員，於完成資產識別與分類後，建立「資產清冊」。

（二）維護資產清冊

ISMS 承辦人於建立資產清冊後，應定期檢視資產與清冊之正確性，並配合資產之異動及資安風險變化情形，進行檢討調整及更新維護作業，維護時機如下：

1. 定期：每年至少進行一次資產清查作業及資產價值評估，以確認實際資產與清冊記載相符，並檢討資產總價值等級之適當性。
2. 資產異動時：資產有新增、汰除或更換時，應配合更新資產清冊。
3. 當營運環境發生變動時：如遇本所組織、業務調整或作業流程有所變更時。
4. 當資訊安全管理系統(ISMS)範圍發生變動時：本所調整 ISMS 驗證或實施範圍時。

六、 資訊資產分級管制之措施

（一）使用控管及標示

保存資訊類的資產(如:文件、隨身碟、外接硬碟)之使用控管及分級標示：

1. 普通等級

(1)無須授權，可供內、外部人員自由使用。

(2)不須標示。

2. 限閱等級

(1)限閱等級資訊資產須經承辦人或主管業務單位主管授權方可使用，未經授權者不得複製、攜出或交由其他單位或人員使用。

(2)須標示「紅色」或「密」。

3. 機密等級

(1)機密等級資訊資產須經業務單位主管、資安長或鎮長授權方可使用。

(2)須標示「黃色」或「機密」。

（二）傳遞方式

1. 書面文件或儲存媒體

(1)機密等級:須由單位主管以上長官或其指定之專人負責傳送。

(2)限閱等級：須以彌封之信封或卷宗包裹，由可信任之人員負責傳送。

(3)普通等級：以一般正常方式傳送。

2. 數位資訊之傳遞（如電子檔案、語音、文字或圖片等）

(1)傳遞機密或限閱等級之數位資訊，得以網路方式傳遞，但應予加密後再行傳送。

（三）複製

1. 屬普通等級之資訊資產，可自由進行複製。

2. 屬限閱等級之資訊資產，須經承辦人或主管業務單位主管同意後，由該業務負責人員進行複製。

3. 屬機密等級之資訊資產，須經業務單位主管核可後，指派專人進行複製。

4. 複本應依原資訊資產之機密等級進行控管。

（四）銷毀控管

1. 銷毀核准

(1)普通等級資訊資產之銷毀，由該業務承辦人員提出，報備單位主管後使得為之。

(2)屬限閱等級資訊資產之銷毀，由該業務承辦人員提出，經單位主管核准後使得為之。

(3)屬機密等級資訊資產之銷毀，由該業務承辦人員提出，經資安長以上長官核准後使得為之。

2. 銷毀處置

(1)資訊資產之銷毀，除另有規定外，應依本程序規定辦理。

(2)經核准待銷毀之資訊資產，應放置於安全場所，以避免遭未經授權之存取、揭露，並應注意運送過程之安全。

(3)資訊資產銷毀應由權責單位管理人員或保管人員會同ISMS稽核小組人員清點確認後，依下列方式進行銷毀：

A. 紙本類資訊資產以碎紙機絞碎或燒毀方式辦理。

B. 電子類資訊資產，依「備份與回復管理程序」有關儲存媒體管理規定辦理。

(4)資訊資產如遇下列緊急情況，得逕行銷毀：如遭遇戰爭、暴動或事變，為保護國家安全或本所安全而須即時銷毀者。

(5)如遇第(4)項情形發生時，處置人員應將其原因及已銷毀之資產、檔案名稱/編號、數量、銷毀時間/地點及方法詳實記錄，緊急狀況結束後陳報權責單位主管。

(6)ISMS承辦人於資產銷毀後，應釐整資產清冊，使其與現況相符。

陸、 參考文件

一、 文書處理手冊。

二、 國家機密保護法。

三、 資訊系統開發與維護管理程序。

四、 通訊與操作管理程序。

五、 存取控制管理程序。

六、 實體與環境安全管理程序。

七、 網路安全管理程序。

八、 人員安全管理程序。

九、 資訊安全組織管理程序。

十、 營運持續管理程序。

十一、資料備份與回復管理程序。

柒、 使用表單

資產清冊。