**XXXX學校**

**資訊資產管理程序書**

機密等級：一般

文件編號：**XXXX-B-003**

版 次：**1.0**

發行日期：**109.XX.XX**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **修　訂　紀　錄** | | | | |
| **版次** | **修訂日期** | **修訂頁次** | **修訂者** | **修訂內容摘要** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**目錄**

[1 目的 1](#_Toc178671756)

[2 適用範圍 1](#_Toc178671757)

[3 權責 1](#_Toc178671758)

[4 名詞定義 2](#_Toc178671759)

[5 作業說明 2](#_Toc178671760)

[6 相關文件 7](#_Toc178671761)

# 目的

建立XXXX學校（以下簡稱「本校」）資訊資產管理規範，訂定資訊資產分類、分級、價值評估、標示及處理之遵循原則，並據以辦理各項資訊資產管理及作業方法。用以保護各類資訊資產，避免因人為疏失、蓄意或自然災害等風險所造成之傷害。

# 適用範圍

本校承辦相關資訊業務作業流程之資訊資產。

# 權責

* 1. 資通安全執行祕書：

負責定期審議資訊資產清單及價值評估結果，並督導相關活動之進行。

* 1. 資通安全小組：

負責定期辦理資訊資產異動調查與彙整，提供最新之資訊資產清單，並陳報資通安全委員會。

* 1. 資訊資產權責單位：

負責所管轄內資訊資產之存取授權，並評估與審核資訊資產分類分級及價值之結果，得另指定資訊資產保管單位。

* 1. 資訊資產保管單位：

對於指定資訊資產，具有落實資訊資產權責單位所委託之保護管理責任。

* 1. 資訊資產使用單位：

對於資訊資產之使用，必須依據權責單位要求，並具有正確使用操作之責任。

# 名詞定義

* 1. 機密性（Confidentiality）  
     確保只有經授權的人，才可以存取資訊。
  2. 完整性（Integrity）  
     確保資訊與處理方法的正確性與完整性。
  3. 可用性（Availability）  
     確保經授權的使用者在需要時可以取得資訊及相關資產。
  4. 資訊資產權責單位  
     對該項資訊資產具有判斷資產價值、決定存取權限或新增、刪除、修改權限之單位，同時也是資訊資產的擁有單位。
  5. 資訊資產保管單位：  
     依據權責單位之需求標準，執行資訊資產日常保護、異動與維護之執行單位。
  6. 資訊資產使用單位：  
     因業務需求，經授權可直接或間接使用該資訊資產之單位。

# 作業說明

* 1. 資訊資產鑑別
     1. 各資訊資產權責單位應鑑別所管轄之資訊資產，並建立「資訊資產清單」。
     2. 各資訊資產權責單位應定期更新與維護所管轄之資訊資產清單。
     3. 資訊資產清單由各權責單位提供，資通安全小組負責彙整，並陳報至資通安全委員會，以確保資訊資產編號及清單之完整性。
  2. 資訊資產分類
     1. 資訊資產依其性質不同，分為7類：人員、文件、軟體、通訊、硬體、資料、環境。
        1. 人員（People / PE）：包含全體同仁，以及委外廠商。
        2. 文件（Document / DC）：以紙本形式存在之文書資料、報表等相關資訊，包含公文、列印之報表、表單、計畫等紙本文件。
        3. 軟體（Software / SW）：作業系統、應用系統程式、套裝軟體等，包含原始程式碼、應用程式執行碼、資料庫等。
        4. 通訊（Communication / CM）：網路設備、網路安全設備、提供資訊傳輸、交換之線路或服務。
        5. 硬體（Hardware / HW）：主機設備等相關硬體設施。
        6. 資料（Data / DA）：儲存於硬碟、磁帶、光碟等儲存媒介之數位資訊。
        7. 環境（Environment / EV）：相關基礎設施及服務，包含辦公室實體、實體機房、電力、消防設施等。
     2. 各類資訊資產機密等級分為4級：一般、限閱、敏感、機密。各等級之評估標準如下：
        1. 一般：無特殊之機密性要求，可對外公開之資訊。
        2. 限閱：僅供組織內部人員或被授權之單位及人員使用。
        3. 敏感：僅供組織內部相關業務承辦人員及其主管，或被授權之單位及人員使用。
        4. 機密：為組織、主管機關或法律所規範之機密資訊。
     3. 資訊資產之機密等級應定期審核，視實際需要予以調整。
     4. 不同等級之資訊資產合併使用或處理時，以其中最高之等級為機密等級。
  3. 資訊資產價值鑑別
     1. 資訊資產權責單位應鑑別其所管轄內所有資訊資產之價值。
     2. 資訊資產價值除考量資訊資產機密等級之外，尚需考量資訊資產之可用性及完整性，其評估標準如下：
        1. 機密性評估標準

|  |  |
| --- | --- |
| 評估標準 | 數值 |
| 此資訊資產無特殊之機密性要求 | 1 |
| 此資訊資產僅供組織內部人員或被授權之單位及人員使用 | 2 |
| 此資訊資產僅供組織內部相關業務承辦人員及其主管，或被授權之單位及人員使用 | 3 |
| 此資訊資產所包含資訊為組織或法律所規範的機密資訊 | 4 |

* + - 1. 完整性評估標準

|  |  |
| --- | --- |
| 評估標準 | 數值 |
| 該資訊資產本身完整性要求極低 | 1 |
| 該資訊資產本身具有完整性要求，當完整性遭受破壞時，不會對組織造成傷害 | 2 |
| 該資訊資產具有完整性要求，當完整性遭受破壞時會對組織造成傷害，但不至於太嚴重 | 3 |
| 該資訊資產具有完整性要求，當完整性遭受破壞時會對組織造成傷害，甚至造成業務終止 | 4 |

* + - 1. 可用性評估標準

|  |  |
| --- | --- |
| 評估標準 | 數值 |
| 該資訊資產可容許失效3工作天以上 | 1 |
| 該資訊資產可容許失效8工作小時以上，3工作天以下 | 2 |
| 該資訊資產僅容許失效4工作小時以上，8工作小時以下 | 3 |
| 該資訊資產僅容許失效4工作小時以下 | 4 |

* + - 1. 資訊資產價值之決定將依據資訊資產之機密性、完整性及可用性評估之後，取3者之最大值以為資訊資產之價值。
  1. 資訊資產清單及價值確認
     1. 資訊資產權責單位應依據資訊資產清單之機密性、可用性及完整性之評估標準，確認資產價值。
     2. 資訊資產清單及價值評估結果，應陳報至資通安全委員會審議。
  2. 資訊資產編號及標示
     1. 除「資通安全管理制度文件」外的資訊資產編碼方式，第1~3碼為權責單位別，第4~5碼為資產類別，第6~8碼為資訊資產流水編號。



* + 1. 已列入機密等級分類的資訊資產，應明確標示其機密等級，避免其機密性遭破壞。
    2. 實體設備之重要等級標示方式：
       1. 實體設備之重要等級應以不同顏色標籤區分（資產價值2為綠色標籤，資產價值3為黃色標籤，資產價值4為藍色標籤）。
       2. 文件之機密等級應於文件封面做明確的標示。系統輸出機密等級為敏感以上的報表，如系統未自動標示，則由資訊資產權責單位做額外的明顯註記。
  1. 資訊資產管理作業
     1. 有關文件、紀錄、相關電子檔及儲存媒體控管原則及方式，請參閱「文件管理程序書」。
     2. 有關人員之控管原則及方式，請參閱「人員安全與教育訓練程序書」。
     3. 有關實體資產，包括：軟體、硬體、通訊及環境等之控管原則及方式，請參閱「實體安全管理程序書」。
     4. 資訊資產異動管理，如：新增、刪除、修改等控管原則，請參閱「資訊資產異動作業說明書」。
  2. 覆核
     1. 權責單位每年至少進行1次資產盤點與資訊資產清單覆核，以更新及確保資訊資產清單的正確性及完整性。
     2. 當範圍內有以下的狀況發生時，則實施不定期的覆核，以更新及確保資訊資產清單的正確性及完整性。
        1. 有新增、變更或移除資訊資產。
        2. 系統有重大異動。
        3. 作業環境改變。
  3. 資訊資產之報廢

資訊資產之報廢（或銷毀）應依「資訊資產異動作業說明書」之相關規定，採取適當之方式進行銷毀。

* 1. 資訊資產之處理規範
     1. 針對價值3或4之資訊資產，應加強安全保護及存取控制管控措施，以防止洩漏或不法及不當的使用。
     2. 價值3或4文件類資訊資產之安全處理應符合以下作業要求：
        1. 紙類文件不再使用時，應銷毀處理。
        2. 系統流程、作業流程、資料結構及授權程序等系統相關文件，應予適當保護，以防止不當利用。
        3. 系統文件應指定專人管理，並鎖在安全的儲櫃或其他安全場所，且發送對象應以最低必要的人員為限。
        4. 電腦產製的文件，應與其應用檔案分開存放，且應建立適當的存取保護措施。
     3. 價值3或4軟體類資訊資產之安全處理作業，請參閱「存取控制管理程序書」及「系統獲取、開發及維護管理程序書」之相關程序。
     4. 價值3或4硬體類資訊資產之安全處理作業，請參閱「實體安全管理程序書」中重要設備之相關程序。
     5. 應定期檢討價值3或4之資訊資產清單內容，以確保重要資產受到適當的安全保護。
  2. 實體媒體傳送  
     實體媒體傳送之管理原則及方式依據「可攜式設備與儲存媒體管理使用作業要點」。

# 相關文件

* 1. 文件管理程序書
  2. 人力資源安全管理程序書
  3. 存取控制管理程序書
  4. 系統獲取、開發及維護管理程序書
  5. 實體安全管理程序書
  6. 資訊資產異動作業說明書
  7. 資訊資產清單
  8. 可攜式設備與儲存媒體管理使用作業要點