



文件編號	ISMS-P-003	文件名稱	資訊資產管理程序書		
機密等級	內部使用	版 次	A	頁次	1 / 15

管理系統文件

文件類別	第二階文件	
文件編號	ISMS-P-003	
文件名稱	資訊資產管理程序書	
發行單位	文件管制小組	
發行日期	104年07月06日	
版 次	A	
訂修廢單位	審 查	核 准
資通安全處理小組	資訊網路中心 中心主任 陳君毓	行政副校長 翁順祥

(原版簽名頁保存於文件管制小組)



文件編號	ISMS-P-003	文件名稱	資訊資產管理程序書		
機密等級	內部使用	版 次	A	頁次	3 / 15

1. 目的

為促使本校各項資訊資產之分類、分級、評價、標示及處理之管理有一明確規範，確保執行各項資訊資產管理之作業均能滿足本校之需求，避免因人為疏忽、蓄意或自然災害等風險所造成之傷害，特制定本程式書。

2. 適用範圍

凡本校各項資訊資產之管理，均適用本程序書。

3. 參考文件

3.1. 中華民國國家標準 CNS 27001 資訊安全管理系統—控制要項。

3.2. ISMS-P-001 文件與紀錄管理程序書。

3.3. ISMS-P-010 人力資源安全管理程序書。

3.4. ISMS-P-011 實體與環境安全管理程序書。

4. 名詞定義

4.1. 資訊資產管理單位

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，以及執行資訊資產日常保護、異動與維護之作業，同時也是資訊資產的擁有單位。

4.2. 資訊資產使用單位

以實際或邏輯方式使用該項資訊資產之人員，對於被授權使用資產之單位或人員，應依各項安全程序正確使用操作資產。

4.3. 資產價值（資產鑑價 C、I、A）

4.3.1. 機密性（Confidentiality，簡稱 C）：

確保只有經過授權的人才能存取資訊（使資訊不可用或不揭露給未經授權之個人、個體或過程的性質）。

4.3.2. 完整性（Integrity，簡稱 I）：

保護資訊及其處理方法的準確性（accuracy）和完整性（completeness）的性質。

4.3.3. 可用性（Availability，簡稱 A）：



文件編號	ISMS-P-003	文件名稱	資訊資產管理程序書		
機密等級	內部使用	版次	A	頁次	4 / 15

確保經授權的使用者，在需要時可以隨時存取資訊並使用相關資訊資產。

5. 作業內容

5.1. 資訊資產管理流程圖

作業流程	權責單位	相關表單
資訊資產驗收	權責單位	
↓		
資訊資產鑑別	資訊資產管理單位 資通安全處理小組 資通安全管理委員會	資訊資產清冊
↓		
資訊資產分類 分級	資訊資產管理單位	資訊資產清冊
↓		
資訊資產價值鑑別	資訊資產管理單位	資訊資產清冊
↓		
資訊資產清單及 價值確認	資訊資產管理單位 資通安全管理委員會	資訊資產清冊
↓		
資訊資產編號 及標示	資訊資產管理單位	資訊資產清冊
↓		
資訊資產管理作業	各需求單位 資訊資產管理單位	資訊資產清冊
↓		
覆核	資訊資產管理單位	資訊資產清冊
↓		
紀錄保存	相關業務承辦人員	資訊資產清冊



文件編號	ISMS-P-003	文件名稱	資訊資產管理程序書		
機密等級	內部使用	版 次	A	頁次	5 / 15

5.2. 資訊資產驗收

各項資訊資產之驗收，由權責單位依據本校相關之驗收程序辦理驗收作業。

5.3. 資訊資產鑑別

5.3.1. 各項資訊資產之管理單位應鑑別所管轄之資訊資產，並建立「ISMS-P-003-01 資訊資產清冊」。

5.3.2. 各項資訊資產管理單位應定期更新與維護所管轄之「ISMS-P-003-01 資訊資產清冊」。

5.3.3. 資訊資產清單由各資訊資產管理單位提供，「資通安全處理小組」負責彙整，並陳報至「資通安全管理委員會」統一控管，以確保資訊資產編號及清單之完整性。

5.4. 資訊資產分類與分級

5.4.1. 資訊資產分類

依資訊資產之價值、對組織運作的關鍵程度或依其可用性和完整性進行分類。資訊資產分為五大類，分別為：人員類、資訊類、硬體類、軟體類、環境保護類，各分類說明如下：

大分類	小分類	範例
人員類 (People / PE)	編制內人員	正式編制人員、臨時人員、工讀生、專案人員、委外承包廠商.....等。
	臨時鐘點人員	
	廠商駐點人員	
	委外廠商	
資訊類 (Information / IF)	作業文件	資料庫與資料檔案、備份資料、原始程式碼、網路架構圖、系統文件、操作或支援程序、使用手冊、教育訓練教材、管理制度文件、緊急應變&復原計畫、營運持續計畫 (BCP)、稽核日誌、合約與協議、報表、表單記錄.....等。
	系統文件	
	合約	
	資訊紀錄 (電子/紙本)	
	系統紀錄 (Log)	
硬體類 (Hardware / HW)	個人電腦	一般硬體：包含電腦設備(伺服器、筆記型電腦、個人電腦、工作站)、
	可攜式電腦	



美 和 科 技 大 學

M e i h o U n i v e r s i t y

文件編號	ISMS-P-003	文件名稱	資訊資產管理程序書		
機密等級	內部使用	版 次	A	頁次	6 / 15

	伺服器	CD/DVD 燒錄器、CD/DVD 光碟機、磁帶機、軟碟機、投影機、PDA、印表機.....等。 通訊設備：集線器、橋接器、網路交換器、路由器、數據機、電話自動交換機 (PBX)、網路纜線、防火牆、入侵偵測系統、視訊會議設備、傳真機、手機。 儲存媒體：CD/DVD (空白)、硬碟 (無資料)、磁片 (空白)、磁帶 (空白)、移動式硬碟 (空白)、錄音/影帶 (無資料)等。
	資安設備	
	網路設備	
	可攜式儲存媒體	
	電腦保護設施	
	其他硬體	
軟體類 (Software / SW)	作業系統	應用系統軟體、作業系統軟體、開發工具、套裝軟體、公用程式、防火牆軟體、防毒軟體、驗證軟體、資料庫管理系統 (DBMS)、加密軟體、文件管理系統、內部開發程式、內部發展系統.....等。
	應用系統	
	套裝軟體	
	軟體開發工具	
	資訊安全系統	
環境保護類 (Environment / EV)	一般辦公區域	建築類：電腦機房、會議室、辦公室、監控室、接待區、交貨區/裝載區.....等。 環境保護設施：不斷電系統、第二電力供應迴路、穩壓器、機櫃、避雷裝置、警報系統、備用發電系統、環境控制系統 (火偵測、熱偵測、水偵測、溫濕度偵測、自動消防滅火系統)等。
	特殊辦公區域	
	電腦機房	
	倉庫/庫房	
	建築保護設施	



文件編號	ISMS-P-003	文件名稱	資訊資產管理程序書		
機密等級	內部使用	版 次	A	頁次	7 / 15

5.4.2. 資訊資產分級

依資訊之特性與實際需要進行資訊資產安全分級。各類資訊資產之機密等級區分為3級，分別為：一般、內部使用、機敏。

各分級之評估標準如下：

分級	評估標準說明
機敏	<ul style="list-style-type: none"> ▪ 含敏感資訊，僅提供少數相關業務承辦人員及其主管，或被授權之單位及人員使用。 ▪ 資訊資產若洩漏，會影響本校聲譽及員工與客戶之權益。組織需採取補救措施。 ▪ 資訊資產存取權限須經由高階主管核准同意。
內部使用	<ul style="list-style-type: none"> ▪ 含部分敏感資訊，僅供組織內部人員或被授權之外部單位使用。 ▪ 資訊資產若洩漏，會對本校造成有形或無形的損害，此損害為組織可承受之範圍。 ▪ 資訊資產存取權限須經由單位權責主管核准同意。
一般	<ul style="list-style-type: none"> ▪ 為一般性資料可對外公開，但須遵守相關發布流程。 ▪ 若流傳至組織外部，不會對組織造成任何有形或無形的傷害。 ▪ 資訊資產存取權限只須經由資訊資產使用者同意。

5.4.2.1. 資訊資產之機密等級應定期審核，視實際需要予以調整及修正，以符合本校需求。

5.4.2.2. 不同等級之資訊資產合併使用或處理時，應以其中最高之等級為其機密等級。

5.5. 資訊資產價值鑑別

5.5.1. 資訊資產管理單位應鑑別其所管轄內所有資訊資產之價值。

5.5.2. 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。

5.5.3. 資訊資產價值評估標準

依資訊資產之特性，分成人員與非人員（含硬體、軟體、資訊及環境保護類）兩大類，其各所對應之機密性、完整性及可用性之



文件編號	ISMS-P-003	文件名稱	資訊資產管理程序書		
機密等級	內部使用	版次	A	頁次	8 / 15

定義與價值評估標準說明如下：

5.5.3.1. 人員類資產

5.5.3.1.1. 機密性評估

著重於保護資產，確保只有獲得授權的人才能存取該資產。

等級	量化值	內容說明
高	3	其工作執掌可存取限定資料(含機敏、內部使用及一般等三類)。
中	2	其工作執掌可存取「內部使用類」資料及「一般類」資料。
低	1	其工作執掌僅可存取「一般類」資料。

5.5.3.1.2. 完整性評估

著重於確保資料的正確性及資產(作業)處理的完整性，以避免因運用錯誤的資料或因資產處理的不完全，而造成對組織的衝擊。

等級	量化值	內容說明
高	3	<ul style="list-style-type: none"> ▪ 未正確執行業務而造成資料不完整，會對業務造成很大的衝擊，甚至造成業務中斷失敗。 ▪ 可能影響全組織對外所提供的服務作業。
中	2	<ul style="list-style-type: none"> ▪ 未正確執行業務而造成資料不完整，可能對業務運作不造成中斷，但降低運作效率及影響。 ▪ 可能影響單一部門運作。
低	1	<ul style="list-style-type: none"> ▪ 未正確執行業務而造成資料不完整，可能對業務運作不會造成中斷或雖降低效率但不會造成影響。 ▪ 僅僅影響少數承辦人的作業。

5.5.3.1.3. 可用性評估

確保資產提供使用者所需的服務，以達成預期之功能，主要為避免因災害而致使組織無法持續運作或提供服務之衝擊。



文件編號	ISMS-P-003	文件名稱	資訊資產管理程序書		
機密等級	內部使用	版 次	A	頁次	9 / 15

等 級	量化值	內 容 說 明
高	3	<ul style="list-style-type: none"> ■ 欲維持業務正常運作，在該等人員無法持續提供服務時，可容忍替換時間為 4 小時。 ■ 業務高度仰賴該員，且一旦該員無法作業時，將影響本校對外所提供的服務作業。
中	2	<ul style="list-style-type: none"> ■ 欲維持業務正常運作，在該等人員無法持續提供服務時，可容忍替換時間為 12 小時以內。 ■ 業務仰賴該員，且一旦該員無法作業時，將影響本校多數部門作業。
低	1	<ul style="list-style-type: none"> ■ 欲維持業務正常運作，在該等人員無法持續提供服務時，可容忍替換時間為 24 小時以上。 ■ 業務仰賴該員，且一旦該員無法作業時只影響少數承辦人員作業，其工作可暫時委由他人替代。

5.5.3.2. 非人員類資產

5.5.3.2.1. 資產機密性評估

A. 評估資產機密性時，應依據該資產現有之機密等級為考量基礎，依 1 至 3 量化等級評估適當數值。

B. 評鑑者：各資產管理單位。

C. 量化標準

等 級	量化值	內 容 說 明
高	3	<ul style="list-style-type: none"> ■ 敏感性資訊處理設施與系統資源，僅開放給必要知道的人使用。 ■ 資料內容若洩漏會影響本校聲譽及員工權益。



文件編號	ISMS-P-003	文件名稱	資訊資產管理程序書		
機密等級	內部使用	版 次	A	頁次	10 / 15

中	2	<ul style="list-style-type: none"> 非公開使用之非敏感性資訊處理設施與系統資源僅開放給內部人員使用。 資料內容若洩漏會對本校造成有形或無形的損害，此損害為組織可承受之範圍（註1）。
低	1	<ul style="list-style-type: none"> 不限制使用資訊處理設施與系統資源等。 資料內容若流傳至組織以外，不會對本校造成任何有形或無形的傷害（註1）。
<p>註1： 有形的傷害如：財務上的賠償、主管機關的懲處； 無形的傷害如：形象上的受損、組織內部員工士氣的低落。</p>		

5.5.3.2.2. 資產完整性評估

- A. 評估資產完整性時，應依據該資產可允許產生之誤差程度為考量基礎，依1至3量化等級評估適當數值。
- B. 評鑑者：各資產管理單位。
- C. 量化標準

等 級	量化值	內 容 說 明
高	3	<ul style="list-style-type: none"> 不當的損失、破壞資訊處理設施與系統資源，會對業務應用造成顯著的衝擊。 資訊系統服務若不完整，將導致本校作業受影響。
中	2	<ul style="list-style-type: none"> 不當的損失、破壞資訊處理設施與系統資源，會對業務應用造成輕微的衝擊。 資訊系統服務若不完整，將造成單一部門作業受影響。
低	1	<ul style="list-style-type: none"> 不當的破壞或竄改資訊、資訊處理設施與系統資源，所造成的業務衝擊可以忽略者。 資訊系統服務若不完整，將造成少數或個別承辦人作業受影響。



文件編號	ISMS-P-003	文件名稱	資訊資產管理程序書		
機密等級	內部使用	版 次	A	頁次	11 / 15

5.5.3.2.3. 資產可用性評估

- A. 評估資產可用性時，應依據該資產可允許停用時間為考量基礎，依 1 至 3 量化等級評估適當數值。
- B. 評鑑者：各資產管理單位。
- C. 量化標準

等 級	量化值	內 容 說 明
高	3	<ul style="list-style-type: none"> ▪ 僅容許短暫時間（4 小時內）無法使用，作業停頓期間極易產生客訴事件，使本校受到損害者。 ▪ 作業完全仰賴資訊資產，且一旦服務中斷時將影響全組織對外所提供的服務作業。
中	2	<ul style="list-style-type: none"> ▪ 容許較長時間（8 小時內）無法使用，會造成部份人員之抱怨，使本校受到輕微損害者。 ▪ 作業仰賴資訊資產，且一旦服務中斷時將影響部門運作。
低	1	<ul style="list-style-type: none"> ▪ 容許長時間（1 天以上）無法使用，作業停頓期間可利用其他替代方案，不致造成本校之損失。 ▪ 作業仰賴資訊資產，且一旦服務中斷時將影響少數承辦人作業。

5.5.4. 資訊資產價值（重要性）之評估

依據 5.5.3 資訊資產價值評估標準，找出資訊資產之機密性（C）、完整性（I）及可用性（A）三者所對應之量化值，再各別將三者相加即為其資訊資產價值（P）。

資訊資產價值（P）= 機密性（C）+ 完整性（I）+ 可用性（A）。

5.6. 資訊資產清單及價值確認

- 5.6.1. 資訊資產管理單位應依據「ISMS-P-003-01 資訊資產清冊」之機密性、可用性、完整性之評估標準，確認資產價值。



文件編號	ISMS-P-003	文件名稱	資訊資產管理程序書		
機密等級	內部使用	版 次	A	頁次	12 / 15

5.6.2. 「ISMS-P-003-01 資訊資產清冊」及價值評估結果，應陳報至「資通安全管理委員會」審議。

5.7. 資訊資產編號及標示

5.7.1. 資訊資產編號

5.7.1.1. 管理制度文件之編碼原則，應依「ISMS-P-001 文件與紀錄管理程序書」之規定辦理

5.7.1.2. 硬體類之資訊資產則依本校財產編號標籤原則辦理，並於明顯處貼上財產標籤及保管單位。

5.7.2. 資訊資產標示

依據本校採用之分類方法，應明確給予各類資訊資產適當之標示（包含：紙本形式及電子形式之資訊）。

5.7.2.1. 硬體類資產機密等級之標示方式

5.7.2.1.1. 機密等級屬「機敏」之實體設備，則黏貼「紅色」標籤進行區分。

5.7.2.1.2. 機密等級屬「一般」或「內部使用」之實體設備，則不黏貼標籤以簡化管理作業。

5.7.2.2. 資訊類資產機密等級之標示方式

5.7.2.2.1. 本校管理制度之各項管理文件，可於文件之封面、內頁的頁首或頁尾上、或是適當之處，標註其機密等級。

5.7.2.2.2. 紙本形式的資訊文件，則由資產管理單位依資料屬性，在明顯處列印或蓋上其所屬機密等級之字樣。

5.7.2.2.3. 電子形式的資訊文件，則由資產管理單位依資料屬性，在明顯處標註其所屬機密等級之字樣。

5.7.2.2.4. 機密等級屬「一般」之資訊資產可無需標示，以便簡化管理作業。

5.7.2.3. 人員、軟體與環境保護類資訊資產之機密等級，應以資訊資產價值之機密性（C）識別於「ISMS-P-003-01 資訊資產清



文件編號	ISMS-P-003	文件名稱	資訊資產管理程序書		
機密等級	內部使用	版 次	A	頁次	13 / 15

冊」。

5.8. 資訊資產管理作業

5.8.1. 文件、紀錄、相關電子檔及儲存媒體

5.8.1.1. 控管原則及方式，應依「ISMS-P-001 文件與紀錄管理程序書」之規定辦理。

5.8.1.2. 各單位若因業務需求，須向權責單位調閱非權限範圍內之機密資料時，須經權責單位主管核准後，由系統或報表負責人，以報表原稿複印或由系統直接列印，並依文件/報表原本或系統之機密等級，於報表頁尾註明其機密等級，以便使用者依據對應之控制措施使用。

5.8.2. 人員之控管原則及方式，應依「ISMS-P-010 人力資源安全管理程序書」之規定辦理。

5.8.3. 實體資產（包括：軟體、硬體、環境保護等）控管原則及方式，應依「ISMS-P-011 實體與環境安全管理程序書」之規定辦理。

5.8.4. 資訊資產異動

5.8.4.1. 資訊資產項目或相關管理項目異動時，須立即更新及調整「ISMS-P-003-01 資訊資產清冊」，以確保資產清冊之正確性與完整性。

5.8.5. 資訊資產使用與管理

資訊資產管理者應依據資訊資產之機密等級，建立資訊資產適當的使用與處理作業規範，包括資訊的複製、儲存、傳輸、報廢等資訊作業活動，如下說明：

等級 使用	機敏	內部使用	一般
控制要點	<ul style="list-style-type: none"> 須經過授權及遵從保密協議並符合本校相關標準作業程式 (SOP) 之規範。 	<ul style="list-style-type: none"> 須經過授權及遵從保密協議。 	<ul style="list-style-type: none"> 可開放予所有有需求的同仁或一般大眾。



文件編號	ISMS-P-003	文件名稱	資訊資產管理程序書		
機密等級	內部使用	版次	A	頁次	14 / 15

校外分送	<ul style="list-style-type: none"> ▪ 檔案透過公開的通訊環境（如 Internet）傳送時需加密碼管制。 ▪ 需經權責主管核准後方可攜出。 ▪ 對外分送時，請選擇以下方式進行： <ol style="list-style-type: none"> 1.以掛號傳遞。 2.專人負責傳送。 3.利用本校電子郵件或透過檔案傳送系統傳遞。 	<ul style="list-style-type: none"> ▪ 需經資訊資產管理者同意後方可攜出。 ▪ 對外分送時，請選擇以下方式進行： <ol style="list-style-type: none"> 1.以掛號傳遞。 2.專人負責傳送。 3.利用本校電子郵件或透過檔案傳送系統傳遞。 	<ul style="list-style-type: none"> ▪ 任何適用之方式。
校內分送	<ul style="list-style-type: none"> ▪ 若為電子形式需加以密碼進行保護。 ▪ 內部分送時，請選擇以下方式進行： <ol style="list-style-type: none"> 1.文件以密封信封袋或紅色卷宗傳遞。 2.專人負責傳送。 3.以本校電子郵件及檔案傳送系統傳遞。 	<ul style="list-style-type: none"> ▪ 內部分送時，請選擇以下方式進行： <ol style="list-style-type: none"> 1.文件以卷宗傳遞。 2.專人負責傳送。 3.以本校電子郵件及檔案傳送系統傳遞。 	<ul style="list-style-type: none"> ▪ 任何適用之方式。
複製	<ul style="list-style-type: none"> ▪ 需經授權核可後方可複製。 ▪ 若為電子形式資料應設密碼保護並將備份妥善保存。 	<ul style="list-style-type: none"> ▪ 需經授權後方可複製。 ▪ 若為電子形式應將備份妥善保存。 	<ul style="list-style-type: none"> ▪ 任何適用之方式。
保存/移轉	<ul style="list-style-type: none"> ▪ 文件資產不用時應鎖在保管櫃或相關被認可安全的管制區域。 ▪ 電子檔應設存取控制，只開放給特定使用者。 ▪ 儲存在個人電腦或工作站的資料需設密碼保護。 	<ul style="list-style-type: none"> ▪ 文件類需置於安全儲櫃或抽屜。 	<ul style="list-style-type: none"> ▪ 無特定需求。
註銷/收回/銷毀	<ul style="list-style-type: none"> ▪ 文件須以碎紙機銷毀。 ▪ 儲存媒體需低階格式化或以亂數資料於覆蓋後，再實體銷毀或與合格的銷毀廢棄廠商簽約處理。 	<ul style="list-style-type: none"> ▪ 依一般程序銷毀。 ▪ 儲存媒體需低階格式化。 	<ul style="list-style-type: none"> ▪ 依一般程序銷毀。

5.9. 覆核

5.9.1. 管理單位每年至少進行 1 次資產盤點作業，並適時更新「ISMS-P-003-01 資訊資產清冊」內容，經權責主管覆核，以確保「ISMS-P-003-01 資訊資產清冊」之正確性及完整性。



文件編號	ISMS-P-003	文件名稱	資訊資產管理程序書		
機密等級	內部使用	版次	A	頁次	15 / 15

5.9.2. 當範圍內有以下的狀況發生時，則實施不定期更新及覆核，以確保「ISMS-P-003-01 資訊資產清冊」之正確性及完整性。

5.9.2.1. 有新增、變更或移除資訊資產。

5.9.2.2. 資訊系統有重大異動。

5.9.2.3. 作業環境調整或改變。

5.10. 紀錄保存

相關業務承辦人員應參照如下規範，妥善保存各項紀錄。

編號	表單名稱	保存地點	保存期限
1	資訊資產清冊	資網中心	至少 1 年

6. 附件

6.1. ISMS-P-003-01 資訊資產清冊。