

資通資產管理					
文件編號	HGSH-ISMS-B-002	機密等級	一般	版次	1.2

1 目的

建立國立新竹女子高級中學（以下簡稱本校）資通資產管理，訂定資通資產分類、分級、價值評估、標示及處理之遵循原則，並據以辦理各項資通資產管理作業，避免因人為疏失、蓄意或自然災害等風險所造成之傷害。

2 適用範圍

本校承辦相關資訊業務作業流程之資通資產。

3 權責

- 3.1 資通安全執行秘書（資通安全官）：負責定期審議「資通資產盤點表」及價值評估結果，並督導相關活動之進行。
- 3.2 資通安全小組：負責定期辦理資通資產異動調查與彙整，提供最新之「資通資產盤點表」，並呈報資通安全委員會。
- 3.3 資通資產權責單位：負責所管轄內資通資產之存取授權，並評估與審核資通資產分類分級及價值之結果，得另指定資通資產保管單位。
- 3.4 資通資產保管單位：對於指定資通資產，具有落實資通資產權責單位所委託之保護管理責任。
- 3.5 資通資產使用單位：對於資通資產之使用，必須依據權責單位要求，並具有正確使用操作之責任。

4 名詞定義

- 4.1 機密性（Confidentiality）：確保只有經授權的人，才可以存取資訊。
- 4.2 完整性（Integrity）：確保資訊與處理方法的正確性與完整性。
- 4.3 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。

資通資產管理					
文件編號	HGSH-ISMS-B-002	機密等級	一般	版次	1.2

4.4 資通資產權責單位：對該項資通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，同時也是資通資產的擁有單位。

4.5 資通資產保管單位：依據權責單位之需求標準，執行資通資產日常保護、異動與維護之執行單位。

4.6 資通資產使用單位：因業務需求，經授權可直接或間接使用該資通資產之單位。

5 作業說明

5.1 資通資產鑑別

5.1.1 各資通資產權責單位應鑑別所管轄之資通資產，並建立「資通資產盤點表」。

5.1.2 各資通資產權責單位應定期更新與維護所管轄之資通資產盤點表。

5.1.3 資通資產盤點表由各權責單位提供，資通安全小組負責彙整，並陳報至資通安全委員會，以確保資通資產編號及清單之完整性。

5.2 資通資產分類

5.2.1 資通資產依其性質不同，分為 7 類：人員、文件、軟體、通訊、硬體、資料、環境。

5.2.1.1 人員 (People/PE)：包含全體同仁，以及委外廠商。

5.2.1.2 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。

5.2.1.3 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。

5.2.1.4 通訊 (Communication/CM)：網通設備、WiFi AP、網路電話、網路安全設備、提供資訊傳輸、交換之線路或服務。

5.2.1.5 硬體 (Hardware/HW)：主機設備等相關硬體設施，如印表機、電子看板、儲存設備。

資通資產管理					
文件編號	HGSH-ISMS-B-002	機密等級	一般	版次	1.2

5.2.1.6 資料 (Data/DA)：儲存於硬碟、磁帶、光碟等儲存媒介之數位資訊。

5.2.1.7 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、網路攝影機、門禁系統等。

5.2.2 各類資通資產機密等級分為 4 級：一般、限閱、敏感、機密。各等級之評估標準如下：

5.2.2.1 一般：無特殊之機密性要求，可對外公開之資訊。

5.2.2.2 限閱：僅供組織內部人員或被授權之單位及人員使用。

5.2.2.3 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。

5.2.2.4 機密：為組織、主管機關或法律所規範之機密資訊。

5.2.3 資通資產之機密等級應定期審核，視實際需要予以調整。

5.2.4 不同等級之資通資產合併使用或處理時，以其中最高之等級為機密等級。

資通資產管理					
文件編號	HGSH-ISMS-B-002	機密等級	一般	版次	1.2

5.3 資通資產價值鑑別

5.3.1 資通資產權責單位應鑑別其所管轄內所有資通資產之價值。

5.3.2 資通資產價值除考量資通資產機密等級之外，尚需考量資通資產之可用性及完整性，其評估標準如下：

5.3.2.1 機密性評估標準

評估標準	數值
此資通資產無特殊之機密性要求	1
此資通資產僅供組織內部人員或被授權之單位及人員使用	2
此資通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
此資通資產含有組織或法律所規範的機密資訊	4

5.3.2.2 完整性評估標準

評估標準	數值
該資通資產本身完整性要求極低	1
該資通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
該資通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
該資通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

5.3.2.3 可用性評估標準

評估標準	數值
該資通資產可容許失效3工作天以上	1
該資通資產可容許失效8工作小時以上，3工作天以下	2

資通資產管理					
文件編號	HGSH-ISMS-B-002	機密等級	一般	版次	1.2

該資通資產僅容許失效4工作小時以上，8工作小時以下	3
該資通資產僅容許失效4工作小時以下	4

5.3.2.4 資通資產價值之決定將依據資通資產之機密性、完整性及可用性評估之後，取3者之最大值以為資通資產之價值。

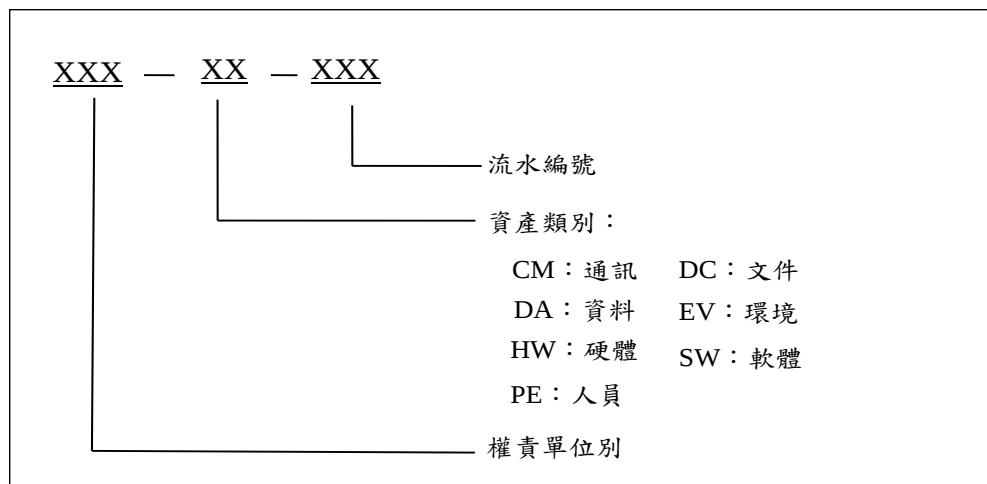
5.4 資通資產盤點表及價值確認

5.4.1 資通資產權責單位應依據資通資產盤點表之機密性、可用性、完整性之評估標準，確認資產價值。

5.4.2 資通資產盤點表及價值評估結果，應呈報資通安全委員會審議。

5.5 資通資產編號及標示

5.5.1 第1~3碼為權責單位別，第4~5碼為資產類別，第6~8碼為資通資產流水編號。



資通資產編碼方式圖

5.5.2 已列入機密等級分類的資通資產，應明確標示其機密等級，避免其機密性遭破壞。

5.5.3 實體設備之重要等級標示方式：

資通資產管理					
文件編號	HGSH-ISMS-B-002	機密等級	一般	版次	1.2

5.5.3.1 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）。

5.5.3.2 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，則由資通資產權責單位做額外的明顯註記。

5.6 資通資產管理作業

5.6.1 資通資產異動管理，如：新增、刪除、修改等控管原則，請參閱「資通資產異動作業」，如附件7。

5.7 覆核

5.7.1 權責單位每年至少進行一次資產盤點與資通資產盤點表覆核，以更新及確保資通資產盤點表的正確性及完整性。

5.7.2 當範圍內有以下的狀況發生時，則實施不定期的覆核，以更新及確保資通資產盤點表的正確性及完整性。

5.7.3 有新增、變更或移除資通資產。

5.7.4 系統有重大異動。

5.7.5 作業環境改變。

5.8 資通資產之報廢

5.8.1 資通資產之報廢或銷毀，應依據「資通資產異動作業」，採取適當之方式進行銷毀。

5.9 資通資產之處理規範

5.9.1 針對價值3或4之資通資產，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。

5.9.2 價值3或4文件類資通資產之安全處理應符合以下作業要求：

5.9.2.1 紙類文件不再使用時，應銷毀處理。

資通資產管理					
文件編號	HGSH-ISMS-B-002	機密等級	一般	版次	1.2

5.9.2.2 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。

5.9.2.3 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。

5.9.2.4 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。

5.9.3 價值 3 或 4 軟體類資通資產之安全處理作業，請參閱「存取控制管理」，如附件 8 及「系統開發與維護」，如附件 11。

5.9.4 價值 3 或 4 硬體類資通資產之安全處理作業，請參閱「實體安全管理」，如附件 9。

5.9.5 應定期檢討價值 3 或 4 之資通資產盤點表內容，以確保重要資產受到適當的安全保護。

6 相關文件及網站

6.1 存取控制管理

6.2 系統開發與維護

6.3 實體安全管理

6.4 資通資產異動作業

6.5 資通資產盤點表

6.6 國立中興大學計算機及資訊網路中心製「資安風險評鑑方法論」，說明資訊資產分類原則及資訊資產分級標準（網址：<https://youtu.be/01JAigkpSgo?t=190>）。

6.7 國立中興大學之資訊資產詳細風險評鑑（網址：<https://sites.google.com/email.nchu.edu.tw/ssdlc/ra2>）。

資通資產盤點表

資產編號	資產類別	資產名稱	資產說明	權責單位	保管單位	使用單位	機密性	完整性	可用性	資產價值
範例1：○	SW	學生學習歷程系統	學生學習歷程服務	教務處	教務處	教務處	3	4	3	4
範例2：○	HW	作業用個人電腦	教務處業務用個人電腦*7	教務處	教務處	教務處	3	2	2	3
範例3：○	PE	系統維護廠商	○○公司（學生學習歷程系統）	教務處	教務處	教務處	1	2	1	2
範例4：○	PE	系統操作人員	業務相關人員	教務處	教務處	教務處	1	2	1	2
範例5：○	PE	系統維護人員	具權限者	教務處	教務處	教務處	1	2	1	2
範例6：○	DA	學籍資料	學生學籍資料	教務處	教務處	教務處	4	4	2	4
範例7：○	CM	網路環境	校園網路	圖書館	圖書館	圖書館	2	2	3	3
範例8：○	EV	辦公室環境	教務處辦公室	教務處	教務處	教務處	4	2	3	4

資產編號	資產類別	資產名稱	資產說明	權責單位	保管單位	使用單位	機密性	完整性	可用性	資產價值
範例9：○	DC	辦公室文件	教務處公務相關文件	教務處	教務處	教務處	3	2	1	3
(以此類推)										