

臺北市立中山女子高級中學

資通安全維護計畫

第 2.0 版

生效日期 111 年 1 月 20 日

文件制 / 修訂紀錄表

文件版本	生效日期	制／修訂摘要說明	承辦單位	承辦人
V1.0	108年1月16日	初次建立,108年1月16日本校資通安全推動小組會議通過	資訊組	韓君尹
V1.1	109年5月11日	新增附件 15.臺北市立中山女子高級中學資安通報流程	資訊組	韓君尹
V2.0	111年1月20日	新增附件 16 臺北市立中山女子高級中學校園網路使用規範	資訊組	韓君尹

# 資通安全維護計畫

## 目 錄

壹、 依據及目的 .....	1
貳、 適用範圍 .....	1
參、 核心業務及重要性 .....	1
一、 核心業務及重要性： .....	1
二、 非核心業務及說明： .....	1
肆、 資通安全政策及目標 .....	2
一、 資通安全政策.....	2
二、 資通安全目標.....	2
三、 資通安全政策及目標之核定程序.....	3
四、 資通安全政策及目標之宣導.....	3
五、 資通安全政策及目標定期檢討程序.....	3
伍、 資通安全推動組織 .....	3
一、 資通安全長.....	3
二、 資通安全推動小組.....	3
陸、 人力及經費配置 .....	4
一、 人力及資源之配置.....	4
二、 經費之配置.....	5
柒、 資訊及資通系統之盤點 .....	5
一、 資訊及資通系統盤點.....	5
二、 機關資通安全責任等級分級.....	6
捌、 資通安全風險評估 .....	6
一、 資通安全風險評估.....	6
二、 資通安全風險之因應.....	6
玖、 資通安全防護及控制措施 .....	6
一、 資訊及資通系統之管理.....	7
二、 存取控制與加密機制管理.....	8
三、 作業與通訊安全管理.....	9
四、 資通安全防護設備.....	11
壹拾、 資通安全事件通報、應變及演練 .....	11
壹拾壹、 資通安全情資之評估及因應 .....	11

一、	資通安全情資之分類評估.....	12
二、	資通安全情資之因應措施.....	12
壹拾貳、	資通系統或服務委外辦理之管理 .....	13
一、	選任受託者應注意事項.....	13
二、	監督受託者資通安全維護情形應注意事項.....	13
壹拾參、	資通安全教育訓練 .....	13
一、	資通安全教育訓練要求.....	13
二、	資通安全教育訓練辦理方式.....	13
壹拾肆、	公務機關所屬人員辦理業務涉及資通安全事項之考核機制 .....	14
壹拾伍、	資通安全維護計畫及實施情形之持續精進及績效管理機制 .....	14
一、	資通安全維護計畫之實施.....	14
二、	資通安全維護計畫之持續精進及績效管理.....	14
壹拾陸、	資通安全維護計畫實施情形之提出 .....	15
壹拾柒、	相關附件 .....	15

## 壹、依據及目的

依據資通安全管理法第 10 條及施行細則第 6 條訂定資通安全維護計畫，作為資訊安全推動之依循及應符合其所屬資通安全責任等級之要求，訂定、修正及實施資通安全維護計畫(以下簡稱本計畫)。為因應資通安全管理法及機關(構)(以下簡稱機關)資通安全責任等級應辦事項要求，以符合法令規定並落實本計畫之資通作業安全。

## 貳、適用範圍

本計畫適用範圍涵蓋本校各處室單位。

## 參、核心業務及重要性

### 一、資通業務及重要性：

本校之核心業務及重要性如下表：

核心業務	核心資通系統	重要性說明	業務失效影響說明	最大可容忍中斷時間
校務行政	校務行政系統	為本機關依組織法執掌，足認為重要者	影響機關行政效率	4 小時

### 二、非核心業務及說明：

本機關之非核心業務及說明如下表：

非核心業務	業務失效影響說明	最大可容忍中斷時間
公文交換	電子公文無法即時送達機關，影響行政效率	4 小時
網路通訊服務	影響行政效率	4 小時
網站服務	影響本校訊息流通	4 小時

## 肆、資通安全政策及目標

### 一、資通安全政策

為使本校業務順利運作，防止資訊或資通系統受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，並確保其機密性（Confidentiality）、完整性（Integrity）及可用性（Availability），特制訂本政策如下，以供全體同仁共同遵循：

- (一) 建立資通安全風險管理機制，定期因應內外資通安全情勢變化，檢討資通安全風險管理之有效性。
- (二) 保護機敏資訊及資通系統之機密性與完整性，避免未經授權的存取與竄改。
- (三) 應強固核心資通系統之韌性，確保機關業務持續營運。
- (四) 因應資通安全威脅情勢變化，辦理資通安全教育訓練，以提高本校同仁之資通安全意識，本校同仁亦應確實參與訓練。
- (五) 針對辦理資通安全業務有功人員應進行獎勵。
- (六) 禁止多人共用單一資通系統帳號。

### 二、資通安全目標

#### (一) 量化型目標

1. 知悉資安事件發生，能於規定的時間完成通報、應變及復原作業。
2. 資通安全教育訓練人員受訓且通過評量合格率達 90%。(含線上學習之人員)
3. 定期舉辦資通安全演練且通過率達 90%。

#### (二) 質化型目標：

1. 適時因應法令與技術之變動，調整資通安全維護之內容，以避免資通系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，以確保其機密性、完整性及可用性。
2. 達成資通安全責任等級分級之要求，並降低遭受資通安全風險之威脅。
3. 提升人員資安防護意識、防止發生中毒或入侵事件。

### 三、資通安全政策及目標之核定程序

資通安全政策由本校資訊組簽陳至資通安全長核定，提校務會議通過實施。

### 四、資通安全政策及目標之宣導

(一)本校之資通安全政策及目標應每年透過教育訓練、內部會議、張貼公告等方式，向所有人員進行宣導，並檢視執行成效。

(二)本校應每年進行資安政策及目標宣導，並檢視執行成效。

### 五、資通安全政策及目標定期檢討程序

資通安全政策及目標應定期於資通安全管理審查會議(資訊小組會議)檢討其適切性。

## 伍、資通安全推動組織

### 一、資通安全長

依資通安全管理法第 11 條之規定，本校訂定校長為資通安全長，負責督導機關資通安全相關事項，其任務包括：

- (一)資通安全管理政策及目標之核定及督導。
- (二)資通安全責任之分配及協調。
- (三)資通安全資源分配。
- (四)資通安全防護措施之監督。
- (五)資通安全事件之檢討及監督。
- (六)資通安全相關規章與程序、制度文件核定。
- (七)資通安全管理年度工作計畫之核定
- (八)資通安全相關工作事項督導及績效管理。
- (九)其他資通安全事項之核定。

### 二、資通安全推動小組

#### (一) 組織

為推動本校之資通安全相關政策、落實資通安全事件通報及相關應變處理，由資通安全長召集各處室代表成立資通安全推動

小組，其任務包括：

1. 跨處室資通安全事項權責分工之協調。
2. 應採用之資通安全技術、方法及程序之協調研議。
3. 整體資通安全措施之協調研議。
4. 資通安全計畫之協調研議。
5. 其他重要資通安全事項之協調研議。

## (二) 分工及職掌

本校之資通安全推動小組依下列分工進行責任分組，並依資通安全長指示負責下列事項，本校資通安全推動小組分組人員名單及職掌應列冊，並適時更新之：

### 1. 策略規劃組：

- (1) 資通安全政策及目標之研議。
- (2) 訂定本校資通安全相關規章與程序、制度文件，並確保相關規章與程序、制度合乎法令及契約之要求。
- (3) 依據資通安全目標擬定年度工作計畫。
- (4) 傳達資通安全政策與目標。
- (5) 其他資通安全事項之規劃。

### 2. 資安防護組：

- (1) 資通安全技術之研究、建置及評估相關事項。
- (2) 資通安全相關規章與程序、制度之執行。
- (3) 資訊及資通系統之盤點及風險評估。
- (4) 資料及資通系統之安全防護事項之執行。
- (5) 資通安全事件之通報及應變機制之執行。
- (6) 其他資通安全事項之辦理與推動。

## 陸、人力及經費配置

### 一、人力及資源之配置

(一)本校依資通安全責任等級分級辦法之規定，屬資通安全責任等



級 D 級，最低應設置資通安全人員 1 人。本校現有資通安全人員名單及職掌應列冊，並適時更新。

(二)本校之承辦單位於辦理資通安全人力資源業務時，應加強資通安全人員之培訓，並提升機關內資通安全專業人員之資通安全管理能力。本校之相關單位於辦理資通安全業務時，如資通安全人力或經驗不足，得洽請相關學者專家或專業機關（構）提供顧問諮詢服務。

(三)本校各級業務主管人員，應負責督導所屬人員之資通安全作業，防範不法及不當行為。

(四)人力資源之配置情形應每年定期檢討，並納入資通安全維護計畫持續改善機制之管理審查。

## 二、經費之配置

(一)資通安全推動小組於規劃配置相關經費及資源時，應考量本校之資通安全政策及目標，並提供建立、實行、維持及持續改善資通安全維護計畫所需之資源。

(二)各單位如有資通安全資源之需求，應配合機關預算規劃期程向資通安全推動小組提出，由資通安全推動小組視整體資通安全資源進行分配，並經資通安全長核定後，進行相關之建置。

(三)資通安全經費、資源之配置情形應每年定期檢討，並納入資通安全維護計畫持續改善機制之管理審查。

## 柒、資訊及資通系統之盤點

### 一、資訊及資通系統盤點

(一)本校每年辦理資訊及資通系統資產盤點，依管理責任指定對應之資產管理人，並依資產屬性進行分類。

(二)資訊及資通系統資產項目如下：

1. 軟體資產：應用軟體、系統軟體、開發工具、套裝軟體及電腦作業系統等。
2. 硬體資產：電腦及通訊設備、可攜式設備及資通系統相關之設備等。
3. 支援服務資產：相關基礎設施級其他機關內部之支援服務，如電力、消防等。

4. 人員資產：內部設備維運管理人員、主管、使用人員，以及委外廠商駐點人員等。
5. 資料資產：以紙本形式儲存之資訊，如計畫、報告、公文、各種應用系統文件及管理手冊，契約、法律文件、軟體使用授權等等。

(三)本校每年度應依資訊及資通系統盤點結果，製作「資訊及資通系統資產清冊」，欄位應包含：資訊及資通系統名稱、資產名稱、資產類別、管理者、存放位置、防護需求等級。

(四)資訊及資通系統資產應以標籤標示於設備明顯處，並載明財產編號、保管人、廠牌、型號等資訊。

(五)各單位管理之資訊或資通系統如有異動，應即時通知資通安全推動小組更新資產清冊。

## 二、機關資通安全責任等級分級

本校因自行辦理資通業務，未維運自行或委外開發之資通系統，為資通安全等級分類 D 級機關。

## 捌、資通安全風險評估

### 一、資通安全風險評估

(一)本校應每年針對資訊及資通系統資產進行風險評估。

(二)執行風險評估時應參考臺北市政府教育局「資訊資產風險評鑑管理辦法」執行相關作業。

### 二、資通安全風險之因應

選擇防護及控制措施時，亦應考量採行該項措施可能對資通安全風險之影響。

## 玖、資通安全防護及控制措施

本校依據前章資通安全風險評估結果、自身資通安全責任等級之應辦事項及資通系統之防護基準，採行相關之防護及控制措施如下：

## 一、資訊及資通系統之管理

### (一) 資訊及資通系統之保管

1. 資訊及資通系統管理人應確保資訊及資通系統已盤點造冊並適切分級，並持續更新以確保其正確性。
2. 資訊及資通系統管理人應確保資訊及資通系統被妥善的保存或備份。
3. 資訊及資通系統管理人應確保重要之資訊及資通系統已採取適當之存取控制政策。

### (二) 資訊及資通系統之使用

1. 本校同仁使用資訊及資通系統前應經其管理人授權。
2. 本校同仁使用資訊及資通系統時，應留意其資通安全要求事項，並負對應之責任。
3. 本機關同仁使用資訊及資通系統後，應依規定之程序歸還。資訊類資訊之歸還應確保相關資訊已正確移轉，並安全地自原設備上抹除。
4. 非本校同仁使用本機關之資訊及資通系統，應確實遵守本機關之相關資通安全要求，且未經授權不得任意複製資訊。
5. 對於資訊及資通系統，宜識別並以文件記錄及實作可被接受使用之規則。

### (三) 資訊及資通系統之刪除或汰除

1. 資訊及資通系統之刪除或汰除前應評估機關是否已無需使用該等資訊及資通系統，或該等資訊及資通系統是否已妥善移轉或備份。
2. 資訊及資通系統之刪除或汰除時宜加以清查，以確保所有機敏性資訊及具使用授權軟體已被移除或安全覆寫。
3. 具機敏性之資訊或具授權軟體之資通系統，宜採取實體銷毀，或以毀損、刪除或覆寫之技術，使原始資訊無法被讀取，並避免僅使用標準刪除或格式化功能。

## 二、存取控制與加密機制管理

### (一) 網路安全控管

#### 1. 網路區域劃分如下：

- (1) 外部網路：對外網路區域，連接外部廣網路(Wide Area Network, WAN)。
- (2) 內部區域網路 (Local Area Network, LAN)：機關內部單位人員及內部伺服器使用之網路區段。

2. 外部網路及內部區域網路間連線需經防火牆進行存取控制，非允許的服務與來源不能進入其他區域。

3. 應定期檢視防火牆政策是否適當，並適時進行防火牆軟、硬體之必要更新或升級。

4. 內部網路之區域應做合理之區隔，使用者應經授權後在授權之範圍內存取網路資源。

5. 使用者應依規定之方式存取網路服務，不得於辦公室內私裝電腦及網路通訊等相關設備。

#### 6. 網域名稱系統(DNS)防護

- (1) 一般伺服器應關閉 DNS 服務，防火牆政策亦應針對 DNS 進行控管，關閉不需要的 DNS 服務存取。
- (2) DNS 伺服器應經常性進行弱點漏洞管理與修補、落實存取管控機制。

#### 7. 無線網路防護

- (1) 機密資料原則不得透過無線網路及設備存取、處理或傳送。
- (2) 用以儲存或傳輸資料且具無線傳輸功能之個人電子設備與工作站，應安裝防毒軟體，並定期更新病毒碼。

### (二) 資通系統權限管理

#### 1. 資通系統應設置通行碼管理，通行碼之要求需滿足：

- (1) 通行碼長度 8 碼以上。
- (2) 通行碼複雜度應包含英文大寫小寫、特殊符號或數字三種以上。
- (3) 使用者每 90 天應更換一次通行碼。

2. 使用者使用資通系統前應經授權，並使用唯一之使用者帳號，除有特殊營運或作業必要經核准並紀錄外，不得共用帳號。
3. 使用者無繼續使用資通系統時，應立即停用或移除使用者帳號，資通系統管理者應定期清查使用者之權限。

### (三) 特權帳號之存取管理

1. 資通系統之特權帳號請應經正式申請授權方能使用，特權帳號授權前應妥善審查其必要性，其授權及審查記錄應留存。
2. 資通系統之特權帳號不得共用。
3. 資通系統之管理者每季應清查系統特權帳號。

### (四) 加密管理

1. 機密資訊於儲存或傳輸時應進行加密。
2. 加密保護措施應遵守下列規定：
  - (1) 應落實使用者更新加密裝置並備份金鑰。
  - (2) 一旦加密資訊具遭破解跡象，應立即更改之。

## 三、作業與通訊安全管理

### (一) 防範惡意軟體之控制措施

1. 主機及個人電腦應安裝防毒軟體，並時進行軟、硬體之必要更新或升級。
2. 使用者未經同意不得私自安裝應用軟體，管理者並應每半年定期針對管理之設備進行軟體清查。
3. 使用者不得私自使用已知或有嫌疑惡意之網站。

### (二) 遠距工作之安全措施

- (1) 提供虛擬桌面存取，以防止於私有設備上處理及儲存資訊。
- (2) 遠距工作終止時之存取權限撤銷，並應返還相關設備。

### (三) 確保實體與環境安全措施

#### 1. 電腦機房之門禁管理

- (1) 電腦機房應進行實體隔離。
- (2) 機關人員或來訪人員應申請及授權後方可進入電腦機房，管

理者並應定期檢視授權人員之名單。

(3) 人員及設備進出應留存記錄。

## 2. 電腦機房之環境控制

(1) 電腦機房之空調、電力應建立備援措施。

(2) 電腦機房應安裝之安全偵測及防護措施，包括熱度及煙霧偵測設備、火災警報設備、溫濕度監控設備、漏水偵測設備、入侵者偵測系統，以減少環境不安全之危險。

## 3. 辦公室區域之實體與環境安全措施

(1) 應考量採用辦公桌面的淨空政策，以減少文件及可移除式媒體等在辦公時間之外遭未被授權的人員取用、遺失或是被破壞的機會。

(2) 機密性及敏感性資訊，不使用或下班時應該上鎖。

### (四) 資料備份

1. 重要資料及資通系統應進行資料備份，其備份之頻率應滿足復原時間點目標之要求，並執行異地存放。

2. 敏感或機密性資訊之備份應加密保護。

### (五) 媒體防護措施

1. 使用隨身碟或磁片等存放資料時，具機密性、敏感性之資料應與一般資料分開儲存，不得混用並妥善保管。

2. 對機密與敏感性資料之儲存媒體實施防護措施，包含機密與敏感之紙本或備份磁帶，應保存於上鎖之櫃子，且需由專人管理鑰匙。

### (六) 電腦使用之安全管理

1. 電腦、業務系統或自然人憑證，若超過十五分鐘不使用時，應立即登出或啟動螢幕保護功能並取出自然人憑證。

2. 連網電腦應隨時配合更新作業系統、應用程式漏洞修補程式及防毒病毒碼等。

3. 筆記型電腦及實體隔離電腦應定期以人工方式更新作業系統、應用程式漏洞修補程式及防毒病毒碼等。

4. 下班時應關閉電腦及螢幕電源。

5. 如發現資安問題，應主動循機關之通報程序通報。

#### (七) 行動設備之安全管理

1. 機密資料不得由未經許可之行動設備存取、處理或傳送。
2. 機敏會議或場所不得攜帶未經許可之行動設備進入

#### (八) 即時通訊軟體之安全管理

1. 使用即時通訊軟體傳遞機關內部公務訊息，其內容不得涉及機密資料。但有業務需求者，應使用經專責機關鑑定相符機密等級保密機制或指定之軟、硬體，並依相關規定辦理。
2. 使用於傳遞公務訊息之即時通訊軟體應具備下列安全性需求：
  - (1) 用戶端應有身分識別及認證機制。
  - (2) 訊息於傳輸過程應有安全加密機制。
  - (3) 應通過經濟部工業局訂定行動化應用軟體之中級檢測項目。
  - (4) 伺服器端之主機設備及通訊紀錄應置於我國境內。
  - (5) 伺服器通訊紀錄 (log) 應至少保存六個月。

#### 四、資通安全防護設備

1. 應建置防毒軟體、網路防火牆、電子郵件過濾裝置，持續使用並適時進行軟、硬體之必要更新或升級。
2. 資安設備應定期備份日誌紀錄，定期檢視並由主管複核執行成果，並檢討執行情形。

#### 壹拾、資通安全事件通報、應變及演練

為即時掌控資通安全事件，並有效降低其所造成之損害，本校應訂定資通安全事件通報、應變及演練，依本校資通安全事件通報應變程序辦理。

#### 壹拾壹、資通安全情資之評估及因應

本校接獲資通安全情資，應評估該情資之內容，並視其對本校之影響、可接受之風險及本校之資源，決定最適當之因應方式，必要時得調整資通安全維護計畫之控制措施，並做成紀錄。

## 一、資通安全情資之分類評估

本校接受資通安全情資後，應指定資通安全人員進行情資分析，並依據情資之性質進行分類及評估，情資分類評估如下：

### (一) 資通安全相關之訊息情資

資通安全情資之內容如包括重大威脅指標情資、資安威脅漏洞與攻擊手法情資、重大資安事件分析報告、資安相關技術或議題之經驗分享、疑似存在系統弱點或可疑程式等內容，屬資通安全相關之訊息情資。

### (二) 入侵攻擊情資

資通安全情資之內容如包含特定網頁遭受攻擊且證據明確、特定網頁內容不當且證據明確、特定網頁發生個資外洩且證據明確、特定系統遭受入侵且證據明確、特定系統進行網路攻擊活動且證據明確等內容，屬入侵攻擊情資。

### (三) 機敏性之情資

資通安全情資之內容如包含姓名、出生年月日、國民身份證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病例、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接識別之個人資料，或涉及個人、法人或團體營業上秘密或經營事業有關之資訊，或情資之公開或提供有侵害公務機關、個人、法人或團體之權利或其他正當利益，或涉及一般公務機密、敏感資訊或國家機密等內容，屬機敏性之情資。

## 二、資通安全情資之因應措施

本校於進行資通安全情資分類評估後，應針對情資之性質進行相應之措施，必要時得調整資通安全維護計畫之控制措施。

### (一) 資通安全相關之訊息情資

由資通安全推動小組彙整情資後進行風險評估，並依據資通安全維護計畫之控制措施採行相應之風險預防機制。

### (二) 入侵攻擊情資

由資通安全人員判斷有無立即之危險，必要時採取立即之通報應變措施，並依據資通安全維護計畫採行相應之風險防護措施，另通知各單位進行相關之預防。



### (三) 機敏性之情資

就涉及個人資料、營業秘密、一般公務機密、敏感資訊或國家機密之內容，應採取遮蔽或刪除之方式排除，例如個人資料及營業秘密，應以遮蔽或刪除該特定區段或文字，或採取去識別化之方式排除之。

## 壹拾貳、資通系統或服務委外辦理之管理

本校委外辦理資通系統之建置、維運或資通服務之提供時，應考量受託者之專業能力與經驗、委外項目之性質及資通安全需求，選任適當之受託者，並監督其資通安全維護情形。

### 一、選任受託者應注意事項

1. 受託者辦理受託業務之相關程序及環境，應具備完善之資通安全管理措施或通過第三方驗證。
2. 受託者應配置充足且經適當之資格訓練、擁有資通安全專業證照或具有類似業務經驗之資通安全專業人員。

### 二、監督受託者資通安全維護情形應注意事項

1. 受託者執行受託業務，違反資通安全相關法令或知悉資通安全事件時，應立即通知委託機關及採行之補救措施。
2. 委託關係終止或解除時，應確認受託者返還、移交、刪除或銷毀履行委託契約而持有之資料。
3. 本校應定期或於知悉受託者發生可能影響受託業務之資通安全事件。

## 壹拾參、資通安全教育訓練

### 一、資通安全教育訓練要求

本校依資通安全責任等級分級屬 D 級，一般使用者與主管，每人每年接受 3 小時以上之一般資通安全教育訓練。

### 二、資通安全教育訓練辦理方式

1. 承辦單位應於每年年初，考量管理、業務及資訊等不同工作類別之需求，擬定資通安全認知宣導及教育訓練計畫，以建立人員資通安全認知，提升機關資通安全水準，並應保存相關之資通安全認知宣導及教育訓練紀錄。

2. 本校資通安全認知宣導及教育訓練之內容得包含：
  - (1) 資通安全政策(含資通安全維護計畫之內容、管理程序、流程、要求事項及人員責任、資通安全事件通報程序等)。
  - (2) 資通安全法令規定。
  - (3) 資通安全作業內容。
  - (4) 資通安全技術訓練。
3. 員工報到時，應使其充分瞭解本校資通安全相關作業規範及其重要性。

#### **壹拾肆、公務機關所屬人員辦理業務涉及資通安全事項之考核機制**

本校所屬人員之平時考核或聘用，依據公務機關所屬人員資通安全事項獎懲辦法、臺北市政府及所屬各機關公務人員平時獎懲標準表，及本校各相關規定辦理之。

#### **壹拾伍、資通安全維護計畫及實施情形之持續精進及績效管理機制**

##### **一、資通安全維護計畫之實施**

為落實本安全維護計畫，使本校之資通安全管理有效運作，相關單位於訂定各階文件、流程、程序或控制措施時，應與本校之資通安全政策、目標及本安全維護計畫之內容相符，並應保存相關之執行成果記錄。

##### **二、資通安全維護計畫之持續精進及績效管理**

1. 本校之資通安全推動小組應每年召開資通安全管理審查會議，確認資通安全維護計畫之實施情形，確保其持續適切性、合宜性及有效性。
2. 管理審查議題應包含下列討論事項：
  - (1) 與資通安全管理系統有關之內部及外部議題的變更，如法令變更、上級機關要求、資通安全推動小組決議事項等。
  - (2) 資通安全維護計畫內容之適切性。
  - (3) 資通安全績效之回饋，包括：
    - A. 資通安全政策及目標之實施情形。
    - B. 人力及資源之配置之實施情形。

- C. 資通安全防護及控制措施之實施情形。
  - D. 不符合項目及矯正措施。
  - (4) 風險評鑑結果及風險處理計畫執行進度。
  - (5) 資通安全事件之處理及改善情形。
  - (6) 利害關係人之回饋。
  - (7) 持續改善之機會。
3. 持續改善機制之管理審查應做成改善績效追蹤報告，相關紀錄並應予保存，以作為管理審查執行之證據。

#### **壹拾陸、資通安全維護計畫實施情形之提出**

本校依據資通安全管理法第 12 條之規定，應於每年向上級或監督機關，提出資通安全維護計畫實施情形，使其得瞭解本校之年度資通安全計畫實施情形。

#### **壹拾柒、相關附件**

附件表單。

# 臺北市立中山女子高級中學

## 資通安全維護計畫 附件

## 資通安全維護計畫相關附件

### 目 次

1. 資通安全管理代表及推動小組成員分工表.....	1
2. 資通安全保密同意書.....	2
3. 資通安全需求申請單.....	3
4. 資訊及資通系統資產清冊.....	4
5. 風險評估表.....	5
6. 風險類型暨風險對策參考表.....	6
7. 管制區域人員進出登記表.....	9
8. 委外廠商執行人員保密切結書、保密同意書.....	10
9. 委外廠商查核項目表.....	14
10. 年度資通安全教育訓練計畫.....	18
11. 資通安全認知宣導及教育訓練簽到表.....	20
12. 資通安全維護計畫實施情形.....	21
13. 審查結果及改善報告.....	23
14. 改善績效追蹤報告.....	24

# 1. 資通安全管理代表及推動小組成員分工表

## 臺北市立中山女子高級中學 資通安全管理代表及推動小組成員及分工表

編號：

製表日期：108 年 06 月 26 日

單位職級	職掌事項	分機	備註 (代理人)
教務主任	策略規劃組： 1. 資通安全政策及目標之研議。 2. 訂定本校資通安全相關規章與程序、制度文件，並確保相關規章與程序、制度合乎法令及契約之要求。 3. 依據資通安全目標擬定年度工作計畫。 4. 傳達資通安全政策與目標。 5. 其他資通安全事項之規劃。	221	策略規劃組成員
學務主任		231	
輔導主任		271	
圖書館主任		281	
秘書		211	
資訊組長		282	
總務主任	資安防護組： 1. 資通安全技術之研究、建置及評估相關事項。 2. 資通安全相關規章與程序、制度之執行。 3. 資訊及資通系統之盤點及風險評估。 4. 資料及資通系統之安全防護事項之執行。 5. 資通安全事件之通報及應變機制之執行。 6. 其他資通安全事項之辦理與推動。	241	資安防護組成員
人事主任		261	
會計主任		251	
主任教官		291	
系統師		283	
各科教師代表			

## 2. 資通安全保密同意書

# 臺北市立中山女子高級中學 資通安全保密同意書

編號：

立同意書人\_\_\_\_\_於民國\_\_\_\_年\_\_\_\_月\_\_\_\_日起於\_\_\_\_\_任職，因業務涉及單位重要之資訊及資通系統，故同意下列保密事項：

- 一、於業務上所知悉之機敏資料及運用之資通系統等，應善盡保管及保密之責。
- 二、相關業務之資訊、文件，不得私自洩漏與業務無關之人員。
- 三、遵守其他本單位資通安全相關之法令及規定。
- 四、如有危害本單位資通安全之行為，願負相關之責任。

立同意書人：\_\_\_\_\_ (簽章)

身份證字號：\_\_\_\_\_

服務機關：\_\_\_\_\_

機關首長：\_\_\_\_\_

中 華 民 國 年 月 日

### 3. 資通安全需求申請單

## 臺北市立中山女子高級中學 資通安全需求申請單

編號：

申請單位		申請日期	年 月 日
申請項目	<input type="checkbox"/> 軟體 <input type="checkbox"/> 硬體 <input type="checkbox"/> 其他	項目名稱	
申請數量		需用日期	年 月 日
申請類別	<input type="checkbox"/> 新購 <input type="checkbox"/> 升級	使用設備	<input type="checkbox"/> 主機 <input type="checkbox"/> 使用者電腦 <input type="checkbox"/> 其他
安裝單位		安裝位置	
用途說明			
申請人		單位主管	
資通安全推動小組	<input type="checkbox"/> 可採購 <input type="checkbox"/> 不可採購	說明：	
資通安全推動小組承辦人員		資通安全長	

註：陳核層級請學校依需求調整



#### 4. 資訊及資通系統資產清冊

### 臺北市立中山女子高級中學資訊及資通系統資產清冊

編號：

製表日期： 年 月 日

項次	資產名稱	類別	擁有人/ 職稱	管理者 (部門)	使用者 (部門)	存放 位置	數量	說明	防護 需求 等級	核心 系統	備註
1.										<input type="checkbox"/> 是 <input type="checkbox"/> 否	
2.										<input type="checkbox"/> 是 <input type="checkbox"/> 否	
3.										<input type="checkbox"/> 是 <input type="checkbox"/> 否	
4.										<input type="checkbox"/> 是 <input type="checkbox"/> 否	
5.										<input type="checkbox"/> 是 <input type="checkbox"/> 否	

註：陳核層級請學校依需求調整

承辦人：

單位主管：

機關首長：

## 5. 風險評估表

# 臺北市立中山女子高級中學 風險評估表

編號：

製表日期： 年 月 日

項次	資產名稱	類別	擁有者/ 職稱	機密性 (C)	完整性 (I)	可用性 (A)	資訊資產 價值 (C,I,A 取 最大值)	發生可能 性/威脅 等級(T)	脆弱等級 (V)	風險值 資訊資產價 值*(T*V)
1.										
2.										
3.										
4.										
5.										

註：

1. 本表可與資訊及資通系統資產清冊合併使用。
2. 陳核層級請學校依需求調整

承辦人員：

單位主管：

機關首長：

## 6. 風險類型暨風險對策參考表

# 臺北市立中山女子高級中學

## 風險類型暨風險對策參考表

風險類型暨風險對策參考表		
作業內容	具體風險類型	風險處理對策
網際網路探尋	網頁搜尋	強化網頁伺服器，避免存放 index.html、default.asp 的檔案資料夾，並禁用相關的目錄索引。使用 robots.txt 指示搜尋引擎不要為其內容編制索引。
	WHOIS 查詢	在 WHOIS 資料庫及 TLS 憑證中，使用平常、單一的網路管理人聯絡資訊，以降低社交工程與撥號攻擊的成功率。
	DNS 查詢	設定 DNS 伺服器，禁止其對不可信任的主機執行區域轉送，並主動從網際網路掃描 TCP 和 UDP 的端口 53，以便發現是否有偽冒的名稱伺服器。刪減 DNS 區域檔案內容，以防洩漏不必要的訊息，例如非公開的 IP 位址和主機名稱，並且於必要時才使用 PTR 紀錄。
	SMTP 探尋	設定 SMTP 伺服器在遇到問題時，例如寄件人不存在時，不要發送 NDN，以防攻擊者藉機列舉內部郵件系統及組態內容。
區域網路攻擊	MITM 和偽冒伺服器攻擊	強制採用傳輸層安全加密與透過具有憑證檢驗功能的身份驗證機制
	802.1X 攻擊	<ul style="list-style-type: none"> <li>● 檢測 X.509 憑證是否有效。</li> <li>● 指定合法驗證者 (RADIUS 伺服器) 之一般名稱值。</li> <li>● 在安全功能發生問題時，禁止提供詳細資訊給終端使用者，以提高故障安全性。</li> </ul>
	資料連結層攻擊	<ul style="list-style-type: none"> <li>● 將交換連接埠設為 access 模式，並關閉動態建立主幹網路的功能。</li> <li>● 關閉未用到的乙太網路連接埠，並歸類在隔離的 VLAN 外。</li> </ul>
	網路層與應用層的攻擊	<ul style="list-style-type: none"> <li>● 如果沒有明確要求，應關閉 IPv6。</li> <li>● 取消對 ICMP 重導向的支援。</li> <li>● 停用群播名稱解析及 Windows 的 NetBIOS over TCP/IP 通訊。</li> </ul>
網路服務漏洞	網路攻擊表面	將不必要的功能關閉。
	伺服器套件包與程式庫	隨時修補存在攻擊表面的已知攻擊。

	攻擊	
	透過傳輸與遠端維護操作之服務進行攻擊	<ul style="list-style-type: none"> <li>● 停用無加密傳輸安全性的 Telnet、FTP、SNMP、VNC 等。</li> <li>● 遠端操作維護須透過安全的身份驗證連接。</li> <li>● 建構封閉的管理網路。</li> </ul>
	SSH 伺服器攻擊	<ul style="list-style-type: none"> <li>● 強制使用 2.0 版本的協定，禁止向下相容特性。</li> <li>● 停用使用者的密碼驗證機制，強制使用者採取一次性密碼 (OTP)、公鑰或多因子驗證，例如可透過 Google Authenticator、Duo Security 或其他平台取得。</li> </ul>
	DNS 伺服器攻擊	<ul style="list-style-type: none"> <li>● 停止支援來自不受信任來源的遞迴查詢。</li> <li>● 確保區域檔案不含多餘或敏感資訊。</li> </ul>
	Kerberos 伺服器攻擊	<ul style="list-style-type: none"> <li>● 停止支援較弱的 HMAC 演算法。</li> <li>● 在微軟環境中，可考慮強制使用最高的網域功能等級。</li> </ul>
郵件服務	SMTP 攻擊	不要將多功能的 SMTP 伺服器公開到網際網路或不受信任的網路。
	不受信任郵件的攻擊	<ul style="list-style-type: none"> <li>● 使用 SPF、DKIM 和 DMARC 防止伺服器傳輸或接收未經授權的內容。</li> <li>● 將對外的 SMTP 介面設定成不接受偽冒的內部網路郵件。</li> <li>● 配置外部內容過濾機制。</li> </ul>
	防毒軟體弱點攻擊	應及時更新病毒碼與維持版本最新。
	電子郵件帳戶攻擊	<ul style="list-style-type: none"> <li>● 建議在用戶端增加一層憑證式的驗證機制。</li> <li>● 強制郵件伺服器使用強密碼政策。</li> <li>● 紀錄郵件服務身份驗證失效的日誌，應制定帳號鎖定原則。</li> </ul>
VPN 服務	VPN 攻擊	<ul style="list-style-type: none"> <li>● 確認 VPN 伺服器的維護作業，並修補到最新版本。</li> <li>● 強制使用 AH 和 ESP 功能身份驗證及機密性服務。</li> <li>● 使用數位憑證取代預置共享金鑰，並要求對設備進行身份驗證。</li> <li>● 過濾內連的 VPN 流量，以便在發生入侵事件時限制網路存取。</li> <li>● 定期稽核已授權的 VPN 使用者，以防有偽冒的帳號。</li> </ul>
網頁應用程式框架	Web 應用伺服器攻擊	<ul style="list-style-type: none"> <li>● 確保應用程式框架組件都已修補至最新版本，包括相依與間接使用的組件。</li> <li>● 禁止將管理介面或特權功能公開在不受信任的網路上。</li> <li>● 在可行的情況下，將開放網頁應用程式和管理功能隔離。</li> </ul>
資料儲存機制	資料庫攻擊	<ul style="list-style-type: none"> <li>● 限制資料服務只與經授權的對象往來，特別是雲端環境中。</li> <li>● 避免使用不支援身份驗證的儲存系統和協定。</li> <li>● 禁止在可公開讀取的儲存裝置，例如 NFS、iSCSI、SMB 和 AFP 等，以未加密狀態儲存機敏資料，包括系統和資料庫的備份檔案通常存有機敏資</li> </ul>

		<p>料，例如密碼、身份憑證。</p> <ul style="list-style-type: none"><li>●確保密碼強度。</li><li>●限制只有受信任的網路才能存取管理服務。</li><li>●稽查和監控身份驗證事件，識別濫用身份憑據和暴力拆解密碼的情形。</li></ul>
--	--	--

參考來源：資安風險評估指南，第三版，Chris McNab，江湖海譯。

7. 管制區域人員進出登記表

臺北市立中山女子高級中學管制區域人員進出登記表

編號：

製表日期： 年 月 日

編號	姓名	單位	配同人員	日期	進入時間	離開時間	事由	權限	進出設備	攜帶物品

註：陳核層級請學校依需求調整

承辦人：

單位主管：

## 8. 委外廠商執行人員保密切結書、保密同意書

# 臺北市立中山女子高級中學

## 委外廠商執行人員保密切結書

立切結書人.....（簽署人姓名）等，受.....（廠商名稱）委派至.....（機關名稱，以下稱機關）處理業務，謹聲明恪遵機關下列工作規定，對工作中所持有、知悉之資訊系統作業機密或敏感性業務檔案資料，均保證善盡保密義務與責任，非經機關權責人員之書面核准，不得擷取、持有、傳遞或以任何方式提供給無業務關係之第三人，如有違反願賠償一切因此所生之損害，並擔負相關民、刑事責任，絕無異議。

- 一、未經申請核准，不得私自將機關之資訊設備、媒體檔案及公務文書攜出。
- 二、未經機關業務相關人員之確認並代為申請核准，不得任意將攜入之資訊設備連接機關網路。若經申請獲准連接機關網路，嚴禁使用數據機或無線傳輸等網路設備連接外部網路。
- 三、經核准攜入之資訊設備欲連接機關網路或其他資訊設備時，須經電腦主機房掃毒專責人員進行病毒、漏洞或後門程式檢測，通過後發給合格標籤，並將其粘貼在設備外觀醒目處以備稽查。
- 四、廠商駐點服務及專責維護人員原則應使用機關配發之個人電腦與週邊設備，並僅開放使用機關內部網路。若因業務需要使用機關電子郵件、目錄服務，應經機關業務相關人員之確認並代為申請核准，另欲連接網際網路亦應經機關業務相關人員之確認並代為申請核准。
- 五、機關得定期或不定期派員檢查或稽核立切結書人是否符合上列工作規定。
- 六、本保密切結書不因立切結書人離職而失效。
- 七、立切結書人因違反本保密切結書應盡之保密義務與責任致生之一切損害，立切結書人所屬公司或廠商應負連帶賠償責任。

立切結書人：

姓名及簽章    身分證字號    聯絡電話及戶籍地址

\_\_\_\_\_

\_\_\_\_\_

立切結書人所屬廠商：

廠商名稱及蓋章    廠商負責人姓名及簽章    廠商聯絡電話及地址

\_\_\_\_\_

填表說明：

- 一、廠商駐點服務人員、專責維護人員，或逗留時間超過三天以上之突發性維護增援、臨時性系統測試或教育訓練人員（以授課時需連結機關網路者為限）及經常到機關洽公之業務人員皆須簽署本切結書。
- 二、廠商駐點服務人員、專責維護人員及經常到機關洽公之業務人員每年簽署本切結書乙次。

中 華 民 國      年      月      日



# 臺北市立中山女子高級中學

## 委外廠商執行人員保密同意書

茲緣於簽署人\_\_\_\_\_（簽署人姓名，以下稱簽署人）參與\_\_\_\_\_（廠商名稱，以下稱廠商）得標\_\_\_\_\_（機關名稱）（以下稱機關）資通業務委外案\_\_\_\_\_（案名）（以下稱「本案」），於本案執行期間有知悉或可得知悉或持有政府公務秘密及業務秘密，為保持其秘密性，簽署人同意恪遵本同意書下列各項規定：

- 第一條 簽署人承諾於本契約有效期間內及本契約期滿或終止後，對於所得知或持有一切機關未標示得對外公開之公務秘密，以及機關依契約或法令對第三人負有保密義務之業務秘密，均應以善良管理人之注意妥為保管及確保其秘密性，並限於本契約目的範圍內，於機關指定之處所內使用之。非經機關事前書面同意，不得為本人或任何第三人之需要而複製、保有、利用該等秘密或將之洩漏、告知、交付第三人或以其他任何方式使第三人知悉或利用該等秘密，或對外發表或出版，亦不得攜至機關或機關所指定處所以外之處所。
- 第二條 簽署人知悉或取得機關公務秘密與業務秘密應限於其執行本契約所必需且僅限於本契約有效期間內。簽署人同意公務秘密與業務秘密，應僅提供、告知有需要知悉該秘密之履約廠商團隊成員人員。
- 第三條 簽署人在下述情況下解除其所應負之保密義務：
- 原負保密義務之資訊，由機關提供以前，已合法持有或已知且無保密必要者。
- 原負保密義務之資訊，依法令業已解密、依契約機關業已不負保密責任、或已為公眾所知之資訊。
- 原負保密義務之資訊，係自第三人處得知或取得，該第三人就該等資訊並無保密義務。
- 第四條 簽署人若違反本同意書之規定，機關得請求簽署人及其任職之廠商賠償機關因此所受之損害及追究簽署人洩密之刑責，如因而致第三人受有損害者，簽署人及其任職之廠商亦應負賠償責任。
- 第五條 簽署人因本同意書所負之保密義務，不因離職或其他原因不參與本案而失其效力。
- 第六條 本同意書一式叁份，機關、簽署人及\_\_\_\_\_（廠商）各執存一份。

簽署人姓名及簽章：

身分證字號：

聯絡電話：

戶籍地址：

所屬廠商名稱及蓋章：

所屬廠商負責人姓名及簽章：

所屬廠商地址：

中 華 民 國      年      月      日

## 9. 委外廠商查核項目表

### 臺北市立中山女子高級中學 委外廠商查核項目表

編號：

填表日期： 年 月 日

查核人員：

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
1. 資通安全政策之推動及目標訂定	1.1 是否定義符合組織需要之資通安全政策及目標？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	1.2 組織是否訂定資通安全政策及目標？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	1.3 組織之資通安全政策文件是否由管理階層核准並正式發布且轉知所有同仁？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	1.4 組織是否對資通安全政策、目標之適切性及有效性，定期作必要之審查及調整？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	1.5 是否隨時公告資通安全相關訊息？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
2. 設置資通安全推動組織	2.1 是否指定適當權責之高階主管負責資通安全管理之協調、推動及督導等事項？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	2.2 是否指定專人或專責單位，負責辦理資通安全政策、計畫、措施之研議，資料、資通系統之使用管理及保護，資安稽核等資安工作事項？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	2.3 是否訂定組織之資通安全責任分工？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
3. 配置適當之資通安全專業人員及適當之資源	3.1 是否訂定人員之安全評估措施？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	3.2 是否符合組織之需求配置專業資安人力？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	3.3 是否具備相關專業資安證照或認證？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	3.4 是否配置適當之資源？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
4. 資訊及資通系統之盤點及風險評估	4.1 是否建立資訊及資通系統資產目錄，並隨時維護更新？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	4.2 各項資產是否有明確之管理者及使用者？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	4.3 是否定有資訊、資通系統分級與處理之相關規範？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	4.4 是否進行資訊、資通系統之風險評估，並採取相應之控制措施？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
5. 資通安全管理措施之實施情況	5.1 人員進入重要實體區域是否訂有安全控制措施？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	5.2 重要實體區域的進出權利是否定期審查並更新？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
5.3	電腦機房及重要地區，對於進出人員是否作必要之限制及監督其活動？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
5.4	電腦機房操作人員是否隨時注意環境監控系統，掌握機房溫度及溼度狀況？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
5.5	各項安全設備是否定期檢查？同仁有否施予適當的安全設備使用訓練？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
5.6	第三方支援服務人員進入重要實體區域是否經過授權並陪同或監視？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
5.7	重要資訊處理設施是否有特別保護機制？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
5.8	重要資通設備之設置地點是否檢查及評估火、煙、水、震動、化學效應、電力供應、電磁幅射或民間暴動等可能對設備之危害？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
5.9	電源之供應及備援電源是否作安全上考量？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
5.10	通訊線路及電纜線是否作安全保護措施？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
5.11	設備是否定期維護，以確保其可用性及完整性？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
5.12	設備送場外維修，對於儲存資訊是否訂有安全保護措施？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
5.13	可攜式的電腦設備是否訂有嚴謹的保護措施(如設通行碼、檔案加密、專人看管)？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
5.14	設備報廢前是否先將機密性、敏感性資料及版權軟體移除或覆寫？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
5.15	公文及儲存媒體在不使用或不在班時是否妥為存放？機密性、敏感性資訊是否妥為收存？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
5.16	系統開發測試及正式作業是否區隔在不同之作業環境？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
5.17	是否全面使用防毒軟體並即時更新病毒碼？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
5.18	是否定期對電腦系統及資料儲存媒體進行病毒掃瞄？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
5.19	是否定期執行各項系統漏洞修補程式？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
5.20	是否要求電子郵件附件及下載檔案在使用前需檢查有無惡意軟體(含病毒、木馬或後門等程式)？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
5.21	重要的資料及軟體是否定期作備份處理？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
5.22	備份資料是否定期回復測試，以確保備份資料之有效性？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
5.23	對於敏感性、機密性資訊之傳送是否採取資料加密等保護措施？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
	5.24 是否訂定可攜式媒體(磁帶、磁片、光碟片、隨身碟及報表等)管理程序？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	5.25 是否訂定使用者存取權限註冊及註銷之作業程序？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	5.26 使用者存取權限是否定期檢查(建議每六個月一次)或在權限變更後立即複檢？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	5.27 通行碼長度是否超過 6 個字元(建議以 8 位或以上為宜)？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	5.28 通行碼是否規定需有大小寫字母、數字及符號組成？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	5.29 是否依網路型態(Internet、Intranet、Extranet)訂定適當的存取權限管理方式？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	5.30 對於重要特定網路服務，是否作必要之控制措施，如身份鑑別、資料加密或網路連線控制？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	5.31 是否訂定行動式電腦設備之管理政策(如實體保護、存取控制、使用之密碼技術、備份及病毒防治要求)？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	5.32 重要系統是否使用憑證作為身份認證？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	5.33 系統變更後其相關控管措施與程序是否檢查仍然有效？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	5.34 是否可及時取得系統弱點的資訊並作風險評估及採取必要措施？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
6.訂定資通安全事件通報及應變之程序及機制	5.1 是否建立資通安全事件發生之通報應變程序？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	5.2 機關同仁及外部使用者是否知悉資通安全事件通報應變程序並依規定辦理？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	5.3 是否留有資通安全事件處理之記錄文件，記錄中並有改善措施？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
7.定期辦理資通安全認知宣導及教育訓練	7.1 是否定期辦理資通安全認知宣導？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	7.2 是否對同仁進行資安評量？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	7.3 同仁是否依層級定期舉辦資通安全教育訓練？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	7.4 同仁是否瞭解單位之資通安全政策、目標及應負之責任？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
8.資通安全維護計畫實施情形之精進改善機	8.1 是否設有稽核機制？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	8.2 是否定有年度稽核計畫？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	8.3 是否定期執行稽核？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
制	8.4 是否改正稽核之缺失？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
9.資通安全維護計畫及實施情形之績效管考機制	10.1 是否訂定安全維護計畫持續改善機制？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	10.2 是否追蹤過去缺失之改善情形？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	10.3 是否定期召開持續改善之管理審查會議？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

註：陳核層級請學校依需求調整

承辦人：

單位主管：

機關首長：

## 10. 年度資通安全教育訓練計畫

### 臺北市立中山女子高級中學 年度資通安全教育訓練計畫

#### 壹、依據

臺北市立中山女子高級中學之資通安全維護計畫辦理。

#### 貳、目的

為精進所屬人員之資通安全意識及職能，並敦促該等人員得以瞭解並執行之資通安全維護計畫，以強化本校之資通安全管理能量，爰要求該等人員應接受資通安全之教育訓練，爰擬定本教育訓練計畫。

#### 參、實施範圍

本機關所屬人員：

人員類別	人數
資通安全人員	
一般人員	
主管人員	
共計	

#### 肆、訓練項目

人員類別	訓練課程	時數
資通安全人員		
資訊人員		
一般人員		
主管人員		

#### 伍、訓練期程

由各學校自行排定教育訓練期程。

## 陸、訓練方式



11. 資通安全認知宣導及教育訓練簽到表

臺北市立中山女子高級中學  
資通安全認知宣導及教育訓練簽到表

編號：

課程名稱：

時 間：

地 點：

單 位	職 稱	姓 名	簽 名

## 12. 資通安全維護計畫實施情形

### 臺北市立中山女子高級中學

### 資通安全維護計畫實施情形

編號：

本校經主管機關核定後本校之資通安全責任等級為 D 級，依資通安全管理法第 12 條之規定，向上級機關提出本年度資通安全維護計畫實施情形、執行成果及相關說明如下表所示：

實施項目	實施內容	實施情形說明
1. 資通業務及其重要性	1.1 資通業務及重要性盤點	
2. 資通安全政策及目標	2.1 資通安全政策訂定及核定	
	2.2 資通安全目標之訂定	
	2.3 資通安全政策及目標宣導	
	2.4 資通安全政策及目標定期檢視	
3. 設置資通安全推動代表	3.1 設定資通安全管理代表	
	3.2 設置資通安全推動小組	
4. 人力及經費之配置	4.1 人員配置	
	4.2 經費之配置	
5. 資訊及資通系統之盤點及資通系統、相關資產之標示	5.1 資訊及資通系統之盤點	
	5.2 資通安全責任等級分級	
6. 資通安全風險評估	6.1 資通安全風險評估	
	6.2 資通安全風險之因應	
7. 資通安全防護及控制措施	7.1 資訊及資通系統之保管	
	7.2 存取控制與加密機制管理	
	7.3 作業及通訊安全管理	

	7.4 資通安全防護設備	
8. 資通安全事件通報、應變及演練	8.1 訂定資通安全事件通報、應變及演練相關機制	
	8.2 資通安全事件通報、應變及演練	
9. 資通安全情資之評估及因應機制	9.1 資通安全情資之分類評估	
	9.2 資通安全情資之因應措施	
10. 資通系統或服務委外辦理之管理	10.1 選任受託者應注意事項	
	10.2 監督受託者資通安全維護情形應注意事項	
11. 資通安全教育訓練	11.1 資通安全教育訓練要求	
	11.2 辦理資通安全教育訓練	
12. 公務機關所屬人員辦理業務涉及資通安全事項之考核機制	12.1 訂定考核機制並進行考核	
13. 資通安全維護計畫及實施情形之持續精進及績效管理機制	13.1 資通安全維護計畫之實施	
	13.2 資通安全維護計畫實施情形之檢核機制	
	13.3 資通安全維護計畫之持續精進及績效管理	
其他說明		

註：陳核層級請學校依需求調整

承辦人：

單位主管：

機關首長：

### 13. 審查結果及改善報告

## 臺北市立中山女子高級中學 審查結果及改善報告

範圍				
日期				
審查日期				
項目				
編號	建議或待改善項目	改善措施	改善期程規劃	相關佐證資料
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				

#### 14. 改善績效追蹤報告

### 臺北市立中山女子高級中學 改善績效追蹤報告

編號：

製表日期： 年 月 日

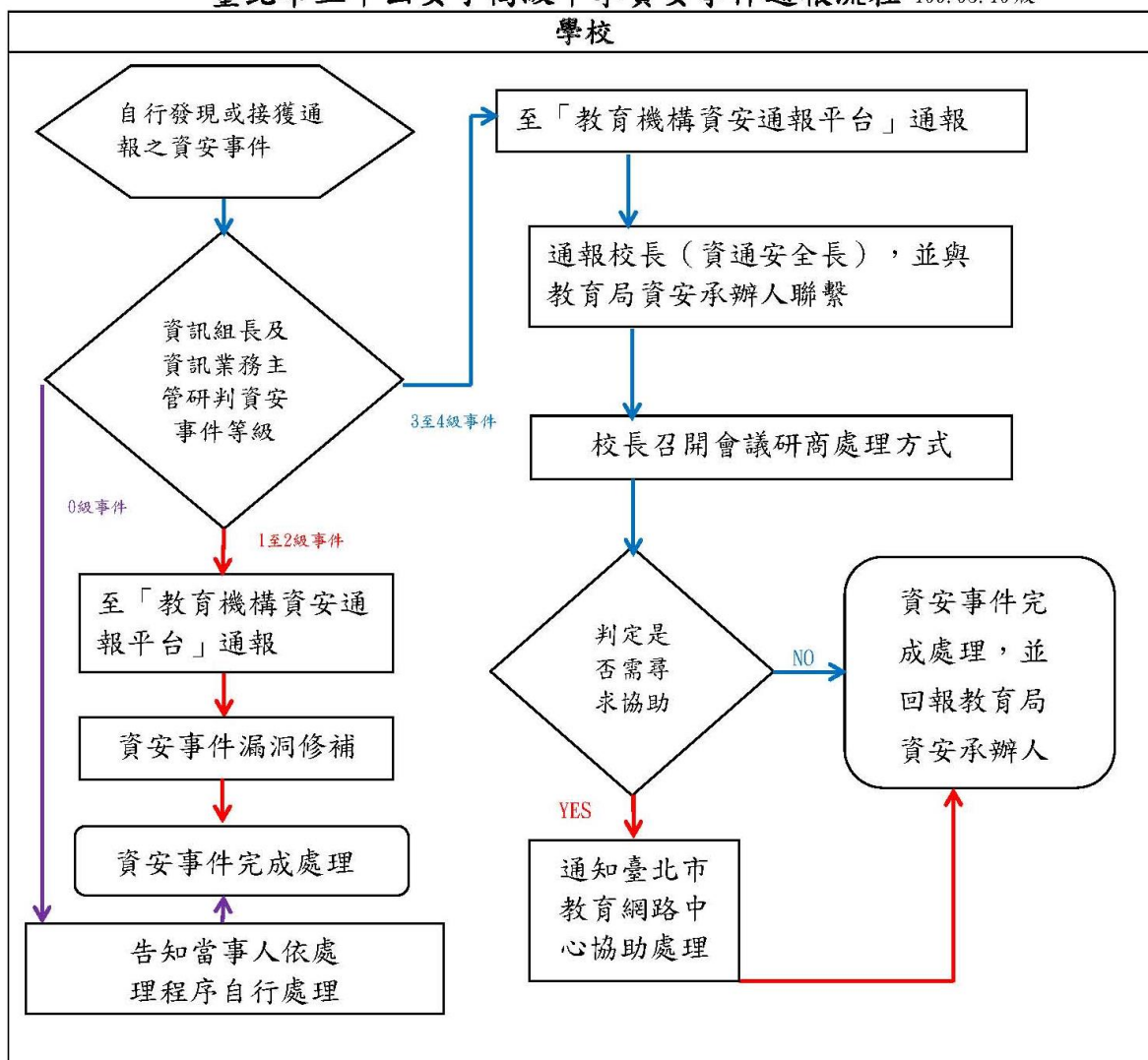
審查發現			
審查日期		受審查單位	
審查區域			
建議或待改善項目與內容			
影響範圍評估			
發生原因分析			
改善措施成效追蹤			
改善措施		預計成效	執行情況
管理面			
技術面			
人力面			
資源面			
作業程序			
其他			
績效管考			

改善措施確認			
經費需求或編列執行金額		經費執行情形	
預定完成日期		實際完成日期	
完成進度或情形說明			
改善成效考核			
後續成效追蹤			
資通安全推動小組承辦人員		資通安全長	

註：陳核層級請學校依需求調整

## 15. 資安通報流程

臺北市立中山女子高級中學資安事件通報流程 109.03.10 版



教育機構資安通報平台網址：<https://info.cert.tanet.edu.tw/prog/index.php>

人員	姓名	聯絡電話
系統管理師	黃建庭	25073148轉283
資訊媒體組長	韓君尹	25073148轉282
資訊單位主管	趙威寧	25073148轉281
校長（資通安全長）	吳麗卿	25073148轉211
教育局資安承辦人	陳伯豪	02-27208889/1999轉1231
臺北市教育網路中心	駐點人員	02-27223004
臺灣學術網路危機處理中心(TACERT)	教育機構資安通報應變小組	07-5250211