臺北市立景美女子高級中學

資通安全維護計畫

第 1.1 版

生效日期：108 年 1 月 18 日

文件制／修訂紀錄表

文件版本	生效日期	制／修定摘要說明	承辦單位	承辦人
V1.0	108 年 1 月 11 日	初次建立	資訊教育科	康睿宸/陳柏翰
V1.1	108 年 1 月 18 日	景美女中資通安全維護計畫	資訊組	孫晉忻

壹、 資通安全推動小組成員及分工表

臺北市立景美女子高級中學資通安全推動小組成員及分工表

單位職級	名稱	職掌事項	分機	備註 （代理人）
校長		督導本校資訊安全事宜	201	教務主任
圖書館主任		規畫本校資訊安全架構藍圖	225	資訊組長
總務主任		規畫本校整體環境安全架構	213	事務組長
資訊組長		建置管理本校資訊安全系統及負責資安事件通報	251	資訊組幹事
事務組長		維護管理本校電力及通訊環境	214	
教師		協助管理本校資訊安全環境	251	

貳、 實施計畫

一、 依據及目的

本計畫依據資通安全管理法第 10 條及施行細則第 6 條訂定。

本計畫依據下列法規訂定：資通安全管理法第 10 條及其施行細則第 6 條。

二、 適用範圍

本計畫適用範圍涵蓋本校。

三、 核心業務及重要性

（一）核心業務及重要性：

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
教務相關： 學生資料、課程規畫、成績計算、修課安排	無(系統已集中至教育局統一管理)	為本校依組織法執掌，足認為重要者	無	無
學務相關： 學生出缺、學生獎懲	無(系統已集中至教育局統一管理)	為本校依組織法執掌，足認為重要者	無	無
人事相關 教職員基本資料	無(系統已集中至臺北市政府統一管理)	為本校依組織法執掌，足認為重要者	無	無

（二）非核心業務及說明：

本校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
學校網站	一般民眾無法瀏覽本校訊息內容	24 小時
DNS	網際網路無法查詢本校相關網站內容	24 小時
DHCP	校內電腦無法即時取得網址連上網路	24 小時
AD	校內教職員無法登入專用無線網路	24 小時
防毒	學校電腦無法由校內取得最新病毒碼	72 小時
調代課系統	無法透過資訊系統列印調課資料	72 小時
物品請購列印	無法透過資訊系統列印請購單	72 小時
健康中心掛號系統	無法透過資訊系統登記學生校內傷病狀況	48 小時
線上課程平台	無法透過網路存取教材	72 小時
網路相簿	無法透過網路瀏覽學校活動照片	96 小時
影音資料平台	無法透過網路瀏覽學校活動影片	96 小時

四、 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，防止資訊或資通業務受未經授權之存取、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，以供本校全體教職員共同遵循：

1. 定期因應內外在資通安全情勢變化，檢討資通安全風險管理之有效性。
2. 針對各資料的機密性與完整性應妥善保護，避免資料遭竄改。
3. 建立資通安全防護，包括全校對外防火牆、校內電腦安裝防毒軟體。
4. 辦理資通安全教育訓練(教職員每人每年 3 小時以上之一般資通安全教育訓練，學生則於資訊課程時融入資訊安全教學)，提升全校資通安全意識。
5. 管制校內帳號，禁止一般使用者多人共用同一帳號。
6. 落實資通安全通報機制。

(二) 資通安全目標

1. 資安事件發生，於規定的時間完成通報、應變及復原作業。
2. 配合上級機關辦理之電子郵件社交工程演練郵件。
3. 屬於學校之資訊設備，全年度資安通報平臺之資安事件等級第 1、2 級發生件數少於 3 件(含)以下，等級第 3、4 級不得發生。
4. 屬於教師或學生個人攜帶至本校之資訊設備，全年度資安通報平臺之資安事件等級第 1、2 級發生件數少於 8 件(含)以下，等級第 3、4 級不得發生。
5. 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。

(三) 資通安全政策及目標核定程序

資通安全政策由圖書館資訊組簽陳至資通安全長，由校務會議通過後實施。

(四) 資通安全政策及目標之宣導

1. 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，向校內所有人員進行宣導，並檢視執行成效。
2. 本校應每年向利害關係人(例如委外廠商提供服務(非本校維運自行或委由廠商建置之資通系統))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校內行政會報中檢討其適切性。

五、 資通安全推動組織

(一) 資通安全長

依本法第 11 條之規定，本校訂定校長為資通安全長，負責督導本校資通安全相關事項，其任務包括：

1. 資通安全管理政策及目標之核定、核轉及督導。
2. 資通安全責任之分配及協調。

3. 資通安全資源分配。
4. 資通安全防護措施之監督。
5. 資通安全事件之檢討及監督。
6. 資通安全相關規章與程序、制度文件核定。
7. 資通安全管理年度工作計畫之核定。
8. 資通安全相關工作事項督導及績效管理。
9. 其他資通安全事項之核定。

（二）資通安全推動小組

1. 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業務部門主管/副主管以上之人員代表成立資通安全推動小組 ，其任務包括：

(1) 校內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。

2. 分工及職掌

本校之資通安全推動小組依下列工作進行責任分工，並適時更新之 ：

(1) 策略規劃(資通安全長與圖書館主任)：
   i. 資通安全政策及目標之研議。
   ii. 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。
   iii. 依據資通安全目標擬定本校年度工作計畫。
   iv. 傳達本校資通安全政策與目標。
   v. 其他資通安全事項之規劃。

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

(3) 績效管理(人事單位或由資通安全長指派)：
   i. 辦理資通安全內部稽核。
   ii. 每年 10 月前召開資通安全管理審查會議，提報資通安全事項執行情形，以利教育部稽核審查使用。

六、 專職人力及經費配置

（一）人力及資源配置

1. 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兼辦人員1人。本校現有資通安全專責人員名單及職掌應列冊，並適時更新 。

   (1) 負責資通系統分級、防護基準及教育訓練業務之推動。

   (2) 負責資通安全防護設施建置及資通安全事件通報及應變業務之推動。

2. 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，並提升校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。

3. 本校負責重要資通設備之管理、維護、設計及操作之人員，應妥適分工，分散權責，若負有機密維護責任者，應簽屬書面約定 ，並視需要實施人員輪調，建立人力備援制度。

4. 本校之首長及各級業務主管人員，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。

5. 專業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）經費配置

1. 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 。

2. 各單位於規劃建置資通系統建置時，應一併規劃資通系統之資安防護需求，並於整體預算中合理分配資通安全預算所佔之比例。

3. 各單位如有資通安全資源之需求，應配合校內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(資通安全管理代表)核定後，進行相關之建置。

4. 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。

七、 資訊及資通系統之盤點

（一）資訊及資通系統盤點

1. 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，分別為資訊資產、軟體資產、實體資產、支援服務資產等。

2. 資訊及資通系統資產項目如下：

資產類別	資產項目
資訊資產	(1)書面管理文件：各項教育局系統(學生證刷卡、校務系統)之操作手冊，以

(未含有個資)	及校內非核心系統之操作說明。 (2)書面紀錄：設備借用記錄、本計畫附件之資通安全檢核表格與稽核記錄。
軟體資產	(1)系統軟體：臺北市高中課程與教學工作圈網站系統。 (2)套裝軟體：智慧大師數位教學平台、行動學習跨平台學習系統、FortiGate 240D 防火牆升級軟體、igt plus 雲端社群播客系統、GIS 應用軟體、臺灣地形 DTM 圖資、臺灣電子地圖圖資、全球電子地圖圖資。 (3)授權軟體：NOD32 防毒軟體、臺灣衛星影像圖資。
硬體資產	(1)個人電腦(含筆記型電腦與平板)：數量以校內財產管理系統記錄為準。 (2)伺服器與網路儲存設備：數量以校內財產管理系統記錄為準。 (3)網路通訊設備：數量以校內財產管理系統記錄為準。 (4)影印設備：數量以總務處租用影印機合約為準。 (5)不斷電系統：數量以校內財產管理系統記錄為準。
服務資產	(1)中華電信網路專線。 (2)市電系統。 (3)影印機租賃維護服務。 (4)校內資訊設備保固年限內服務(依各項設備採購合約為準)。
人員資產	(1)內部同仁：資訊組同仁。
個資資產	(1)檔案形式個資：個人電腦中或主機內個人資料檔案等。

3. 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。

（二）機關資通安全責任等級分級

本校自行辦理資通業務，未維運自行或委外開發之資通系統者，其資通安全責任等級為 D 級。

八、 資通安全風險評估

（一）本校應每年針對資訊及資通設備資產進行風險評估。

（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。

（三）本校每年依據資通安全責任等級分級辦法之規定，分別就機密性、完整性、可用性、法律遵循性等構面評估。

九、 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，全校之防護及控制措施詳如本校資通安全維護計畫，採行相關之防護及控制措施如下:

（一）資訊及資通設備之管理

1. 資訊及資通設備之使用

(1) 本校教職員使用資訊及資通設備須遵守設備管理相關規範。

(2) 本校教職員使用資訊及資通設備時，應留意其資通安全要求事項，並負對應之責任。

(3) 本校教職員使用資訊及資通設備後，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。

(4) 本校教職員使用本校之資訊及資通設備，應確實遵守本校之相關資通安全要求，且未經授權不得任意複製資訊。

(5) 對於資訊及資通設備，宜識別並以文件記錄及實作可被接受使用之規則。

(二) 存取控制與加密機制管理

1. 網路安全控管

(1) 本校之防火牆由資訊組自行管理，區域劃分如下：

I. 外部網路：對外網路區域，連接外部廣網路(Wide Area Network, WAN)。

II. 內部區域網路 (Local Area Network, LAN) ：學校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) 本校應定期檢視防火牆政策是否適當。

(4) 本校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) 對網路系統管理人員或資通安全主管人員的操作，均應建立詳細的紀錄。並應定期檢視網路安全相關設備設定規則與其日誌紀錄，並檢討執行情形。

(6) 使用者應依合法並符合本校規定之方式存取網路服務。

(7) 網域名稱系統(DNS)防護

I. 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。

II. 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。

III. 校內主機位置查詢應以本校內部 DNS 伺服器或安全認證 DNS 伺服器為主。

(8) 無線網路防護

I. 機密資料原則不得透過無線網路及設備存取、處理或傳送。

II. 無線設備應具備安全防護機制以降低阻斷式攻擊風險，且無線網路之安全防護機制應包含外來威脅及預防內部潛在干擾。

III. 行動通訊或紅外線傳輸等無線設備原則不得攜入涉及或處理機密資料之區域。

IV. 用以儲存或傳輸資料且具無線傳輸功能之校內資訊設備，應安裝防毒軟體，並定期更新病毒碼。

2. 資通業務權限管理

(1) 本校之資通業務應設置通行碼管理，通行碼之要求需滿足：

I. 通行碼長度 6 碼以上。

II. 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。

III. 使用者應定期更換通行碼。

(2) 使用者辦理資通業務前應經授權，並使用唯一之使用者 ID，除有特殊營運或作業必要經核准並紀錄外，不得共用 ID。

(3) 使用者無繼續辦理資通業務時，應立即停用或移除使用者 ID，資通業務管理者應定期清查使用者之權限。

3. 特權帳號之存取管理

(1) 資通設備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) 資通設備之特權帳號不得共用。

(3) 對於特權帳號，宜指派與該使用者日常公務使用之不同使用者 ID。

(4) 資通設備之特權帳號應妥善管理，並應留存特殊權限帳號之使用軌跡。

(5) 資通設備之管理者每季應清查系統特權帳號並劃定特權帳號逾期之處理方式。

4. 加密管理

(1) 本校之機密資訊於儲存或傳輸時應進行加密。

(2) 本校之加密保護措施應遵守下列規定：

I. 應落實使用者更新加密裝置並備份金鑰。

II. 應避免留存解密資訊。

III. 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

1. 防範惡意軟體之控制措施

(1) 本校之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) 管理者並應每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。

(4) 使用者應定期進行作業系統及軟體更新，以避免惡意軟體利用系統或軟體漏洞進行攻擊。

2. 遠距工作之安全措施

(1) 本校資通業務之操作及維護以現場操作為原則，避免使用遠距工作，如有緊急需求時，應申請並經資通安全推動小組同意後始可開通。

(2) 資通安全推動小組應定期審查已授權之遠距工作需求是否適當。

(3) 針對遠距工作之連線應採適當之防護措施(並包含伺服器端之集中過濾機制檢查使用者之授權)，並且記錄其登入情形。

I. 提供適當通訊設備，並指定遠端存取之方式。

II. 提供虛擬桌面存取，以防止於私有設備上處理及儲存資訊。

III. 遠距工作終止時之存取權限撤銷，並應返還相關設備。

3. 電子郵件安全管理

(1) 使用者使用電子郵件時應提高警覺，避免讀取來歷不明之郵件或含有巨集檔案之郵件。

(2) 原則不得電子郵件傳送機密性或敏感性之資料，如有業務需求者應依相關規定進行加密或其他之防護措施。

(3) 使用者不得利用本校所提供電子郵件服務從事侵害他人權益或違法之行為。

(4) 使用者應確保電子郵件傳送時之傳遞正確性。

(5) 本校應配合上級機關辦理電子郵件社交工程演練，並檢討執行情形。

4. 確保實體與環境安全措施

(1) 通訊機房(機櫃)之管理

I. 通訊機房(機櫃)應進行實體隔離。

II. 校內人員或來訪人員應申請及授權後方可進入通訊機房。

III. 人員進入管制區應配載身分識別之標示，並隨時注意身分不明或可疑人員。

IV. 僅於必要時，得准許外部支援人員進入通訊機房。

(2) 通訊機房(機櫃)之環境控制

I. 通訊機房(機櫃)之空調、電力得建立備援措施。

II. 通訊機房(機櫃)得安裝之安全偵測及防護措施，包括火災警報設備、入侵者偵測系統，以減少環境不安全引發之危險。

III. 各項安全設備應定期執行檢查、維修，並應定時針對設備之管理者進行適當之安全設備使用訓練。

(3) 辦公室區域之實體與環境安全措施

I. 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。

II. 文件及可移除式媒體在不使用或不上班時，應存放在櫃子內。

III. 機密性及敏感性資訊，不使用或下班時應該上鎖。

IV. 機密資訊或處理機密資訊之資通業務應避免存放或設置於公眾可接觸之場域。

V. 顯示存放機密資訊或具處理機密資訊之資通業務地點之通訊錄及內部人員電話簿，不宜讓未經授權者輕易取得。

VI. 資訊或資通業務相關設備，未經管理人授權，不得被帶離辦公室。

5. 資料備份

(1) 重要資料應進行資料備份，其備份之頻率應滿足復原時間點目標之要求。

(2) 本校應每季確認重要資料備份之有效性。且測試該等資料備份時，宜於專屬之測試系統上執行，而非直接於覆寫回原資通設備。

(3) 敏感或機密性資訊之備份應加密保護。

6. 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) 資訊如以實體儲存媒體方式傳送，應留意實體儲存媒體之包裝，選擇適當人員進行傳送，並應保留傳送及簽收之記錄。

(3) 為降低媒體劣化之風險，宜於所儲存資訊因相關原因而無法讀取前，將其傳送至其他媒體。

(4) 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。

7. 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。

(2) 禁止私自安裝點對點檔案分享軟體及未經合法授權軟體。

(3) 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。

(4) 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。

(5) 下班時應關閉電腦及螢幕電源。

(6) 如發現資安問題，應主動循校內之通報程序通報。

(7) 支援資訊作業的相關設施如影印機、傳真機等，應安置在適當地點，以降低未經授權之人員進入管制區的風險，及減少敏感性資訊遭破解或洩漏之機會。

8. 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

(四) 資通安全防護設備

1. 本校應建置防毒軟體、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。

十、 資通安全事件通報、應變及演練相關機制

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、應變及演練相關機制，詳**資通安全事件通報應變程序**。

十一、 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、本校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。

1. 資通安全情資之分類評估

本校接受資通安全情資後，應指定資通安全專責(兼職)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：

(1) 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。

(2) 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。

(3) 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。

(4) 涉及核心業務、核心資通系統之情資

資通安全情資之內容如包含本校內部之核心業務資訊、核心資通系統、涉及關鍵基礎設施維運之核心業務或核心資通系統之運作等內容，屬涉及核心業務、核心資通系統之情資。

2. 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。

(1) 資通安全相關之訊息情資

由資通安全推動小組(資訊小組)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。

(2) 入侵攻擊情資

由資通安全專責(兼職)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。

3. 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。

4. 涉及核心業務、核心資通系統之情資

資通安全推動小組應就涉及核心業務、核心資通系統之情資評估其是否對於本校之運作產生影響，並依據資通安全維護計畫採行相應之風險管理機制。

十二、 資通系統或服務委外辦理之管理

本校(目前)無委外辦理資通系統之建置、維運或資通服務之提供，若另有需求時得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。

十三、 資通安全教育訓練

1. 資通安全教育訓練要求
   (1) 資安兼任或資訊人員每人每年至少接受 6 小時以上之資安專業課程訓練。
   (2) 本校之一般教職員與主管，每人每年接受 3 小時以上之一般資通安全教育訓練。
2. 資通安全教育訓練辦理方式
   (1) 承辦單位應於每**學**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，以建立員工資通安全認知，提升本校資通安全水準，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：
      I. 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)。
      II. 資通安全法令規定。
      III. 資通安全作業內容。
      IV. 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。
   (4) 資通安全教育及訓練之政策，除適用本校教職員外，對學校外部的使用者，亦應一體適用。

十四、 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學校公務人員平時獎懲標準表，及臺北市立高級中等學校組織規程準則規定辦理之。

十五、 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

1. 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。

2. 資通安全維護計畫實施情形之稽核機制
   (1) 稽核機制之實施
      I. 資通安全推動小組應定期(至少每年一次)或於系統重大變更或組織改造後執行一次內部稽核作業，以確認人員是否遵循本校規範程序要求，並有效實作及維持管理制度。

II. 辦理稽核前資通安全推動小組應擬定資通安全稽核計畫並安排稽核成員，稽核計畫應包括稽核之依據與目的、期間、重點領域、稽核小組組成方式、保密義務、稽核方式、基準與項目及受稽單位協助事項，並應將前次稽核之結果納入稽核範圍。

III. 辦理稽核時，資通安全推動小組應於執行稽核前 14 日，通知受稽核單位，並將稽核期程、稽核項目紀錄表 10 及稽核流程等相關資訊提供受稽單位。

IV. 本校之稽核人員不得稽核自身經辦業務，以確保稽核過程之客觀性及公平性；另，於執行稽核時，應填具稽核項目紀錄表，待稽核結束後，應將稽核項目紀錄表內容彙整至稽核結果及改善報告中，並提供給受稽單位填寫辦理情形。

V. 稽核結果應對相關管理階層(含資安長)報告，並留存稽核過程之相關紀錄以作為資通安全稽核計畫及稽核事件之證據。

VI. 稽核人員於執行稽核時，應至少執行一項特定之稽核項目（如是否瞭解資通安全政策及應負之資安責任、是否訂定人員之資通安全作業程序與權責、是否定期更改密碼)。

(2) 稽核改善報告

I. 受稽單位於稽核實施後發現有缺失或待改善項目者，應對缺失或待改善之項目研議改善措施、改善進度規劃，並落實執行。

II. 受稽單位於稽核實施後發現有缺失或待改善者，應判定其發生之原因，並評估是否有其類似之缺失或待改善之項目存在。

III. 受稽單位於判定缺失或待改善之原因後，應據此提出並執行相關之改善措施及改善進度規劃，必要時得考量對現行資通安全管理制度或相關文件進行變更。

IV. 學校應定期審查受稽單位缺失或待改善項目所採取之改善措施、改善進度規劃及佐證資料之有效性。

V. 受稽單位於執行改善措施時，應留存相關之執行紀錄，並填寫稽核結果及改善報告。

3. 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於每年 10 月底前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：

I. 過往管理審查議案之處理狀態。

II. 與資通安全管理業務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。

III. 資通安全維護計畫內容之適切性。

IV. 資通安全績效之回饋，包括：

i. 資通安全政策及目標之實施情形。

ii. 資通安全人力及資源之配置之實施情形。

iii. 資通安全防護及控制措施之實施情形。

iv. 內外部稽核結果。

v. 不符合項目及矯正措施。

V. 風險評鑑結果及風險處理計畫執行進度。

VI. 重大資通安全事件之處理及改善情形。

VII. 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。

十六、 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 11 月中向臺北市政府教育局資訊教育科，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。

十七、 相關程序及表單(如附件)

1. 資通安全推動小組成員及分工表。
2. 資通安全保密同意書。
3. 資通安全需求申請單。
4. 資訊及資通資產清冊。
5. 風險評估表。
6. 風險類型暨風險對策參考表。
7. 資通安全事件通報及應變程序。
8. 管制區域人員進出登記表。
9. 委外廠商執行人員保密切結書。
10. 委外廠商執行人員保密同意書。
11. 委外廠商保密切結書。
12. 年度資通安全教育訓練計畫。
13. 資通安全認知宣導及教育訓練簽到表。
14. 資通安全維護計畫實施情形。
15. 年度資通安全稽核計畫
16. 稽核項目紀錄表。
17. 稽核委員聘任同意暨保密切結書。
18. 稽核結果及改善報告。
19. 改善績效追蹤報告。

臺北市立景美女子高級中學資通安全維護計畫附件

目　次

臺北市立景美女子高級中學資通安全維護計畫附件.....17
一、　臺北市立景美女子高級中學資通安全推動小組成員及分工表.....18
二、　臺北市立景美女子高級中學資通安全保密同意書.....19
三、　臺北市立景美女子高級中學資通安全需求申請單.....20
四、　臺北市立景美女子高級中學資訊及資通資產清冊.....21
五、　臺北市立景美女子高級中學風險評估表.....22
六、　臺北市立景美女子高級中學風險類型暨風險對策參考表.....23
七、　臺北市立景美女子高級中學管制區域人員進出登記表.....25
八、　臺北市立景美女子高級中學委外廠商執行人員保密切結書.....26
九、　臺北市立景美女子高級中學委外廠商執行人員保密同意書.....28
十、　臺北市立景美女子高級中學委外廠商保密切結書.....29
十一、　臺北市立景美女子高級中學年度資通安全教育訓練計畫.....30
十二、　臺北市立景美女子高級中學資通安全認知宣導及教育訓練簽到表.....31
十三、　臺北市立景美女子高級中學資通安全維護計畫實施情形.....32
十四、　臺北市立景美女子高級中學年度資通安全稽核計畫.....34
十五、　臺北市立景美女子高級中學稽核項目紀錄表.....35
十六、　臺北市立景美女子高級中學稽核委員聘任同意暨保密切結書.....36
十七、　臺北市立景美女子高級中學稽核結果及改善報告.....38
十八、　臺北市立景美女子高級中學改善績效追蹤報告.....39

一、臺北市立景美女子高級中學資通安全推動小組成員及分工表

臺北市立景美女子高級中學資通安全推動小組成員及分工表

單位職級	名稱	職掌事項	分機	備註 (代理人)
校長		督導本校資訊安全事宜	201	教務主任
圖書館主任		規畫本校資訊安全架構藍圖	225	資訊組長
總務主任		規畫本校整體環境安全架構	213	事務組長
資訊組長		建置管理本校資訊安全系統及負責資安事件通報	251	資訊組幹事
事務組長		維護管理本校電力及通訊環境	214	
教師		協助管理本校資訊安全環境	251	

承辦人：　　單位業務主管：　　資通安全長：

二、臺北市立景美女子高級中學資通安全保密同意書

臺北市立景美女子高級中學資通安全保密同意書

立同意書人＿＿＿＿＿＿＿＿於民國＿＿年＿＿月＿＿日起於臺北市立景美女子高級中學任職，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：臺北市立景美女子高級中學

機關首長：＿＿＿＿＿＿＿＿

中　華　民　國　　年　　月　　日

三、臺北市立景美女子高級中學資通安全需求申請單

臺北市立景美女子高級中學資通安全需求申請單

申請單位		申請日期	年　　月　　日
申請項目	□軟體 □硬體 □其他	項目名稱	
申請數量		需用日期	年　　月　　日
申請類別	□新購 □升級	使用設備	□主機 □使用者電腦 □其他
安裝單位		安裝位置	
用途說明			
申請人		申請單位主管	
資通安全推動小組	□可採購 □不可採購	說明：	

承辦人員		單位業務主管		資通安全長	

四、臺北市立景美女子高級中學資訊及資通資產清冊

資產編號	資產名稱	資產類別	擁有者	管理者	使用者	存放位置	防護需求
例:107-IF-01	行政業務檔案	IF	資訊組	資訊組	資訊組	教務處	普

資產類別：IF(資訊) 、SW(軟體)、HW(硬體)、SE(服務)、PE(人員)、PI(個

五、臺北市立景美女子高級中學風險評估表

臺北市立景美女子高級中學風險評估表

製表日期：　　年　　月　　日

風險列表	風險評估				發生可能性	影響後果	風險等級	管理機制
	機密性	完整性	可用性	法律遵循性				
電力中斷		V	V					
網路設備損壞		V	V					
電腦系統損壞		V	V					
資料損壞	V	V	V					
內部人員操作不當	V	V	V	V				
外部入侵	V			V				

承辦人員：　　單位主管：　　資通安全長：

六、臺北市立景美女子高級中學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（建議）
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秘與透過具有憑證檢驗功能的身份驗證機制
	802.1X 攻擊	●檢測 X.509 憑證是否有效。 ●指定合法驗證者（RADIUS 伺服器）之一般名稱值。 ●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。
	資料連結層攻擊	●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。 ●關閉未用到的乙太網路連接埠，並歸類在隔離的 VLAN 外。
	網路層與應用層的攻擊	●如果沒有明確要求，應關閉 IPv6。 ●取消對 ICMP 重導向的支援。 ●停用群播名稱解析及 Windows 的 NetBIOS over TCP/IP 通訊。
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攻擊	隨時修補存在攻擊表面的已知攻擊。
	透過傳輸與遠端維護操作之服務進行攻擊	●停用無加密傳輸安全性的 Telnet、FTP、SNMP、VNC 等。 ●遠端操作維護須透過安全的身份驗證連接。 ●建構封閉的管理網路。
	SSH 伺服器攻擊	●強制使用 2.0 版本的協定，禁止向下相容特性。 ●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。
	DNS 伺服器攻擊	●停止支援來自不受信任來源的遞回查詢。 ●確保區域檔案不含多餘或敏感資訊。
	Kerberos 伺服器攻擊	●停止支援較弱的 HMAC 演算法。 ●在微軟環境中，可考慮強制使用最高的網域功能等級。
VPN 服務	VPN 攻擊	●確認 VPN 伺服器的維護作業，並修補到最新版本。 ●強制使用 AH 和 ESP 功能身份驗證及機密性服務。 ●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。 ●過濾內連的 VPN 流量，以便在發生入侵事件時限制網路存取。 ●定期稽核已授權的 VPN 使用者，以防有偽冒的帳號。
網頁應用程式框架	Web 應用伺服 器攻擊	●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。 ●禁止將管理介面或特權功能公開在不受信任的網路上。 ●在可行的情況下，將開放網頁應用程式和管理功能隔離。
資料儲存機制	資料庫攻擊	●限制資料服務只與經授權的對象往來，特別是雲端環境中。 ●避免使用不支援身份驗證的儲存系統和協定。 ●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料，例如密碼、身份憑證。 ●確保密碼強度。 ●限制只有受信任的網路才能存取管理服務。 ●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。
參考來源：資安風險評估指南，第三版，Chris McNab，江湖海譯		

七、臺北市立景美女子高級中學管制區域人員進出登記表

製表日期：　　年　　月　　日

編號	單 位 姓 名	陪同人員	日期	進出時間	事由	進出設備 (物品)
1	單 位： 姓 名：			進去： 離去：		
2	單 位： 姓 名：			進去： 離去：		
3	單 位： 姓 名：			進去： 離去：		
4	單 位： 姓 名：			進去： 離去：		
5	單 位： 姓 名：			進去： 離去：		
6	單 位： 姓 名：			進去： 離去：		
7	單 位： 姓 名：			進去： 離去：		
8	單 位： 姓 名：			進去： 離去：		
9	單 位： 姓 名：			進去： 離去：		
10	單 位： 姓 名：			進去： 離去：		

承辦人員：　　單位主管：　　資通安全長：

八、臺北市立景美女子高級中學委外廠商執行人員保密切結書

立切結書人.....等，受.....委派至 臺北市立景美女子高級中學 處理業務，謹聲明恪遵學校下列工作規定，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，非經本校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，不得私自將本校之資訊設備、媒體檔案及公務文書攜出。

二、 未經學校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學校網路。若經申請獲准連接學校網路，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學校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學校配發之個人電腦與週邊設備，並僅開放使用學校內部網路。若因業務需要使用學校電子郵件、目錄服務，應經資訊組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學校業務相關人員之確認並代為申請核准。

五、 本校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 (以授課時需連結學校網路者為限) 及經常到校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校洽公之業務人員每年簽署本切結書乙次。

中　　華　　民　　國　　年　　月　　日

九、臺北市立景美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----------（以下稱廠商）得標臺北市立景美女子高級中學資通業務委外案----------（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，學校、簽署人及----------（廠商）各執存一份。

簽署人姓名及簽章：

身分證字號：

戶籍地址：　　聯絡電話：

所屬廠商名稱及蓋章：

所屬廠商地址：

中　　華　　民　　國　　年　　月　　日

十、臺北市立景美女子高級中學委外廠商保密切結書

_____ 公司(以下簡稱乙方) 承攬臺北市立景美女子高級中學 (以下簡稱甲方)「　　」(以下簡稱本專案)，於執行過程中，乙方自甲方所取得之公務(機密)資訊，具結依下列規定保密並履行責任：

一、乙方應遵守「電腦處理個人資料保護法」、「刑法」、「行政院及所屬各機關資訊安全管理要點」、「行政院及所屬各機關資訊安全管理規範」等相關法令，不私自蒐集本專案範圍外任何資訊。

二、乙方於本專案進行期間，依契約所產生或接觸之公務(機密)資料，，非經甲方同意或授權，不得以任何形式洩漏或將上開資料再使用或交付第三人。對所獲得或知悉之上述公務(機密)資料，乙方須負保密責任。其因法令或主管機關規定需向公務機關提供時，應在第一時間通知甲方。

三、公務（機密）資料保密期限，不受本專案工作完成（結案）及乙方不同工作地點及時間之限制。乙方持有或獲知公務（機密）資料，不得洩漏或轉讓於第三人。若因本專案終止，公務（機密）資料無再使用之必要，乙方應進行資料銷毀，不得以任何形式保存。

四、乙方違反本資訊安全保密切結書之規定，致造成甲方或第三人之損害或賠償，乙方同意無條件負擔全部責任，包括因此所致甲方或第三人涉訟，所須支付之一切費用及賠償。於第三人對甲方提出請求、訴訟，經甲方以書面通知乙方提供相關資料，乙方應合作提供，絕無異議。

此致

臺北市立景美女子高級中學

立切結書人

廠商名稱及蓋章：

廠商負責人姓名及簽章：

統一編號：

公司地址：

中　　華　　民　　國　　年　　月　　日

十一、 臺北市立景美女子高級中學年度資通安全教育訓練計畫

壹、依據

臺北市立景美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本校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

本校所屬人員：

人員類別		人數
教師兼資訊人員		
一般主管		
一般使用者	教師(不含兼任資通人員)	
	職員	
共計		

肆、訓練項目

人員類別	訓練課程	時數
教師兼資通安全人員 教師兼資訊人員	資通安全管理制度 資訊系統風險管理 資通安全稽核 資安事故處理 業務持續運作管理	
一般主管、使用者	資安基本認知 資通安全管理制度	

伍、訓練期程：由本校自行排定教育訓練期程。

陸、訓練方式：由本校自行依課程內容，採取合宜教育訓練方式(實體課程、線上課程)。

十二、 臺北市立景美女子高級中學資通安全認知宣導及教育訓練簽到表

課程名稱：_____

時　　間：

地　　點：_____

單　位	職　稱	姓　名	簽　名

十三、 臺北市立景美女子高級中學資通安全維護計畫實施情形

本校之業務因涉及全國性民眾個人資料檔案之持有及處理，經主管機關核定後本單位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 鈞局提出本（108）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. 核心業務及其重要性	1.1 核心業務及重要性盤點	本校核心業務及重要性詳參資通安全維護計畫(詳附件，下同)。
2. 資通安全政策及目標之訂定	2.1 資通安全政策訂定及核定	本校已訂定資通安全政策，詳參資通安全維護計畫，並經資安長核定(詳公文附件)。
	2.2 資通安全目標之訂定	本校已訂定資通安全目標，詳參資通安全維護計畫。
	2.3 資通安全政策及目標宣導	本校為推動資通安全政策，已定期向同仁進行宣達。
	2.4 資通安全政策及目標定期檢視	本校已定期召開資通安全管理審查會議中檢討資通安全政策及目標之適切性(詳會議記錄)。
3. 設置資通安全推動組織	3.1 設定資通安全長	本校已指定校長為資通安全長，其職掌詳參資通安全維護計畫。
	3.2 設置資通安全推動小組	本校已設置資通安全推動小組，其組織、分工及職常詳參資通安全維護計畫。
4. 人力及經費之配置	4.1 專職(責)人員配置	本校依規定配置資通安全兼任人員1人。另因其業務內容將涉及機密性資料，故已進行相關安全評估。
	4.2 經費之配置	本校今年視需求已合理分資安經費，資安經費佔資訊經費之 1%。
5. 資訊及資通系統之盤點及核心資通系統、相關資產之標示	5.1 資訊及資通系統之盤點	本校已於今年01月盤點本校之資訊、資通系統，建立資產目錄。
	5.2 機關資通安全責任等級分級	本校依資通安全責任等級分級辦法，為資通安全責任等級 D 級機關。
6. 資通安全風險評估	6.1 資通安全風險評估	本校已於今年01月完成本校之資訊、資通系統及相關資產之風險分析評估及處理。
	6.2 資通安全風險之因應	本校已依資通安全風險評估之結果擬定對應之資通安全防護及控制措施。
7. 資通安全防護及控制措施	7.1 資訊及通系統之保管	本校已依安全維護計畫辦理，詳附件資料。

	7.2 存取控制與加密機制管理	本校已依安全維護計畫辦理。
	7.3 作業及通訊安全管理	本校已依安全維護計畫辦理。
	7.4 系統獲取、開發及維護	本校已依安全維護計畫辦理。
8. 資通安全事件通報、應變及演練相關機制	8.1 訂定資通安全事件通報、應變及演練相關機制	本校已依規定訂定資通安全事件通報應變程序。
	8.2 資通安全事件通報、應變及演練	本校已依規定進行資通安全事件通報，每年9月辦理通報應變演練。
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	本校接受情資後，已進行分類評估。
	9.2 資通安全情資之因應措施	本校已接受情資之分類，採取對應之因應措施。
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	本校資通系統或服務委外辦理時，已將選任受託者應注意事項加入招標文件中。
	10.2 監督受託者資通安全維護情形應注意事項	本校已依規定監督受託者資通安全維護情形，客製他資通系統開發者，已要求其出具安全性檢測證明。
11. 資通安全教育訓練	11.1 資通安全教育訓練要求	本校人員已規定進行資通安全教育訓練。
	11.2 辦理資通安全教育訓練	本校已於今年1月辦理資通安全教育訓練。
12. 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	本校已依規定訂定各階文件、流程、程序或控制措施，據以實施並保 存相關之執行成果記錄。
	13.2 資通安全維護計畫實施情形之稽核機制	本校已依規定辦理內部稽核。
	13.3 資通安全維護計畫之持續精進及績效管理	本校已依規定辦理內部召開管理審查會議，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。
其他說明		

業務承辦人：　　單位主管：　　資通安全長：

十四、 臺北市立景美女子高級中學年度資通安全稽核計畫

壹、依據

一、本校之資通安全維護計畫辦理。

二、資通安全管理法第十三條規定辦理。

貳、目的

為瞭解本校資通安全維護計畫執行之有效性，爰擬定本稽核計畫，執行稽核作業。

參、稽核期程

於每年10月前召開資通安全管理審查會議進行稽核。

肆、稽核團隊成員

資通安全長及各單位主管兼任。

伍、稽核範圍

全機關

陸、稽核項目及內容

依據本校安全維護之內容，本年度之稽核項目、內容如下：

一、核心業務及其重要性盤點：詳參本校資通安全維護計畫，下同。

二、資通安全政策及目標：資安政策宣導及定期召開資安管理會議。

三、資通安全推動組織。

四、人力及經費之配置。

五、公務機關資通安全長之配置。

六、資訊及資通系統之盤點，並標示核心資通系統及相關資產，建立資產目錄。

七、資通安全風險評估。

八、資通安全防護及控制措施。

九、資通安全事件通報、應變及演練相關機制。

十、資通安全情資之評估及因應機制。

十一、資通系統或服務委外辦理之管理措施。

十二、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。

十三、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。

柒、改善作業

本校經評估對於稽核結果表現優良者依公務機關所屬人員資通安全事項獎懲辦法給予行政獎勵，並針對缺失或待改善項目者研擬後續追蹤方式及頻率(如將前次稽核結果納入本次稽核範圍中，並追蹤辦理情形及進度)。

十五、 臺北市立景美女子高級中學稽核項目紀錄表

稽核日期：　　年　　月　　日

稽核範圍：全機關

受稽核單位	稽核項目	稽核結果	備註
		□符合 □不符合 □不適用	
		□符合 □不符合 □不適用	
		□符合 □不符合 □不適用	
		□符合 □不符合 □不適用	
		□符合 □不符合 □不適用	
		□符合 □不符合 □不適用	
附註			
受稽核人員：			受稽核單位主管：

十六、 臺北市立景美女子高級中學稽核委員聘任同意暨保密切結書

本人＿＿＿＿＿＿＿＿（以下簡稱甲方）為協助○○○（以下簡稱乙方）執行「○○○」（以下簡稱本計畫），接受乙方之邀請，擔任 107 年資安稽核團隊之稽核委員，特立書同意事項如下：

一、 甲方應遵守國家機密保護法、個人資料保護法、行政院及所屬各機關資訊安全管理要點、行政院及所屬各機關資訊安全管理規範、著作權法及其他相關法令之規定，並對因執行本計畫或因執行本計畫之機會所知悉之機密資訊負有保密義務;且上開各義務不因甲方與乙方或與技服中心間，就本年度擔任稽核委員相關事宜之法律關係解除、終止或完成而失其效力。

二、 甲方就因執行本計畫或因執行本計畫之機會，所知悉或接觸之乙方、受稽機關或其他第三人之機密資訊，除因執行本計畫所必須，且事先經乙方書面同意者，或法律另有明文規定外，不得有下列行為：

（一）全部或一部重製或留存上開機密資訊；

（二）以任何方式向任何第三人揭露上開機密資訊之全部或一部；

（三）以任何方式使任何第三人知悉、持有或使用上開機密資訊之全部或一部；

（四）以任何方式使自己或任何第三人就上開機密資訊之全部或一部取得任何權利；

（五）揭露、公開或使用上開機密資訊之全部或一部。

三、 甲方因執行本計畫所製作之報告、文件或其他產出，其智慧財產權及其他權利均歸屬乙方所有。

四、 甲方與受稽機關有下列情形之一者，就與該受稽機關之稽核相關事宜，應主動迴避，或事先以書面告知乙方，以確認是否得免予迴避：

（一）甲方、甲方之配偶、甲方三親等以內血親或姻親、與甲方有共同生活關係之家屬、或上開人員財產信託之受託人，與受稽機關間，有財產上或非財產上利益之利害關係者；

（二）甲方、甲方之配偶、甲方三親等以內血親或姻親、與甲方有共同生活關係之家屬，與受稽機關或其負責人間現有或於過去兩年間曾有僱傭、承攬、委任、代理或其他類似之關係者；

（三）甲方或其現任職或於過去兩年內曾任職之機關，於民國 105 年至本次稽核期間， 曾為受稽機關進行與受稽事項相關之顧問輔導者。

五、 前條所稱財產上利益，係指動產、不動產、現金、有價證券、債權、其他財產上權利、具有經濟價值或得以金錢交易取得之利益；所稱非財產上利益，係指有利於甲方之配偶、甲方三親等以內血親或姻親、與甲方有共同生活關係之家屬、或上開人員財產信託之受託人於受稽機關或其關聯機關之任用、陞遷、調動及其他人事措施。

六、 有其他情形足認甲方有不能公正執行職務之虞，經受稽機關敘明理由，並由乙方作成迴避決定者，甲方應迴避之。

七、 甲方有第四條各款情形之一，而未自行迴避，亦未事先以書面告知乙方相關情事，並經乙方書面同意免予迴避者，乙方得終止本契約，甲方應返還已收取之報酬，如乙方， 因此認有必要對受稽核機關重為全部或一部稽核，或受有其他不利益時，甲方並應賠償乙方因此所生之一切損

失及費用（包括但不限於賠償金、和解金、律師費及訴訟費用等）。

八、 甲方如違反第二條或就相關事宜涉及其他不法情事，將移送司法機關處理；如致乙方、受稽機關，遭受任何不利益，或受第三人法律上請求或訴追者，甲方應賠償乙方、受稽機關，因此所生之一切損失及費用（包括但不限於賠償金、和解金、律師費及訴訟費用等）。

九、 甲方應公正執行職務，並應避免使人誤認推薦特定廠商、產品或服務；且處理稽核相關事務或出席會議，應親自為之。

此　致

臺北市立景美女子高級中學

立 同 意 書 人

姓　名：　　（簽章）

身 份 證 字 號：

中　　華　　民　　國　　年　　月　　日

十七、 臺北市立景美女子高級中學稽核結果及改善報告

稽核範圍				
稽核日期				
審查日期				
改善措施				
編號	稽核缺失或待改善稽核項目	改善措施	改善期程規劃	相關證明資料
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				

業務承辦人：　　單位主管：　　資通安全長：

十八、 臺北市立景美女子高級中學改善績效追蹤報告

製表日期：

稽核發現					
稽核日期			受稽核單位		
稽核區域					
缺失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					
業務承辦人		單位主管		資通安全長	