臺北市立第一女子高級中學

資通安全維護計畫

第 1.3 版

生效日期：112 年 10 月 11 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 19 日	初次建立，108 年 1 月 18 日本校資通安全推動小組會議通過	資訊組	黃芳蘭
V1.1	109 年 5 月 11 日	修訂資通安全長姓名；新增附件十五、臺北市立第一女子高級中學稽核結果及改善報告；新增附件十六、臺北市立第一女子高級中學改善績效追蹤報告。	資訊組	張清俊
V1.2	111 年 10 月 27 日	刪除校內非核心業務主機兩台(www、國語文學科中心虛擬主機已經向上集中至臺北市政府教育局機房)	資訊組	楊喻文
V1.3	112 年 10 月 11 日	修訂第十三條第一項資通安全教育訓練要求；修訂附件一、臺北市立第一女子高級中學資訊安全推動小組成員及分工表。	資訊組	楊喻文

資通安全長：陳智源校長

壹、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：

(一) 資通安全管理法第 10 條及其施行細則第 6 條。

(二) 其他業務法規名稱。

二、適用範圍：本計畫適用範圍涵蓋本校各單位。

三、核心業務及重要性

(一) 核心業務及重要性：本校核心業務主要在臺北市高中校務行政系統執行，由臺北市政府教育局集中管理。其他系統將配合臺北市政府教育局向上集中管理政策，集中於臺北市政府教育局，故本校將無重要的核心系統置放於校內。

(二) 非核心業務及說明：對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
DNS	影響網域名稱查詢	72 小時
自建圖書館系統	影響圖書館業務效率	72 小時
北一女中數位校園	影響學校行政效率(如文字廣播、線上報修、場地設備借用、線上報名、投票系統、線上選課、社團選社、自習教室線上登記…)	72 小時
綠熠認證數位學習平台	影響輔導室業務執行效率	1 週
教學平台	影響部分教師教學品質	1 週
雲端社群播課系統	影響部分教師教學品質	1 週
Moodle、Blog	影響部分教師教學品質	1 週
學生健康資訊系統	影響學生健康資訊業務執行效率	1 週
校內升學報名系統	影響報名作業行政效率	1 週
防毒軟體中控系統	影響防毒軟體監控，但不影響防毒功能	1 週
程式競賽系統	影響學生程式設計競賽，但仍可使用其他系統	1 年

四、資通安全政策及目標

(一) 資通安全政策

為使本學業務順利運作，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，以供全體同仁共同遵循：

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(如:防火牆、防毒軟體)。
4. 辦理資通安全教育訓練(一般使用者與主管，每人每年 3 小時以上之一般資通安全教育訓練)，提升同仁資通安全意識。
5. 針對辦理資通安全業務有功相關人員應依資通安全管理法子法之「公務學校所屬人員資通安全事項獎懲辦法」進行獎勵。
6. 禁止多人共用同一帳號。

7. 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. 全年度資安通報平臺之資安事件不超過 20 件。

3. 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：資通安全政策由資通安全推動小組會議通過簽請校長核定後實施，修正時亦同。

(四) 資通安全政策及目標之宣導：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，向學校內所有人員進行宣導。

(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推動小組會議（得與資訊教育推動小組會議合併召開）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，負責督導學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處室主任以上之人員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。

2. 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，並依資通安全長之指示負責下列事項，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

(a) 資通安全政策及目標之研議。

(b) 訂定學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。

(c) 依據資通安全目標擬定學校年度工作計畫。

(d) 傳達學校資通安全政策與目標。

(e) 其他資通安全事項之規劃。

(2) 資安防護組

(a) 資通安全技術之研究、建置及評估相關事項。

(b) 資通安全相關規章與程序、制度之執行。

(c) 資訊及資通系統之盤點及風險評估。

(d) 資料及資通系統之安全防護事項之執行。

(e) 資通安全事件之通報及應變機制之執行。

(f) 其他資通安全事項之辦理與推動。

(3) 績效管理組

(a) 配合上級單位辦理資通安全稽核。

(b) 定期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，由資安防護組辦理相關工作內容如下：
(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，並提升學校內資通安全專業人員之資通安全管理能力。本校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學校（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，應配合學校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。

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. 資訊硬體資產為全校財物納管，併財管人員年度盤點作業處理；軟體資產透過行政院主計總處之軟體攤銷系統納管。

2. 資訊及資通系統資產項目如下（一般服務使用為主）：

資產類別	資產項目
資訊資產	以數位等形式儲存之資訊，如作業程序、會議記錄、系統文件、操作手冊之資訊等
軟體資產	(1) 系統軟體，例如：windows server。 (2) 套裝軟體，例如：防毒軟體等。
硬體資產	(1) 電腦設備，例如：伺服器。 (2) 通訊設備，例如：路由器、網路交換器。
服務資產	一般維運支援性服務，例如：電信網路專線。
人員資產	圖書館主任及資訊組相關人員。
個資資產	併本校保有個人資料彙整一覽表處理。

3. 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、擁有者、管理者、使用者、存放位置、防護需求等級。

4. 資訊及資通之硬體資產清冊之建立、標籤標示，由本校財物管理人員辦理。

5. 硬體資產清冊同臺北市政府財產管理系統中之資料，軟體資產清冊同行政院主計總處之軟體攤銷系統中之資料，清冊防護需求由本校資通安全管理人員維護。

6. 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) 學校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 2 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) 本校應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，全學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. 本校同仁使用資訊及資通設備須遵守設備管理學校相關規範。

2. 本校同仁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. 本校同仁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，並安全地自原設備上抹除。

4. 非本校同仁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) 本校之防火牆由本校自行管理，區域劃分如下：

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

(b) 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) 使用者應依學校規定之方式存取網路服務。

(7) 網域名稱系統(DNS)防護

(a) 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。

(b) 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。

(c) 內部主機位置查詢應指向學校內部 DNS 伺服器。

(8) 無線網路防護

(a) 機密資料原則不得透過無線網路及設備存取、處理或傳送。

(b) 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。

(c) 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。

(d) 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。

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：

(a) 通行碼長度 8 碼以上。

(b) 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。

(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：

(a) 應落實使用者更新加密裝置並備份金鑰。

(b) 應避免留存解密資訊。

(c) 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。

(a) 經任何形式之儲存媒體所取得之檔案，於使用前應先掃描有無惡意軟體。

(b) 電子郵件附件及下載檔案於使用前，宜於他處先掃描有無惡意軟體。

(c) 確實執行網頁惡意軟體掃描。

(2) 管理者並應每 2 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之資安防護組同意後始可開通。

(2) 資通安全推動小組之資安防護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。

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，並使用純文字模式瀏覽，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) 使用者不得利用學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) 本校應配合上級學校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

(a) 通訊機房(機櫃)應進行實體隔離。

(b) 學校人員或來訪人員應申請及授權後方可進入通訊機房(機櫃)，通訊機房(機櫃)管理者並應定期檢視授權人員之名單。

(c) 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。

(d) 僅於必要時，得准許外部支援人員進入通訊機房(機櫃)。

(e) 人員及設備進出通訊機房(機櫃)應留存記錄。

(2) 通訊機房(機櫃)之環境控制

(a) 通訊機房(機櫃)之空調、電力得建立備援措施。

(b) 通訊機房(機櫃)得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，以減少環境不安全引發之危險。

(c) 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

(a) 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。

(b) 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。

(c) 機密性及敏感性資訊，不使用或下班時應該上鎖。

(d) 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。

(e) 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。

(f) 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，並執行異地存放。

(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並取出自然人憑證。

(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) 連網電腦應隨時得配合更新作業系統、應用程式漏洞修補程式及防毒病毒碼等或以其他安全防護方式進行管理（如還原卡）。

(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，應主動循學校之通報程序通報。

(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。

(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學校、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。

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。

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

(一) 資通安全教育訓練要求

1. 資訊業務主管(圖書館主任)每年需接受 3 小時政策面、4 小時管理面、3 小時法制面資通職能課程訓練，若主管無具備資通基礎技術背景，需另外接受 4 小時技術面資通職能課程訓練。

2. 資訊業務人員(資訊組長)每年需接受 3 小時政策面、6 小時管理面、3 小時法制面資通職能課程訓練。

3. 其餘資安防護組人員每人每年至少接受 6 小時以上之資安專業課程訓練。

4. 本校之一般使用者與主管，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，提升學校資通安全水

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：

(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。

4. 資通安全教育及訓練之政策，除適用所屬員工外，對學校外部的使用者，亦應一體適用。

十四、公務學校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，依據公務學校所屬人員資通安全事項獎懲辦法、臺北市政府及所屬各學校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

(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) 資通安全維護計畫實施情形之稽核機制

1. 稽核機制之實施

配合歷年上級單位資訊安全管理系統評核填報作業期程進行。

2. 稽核改善報告

學校應配合上級單位資訊安全管理系統評核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。

(三) 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月底前或上級單位資訊安全管理系統填報期限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：

(1) 過往管理審查議案之處理狀態。

(2) 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、上級學校要求、資通安全推動小組決議事項等。

(3) 資通安全維護計畫內容之適切性。

(4) 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) 資通安全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。

(5) 重大資通安全事件之處理及改善情形。

(6) 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、相關法規、程序及表單

(一)相關法規及參考文件

1. 資通安全管理法
2. 資通安全管理法施行細則
3. 資通安全責任等級分級辦法
4. 資通安全事件通報及應變辦法
5. 資通安全情資分享辦法
6. 公務學校所屬人員資通安全事項獎懲辦法
7. 資訊系統風險評鑑參考指引
8. 政府資訊作業委外安全參考指引
9. 無線網路安全參考指引
10. 網路架構規劃參考指引
11. 行政裝置資安防護參考指引
12. 政府行動化安全防護規劃報告
13. 安全軟體發展流程指引
14. 安全軟體設計指引
15. 安全軟體測試指引
16. 資訊作業委外安全參考指引
17. 本校資通安全事件通報及應變程序

(二)附件表單

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. 資訊及資通資產清冊
4. 風險評估表
5. 風險類型暨風險對策參考表
6. 管制區域人員進出登記表
7. 委外廠商執行人員保密切結書、保密同意書

8. 委外廠商查核項目自評表

9. 年度資通安全教育訓練計畫

10. 資通安全認知宣導及教育訓練簽到表

11. 資通安全維護計畫實施情形

貳、附件

一、臺北市立第一女子高級中學資訊安全推動小組成員及分工表

臺北市立第一女子高級中學資訊安全推動小組成員及分工表

<table>
<tr><th>單位職級</th><th>組別</th><th>職掌事項</th><th>分機</th></tr>
<tr><td>校長</td><td>資通安全長</td><td>執掌事項詳列於本校資通安全管理計畫中。</td><td>200</td></tr>
<tr><td>教務主任
(組長)</td><td rowspan="6">策略規劃組</td><td rowspan="6">1. 資通安全政策及目標之研議。
2. 訂定學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學校年度工作計畫。
4. 傳達學校資通安全政策與目標。
5. 其他資通安全事項之規劃。</td><td>300</td></tr>
<tr><td>學務主任</td><td>500</td></tr>
<tr><td>總務主任</td><td>600</td></tr>
<tr><td>輔導主任</td><td>700</td></tr>
<tr><td>主任教官</td><td>550</td></tr>
<tr><td>圖書館主任</td><td>800</td></tr>
<tr><td>總務主任
(組長)</td><td rowspan="6">績效管理組</td><td rowspan="6">1. 配合上級單位辦理資通安全稽核。
2. 定期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。</td><td>600</td></tr>
<tr><td>人事室主任</td><td>210</td></tr>
<tr><td>會計室主任</td><td>220</td></tr>
<tr><td>秘書</td><td>201</td></tr>
<tr><td>圖書館主任</td><td>800</td></tr>
<tr><td>文書組長</td><td>610</td></tr>
<tr><td>圖書館主任
(組長)</td><td rowspan="4">資安防護組</td><td rowspan="4">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。</td><td>800</td></tr>
<tr><td>資訊組長</td><td>850</td></tr>
<tr><td>系統管理師</td><td>852</td></tr>
<tr><td>技士</td><td>851</td></tr>
</table>

二、臺北市立第一女子高級中學資通安全保密同意書

保密切結書

本人 _____ 將嚴守工作保密規定與國家相關法令對業務機密負完全保密之責，保護所接觸到的個人資料，並尊重智慧財產權。絕不擅自洩漏、傳播職務上任何業務相關資料及任職期間經辦、保管或接觸之所有須保密訊息資料；絕不擅自複製、傳播任何侵害智慧財產權之任何程式、軟體，違者願負法律責任。

此致

臺北市立第一女子高級中學

立 同 意 書 人：_____

身 分 證 字 號：_____

電　　話：_____

住　　址：_____

中　華　民　國　　年　　月　　日

《後續--個人資料提供同意書》

個人資料提供同意書

本同意書說明臺北市立第一女子高級中學（以下簡稱本校）將如何處理本表單所蒐集到的個人資料，當您勾選「我同意」並簽署本同意書時，表示您已閱讀、瞭解並同意接受本同意書之所有內容及其後修改變更規定。

1. 本校因執行業務蒐集您的個人資料包括姓名、身分證字號、電話、地址等。
2. 若您的個人資料有任何異動，請主動向本校人事室申請更正，使其保持正確、最新及完整。
3. 若您提供錯誤、不實、過時或不完整或具誤導性的資料，您將損失相關權益。
4. 您可依中華民國「個人資料保護法」，就您的個人資料行使以下權利：
   (1) 請求查詢或閱覽。
   (2) 製給複製本。
   (3) 請求補充或更正。
   (4) 請求停止蒐集、處理及利用。
   (5) 請求刪求。
5. 本校利用您的個人資料期間為即日起至_____年，利用地區為臺灣地區。
6. 除非取得您的同意或其他法令之特別規定，本校絕不會將您的個人資料揭露予第三人或使用。
7. 僅有經過授權的人員才能接觸您的個人資料，相關處理人員皆簽有保密合約，如有違反保密義務者，將會受到相關的法律處分。
8. 本同意書可能會因應個人資料保護法或其他相關法規、以及實際需求進行修正。

☐ 我瞭解與同意以上文字

_____簽章

中　　華　　民　　國　　年　　月　　日

三、臺北市立第一女子高級中學資訊及資通資產清冊

臺北市立第一女子高級中學資訊及資通資產清冊

四、臺北市立第一女子高級中學風險評估表

臺北市立第一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				

承辦人員：　　單位主管：

五、臺北市立第一女子高級中學風險類型暨風險對策參考表

臺北市立第一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，例示非列舉）
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。		

六、臺北市立第一女子高級中學管制區域人員進出登記表

臺北市立第一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	單位及姓名	配同人員	日期	進出時間	事由	進出設備 (物品)
1	單 位： 姓 名：			進： 出：		
2	單 位： 姓 名：			進： 出：		
3	單 位： 姓 名：			進： 出：		
4	單 位： 姓 名：			進： 出：		
5	單 位： 姓 名：			進： 出：		
6	單 位： 姓 名：			進： 出：		
7	單 位： 姓 名：			進： 出：		
8	單 位： 姓 名：			進： 出：		
9	單 位： 姓 名：			進： 出：		
10	單 位： 姓 名：			進： 出：		

承辦人員：　　單位主管：

七、臺北市立第一女子高級中學委外廠商執行人員保密切結書

臺北市立第一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應簽署本切結書。

中　華　民　國　　年　　月　　日

八、臺北市立第一女子高級中學委外廠商執行人員保密同意書

臺北市立第一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：

甲、 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。

乙、 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。

丙、 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

九、臺北市立第一女子高級中學委外廠商保密切結書

臺北市立第一女子高級中學委外廠商保密切結書

_____ 公司(以下簡稱乙方) 承攬臺北市立第一女子高級中學(以下簡稱甲方)

「 (填寫服務名稱)」(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「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

臺北市立第一女子高級中學

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

十、臺北市立第一女子高級中學委外廠商查核項目自評表

臺北市立第一女子高級中學委外廠商查核項目自評表

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？				已訂定資通安全政策及目標。
	1.2 組織是否訂定資通安全政策及目標？				政策及目標符合機關之需求。
	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？				依規定按時進行教育訓練之宣達。
	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？				定期進行政策及目標之檢視、調整。
	1.5 是否隨時公告資通安全相關訊息？				將資安訊息公告於布告欄。
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？				指派副首長擔任資安長。
	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？				有設置內部資通安全推動小組，並制訂相關之權責分工。
	2.3 是否訂定組織之資通安全責任分工？				機關內部訂有資安責任分工組織。
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？				有訂定人員錄用之安全評估措施
	3.2 是否符合組織之需求配置專業資安人力？				機關依規定配置資安人員2人。
	3.3 是否具備相關專業資安證照或認證？				專業人員具備ISO27001之證照
	3.4 是否配置適當之資源？				機關並未投入足夠資安資源。
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？				依規定建置資產目錄，並定時盤點。
	4.2 各項資產是否有明確之管理者及使用者？				資產依規定指定管理者及使用者。
	4.3 是否定有資訊、資通系統分級與處理之相關規範？				資訊訂有分級處理之作業規範。

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
	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？				已進行風險評估及擬定相應之控制措施。
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？				機房訂有門禁管制措施。
	5.2 重要實體區域的進出權利是否定期審查並更新？				離職人員之權限未刪除。
	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？				對於進出人員並未監督其活動。
	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？				按時檢測機房物理面之情況。
	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？				依規定定期檢查並按時提供同仁安全設備之使用訓練。
	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？				並未陪同或監視第三方支援人員。
	5.7 重要資訊處理設施是否有特別保護機制？				對於核心系統主機並未設置特別保護機制。
	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？				定期檢查物理面之風險。
	5.9 電源之供應及備援電源是否作安全上考量？				有設置備用電源。
	5.10 通訊線路及電纜線是否作安全保護措施？				電纜線老舊，並未設有安全保護措施。
	5.11 設備是否定期維護，以確保其可用性及完整性？				設備按期維護。
	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？				訂有相關之保護措施。
	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)？				攜帶式設備訂有保護措施。
	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？				設備報廢前均有進行資料清除程序。
	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？				人員下班後並未將機敏性公文妥善存放。
	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？				系統開發測試與正式作業區隔。

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
	5.17 是否全面使用防毒軟體並即時更新病毒碼？				按時更新病毒碼。
	5.18 是否定期對電腦系統及資料儲存媒體進行病毒掃瞄？				定期進行相關系統之病毒掃瞄。
	5.19 是否定期執行各項系統漏洞修補程式？				定期進行漏洞修補。
	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)？				系統設有檢查之機制。
	5.21 重要的資料及軟體是否定期作備份處理？				有定期做備份處理。
	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？				備份資料均已測試。
	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？				均設有加密之保護措施。
	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？				訂有可攜式媒體之管理程序。
	5.25 是否訂定使用者存取權限註冊及註銷之作業程序？				訂有使用者存取權限註冊及註銷之作業程序。
	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？				未定期檢視使用者存取權限。
	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)？				通行碼符合規定。
	5.28 通行碼是否規定需有大小寫字母、數字及符號組成？				通行碼符合規定。
	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？				依規定訂定適當之存取權限。
	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？				對於特定網路有訂定相關之控制措施。
	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)？				有針對行動式電腦訂定管理政策。
	5.32 重要系統是否使用憑證作為身份認證？				針對重要系統設有身份認證。
	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？				系統更新後相關措施仍有效。

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
	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？				可即時取得系統弱點並採取應變措施。
6. 訂定資通安全事件通報及應變之程序及機制	6.1 是否建立資通安全事件發生之通報應變程序？				有訂定通報應變程序。
	6.2 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？				同仁及委外廠商均知悉通報應變程序，並定期宣導。
	6.3 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？				有留存相關紀錄。
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？				有定期辦理宣導。
	7.2 是否對同仁進行資安評量？				按期進行資安評量。
	7.3 同仁是否依層級定期舉辦資通安全教育訓練？				有定期辦理教育訓練。
	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？				同仁均瞭解單位之資通安全政策及目標。
8. 資通安全維護計畫實施情形之精進改善機制	8.1 是否設有稽核機制？				訂有稽核機制。
	8.2 是否定有年度稽核計畫？				有訂定年度稽核計畫。
	8.3 是否定期執行稽核？				有按期執行稽核。
	8.4 是否改正稽核之缺失？				訂有稽核後之缺失改正措施。
9. 資通安全維護計畫及實施情形之績效管考機制	9.1 是否訂定安全維護計畫持續改善機制？				有訂定持續改善措施。
	9.2 是否追蹤過去缺失之改善情形？				有追蹤缺失改善之情形。
	9.3 是否定期召開持續改善之管理審查會議？				定期召開管理審查會議。

廠商名稱及蓋章：

廠商負責人姓名及簽章：

十一、 臺北市立第一女子高級中學申請遠距工作保密切結書

臺北市立第一女子高級中學申請遠距工作保密切結書

編號：_____-_____

具保密切結（人員）　　(以下簡稱乙方)於民國　　年　　月　　日起於臺北市立第一女子高級中學執行因行政業務（或專案）需求，申請使用電腦遠端桌面連線服務「　　(請填軟體或服務名稱)」(以下簡稱本服務)，使用期間接觸公務(機密)資料，將恪遵以下保密規定：

一、乙方不得將公務(機密)資料以任何形式利用或洩漏、告知、交付、移轉予任何第三人，如有違誤願負法律上之責任。

二、本服務僅限乙方個人使用，乙方應嚴守資安規定，不得將本服務以任何形式轉予第三人使用，如有違誤願負法律上之責任。

此致

臺北市立第一女子高級中學

具切結書委外（人員）:　　（簽章）

十二、 臺北市立第一女子高級中學 108 年度資通安全教育訓練計畫

臺北市立第一女子高級中學 108 年度資通安全教育訓練計畫

壹、依據

臺北市立第一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
資通安全人員		
一般主管		
一般使用者	教師(不含兼任資通人員)	
	職員	
	技工及工友	
	警衛	
	共計	

肆、訓練項目

人員類別	訓練課程	時數
資通安全人員	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	資通安全基本認知 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或配合上級單位政策辦理訓練。

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、線上課程等等)。

十三、 臺北市立第一女子高級中學資通安全認知宣導及教育訓練簽到表

臺北市立第一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

十四、　臺北市立第一女子高級中學資通安全維護計畫實施情形

臺北市立第一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	
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	
	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.設置資通安全推動組織	3.1 設定資通安全長	
	3.2 設置資通安全推動小組	
4.人力及經費之配置	4.1 專職(責)人員配置	
	4.2 經費之配置	
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	
	5.2 機關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 資訊及通系統之保管	

實施項目	實施內容	實施情形說明
	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 系統獲取、開發及維護	
	7.5 執行資通安全健診	
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	
	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稽核機制	
	13.3 資通安全維護計畫之持續精進及績效管理	
其他說明		

業務承辦人：　　單位主管：　　資通安全長：

十五、　臺北市立第一女子高級中學稽核結果及改善報告

臺北市立第一女子高級中學稽核結果及改善報告

稽核範圍	配合「教育部全國高中職資訊安全管理系統」評核項目辦理			
稽核日期	_____年_____月_____日			
審查日期	_____年_____月_____日			
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				

單位主管：　　資通安全長：

十六、　臺北市立第一女子高級中學改善績效追蹤報告

臺北市立第一女子高級中學改善績效追蹤報告

編　　號：

製表日期：　　年　　月　　日

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	待改善項目： 缺失項目：		
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	☐ 合格／完成 ☐ 待追蹤(追蹤期限：_____年_____月_____日) ☐ 不合格(說明：_____)		
經費需求或編列執行金額	需_____萬元	經費執行情形	已進行相關_____ 更新採購， 共執行_____萬元。
預定完成日期	年　　月　　日	實際完成日期	年　　月　　日
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		資通安全長	

本文件之智慧財產權屬行政院資通安全處擁有。