臺北市立麗山高級中學

資通安全維護計畫

第 4.0 版

生效日期：115 年 3 月 12 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 18 日	初次建立	資訊組	何信億
V2.0	111 年 2 月 1 日	初次修訂 更新目錄、增加頁碼 內容勘誤 新增附錄：圖書館資訊設備管理辦法、校園網路使用管理辦法、網路硬碟伺服器(NAS)使用管理辦法、資訊設備維護管理與分工規範、行動載具管理規範	資訊組	陳佳宜
V3.0	114 年 1 月 20 日	新增各單位職級代理人 新增圖書館主任職務 修訂資通安全計畫之建立及修訂由資通安全管理審查會議通過，簽陳至資通安全長後實施。 依 113 年 10 月 16 日北市教資字第 1133102825 號函附件-臺北市教育局所屬各級學校「資通安全維護計畫」範本酌修文字敘述。	資訊組	陳佳宜
V4.0	115 年 3 月 12 日	1. 修訂資通安全政策，刪除教育訓練時數標記文字。 2. 修訂社交工程演練容許率目標。 3. 修訂資通安全政策及目標核定程序：得併同本校「圖書暨資訊委員會議」或「擴大行政會議」合併召開。 4. 於「資訊及資通系統之盤點」限制使用危害國家資通安全產品。 5. 新增第八點：資通安全風險評估及第九點：資通安全防護及控制措施。原第八點及其後之點次，依序遞延。 6. 修訂資通安全教育訓練要求。 7. 增刪部分相關法規及參考文件、附件表單。 8. 調整全文排版：調整部分段落文字層級與縮排，並統一設定為最小行高、字距 0、新增段落前後的空間。	資訊組	方珮雯

目錄

壹、 資通安全推動小組成員及分工表

臺北市立麗山高級中學

資通安全推動小組成員及分工表

單位職級	組別	職掌事項	分機	代理人
校長	策略規劃暨績效管理組	資通安全長。執掌事項詳列於本校資通安全管理計畫中。	100	秘書
教務主任		1.資通安全政策及目標之研議。 2.訂定機關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機關年度工作計畫。 4.傳達機關資通安全政策與目標。其他資通安全事項之規劃。 5.辦理資通安全內部稽核	200	學務主任
學務主任			300	教務主任
總務主任			400	秘書
輔導主任			500	圖書館主任
圖書館主任			800	輔導主任
教師兼任資訊組長	資安管理組	1.資訊組長兼任策略規劃組顧問，並辦理資通行政業務，系管師協辦。 2.資通安全技術之研究、建置及評估相關事項。 3.資通安全相關規章與程序、制度之執行。 4.資訊及資通業務之盤點及風險評估。 5.資料及資通業務之安全防護事項之執行。 6.資通安全事件之通報及應變機制之執行。 7.其他資通安全事項之辦理與推動。	801	系統管理師
教師兼任系統管理師			704	資訊組長
人事主任	績效管理組	辦理資通安全內部稽核	110	人事組員

承辦人：　　單位業務主管：　　資通安全長：

教師兼資訊組組長 方珮雯　　教師兼圖書館主任 白偉民　　臺北市立麗山高級中學 陳汶靖

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。

二、 適用範圍

本計畫適用範圍涵蓋本機關。

三、 核心業務及重要性

(一) 核心業務及重要性：

本機關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：負責教學、課程安排、成績處理、教學設備等業務。	無	為本機關依組織法執掌，足認為重要者	學校教學業務無法運作。	8 小時
學務：負責學生(社團)活動、衛生保健、體育等業務。	無	為本機關依組織法執掌，足認為重要者	學校學生事務業務無法運作。	8 小時
總務：負責校內財產、場地借用、文書事務等業務。	無	為本機關依組織法執掌，足認為重要者	學校學生總務業務無法運作。	8 小時
輔導：負責學生諮商、暴力防治、性別平等等業務。	無	為本機關依組織法執掌，足認為重要者	學校學生輔導業務無法運作。	8 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
人事：辦理人事管理業務	人事業務無法運作	24 小時
會計：辦理歲計、會計等業務	會計業務無法運作	24 小時

四、 資通安全政策及目標

(一) 資通安全政策

為使本機關業務順利運作，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，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「公務機關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. 配合上級機關辦理之電子郵件社交工程演練郵件開啟率及附件點閱率分別低於 5%及 2%。
3. 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. 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

1. 資通安全計畫之建立及修訂，須由資通安全管理審查會議通過，簽陳至資通安全長核定後實施。
2. 為提升行政執行效率，前項資通安全管理審查會議，得併同本校「圖書暨資訊委員會議」或「擴大行政會議」合併召開。

(四) 資通安全政策及目標之宣導

1. 本機關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，向機關內所有人員進行宣導，並檢視執行成效。
2. 本機關應每年向利害關係人(例如委由廠商提供服務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資通安全管理審查會議(資訊小組會議)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，本機關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

為推動本機關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) 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

本機關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，本機關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：

I. 資通安全政策及目標之研議。

II. 訂定機關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機關年度工作計畫。

IV. 傳達機關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) 資績效管理組：

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。

III. 成員由資通安全長指派之。

六、 專職人力及經費配置

(一) 人力及資源配置

1. 本機關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，其分工如下，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、內部資通安全稽核、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. 本機關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。本機關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. 本機關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. 本機關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，應考量本機關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(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. 本機關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	
軟體資產	(1) 應用軟體，例如：威力導演 13、ADOBE CS6 Master 等。 (2) 套裝軟體，例如：校園無聲廣系統等。
硬體資產	(1) 電腦設備，例如：伺服器、個人主機、筆記型電腦及平板電腦等。 (2) 通訊設備，例如：路由器、網路交換器、印表機等。 (3) 儲存媒體，例如：隨身碟、光碟及光碟機等。 (4) 其他支援設備，例如：監視器、不斷電系統、空調系統、消防系統等。
服務資產	(1) 一般維運支援性服務，例如：學術網路專線、市電系統、供水服務等。 (2) 委外服務，例如：台北市高中校務行政系統、公文交換系統等。
人員資產	(1) 內部同仁，例如：資訊組同仁等。 (2) 外部(常駐型)人員，例如：合志公司駐點人員等。
個資資產	(1) 紙本個資，例如：通訊錄、報名表、履歷表等。 (2) 檔案形式個資，例如：個人電腦中或主機內個人資料檔案等。

3. 本機關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。

5. 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。

6. 本校不得下載、安裝或使用危害國家資通安全產品；發配供業務使用之資通訊設備亦同。

(二) 資通訊資產管理

1. 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) 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。

(3) 機密性及敏感性資訊，不使用或下班時應該上鎖。

(4) 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。

(5) 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。

(6) 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。

2. 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) 本機關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。

3. 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。

4. 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，應主動循機關之通報程序通報。

(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。

5. 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

(三) 資通安全防護設備

1. 本機關應建置防毒軟體、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。

八、 資通安全風險評估

依「臺北市政府資通訊資產及電子資料安全作業指引」各規定辦理。

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及核心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

依「臺北市政府資通系統安全作業指引」、「臺北市政府資通訊資產及電子資料安全作業指引」及「臺北市政府資通訊業務委外作業指引」規定及相關程序辦理。

(二) 存取控制與加密機制管理

依「臺北市政府資通系統安全作業指引」規定及相關程序辦理。

(三) 作業與通訊安全管理

依教育部「臺灣學術網路管理規範」及「臺北市政府資通系統安全作業指引」規定及相關程序辦理。

(四) 資通安全防護設備

網路安全防護應依教育部「臺灣學術網路管理規範」辦理。端點安全（包含防毒、沙箱與端點偵測及回應），應優先使用市府或教育局提供之軟體與管理規範辦理。

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

本機關接獲資通安全情資，應評估該情資之內容，並視其對本機關之影響、本機關可接受之風險及本機關之資源，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

本機關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學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。

(二) 資通安全情資之因應措施

本機關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機關之運作產生影響，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

本機關(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) 資訊及資通系統之管理資通安全教育訓練要求

1. 本校之資安兼任或資訊人員，每人每 2 年至少接受 3 小時以上之資通安全專業課程訓練或資通安全職能訓練，且每年接受三小時以上之資通安全通識教育訓練。

2. 本校之一般使用者與主管，每人每年至少接受 3 小時以上之資通安全通識教育訓練。

3. 資通安全專業課程訓練得以遠距即時課程辦理，惟每人每年認定上限為 6 小時。

(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 6，以建立員工資通安全認知，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. 本機關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、 公務機關所屬人員辦理業務涉及資通安全事項之考核機制

本機關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，使本機關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，應與本機關之資通安全政策、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

(1) 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規範與機關之管理程序要求，並有效實作及維持管理制度。

(2) 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。

(3) 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、稽核項目紀錄表及稽核流程等相關資訊提供受稽單位。

(4) 本機關之稽核人員應受適當培訓並具備稽核能力，且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。

(5) 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。

(6) 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

(1) 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。

(2) 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。

(3) 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。

(4) 機關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。

(5) 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。

(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每年至少一次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、上級機關要求、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：

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。

(5) 風險評鑑結果及風險處理計畫執行進度。

(6) 重大資通安全事件之處理及改善情形。

(7) 利害關係人之回饋。

(8) 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[13]，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. 臺北市政府資通安全管理規定
5. 臺北市政府資通訊業務委外作業指引
6. 臺北市政府使用物聯網安全作業指引
7. 臺北市政府資通系統安全作業指引
8. 臺北市政府資通訊資產及電子資料安全作業指引
9. 臺灣學術網路管理規範
10. 臺灣學術網路各級學校資通安全通報應變作業程序
11. 危害國家資通安全產品審查辦法