

臺北市大安區幸安國民小學

資通安全維護計畫

第 2.0 版

生效日期：114 年 03 月 31 日

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
肆、 資通安全政策及目標	2
伍、 資通安全推動組織	3
陸、 專職人力及經費配置	4
柒、 資訊及資通系統之盤點	5
捌、 資通安全風險評估	5
玖、 資通安全防護及控制措施	5
壹拾、 資通安全事件通報、應變及演練相關機制	5
壹拾壹、 資通安全情資之評估及因應	6
壹拾貳、 資通系統或服務委外辦理之管理	6
壹拾參、 資通安全教育訓練	6
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	6
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	6
壹拾陸、 資通安全維護計畫實施情形之提出	7
壹拾柒、 相關法規、程序及表單	8

壹、依據及目的

本計畫依據下列法規訂定：

- (一)資通安全管理法第 10 條及施行細則第 6 條。
- (二)臺北市政府資通安全管理規定。

貳、適用範圍

本計畫適用範圍涵蓋本校全機關及附屬單位。

參、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	依組織法職掌，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	依組織法職掌，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	依組織法職掌，足認為重要者	學校總務業務無法運作	8 小時
輔導：負責學生諮商、暴力防治、性別平等業務	無	依組織法職掌，足認為重要者	學校輔導業務無法運作	8 小時
附設幼兒園：負責學齡前幼生之教保活動、招生註冊、各項就學補助、教學環境及設備規畫管理及相關事項。	無	依組織法職掌，足認為重要者	學校學齡前幼生教學業務等相關事務無法運作	8 小時

各欄位定義：

1. 核心業務名稱：請參考資通安全管理法施行細則第 7 條之規定列示。
2. 作業名稱：該項業務內各項作業程序的名稱。
3. 重要性說明：說明該業務對機關之重要性，例如對機關財務及信譽上影響，對民眾影響，對社會經濟影響，對其他機關業務運作影響，法律遵循性影響或其他重要性之說明。
4. 最大可容忍中斷時間單位以小時計。

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	8 小時
會計：辦理歲計、會計等業務	會計業務無法運作	8 小時

肆、資通安全政策及目標

一、資通安全政策依「臺北市府資通安全管理規定」壹、總則各規定辦理。

二、資通安全量化型目標

- (一) 知悉資安事件發生後於規定之時間完成通報、應變及復原作業。
- (二) 配合上級進行社交工程信件演練，開啟率及連結或檔案點閱率標準分別為低於 5% 及 2%。

三、資通安全政策及目標核定程序

資通安全政策由本機關資訊組簽陳至資通安全長核定，經校長核准後實施。

四、資通安全政策及目標之宣導

- (一) 本機關之資通安全政策及目標應透過教育訓練、內部會議、張貼公告等方式，向機關內所有人員進行宣導。
- (二) 非本機關自行維運或委由廠商建置之資通系統，本機關各業務單位應向利害關係人(例如：社團報名系統委由廠商提供服務)進行資安政策及目標宣導。

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管理審查會議中檢討其適切性。

伍、資通安全推動組織

一、資通安全長

依本法第 11 條之規定，本機關訂定教務主任為資通安全長，負責督導機關資通安全相關事項，其任務包括：

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

(一) 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，由行政、教學代表所組成的資訊小組成員兼任資通安全推動小組，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. 資安技術組：

- I. 資通安全政策及目標之研議。
- II. 依據資通安全目標擬定機關年度工作計畫。
- III. 依相關法令或規定訂定機關資通安全相關規章與程序。
- IV. 資通安全技術之研究、建置及評估相關事項。
- V. 資通安全相關規章與程序、制度之執行。
- VI. 資料及資通系統之安全防護事項之執行。
- VII. 資通安全事件之通報及應變機制之執行。

2. 教育推廣組：

- I. 傳達機關資通安全政策與目標。
- II. 其他資通安全事項之辦理與推動。

陸、專職人力及經費配置

一、人力及資源配置

- (一) 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，無需設置資通安全專職人員，本校仍設置資通安全兼辦人員 1 人。
- (二) 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。
- (三) 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。
- (四) 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

- (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。
- (二) 各單位於規劃建置資通系統時，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。
- (三) 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。
- (四) 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) 依「臺北市政府資通訊資產及電子資料安全作業指引」及「臺北市政府使用物聯網安全作業指引」各規定辦理。
- (二) 本校每年度應依資訊及資通系統盤點結果，並落實填報管考系統。

二、 機關資通安全責任等級分級

本機關自行辦理資通業務，無自行維運或委外開發之資通系統，為資通安全責任等級為 D 級。

捌、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。本機關資通安全責任等級為 D 級。

玖、資通安全防護及控制措施

本校依據前條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、 資訊及資通設備之管理

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。

壹拾、資通安全事件通報、應變及演練相關機制

依「臺灣學術網路各級學校資通安全通報應變作業程序」規定辦理。並配合上級機關進行相關演練。

壹拾壹、資通安全情資之評估及因應

依「臺灣學術網路各級學校資通安全通報應變作業程序」與「臺北市政府資通安全管理規定」辦理。

壹拾貳、資通系統或服務委外辦理之管理

依「臺北市政府資通訊業務委外作業指引」及「臺北市政府資通安全管理規定」玖、受託業務之資通安全管理規定辦理。。

壹拾參、資通安全教育訓練

一、資通安全教育訓練要求

本機關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

- (一) 承辦單位應於每學年開始，依資安防護需求安排資通安全認知宣導或教育訓練，以建立員工資通安全認知，提升機關資通安全水準。
- (二) 本機關資通安全認知宣導或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。
- (三) 員工報到時，應使其充分瞭解本機關資通安全相關作業規範及其重要性。
- (四) 資通安全教育及訓練之政策，除適用所屬員工外，對機關外部的使用者，亦應一體適用。

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

本機關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」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、資通安全維護計畫之持續精進及績效管理

(一) 本機關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。

(二) 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：
 - (1) 資通安全政策及目標之實施情形。
 - (2) 資通安全人力及資源之配置之實施情形。
 - (3) 資通安全防護及控制措施之實施情形。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。

三、持續管理審查追蹤改善，以精進管理成效。

壹拾陸、資通安全維護計畫實施情形之提出

本機關依據資通安全管理法第 12 條之規定，應依臺北市政府教育局資訊教育科要求，提出資通安全維護計畫實施情形，使其得瞭解本機關之年度資通安全計畫實施情形。

壹拾柒、相關法規、程序及表單

一、 相關法規及參考文件

- (一) 資通安全管理法
- (二) 資通安全管理法施行細則
- (三) 資通安全責任等級分級辦法
- (四) 資通安全事件通報及應變辦法
- (五) 資通安全情資分享辦法
- (六) 公務機關所屬人員資通安全事項獎懲辦法
- (七) 資訊系統風險評鑑參考指引
- (八) 政府資訊作業委外安全參考指引
- (九) 無線網路安全參考指引
- (十) 網路架構規劃參考指引
- (十一) 行政裝置資安防護參考指引
- (十二) 政府行動化安全防護規劃報告
- (十三) 安全軟體發展流程指引
- (十四) 安全軟體設計指引
- (十五) 安全軟體測試指引
- (十六) 資訊作業委外安全參考指引
- (十七) 本機關資通安全事件通報及應變程序
- (十八) 臺北市市有財產管理作業要點
- (十九) 臺北市政府及所屬各機關學校公務人員平時獎懲標準
- (二十) 臺北市國民小學組織規程準則

二、 附件表單

- (一) 資通安全推動小組成員及分工表
- (二) 資通安全保密同意書
- (三) 資通安全需求申請單
- (四) 資訊及資通資產清冊
- (五) 風險評估表

- (六) 風險類型暨風險對策參考表
- (七) 管制區域人員進出登記表
- (八) 委外廠商執行人員保密切結書、保密同意書
- (九) 委外廠商查核項目表
- (十) 年度資通安全教育訓練計畫
- (十一) 資通安全認知宣導及教育訓練簽到表
- (十二) 資通安全維護計畫實施情形
- (十三) 資通安全稽核計畫
- (十四) 稽核項目紀錄表
- (十五) 稽核結果紀錄表
- (十六) 稽核委員聘任同意保密切結書
- (十七) 稽核結果及改善報告
- (十八) 改善績效追蹤報告

承辦人：

資通安全長：

校長：

