

臺北市立西松高級中學 資通安全維護計畫

第 2.0 版

生效日期：114 年 2 月 10 日

文件制/修訂紀錄表

[illegible]

資訊安全維護計畫目錄

壹、實施計畫.....	1
一、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：	2
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	3
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.....	4
一、資通安全長	4
二、資通安全推動小組.....	4
陸、專職人力及經費配置.....	5
一、專職人力及資源之配置.....	5
二、經費之配置	6
柒、資訊及資通系統之盤點.....	6
一、資訊及資通資產盤點.....	6
二、本校資通安全責任等級分級	6
捌、資通安全風險評估	7
一、資通安全風險評估	7
玖、資通安全防護及控制措施.....	7
一、資訊及資通設備之管理.....	7
二、存取控制與加密機制管理	7
三、作業與通訊安全管理.....	7
四、資通安全防護設備.....	7
壹拾、資通安全事件通報、應變及演練相關機制	7
壹拾壹、資通安全情資之評估及因應	7
壹拾貳、資通系統或服務委外辦理之管理.....	8
壹拾參、資通安全教育訓練.....	8
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.....	8
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.....	8
一、資通安全維護計畫之實施	8
二、資通安全維護計畫之持續精進及績效管理	8

壹拾陸、資通安全維護計畫實施情形之提出.....	9
壹拾柒、相關法規、程序.....	10
一、 相關法規.....	10
二、 附件一：資通安全推動小組成員及分工表	10
三、 附件二：資通安全保密同意書	10

壹、實施計畫

一、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 條及其施行細則第 6 條。

(二)臺北市政府資通安全政策。

貳、適用範圍

本計畫適用範圍涵蓋本校所有行政業務及教學單位。

參、核心業務及重要性

一、核心業務及重要性：

核心業務	業務內有無核心資通系統	重要性說明	業務失效影響說明	最大可容忍中斷時間
教務業務： 課程發展、課程編排、教學實施、學籍管理、成績評量、教學設備、教具圖書資料供應、教學研究及教學評鑑，並與輔導單位配合實施教育輔導等事項	無	為本校依組織法執掌，足認為重要者。	學校教務業務無法運作	8HR
學生事務： 公民教育、道德教育、生活教育、體育衛生保健、學生團體活動及生活管理，並與輔導單位配合實施生活輔導等事項。	無	為本校依組織法執掌，足認為重要者。	學校學務業務無法運作	8HR
總務業務： 學校文書、事務及出納等事項。	無	為本校依組織法執掌，足認為重要者。	學校總務業務無法運作	8HR

核心業務	業務內有無核心資通系統	重要性說明	業務失效影響說明	最大可容忍中斷時間
輔導業務： 負責學生諮商、暴力防治、性別平等業務	無	為本校依組織法執掌，足認為重要者。	學校輔導業務無法運作	8HR

二、非核心業務及說明：

核心業務	業務失效影響說明	最大可容忍中斷時間
人事業務： 辦理人事管理業務	人事業務無法運作	24HR
會計業務： 辦理歲計、會計等業務	會計業務無法運作	24HR

肆、資通安全政策及目標

一、資通安全政策

依「臺北市政府資通安全管理規定」壹、總則各規定辦理。

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、完整性、可用性、法律遵循性，特制訂本政策如下，以供全體同仁共同遵循：

- (一)機密性：確保經授權之人員始得使用資訊。
- (二)完整性：確保資訊之準確性及可靠性。
- (三)可用性：確保被授權之人員能取得所需資訊。
- (四)法律遵循性：確實遵循資通系統設置或運作涉及之資通安全相關法令。

(五)本校政策

1. 應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。
2. 應保護機密資訊及資通業務之機密性與完整性，避免未經授權的存取與竄改。
3. 應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。
4. 針對辦理資通安全業務有功人員應進行獎勵。
5. 勿開啟來路不明或無法明確辨識寄件人之電子郵件。
6. 禁止多人共用單一資通業務帳號(如:檔案分享伺服器)。
7. 落實資通安全通報機制。

二、資通安全目標

- (一)資安事件發生，於規定的時間完成通報、應變及復原作業。
- (二)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%。
- (三)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之核定程序

資通安全政策由本校圖書館資訊組簽陳資通安全長經由校務會議通過實施。

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，向本校內所有人員進行宣導，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。

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，負責督導本校資通安全相關事項，其任務包括：

- (一)資通安全管理政策及目標之核定、核轉及督導。
- (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主任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：

- (1)資通安全政策及目標之研議。
- (2)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)資通安全目標擬定本校年度工作計畫。
- (4)資通安全政策與目標。
- (5)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)資訊及資通業務之盤點及風險評估。
- (4)資料及資通業務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、專職人力及經費配置

一、專職人力及資源之配置

- (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，設置資通安全承辦人員2人。
- (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，並提升本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。
- (三)本校負責重要資通設備之管理、維護、設計及操作之人員，若負有機密維護責任者，應簽屬書面約定。

(四)本校之校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。

(五)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)各單位於規劃資通業務時，應一併規劃資通業務之資安防護需求，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，應配合本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。

(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、資訊及資通資產盤點

(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、本校資通安全責任等級分級

本校自行辦理資通業務，未維運自行或委外設置、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

一、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。

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，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。

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

依「資通安全責任等級D級之各機關應辦事項」資通安全教育訓練規定辦理。

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

本校資訊相關人員其獎懲係依據「公務機關所屬人員資通安全事項獎懲辦法」辦理。

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，本校執行資通安全管理應與本校資通安全政策、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。

(二)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：

(1)政策及目標之實施情形。

(2)人力及資源之配置之實施情形。

(3)防護及控制措施之實施情形。

4. 資訊及資通系統之盤點及風險評估。

5. 重大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。

(三) 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，每年需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；實際提出日期依教育局資訊教育科來函為主。

壹拾柒、相關法規、程序

為使本校資通安全管理有效運作，本校應依相關文件、流程、程序或控制措施確實執行，並應保存相關之執行紀錄；如本校已有資通安全管理系統之文件，應與本校資通安全政策、目標及本安全維護計畫之內容相符。

一、相關法規

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

二、附件一：資通安全推動小組成員及分工表

三、附件二：資通安全保密同意書

附件一：資通安全推動小組成員及分工表

臺北市立西松高級中學

資通安全推動小組成員及分工表

編號：1

製表日期：113 年 10 月 18 日

單位職級	組別	業務事項	分機	備註 (代理人)
校長	資通安全長	執掌事項詳列於本校資通安全管理計畫中	101	秘書
教務主任 (組長)	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本校年度工作計畫。 4. 傳達資通安全政策與目標。 5. 其他資通安全事項之規劃。	201	圖書館主任
學務主任			211	
總務主任			111	
輔導主任			221	
主任教官			220	
圖書館主任			231	
國際處主任			601	
圖書館主任 (組長)	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. 資訊及資通業務之盤點及風險評估。 4. 資料及資通業務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。	231	資訊組長
資訊組長			233	
系統管理師				

承辦人：

單位主管：

資通安全長：

附件二：資通安全保密同意書

臺北市立西松高級中學

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