國立竹南高級中學
資通安全維護計畫

目　　錄

壹、依據及目的

依據資通安全管理法第10條及施行細則第6條訂定資通安全維護計畫，作為資訊安全推動之依循及應符合其所屬資通安全責任等級之要求，訂定、修正及實施資通安全維護計畫。為因應資通安全管理法及資通安全責任等級應辦事項要求，以符合法令規定並落實本計畫之資通作業安全。

貳、適用範圍

本計畫適用範圍涵蓋國立竹南高級中學全機關（以下簡稱本校）

參、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：

核心業務系統	重要性說明	業務失效影響說明	最大容忍中斷時間	復原時間目標（RTO）	復原點目標（RPO）	資通系統分級
校務行政系統	為本校依組織法執掌，足認為重要者	課程安排、出缺勤紀錄、成績輸入等作業。	48	48	24	中
校園網頁系統	為本校依組織法執掌，足認為重要者	瀏覽或校園網頁的各項功能使用。	48	48	24	普
學習歷程系統	為本校依組織法執掌，足認為重要者	登錄或審核學習歷程檔案。	48	48	24	中
郵件系統（教育雲）	為本校依組織法執掌，足認為重要者	郵件收發	48	48	24	普
DNS 系統（向上集中至成大）	為本校依組織法執掌，足認為重要者	網頁瀏覽	48	48	24	普

二、 非核心業務及說明：

本校之非核心業務及說明如下表：

非核心業務系統	業務失效影響	最大容忍中斷時間	復原時間目標（RTO）	復原點目標（RPO）	資通系統分級
電子公文系統	公文收發作業。	72	72	24	普
會計系統	採購、出納等會計作業。	72	72	24	普
薪資、零用金、財產管理系統	採購、出納等總務作業。	72	72	24	普
圖書館系統	館藏登錄與借還書作業。	72	72	24	普
差勤系統	差勤作業。	72	72	24	普
多元選修系統	選課。	72	72	24	普

※時間單位以小時計。

肆、資通安全政策及目標

一、資通安全政策

為使業務順利運作，防止資訊或資通系統受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，並確保其機密性、完整性及可用性，特制訂本政策如下，供全體同仁共同遵循：

(一) 應建立資通安全風險管理機制，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。

(二) 應保護機敏資訊及資通系統之機密性與完整性，避免未經授權的存取與竄改。

(三) 應強化核心資通系統之韌性，確保機關業務持續營運。

(四) 應因應資通安全威脅情勢變化，宣導資通安全，以提高同仁之資通安全意識，同仁每年度亦應確實參與資通安全教育訓練。

(五) 針對辦理資通安全業務有功人員應進行獎勵。

(六) 個人應遵循之資通安全相關事項，訂於「人員資訊安全守則」(如附件一)。

二、 資通安全目標

(一) 量化型目標

1. 核心資通系統中斷時數/運作時數低於1%。

2. 獲悉資安事件發生，於規定時間內完成通報、應變及復原作業。

3. 電子郵件社交工程演練之郵件開啟率及附件點閱率分別低於5%及2%。

(二) 質化型目標：

1. 適時因應法令與技術之變動，調整資通安全維護之內容，以避免資通系統或資訊遭受未經授權之侵害，以確保其機密性、完整性及可用性。

2. 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。

3. 提升人員資安防護意識、有效偵測與預防外部攻擊。

三、資通安全政策及目標之核定程序

資通安全政策由負責單位簽陳資通安全長核定。

四、資通安全政策及目標之宣導

資通安全政策及目標應每年透過教育訓練、內部會議、公告等方式向所有人員進行宣導。

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中檢討其適切性。

伍、資通安全推動組織

一、資通安全長

機關首長為資通安全長，負責督導機關資通安全相關事項，其任務包括：

1. 資通安目標之核定及督導。

2. 資通安全責任之分配及協調。

3. 資通安全資源分配。

4. 資通安全事件及防護措施之檢討及監督。

5. 資通安全相關計畫及制度之核定。

6. 資通安全相關工作事項之督導及績效管理。

7. 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主管、資訊媒體組長、設備組長及科技領域教師成立資通安全推動小組，其任務包括：

1. 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. 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工作項目如下，小組人員名單及職掌應列冊並適時更新：

1. 策略規劃組

（1）資通安全政策及目標之研議。

（2）訂定機關資通安全相關計畫與制度，並確保合乎法令之要求。

（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。

（5）資通安全技術之研究、建置及評估相關事項。

（6）其他資通安全事項規劃。

2. 資通防護組

（1）資訊及資通系統之盤點及風險評估。

（2）資料及資通系統之安全防護事項之執行。

（3）資通安全事件之通報及應變機制之執行。

3. 資安稽核組

（1）辦理資通安全內部稽核。

（2）每學期召開資通安全管理審查會議，於校務會議提報資通安全事項執行情形。

陸、專職(責)人力及經費配置

一、 專職(責)人力及資源之配置

1. 依資通安全責任等級分級辦法第6條之規定，本校已完成核心系統向上集中，110年度起評定等級為Ｄ級。
2. 本校現有資通安全專責人員名單及職掌列於「資通安全組織成員及分工表」，如附件二。負責資通系統防護規畫及建置、安全性檢測、資安稽核及教育訓練、資安事件通報應變等業務推動。
3. 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責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提供顧問諮詢服務。
4. 資安專責人員應參加主管機關辦理之相關專業研習，並鼓勵取得資通安全專業證照及資通安全職能評量證書。
5. 本校負責重要資通系統之管理、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，應簽署「校內人員保密切結書」，如附件三，並視需要實施人員輪調，建立人力備援制度。
6. 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。
7. 專責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

1. 資通安全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，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. 各單位如有資通資源需求，應配合本校預算規劃期程向資通安全小組提出需求，由資通安全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。

柒、資訊及資通系統之盤點

一、 資訊及資通系統盤點

1. 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。
2. 每年應依資訊及資通系統盤點結果，製作財產清冊，欄位應包含：財產名稱、財產編號、保管人、存放位置。
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、取得日期、置放地點等資訊。
4. 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。
5. 為防止國家資通安全遭危害，現有之大陸廠牌資通產品應造冊列管並逐年汰換。

二、 機關資通安全責任等級分級

依據行政院108年7月24日院臺護字第1080180748號函及資通安全責任等級分級辦法第6條辦理，考量本校已有核心系統向上集中規劃，依同法第10條第4款調降等級為D級機關。

捌、資通安全風險評估

一、 資通安全風險評估

1. 應每年針對資訊及資通系統資產進行風險評估。
2. 執行風險評估時應參考行政院國家資通安全會報頒布之最新「資訊系統風險評鑑參考指引」，並依其中之「2.4.2 詳細風險評鑑作法」進行風險評估之工作。

3. 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自行或委外開發之資通系統防護需求分級。

二、 核心資通系統及最大可容忍中斷時間

核心資通系統	資訊資產	核心資通系統主要功能	復原時間目標（RTO）	復原點目標（RPO）
校務行政系統	向上集中	管理學籍、課程、出缺席等	48	24
校園網頁系統	向上集中	網頁服務	48	24
DNS 系統	向上集中	網頁連結	48	24
學習歷程系統	向上集中	登錄及審核學習歷程	48	24
核心網路交換器	Cisco WS-C3850-12XS-S 一台	網路服務	48	24
防火牆	Fortigate100E 一台	資訊安全防護及網路服務	48	24

※時間以小時計。

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

依本校「資訊資產異動作業守則」施行，如附件四。

二、 存取控制與加密機制管理

依本校「存取控制管理守則」施行，如附件五。

三、 作業與通訊安全管理

依本校「實體安全管理守則」及「通信與作業管理守則」施行，如附件六、附件七。

四、 資通安全防護設備

1. 應建置防毒軟體、防火牆，持續使用並適時進行必要更新或升級。

2. 重要系統設備或資料應定期備份。

壹拾、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，詳如本校「資通安全事件通報應變程序」。

壹拾壹、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：

(一) 資安訊息

最新資安局勢、資安技術或重大資安事件等，屬資安訊息情資。

(二) 入侵攻擊

遭受入侵攻擊、系統設備進行網路攻擊活動等，屬入侵攻擊情資。

(三) 機敏資料

個資或機密資料外洩，屬機敏性之情資。

(四) 核心業務

機關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，屬核心業務情資。

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。

(一) 資安訊息

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。

(二) 入侵攻擊

由資通安全專責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。

(三) 機敏資料

就涉及個人資料、公務機密、敏感資訊之內容，應採取遮蔽或刪除之方式排除，例如

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。

(四)核心業務

資訊安全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。

壹拾貳、資通系統或服務委外辦理之管理

本校委外辦理資通系統之建置、維運或資通服務之提供時，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。

一、選任受託者應注意事項

(一)受託者辦理受託業務之相關程序及環境，應具備完善之資通安全管理措施或通過第三方驗證。受委託之相關人員應簽署「委外人員服務保密切結書」(如附件八)。

(二)受託者應配置充足且經適當之資格訓練、擁有資通安全專業證照或具有類似業務經驗之資通安全專業人員。

(三)受託者辦理受託業務得否複委託、得複委託之範圍與對象，及複委託之受託者應具備之資通安全維護措施。

二、監督受託者資通安全維護情形應注意事項

(一)受託業務包括客製化資通系統開發者，受託者應提供該資通系統之第三方安全性檢測證明；涉及利用非自行開發之系統或資源者，並應標示非自行開發之內容與其來源及提供授權證明。

(二)受託者執行受託業務，違反資通安全相關法令或知悉資通安全事件時，應立即通知委託機關及採行之補救措施。

(三)委託關係終止或解除時，應確認受託者返還、移交、刪除或銷毀履行委託契約而持有之資料。

(四)與委外廠商簽訂契約時，應審查契約中保密條款，並要求委外廠商之相關人員簽署「委外廠商保密切結書」(如附件九)。

(五)本校應定期或於知悉受託者發生可能影響受託業務之資通安全事件時，以本校「委外廠商受查核項目表」(如附件十）進行查核，以確認受託業務執行情形。

壹拾參、資通安全教育訓練

一、 資通安全教育訓練要求

(一)本校資安專責人員每年至少接受12小時以上之資安專業課程訓練或資安職能訓練。

(二)本校教職員每年接受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)資通安全小組應考量管理、業務及資訊等不同工作類別之需求，推動資通安全教育訓練，以建立同仁資通安全概念，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。

(二)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。

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)教職員報到時，應使其充分瞭解本校資通安全相關作業規範及其重要性。

(四)資通安全教育及訓練之政策，除適用所屬教職員外，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、本校教職員獎懲實施要點及各相關規定辦理之。

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，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

(一)稽核機制之實施

1. 資訊安全稽核小組應至少每二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. 稽核方式依「國立竹南高中校內資安稽核計畫」辦理。

3. 本校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；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「內部稽核結果及改善報告」中，並提供給受稽單位填寫辦理情形。

4. 稽核結果應於資通安全會議審視，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。

(二)稽核改善報告

1. 受稽單位有缺失或待改善項目者，應規劃改善方式及進度，落實執行。並檢視其他類似項目，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。

2. 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。

3. 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

(一)本校之資通安全小組應每學期至少一次、每年至少二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：(上面的人說這六項不要改)

1. 管理審查議案及資通安全事件之處理與改善。

2. 與資通安全管理有關之最新議題及情資。

3. 資通安全有關人員之回饋。

4. 資通安全計畫實施情形、稽核結果與改善機制。

5. 風險評鑑結果及風險處理進度。

6. 資通安全維護計畫內容之適切性。

(三)相關改善行為應製作「資安問題改善記錄表」並保存，作為管理審查執行之證據。

(四)應填寫資通安全維護計畫目標達成自檢表（如附件十一），並於管審會議上檢視。

壹拾陸、資通安全維護計畫實施情形之提出

本校依據資通安全法第12條之規定，應依規定向上級或監督機關填報「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。