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	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	影響課程安排、出缺勤紀錄、成績輸入等作業。	48	24	中
校園網頁系統	為本校依組織法執掌，足認為重要者	影響瀏覽或校園網頁的各項功能使用。	48	24	普
學習歷程系統	為本校依組織法執掌，足認為重要者	影響登錄或審核學習歷程檔案。	48	24	中

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	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	影響公文收發作業。	72	24	普
會計系統	影響採購、出納等會計作業。	72	24	普
薪資、零用金、財產管理系統	影響採購、出納等總務作業。	72	24	普
圖書館系統	影響館藏登錄與借還書作業。	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，以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) 應強固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，辦理資通安全教育訓練，以提高同仁之資通安全意識，同仁亦應確實參與訓練。

(五) 針對辦理資通安全業務有功人員應進行獎勵。

(六) 勿開啟來路不明或無法明確辨識寄件人之電子郵件。

(七) 禁止多人共用單一資通系統帳號。

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存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，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

(一) 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。

(二) 應每年向資通安全關係人員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）每半年定期召開資通安全管理審查會議，合併期末校內擴大行政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」，如附件一。

(1) 資通安全管理面業務：負責推動資通系統防護需求分級、資通安全管理系統導入及驗證、內部資通安全稽核及教育訓練等業務之推動。

(2) 資通系統安全管理業務：負責資通系統分級及防護基準、安全性檢測、業務持續運作演練等業務之推動。

(3) 資通安全防護業務：負責資通安全監控管理機制、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。

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「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，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	Fortigate400E 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「資訊資產異動作業規定」施行，如附件四。

二、 存取控制與加密機制管理

依本校「存取控制管理規定」施行，如附件五。

三、 作業與通訊安全管理

依本校「實體安全管理規定」及「通信與作業管理規定」施行，如附件六、附件七。

四、 業務持續運作演練

本校應針對核心資通系統制定業務持續運作計畫，並每二年辦理一次核心資通系統持續運作演練。

五、 執行資通安全健診

1. 本校應每二年辦理一次資通安全健診，至少包含下列項目，並檢討執行情形：

(1) 網路架構檢視。

(2) 網路惡意活動檢視。

(3) 使用者端電腦惡意活動檢視。

(4) 伺服器主機惡意活動檢視。

(5) 安全設定檢視。

六、 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。

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：

(一) 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。

(二) 入侵攻擊情資

資通安全情資之內容如包含網頁遭受攻擊、網頁內容不當、網頁發生個資外洩、系統遭受入侵、系統進行網路攻擊活動等內容，屬入侵攻擊情資。

(三) 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、家庭、教育、職業、病例、醫療、健康檢查、聯絡方式及其他得以直接或間接識別之個人資料，或涉及公務機密、敏感資訊等內容，屬機敏性之情資。

(四) 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) 資通安全相關之訊息情資

由資訊安全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。

(二) 入侵攻擊情資

由資通安全專職(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) 機敏性之情資

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) 涉及核心業務、核心資通系統之情資

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。

(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，並要求委外廠商之業務執行人員簽署委外廠商執行人員保密切結書。

(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」進行稽核，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，擬定資通安全教育訓練計畫，以建立教職員生資通安全認知，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。

(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，除適用所屬教職員生外，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. 辦理稽核前，資通安全小組應擬定「校內資安稽核計畫」，安排稽核成員，並提供稽核期程、校內資安稽核表及稽核流程等相關資訊予受稽單位。

3. 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。

4. 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。

5. 稽核結果應對相關管理階層報告，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。

(二)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

(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：

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)改善機制之管理審查應做成「矯正與預防處理單」，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。

壹拾柒、相關法規、程序及表單

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. 公務機關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

承辦人/專責人員　　單位主管　　校長

附件一

國立竹南高級中學

112學年度資訊安全組織成員及分工表

一、 組織成員

職務	職稱	姓名	執掌事項
資安長	校長	呂淑美	督導資通安全工作
組員	圖書館主任	鄒永灝	擔任本校資安專責人員 統籌資通安全相關業務
組員	教務主任	陳廷宇	協助資安工作
組員	學務主任	黃靜宜	協助資安工作
組員	總務主任	陳怡君	協助資安工作
組員	實習處主任	林麗悅	協助資安工作
組員	輔導主任	李淑媛	協助資安工作
組員	人事主任	郭素貞	協助資安工作
組員	主計主任	陳一中	協助資安工作
組員	秘書	張美珠	協助資安工作
組員	主任教官	陳瑞文	協助資安工作
組員	資訊媒體組長	陳書誼	協助資安工作
組員	設備組長	林　俐	協助資安工作
組員	資訊科教師	劉素雲	協助資安工作
組員	生活科技教師	魏晨峰	協助資安工作

二、 分工執掌

(一)策略規劃組

組長	圖書館主任	鄒永灝	規劃資安相關策略
組員	資訊媒體組長	陳書誼	規劃資安相關策略

(二)資安防護組

組長	圖書館主任	鄒永灝	資安維護工作
組員	資訊媒體組長	陳書誼	資安維護工作
組員	設備組長	林　俐	資安維護工作
組員	資訊科教師	劉素雲	資安維護工作
組員	生活科技教師	魏晨峰	資安維護工作

(三)資安稽核組

組長	資訊媒體組長	陳書誼	稽核資安相關事宜
組員	圖書館主任	鄒永灝	稽核資安相關事宜

附件二

國立竹南高級中學
人員資訊安全守則

一、目的：為落實本校資通安全作業，維護資訊及資通系統之機密性、完整性及可用性，特訂定本守則。

二、適用對象：本校所有教職員工。

三、作業守則內容

（一）個人電腦應設定十分鐘內自動啟動螢幕保護程式，並設定鎖定通行碼。

（二）個人電腦之作業系統應即時更新。

（三）個人電腦應安裝防毒軟體並即時更新病毒碼。

（四）應定期備份重要資料。

（五）除管理需求及經授權外，禁止使用密碼破解、網路監聽工具軟體，並不得突破他人帳號，中斷系統服務。

（六）不得在任何公開的群組、論壇或公佈欄中透露任何有關本校資訊細節。

（七）在丟棄任何曾經儲存本校資訊之電子媒體前，應將電子媒體中的資訊刪除，並徹底消磁或銷毀使其無法讀取。

（八）包含機密與敏感資訊之紙本文件應妥善保存；若不再使用時，應以碎紙機銷毀該份紙本文件。

（九）重要機密電子檔應設定保護密碼；若不再使用應立即刪除。

（十）使用電子郵件時應提高警覺，避免讀取來歷不明之郵件或含有聚集檔案之郵件，以防個資外洩或電腦中毒等資安問題。

（十一）使用即時通訊軟體傳遞本校內部公務訊息，其內容不得涉及機密資料。有業務需求者，應使用經專責機關鑑定相符機密等級保護機制或指定之軟、硬體，並依相關規定辦理。

（十一）當系統可能中毒或出現其它資安問題時，應儘速通知管理人員。

（十二）禁止濫用系統及網路資源，複製與下載非法軟體。

（十三）應遵守「個人資料保護法」規範，保護個人資料使用合法性及機密性。

四、通行碼使用原則

（一）應保護通行碼，維持通行碼的機密性。使用者應每3個月更換通行碼。

（二）避免將通行碼記錄在書面上或張貼於個人電腦、螢幕及其它容易取得或洩漏之場所。

（三）一旦加密資訊具遭破解跡象，應立即更改之。

（四）通行碼的長度至少8碼以上。

（五）通行碼複雜度應包含英文大寫小寫、特殊符號或數字其中三種以上。

（六）通行碼設置原則，應儘量避免使用易猜測或公開資訊為設定。

五、本校電腦軟體版權之使用與管理

（一）禁止使用未經授權之電腦軟體，遵守智慧財產權相關規定。

（二）本校資訊機房伺服器所使用之電腦軟體均須具有合法版權，人員不得私自安裝非法電腦軟體。

（三）本校人員若有安裝機房伺服器軟體需求時，需填寫「設備進出記錄表」，經權責主管核准。

附件三

國立竹南高級中學

校內人員保密切結書

本人　　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，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。保密之義務，不因調職或離職而終止。如有違反，依法負刑事、民事及行政責任。

此致

國立竹南高級中學

立同意書人簽名：

身分證字號(末四碼)：

聯絡電話：

中　　華　　民　　國　　年　　月　　日

附件四

國立竹南高級中學資訊資產異動作業守則

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、資訊及資通系統之保管

(一)資訊及資通系統管理人應確保資訊及資通系統已盤點造冊並適切分級，並持續更新以確保其正確性。

(二)資訊及資通系統管理人應確保資訊及資通系統被妥善保存或備份。

(三)資訊及資通系統管理人應確保重要之資訊及資通系統已採取適當之存取控制政策。

二、資訊及資通系統之使用

(一)機關同仁使用資訊及資通系統應經其管理人授權。

(二)機關同仁使用資訊及資通系統時，應留意其資通安全要求事項，並負對應之責任。

(三)機關同仁使用資訊及資通系統後，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。

(四)本機關同仁使用本機關之資訊及資通系統，應確 實遵守相關資通安全要求，且未經授權不得任意複製資訊。

(五)對於資訊及資通系統，宜識別並以文件記錄及實作可被接受使用之規則。

三、資訊及資通系統之刪除或汰除

(一)資訊及資通系統之刪除或汰除前應評估機關是否已無需使用該等資訊及資通系統，或該等資訊及資通系統是否已妥善移轉或備份。

(二)資訊及資通系統之刪除或汰除時宜加以清查，以 確保所有機敏性資訊及具使用授權軟體已被移除或安全覆寫。

(三)具機敏性之資訊或具授權軟體之資通系統，宜採取實體銷毀，或以毀損、刪除或覆寫之技術，使原始資訊無法被讀取，並避免僅使用標準刪除或格式化功能。

附件五

國立竹南高級中學
存取控制管理守則

一、網路安全控管

（一）本機關之網路區域劃分如下：

1. 外部網路：對外網路區域，連接外部廣網路 (Wide Area Network, WAN)。
2. 非軍事區(DMZ)：放置對外服務伺服器之區段。
3. 內部區域網路 (Local Area Network, LAN) ：內部單位人員及內部伺服器使用之網路區段。

（二）外部網路、非軍事區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。

（三）應定期檢視防火牆政策是否適當，並適時進行防火牆軟、硬體之必要更新或升級。

（四）對於通過防火牆之來源端主機 IP 位址、目的端主機 IP 位址、來源通訊埠編號、目的地通訊埠編號、通訊協定、登入登出時間、存取時間以及採取的行動，均應予確實記錄。

（五）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。

（六）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。

（七）使用者應依規定之方式存取網路服務，不得於辦公室內私裝電腦及網路通訊等相關設備。

（八）網域名稱系統(DNS)防護

1. 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。
2. 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。
3. 內部主機位置查詢應指向機關內部 DNS 伺服器。

（九）無線網路防護

1. 機密資料原則不得透過無線網路及設備存取、處理或傳送。
2. 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。
3. 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。

4. 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。

二、 資通系統權限管理

（一）本機關之資通系統應設置通行碼管理，通行碼之要求需滿足：

1. 通行碼長度8碼以上。

2. 通行碼複雜度應包含英文大寫小寫、特殊符號或數字其中三種以上。

3. 使用者每90天應更換一次通行碼。

（二）使用者使用資通系統前應填妥本校資訊服務申請表，經授權後務必遵守資安相關使用規範。

（三）使用者應使用唯一之使用者 ID，除有特殊營運或作業必要經核准並紀錄外，不得共用 ID。

（四）使用者無繼續使用資通系統時，應立即停用或移除使用者 ID，資通系統管理者應定期清查使用者之權限。

三、特權帳號之存取管理

（一)資通系統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。

（二）資通系統之特權帳號不得共用。

（三）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。

（四）資通系統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。

（五）資通系統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。

四、加密管理

（一）機密資訊於儲存或傳輸時應進行加密。

（二）加密保護措施應遵守下列規定：

1. 應落實使用者更新加密裝置並備份金鑰。

2. 應避免留存解密資訊。

3. 一旦加密資訊具遭破解跡象，應立即更改之。

附件六

國立竹南高級中學
實體安全管理守則

一、電腦機房之門禁管理

1. 電腦機房應進行實體隔離。
2. 機關人員或來訪人員應申請及授權後方可進入電腦機房，電腦機房管理者並應定期檢視授權人員之名單。
3. 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。
4. 僅於必要時，得准許外部支援人員進入電腦機房。
5. 設備進出電腦機房應留存記錄。

二、電腦機房之環境控制

1. 電腦機房之空調、電力應建立備援措施。
2. 電腦機房之溫度維持在攝氏20至25度，濕度管控在40%至60%之間。
3. 電腦機房應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。
4. 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。

三、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系統應避免存放或設置於公眾可接觸場域。
5. 顯示存放機密資訊或具處理機密資訊之資通系統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. 資訊或資通系統相關設備，未經管理人授權，不得被帶離辦公室。

附件七

國立竹南高級中學
通信與作業管理守則

一、防範惡意軟體之控制措施

(一)主機及個人電腦應安裝防毒軟體，並時時進行軟、硬體必要更新或升級。

1. 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。

2. 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。

3. 確實執行網頁惡意軟體掃描。

(二)使用者未經同意不得私自安裝應用軟體，管理者並應每半年定期針對管理之設備進行軟體清查。

(三)使用者不得私自使用已知或有嫌疑惡意之網站。

(四)設備管理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。

二、遠距工作之安全措施

(一)資通系統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同意後始可開通。

(二)資通安全推動小組應定期審查已授權之遠距工作需　求是否適當。

(三)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。

1. 提供適當通訊設備，並指定遠端存取之方式。

2. 提供虛擬桌面存取，以防止於私有設備上處理及儲存資訊。

3. 進行遠距工作時之安全監視。

4. 遠距工作終止時之存取權限撤銷，並應返還相關設備。

三、電子郵件安全管理

(一)本機關人員到職後應經申請方可使用電子郵件帳號，並應於人員離職後刪除電子郵件帳號之使用。

(二)電子郵件系統管理人應定期進行電子郵件帳號清查。

(三)電子郵件伺服器應設置防毒及過濾機制，並適時進行軟硬體之必要更新。

(四)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。

(五)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。

(六)使用者不得利用機關所提供電子郵件服務從事侵害他人權益(七) 使用者應確保電子郵件傳送時之傳遞正確性。

(八)使用者使用電子郵件時，應注意電子簽章之要求事項。

(九)本機關應定期舉辦(或配合上級機關舉辦)電子郵件社交工程演練，並檢討執行情形。

四、資料備份

(一)重要資料及核心資通系統應進行資料備份，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。

(二)本機關應每季確認核心資通系統資料備份之有效性，且測試該等資料備份時，宜於專屬之測試系統上執行，而非直接覆寫原資通系統。

(三)敏感或機密性資訊之備份應加密保護。

五、儲存媒體防護措施

(一)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。

(二)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。

(三)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。

(四)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。

(五)儲存資訊之媒體若移作他用，則需將原資料完全清除。儲存機密等級資訊之媒體不可移作他用。

(六)儲存資訊之媒體若報廢，則需進行銷毀作業：

1. 硬碟或隨身碟：清除硬碟資料後破壞實體，使其無法讀取。
2. 光碟：兩面製造刮痕後切碎，使其無法讀取。
3. 磁帶或磁片：消磁後切碎，使其無法讀取。

六、電腦使用之安全管理

(一)電腦、業務系統或自然人憑證，若不使用超過十五分鐘時，應立即登出或啟動螢幕保護功能並取出自然人憑證。

(二)禁止私自安裝點對點檔案分享軟體及未經合法授權　軟體。

(三)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。

(四)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。

(五)下班時應關閉電腦及螢幕電源。

(六)如發現資安問題，應主動循機關之通報程序通報。

(七)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。

七、行動設備之安全管理

(一)機密資料不得由未經許可之行動設備存取、處理或傳送。

(二)機敏會議或場所不得攜帶未經許可之行動設備進入

八、即時通訊軟體之安全管理

(一)用即時通訊軟體傳遞機關內部公務訊息，其內容不得涉及機密資料。有業務需求者，應使用經專責機關鑑定相符機密等級保密機制或指定之軟、硬體，並依相關規定辦理。

(二)使用於傳遞公務訊息之即時通訊軟體應具備下列安全性需求：

1. 用戶端應有身分識別及認證機制。
2. 訊息於傳輸過程應有安全加密機制。
3. 應通過經濟部工業局訂定行動化應用軟體之中級檢測項目。
4. 伺服器端之主機設備及通訊紀錄應置於我國境內。
5. 伺服器通訊紀錄（log）應至少保存六個月。

附件八

國立竹南高級中學委外人員服務保密切結書

茲緣於簽署人＿＿＿＿＿＿＿＿（簽署人姓名）受＿＿＿＿＿＿＿＿＿＿＿＿（廠商名稱）委派至國立竹南高級中學執行業務，於業務執行期間有知悉或可得知悉或持有學校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　簽署人承諾於業務工作期間內及業務期滿或終止後，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，於學校指定之處所內使用之。非經學校事前書面同意，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露、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，亦不得攜至學校或學校所指定以外之處所。

第二條　簽署人知悉或取得學校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限內。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委派廠商人員。

第三條　簽署人不得私自將學校設備、檔案、文件等攜出，或對學校設備、檔案、文件等進行複製、擷取、記錄、傳遞等行為，也不得任意自校內或由校外遠端連結學校之網路與設備，若有需要，需經學校相關業務單位審核同意。

第四條　簽署人在下述情況下解除其應負之保密義務：

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不保密必要者。

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。

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。

第五條　簽署人若違反本同意書之規定，學校得請求簽署人及其任職之廠商賠償學校因此所受之損害並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。

第六條　簽署人因本同意書所負之保密義務，不因離職或其他原因失其效力。

第七條　本同意書壹式參份，學校、簽署人及廠商各執存一份。

簽署人簽名：

身份證字號(末四碼)：

聯絡電話：

所屬廠商及負責人簽章：

所屬廠商聯絡電話：

所屬廠商地址：

中　　華　　民　　國　　年　　月　　日

附件九

國立竹南高級中學委外廠商保密切結書

_____（廠商名稱，以下簡稱乙方）受 國立竹南高級中學（以下簡稱甲方）委託辦理_____（以下簡稱本案），乙方執行本案接觸之公務資料，具結依下列規定保密並履行責任：

第一條　乙方於本案進行期間因進行調查、搜集依合約所產生或所接觸之公務（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者。對所獲得或知悉之上述公務（機密）資料，乙方須負保密責任。

第二條　公務資料保密期限，不受本案工作完成（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資料，未經甲方書面同意或授權，不得洩漏或轉讓於第三者。

第三條　乙方違反資訊安全保密切結書之規定，致造成甲方或第三者之損害賠償，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。

第四條　本同意書壹式兩份，學校及廠商各執存一份。

此致

國立竹南高級中學

廠商代表人簽章：

具切結書廠商核章：

統一編號：

廠商地址：

廠商聯絡電話：

中　　華　　民　　國　　年　　月　　日

附件十

國立竹南高級中學
委外廠商受查核項目表

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。

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
	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。
	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運練。
	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。

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
	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。
	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？	☐	☐	☐	備份資料均有測試。
	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？	☐	☐	☐	均有設加密之保護措施。
	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。

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
	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。
	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	5.1 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。
	5.2 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。
	5.3 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	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

形之精進改善機制					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	10.1 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。
	10.2 是否追蹤過去缺失之改善情形？	□	□	□	有追蹤缺失改善之情形。
	10.3 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。

承辦人　　單位主管　　資通安全長