苗栗縣立文林國民中學

資通安全維護計畫

機密等級：一般

承辦人簽章：

單位主管簽章：

校長(資安長)簽章：

目　　錄

壹、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。

貳、適用範圍

本計畫適用範圍涵蓋苗栗縣立文林國民中學 (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	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	校務行政系統（向上集中）	■機關維運必要之業務	可能使本校部分業務中斷	由上級管理單位訂之
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。	校務行政系統（向上集中）	為本校依組織法執掌，足認為重要者。	可能使本校部分業務中斷	由上級管理單位訂之
輔導業務： 學生資料蒐集與分析、學生智力、性向、人格等測驗之實施，學生興趣、學習成就與志願之調查、輔導諮商之進行，並辦理	校務行政系統（向上集中）	為本校依組織法執掌，足認為重要者。	可能使本校部分業務中斷	由上級管理單位訂之

特殊教育及親職教育等事項。				
總務業務： 學校文書、事務及出納等事項。	校務行政系統（向上集中）	為本校依組織法執掌，足認為重要者。	可能使本校部分業務中斷	由上級管理單位訂之

二、 非核心業務及說明

非核心業務	業務失效影響說明	最大可容忍中斷時間
公文系統(向上集中)	可能使本校部分業務中斷	由上級管理單位訂之

本校之非核心業務及其最大可容忍中斷時間皆為 24 小時。

肆、資通安全政策及目標

一、 資通安全政策

(一)本校遵守最新版「苗栗縣政府資訊安全政策」。

二、 資通安全目標

(一)量化型目標

1. 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10%及 6%。
2. 主管及一般人員資通安全教育訓練，人員受訓且通過評量合格率達 90%。(含線上學習之人員)
3. 知悉資安事件發生，能於規定的時間完成通報、應變及復原作業。

(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。

三、 資通安全政策及目標之核定程序

資通安全政策、資通安全目標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，本校訂定校長為資通安全長，負責督導機關資通安全相關事項，其任務包括：

(二) 資通安全管理政策及目標之核定及督導。
(三) 資通安全責任之分配及協調。
(四) 資通安全資源分配。
(五) 資通安全防護措施之監督。
(六) 資通安全事件之檢討及監督。
(七) 資通安全相關規章與程序、制度文件核定。
(八) 資通安全管理年度工作計畫之核定
(九) 資通安全相關工作事項督導及績效管理。
(十) 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，由資通安全長召集人員代表成立「資通安全推動小組」，其任務包括：

1.跨部門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。

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) 資訊及資通系統之盤點及風險評估。
   (4) 資料及資通系統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規劃、辦理與推動。

陸、專職（責）人力及經費配置

一、 專職（責）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，本校現有資通安全人員名單及職掌應列冊，並適時更新。
   (1) 資通安全認知與訓練業務，負責推動資通安全教育訓練等業務之推動。
   (2) 資通安全防護業務，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) 資通安全管理法法遵事項業務，負責本校各處室法遵義務執行事宜。

(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，並提升機關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。

(四) 專業人力資源之配置情形應每年定期檢討。

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，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訊安全執行小組提出，由資訊安全執行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。

柒、資訊及資通系統之盤點

一、 資訊及資通系統盤點

（一）本校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。

二、 資訊及資通系統資產項目如下:

（一）資訊資產:以數位等形式儲存之資訊，如資料庫、資料檔案、系統文件、操作手冊、訓練教材、研究報告、作業程序、永續運作計畫、稽核紀錄及歸檔之資訊等。

（二）軟體資產:應用軟體、系統軟體、開發工具、套裝軟體及電腦作業系統等。

（三）實體資產:電腦及通訊設備、可攜式設備及資通系統相關之設備等。

（四）支援服務資產:相關基礎設施級其他機關內部之支援服務，如電力、消防等。

三、 本校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。

四、 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。核心資通系統及相關資產，並應加註標示。

五、 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。

六、 本校因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 D 級機關。

捌、資通安全風險評估

一、 資通安全風險評估

（一）本校每年針對資訊及資通系統資產進行風險評估。
資訊資源向上集中計畫，資訊系統由上級或監督機關兼辦或代管，則不需進行。

（二）本校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

本校配合資訊資源向上集中計畫，核心資訊系統均由上級或監督機關兼辦或代管，不再另行訂定。

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、 存取控制與加密機制管理

（一）網路安全控管

1. 本校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。
2. 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。

（二）加密管理

1.本校之機密資訊於儲存或傳輸時應進行加密。
2.本校之加密保護措施應遵守下列規定:
(1) 應避免留存解密資訊。
(2) 一旦加密資訊具遭破解跡象，應立即更改之。

二、 作業與通訊安全管理

（一）防範惡意軟體之控制措施

1.本校之主機及個人電腦應安裝防毒軟體，並時進行軟、硬體之必要更新或升級。
2.使用者未經同意不得私自安裝應用軟體。
3.使用者不得私自使用已知或有嫌疑惡意之網站。

（二）電子郵件安全管理

1.本校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。
2.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。
3.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。
4.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或違法之行為。
5.使用者應確保電子郵件傳送時之傳遞正確性。
6.使用者使用電子郵件時，應注意電子簽章之要求事項。
7.本校應定期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。

（三）確保實體與環境安全措施

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系統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。

（四）資料備份

1.敏感或機密性資訊之備份應加密保護。

（五）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.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。
3.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。

（六）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。

（七）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。

（八）即時通訊軟體之安全管理

使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。但有業務需求者，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。

三、 資通安全防護設備

（一）本校應建置防毒軟體、網路防火牆，持續使用並適時進行軟、硬體之必要更新或升級。

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，依本校資通安全事件通報應變程序辦理。

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。

（一）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。

（二）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。

（三）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

由資通安全推動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、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。

（四）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。

壹拾貳、資通系統或服務委外辦理之管理

本校為 D 級機關，無針對資通系統或服務辦理委外之管理需求。

壹拾參、資通安全教育訓練

一、 資通安全教育訓練要求

本校依資通安全責任等級 D 級之公務機關應辦事項辦理。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，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。

（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(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，應使其充分瞭解本校資通安全相關作業規範及其重要性。

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、苗栗縣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，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. 本校應配合上級或監督機關之規定辦理稽核作業，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。

（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，應配合上級或監督機關之規定辦理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。

三、 資通安全維護計畫之持續精進及績效管理

本校應於每年召開一次內部會議，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。

壹拾陸、資通安全維護計畫實施情形之提出

本校依據本法第 12 條之規定，應於每年定期向苗栗縣政府，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。

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）苗栗縣政府資訊安全政策

（八）苗栗縣政府及所屬各機關學校公務人員平時獎懲標準表