

# 資通安全維護計畫

## 目 錄

壹、 依據及目的 .....	4
貳、 適用範圍 .....	4
參、 核心業務及重要性 .....	4
一、 資通業務及重要性：.....	4
二、 非核心業務及說明：.....	4
肆、 資通安全政策及目標 .....	5
一、 資通安全政策.....	5
二、 資通安全目標.....	5
三、 資通安全政策及目標之核定程序.....	6
四、 資通安全政策及目標之宣導.....	6
五、 資通安全政策及目標定期檢討程序.....	6
伍、 資通安全推動組織 .....	6
一、 資通安全長.....	6
二、 資通安全推動小組.....	6
陸、 專責人力及經費配置 .....	7
一、 專責人力及資源之配置.....	7
二、 經費之配置.....	8
柒、 資訊及資通系統之盤點 .....	8
一、 資訊及資通系統盤點.....	8
二、 機關資通安全責任等級分級.....	9
捌、 資通安全風險評估 .....	9
一、 資通安全風險評估.....	9
二、 資通安全風險之因應.....	9
玖、 資通安全防護及控制措施 .....	9

一、 資訊及資通系統之管理.....	9
二、 存取控制與加密機制管理.....	10
三、 作業與通訊安全管理.....	11
四、 資通安全防護設備.....	12
壹拾、 資通安全事件通報、應變及演練 .....	12
壹拾壹、 資通安全情資之評估及因應 .....	12
一、 資通安全情資之因應措施.....	12
壹拾貳、 資通安全教育訓練 .....	13
一、 資通安全教育訓練要求.....	13
二、 資通安全教育訓練辦理方式.....	13
壹拾參、 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 .....	13
一、 資通安全維護計畫之實施.....	13
二、 資通安全維護計畫之持續精進及績效管理.....	13
壹拾肆、 資通安全維護計畫實施情形之提出 ....	14
壹拾伍、 相關表單 .....	14
一、 附件表單.....	14

## 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。

## 貳、適用範圍

本計畫適用範圍涵蓋台南市麻豆區麻豆國民小學(及附設幼兒園)。

## 參、核心業務及重要性

### 一、資通業務及重要性：

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	規定向上集中
教務業務	成績系統	為本校依組織法執掌，足認為重要者	影響學校部分教學業務運作	已完成
學生事務業務	學籍系統	為本校依組織法執掌，足認為重要者	影響學校部分教學業務運作	已完成
輔導業務	輔導系統	為本校依組織法執掌，足認為重要者	影響學校部分教學業務運作	已完成

### 二、非核心業務及說明：

非核心業務及說明如下表：

非核心業務	非核心資通系統	業務失效影響說明	規定向上集中
人事業務	行政院人事行政總處人事服務網	人事部份業務無法運作	已完成
會計業務	地方教育發展基金會會計資訊系統	會計部分業務無法運作	已完成
資訊組業務	校園網站	對外公告資訊無法運作	已完成

## 肆、資通安全政策及目標

### 一、資通安全政策

為使本校業務順利運作，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（Confidentiality）、完整性（Integrity）及可用性（Availability），特制訂本政策如下，以供全體同仁共同遵循：

1. 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. 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。
3. 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系統帳號。
7. 校內同仁及外部廠商須簽屬相關資通安全保密切結與同意書。

### 二、資通安全目標

#### （一）量化型目標

1. 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。
2. 校園電腦防毒軟體 100%啟用，並持續使用及適時進行軟、硬體之必要更新或升級。
3. 每人每年接受三小時以上之一般資通安全教育訓練。

#### （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、防止發生中毒或入侵事件。

### 三、資通安全政策及目標之核定程序

資通安全政策由本校校長核定並公告之。

### 四、資通安全政策及目標之宣導

1. 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，向所有人員進行宣導，並檢視執行成效。
2. 本校應每年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

依資通安全法第 11 條之規定，本校訂定校長為資通安全管理代表，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

本校設置「資通安全推動小組」負責督導校內資訊安全相

關事項，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，由資通安全管理代表召集各業務人員代表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，並依資通安全管理代表指示負責下列事項，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. 資通安全推動小組：
  - (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。
  - (6) 資訊及資通系統之盤點及風險評估。
  - (7) 資通安全相關規章與程序、制度之執行。
  - (8) 資料及資通系統之安全防護事項之執行。
  - (9) 資通安全事件之通報及應變機制之執行。
  - (10) 每年得須參加縣市辦理之相關資訊安全研習。

## 陸、專責人力及經費配置

### 一、專責人力及資源之配置

1. 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。

2. 本校之承辦單位於辦理資通安全業務時，應加強資通安全人員之培訓，並提升校內資通安全專業人員之資通安全管理能力。如資通安全人力或經驗不足，得洽請台南市教育局或相關專業機關之人員，提供顧問諮詢服務。
3. 本校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。
4. 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。
2. 校內如有資通安全資源之需求，應向上級機關提出申請，由上級機關審核後，進行相關之建置。
3. 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. 本校每年辦理資訊及資通系統資產盤點，依管理責任及使用人員指定對應之資產管理人，並依資產屬性進行分類，分別為資訊資產、軟體資產、實體資產、支援服務資產等。
2. 資訊及資通系統資產項目如下：
  - (1) 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。
  - (2) 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。
  - (3) 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。
  - (4) 支援服務資產：相關基礎設施及其他機關內部之支援服務，

如電力、消防等。

- (5) 人員資產：校內各項資訊系統與設備使用人員清冊。
- (6) 資料資產：以紙本形式儲存之資訊，如程序、清單、計畫、報告、指引手冊、政策、公文、作業紀錄、作業規範、各種應用系統文件及管理手冊，契約、法律文件、軟體使用授權等等。

## 二、機關資通安全責任等級分級

依據教育部臺教資(四)字第 1070202157 號函文，本校為公立高級中等以下學校，且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，其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

本校配合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，不需進行。

### 二、資通安全風險之因應

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

#### (一) 資訊及資通系統之使用

1. 本校同仁使用資訊及資通系統前應經其管理人授權。
2. 本校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。
3. 本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。

4. 非本校同仁使用本機關之資訊及資通系統，應確實遵守本機關之相關資通安全要求，且未經授權不得任意複製資訊。
5. 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。

## 二、存取控制與加密機制管理

### (一) 網路安全控管

#### 1. 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) 內部區域網路 (Local Area Network, LAN)：機關內部單位人員及內部伺服器使用之網路區段。
2. 外部網路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。
  3. 本校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。若為向上集中管理，則由上級單位統一辦理更新與升級。
  4. 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。
  5. 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) 資通系統權限管理

1. 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。資通系統通行碼依上級或監督機關之要求進行設置。
2. 使用者使用資通系統前應經授權，並使用唯一之使用者 ID，除有特殊營運或作業必要經核准並紀錄外，不得共用 ID。
3. 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、作業與通訊安全管理

#### (一) 防範惡意軟體之控制措施

1. 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。
  - (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
2. 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。
3. 使用者不得私自使用已知或有嫌疑惡意之網站。
4. 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) 確保實體與環境安全措施

1. 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，管理者並應定期檢視授權人員之名單。
  - (3) 人員及設備進出應留存記錄。
2. 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，以減少環境不安全之危險。
3. 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) 機密性及敏感性資訊，不使用或下班時應該上鎖。

### (三) 資料備份

1. 重要資料及資通系統應進行資料備份，並執行異地存放。
2. 敏感或機密性資訊之備份應加密保護。

### (四) 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。

## 四、資通安全防護設備

1. 防火牆、電子郵件伺服器為向上集中管理，由上級單位統一辦理更新與升級。

## 壹拾、資通安全事件通報、應變及演練

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，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、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。

## 壹拾貳、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

1. 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，以建立人員資通安全認知，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。
2. 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。
3. 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。

## 壹拾參、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、資通安全維護計畫之持續精進及績效管理

1. 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。
2. 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：
    - A. 資通安全政策及目標之實施情形。
    - B. 人力及資源之配置之實施情形。
    - C. 資通安全防護及控制措施之實施情形。
    - D. 不符合項目及矯正措施。
  - (4) 資通安全事件之處理及改善情形。
  - (5) 利害關係人之回饋。
  - (6) 持續改善之機會。
3. 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。

#### 壹拾肆、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，向上級或監督機關，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。

#### 壹拾伍、相關表單

##### 一、附件表單

1. 資通安全推動小組成員及分工表
2. 資通安全保密同意書
3. 資通安全需求申請單
4. 資訊及資通系統資產清冊
5. 風險評估表
6. 管制區域人員進出登記表
7. 年度資通安全教育訓練計畫
8. 資通安全認知宣導及教育訓練簽到表
9. 資通安全維護計畫實施情形

10. 審查結果及改善報告

11. 改善績效追蹤報告