臺南市善化區小新國民小學

資通安全維護計畫

機密等級：一般

承辦人簽章：教師兼事務組長蘇育志

單位主管簽章：教師兼教務主任黃靜慧

資安長簽章：校長謝慶皇

校長簽章：校長謝慶皇

資通安全維護計畫

目　　錄

壹、 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、 臺南市政府資訊安全政策。

三、 其他相關業務法規名稱。

貳、 適用範圍

本計畫適用範圍涵蓋臺南市善化區小新國民小學（以下簡稱本機關）。

參、 核心業務及重要性

一、 核心業務及重要性：

本機關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	國小學籍系統（向上集中） 國小成績系統（向上集中）	為本機關依組織法執掌，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
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	為本機關依組織法執掌，足認為重要者。	無	無
總務業務：學校文書、事務及出納等事項	公文系統（向上集中）	為本機關依組織法執掌，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、	國小輔導系統（向上集中）	為本機關依組織法執掌，足認為	可能使本校部分業務中	由上級管理單

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，並辦理特殊教育及親職教育等事項。		重要者。	斷	位訂之

各欄位定義：

1. 核心業務：請參考資通安全管理法施行細則第 7 條之規定列示。

2. 核心資通系統：該項核心業務所必須使用之資通系統名稱。

3. 重要性說明：說明該業務對機關之重要性，例如對機關財務及信譽上影響，對民眾影響，對社會經濟影響，對其他機關業務運作影響，法律遵循性影響或其他重要性之說明。

4. 業務失效影響說明：該項業務使用之系統失效後，機關業務運作有何影響。

5. 最大可容忍中斷時間單位以小時計(對外服務以小時，對內服務以工作小時計)。

二、 非核心業務及說明：

本機關之非核心業務及說明如下表：

非核心業務	業務失效影響說明	最大可容忍中斷時間
學校首頁(向上集中)	可能使本校部分業務中斷	24小時

各欄位定義：

1. 非核心業務系統：公務機關非核心業務相關之資通系統，如郵件服務、用戶端服務等。

2. 業務失效影響說明：該項業務使用之系統失效後，機關業務運作有何影響。

3. 最大可容忍中斷時間單位以小時計(對外服務以小時，對內服務以工作小時計)。

肆、 資通安全政策及目標

一、 資通安全政策

為使本機關業務順利運作，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），依據臺南市政府資訊安全政策如下，以供全體同仁共同遵循：

1. 安全：確保資訊不遭竊取、竄改、滅失或遺漏。
2. 正確：資訊內容及處理過程精準無誤。
3. 迅速：對資安事件之處理、通報與回復能快速完成。

二、 資通安全目標

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

資通安全政策由本機關簽陳資通安全長核定。

四、 資通安全政策及目標之宣導

1. 本機關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，向機關內所有人員進行宣導。
2. 本機關應每年向利害關係人(例如 IT 服務供應商、與機關連線作業有關單位)進行資安政策及目標宣導。

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管理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

依本法第11條之規定，本機關擇請校長兼任本機關資通安全

長，負責督導機關資通安全相關事項，其任務包括：

1. 資通安全管理政策及目標之核定、核轉及督導。

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、 資通安全推動組織

(一) 本機關設置「資通安全推動小組」負責督導機關資通安全相關事項，為推動本機關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，其任務宜包括：

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

本機關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，本機關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，其工作內容得參考下列事項：

(1) 資通安全政策及目標之研議。

(2) 訂定機關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機關年度工作計畫。

(4) 傳達機關資通安全政策與目標。

(5) 其他資通安全事項之規劃。

(6) 資通安全技術之研究、建置及評估相關事項。

(7) 資通安全相關規章與程序、制度之執行。

(8) 資訊及資通系統之盤點及風險評估。

(9) 資料及資通系統之安全防護事項之執行。

(10)資通安全事件之通報及應變機制之執行。

(11)其他資通安全事項之辦理與推動。

(12)每年定期召開資通安全管理審查會議，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. 本機關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，其分工如下。

   (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，負責本機關對所屬公務務機關或所管特定非公務機關之法遵義務執行事宜。

2. 本機關之承辦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。

3. 本機關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，應簽屬書面約定，並視需要實施人員輪調，建立人力備援制度。

4. 本機關之首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。

5. 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

1. 資通安全推動小組於規劃配置相關經費及資源時，應考量本機關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. 各單位如有資通安全資源之需求，應配合機關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。

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

本機關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。相關事項本機關未訂者得參考引用 ISMS-02-06 資訊資產管理規範」要求辦理。

二、 機關資通安全責任等級分級

依據教育部臺教資(四)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

1. 本機關應每年針對資訊及資通系統資產進行風險評估，若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，則不需進行。

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「詳細風險評鑑方法」進行風險評估之工作。

3. 相關事項本機關未訂者得參考引用 ISMS-02-01 風險評鑑與管理規範」要求辦理。

4. 本機關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

本機關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

(一) 資訊及資通系統之保管

1. 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。

2. 資訊及資通系統管理人應確保資訊及資通系統被妥善的保存或備份。

3. 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

1. 本機關同仁使用資訊及資通系統前應經其管理人授權。

2. 本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。

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. 非本機關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。

(三) 資訊及資通系統之刪除或汰除

1. 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。

2. 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。

3. 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。

二、 存取控制與加密機制管理

(一) 網路安全控管

1. 本機關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。

2. 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。

3. 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。

4. 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。

5. 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

1. 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、特殊符號或數字三種以上。

(3) 使用者每90天應更換一次通行碼。

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) 特權帳號之存取管理

1. 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。

2. 資通系統之特權帳號不得共用。

3. 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。

4. 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。

5. 資通系統之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

1. 本機關之機密資訊於儲存或傳輸時應進行加密。

2. 本機關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。

(五) 其它相關事項本機關未訂者得參考引用 ISMS-02-11 存取控制管理規範」與「ISMS-03-11 帳號註冊註銷作業

程序書」要求辦理。

三、 作業與通訊安全管理

(一) 防範惡意軟體之控制措施

1. 本機關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。

(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) 遠距工作之安全措施

1. 本機關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。

2. 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) 電子郵件安全管理

1. 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。

2. 應定期進行電子郵件帳號清查。

3. 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，若為向上集中管理，則由上級單位統一辦理。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。

4. 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。

5. 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。

6. 使用者應確保電子郵件傳送時之傳遞正確性。

7. 使用者使用電子郵件時，應注意電子簽章之要求事項。

8. 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) 確保實體與環境安全措施

1. 資料中心及電腦機房之門禁管理

(1) 資料中心及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資料中心及電腦機房，資料中心及電腦機房管理者並應定期檢視授權人員之名單。

(3) 機關人員應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資料中心及電腦機房。

(5) 人員及設備進出資料中心及電腦機房應留存記錄。

(6) 其它本機關未訂者得參考引用 ISMS-02-08 實體及環境安全規範」要求事項辦理。

2. 資料中心及電腦機房之環境控制

(1) 資料中心及電腦機房應安裝之安全偵測及防護措施，如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。

(2) 各項安全設備應定期執行檢查、維修。

(3) 其它本機關未訂者得參考引用 ISMS-03-04 電腦機房管理作業程序書」要求事項辦理。

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) 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。

(7) 其它本機關未訂者得參考引用 ISMS-02-08 實體及環境安全規範」要求事項辦理。

(五) 資料備份

1. 重要資料及核心資通系統應進行資料備份，並執行異地存放。

2. 本機關應定期確認核心資通系統資料備份之有效性。

3. 敏感或機密性資訊之備份應加密保護。

4. 其它本機關未訂者得參考引用 ISMS-03-05 備份管理作業程序書」要求事項辦理。

(六) 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. 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。

3. 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。

4. 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。

5. 其它本機關未訂者得參考引用 ISMS-03-02 電腦設備及媒體管理作業程序書」要求事項辦理。

(七) 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。

(八) 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

3. 其它本機關未訂者得參考引用 ISMS-02-10 網路安全管理規範」要求事項辦理。

(九) 即時通訊軟體之安全管理

1. 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。

2. 使用於傳遞公務訊息之即時通訊軟體宜考量下列安全性需求：

(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。

四、 系統獲取、開發及維護

1. 本機關之資通系統應依「資通安全責任等級分級辦法」之規定完成系統防護需求分級，依分級之結果，完成資通系統防護基準，並注意下列事項：

(1) 如涉及個人資料，開發過程請依安全系統發展生命週期

(Secure Software Development Life Cycle, SSDLC)納入資安要求，並參考行政院國家資通安全會報頒布之最新「安全軟體發展流程指引」、「安全軟體設計指引」及「安全軟體測試指引」。

(2) 於資通系統開發前，設計安全性要求，並檢討執行情形。

(3) 於上線前執行安全性要求測試，並檢討執行情形。

(4) 執行資通系統源碼安全措施，包含源碼存取控制與版本控管，並檢討執行情形。

2. 其它本機關未訂者得參考引用 ISMS-02-12 系統開發與維護規範」要求事項辦理。

五、 業務持續運作演練

本機關為 D 級機關無需針對核心資通系統制定業務持續運作計畫與演練。

六、 執行資通安全健診

本機關為 D 級機關無需執行資通安全健診作業。

七、 資通安全防護設備

1. 本機關應建置防毒軟體、防火牆，如有設置電子郵件伺服器應建立電子郵件過濾裝置，持續使用並適時進行軟、硬體之必要更新或升級。前項之防火牆、電子郵件伺服器若為向上集中管理，則由上級單位統一辦理更新與升級。

2. 資安設備設定異動應保留相關修改紀錄，並定期檢討執行情形。

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，本機關應訂定資通安全事件通報、應變及演練相關機制，詳資通安全事件通報應變程序。

其它本機關未訂者得參考引用臺南市政府及所屬機關資通安全事件通報及應變管理程序」與「ISMS-02-13 安全事件回報及處理規範」要求事項辦理。

壹拾壹、 資通安全情資之評估及因應

本機關接獲資通安全情資，應評估該情資之內容，並視其對本

機關之影響、本機關可接受之風險及本機關之資源，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

本機關接受資通安全情資後，應指定人員進行情資分析，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。

(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、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。

(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

本機關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

由經指派之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

本機關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。

其它本機關未訂者得參考引用 ISMS-02-05 資訊作業委外管理規範」要求事項辦理。

壹拾參、 資通安全教育訓練

一、 資通安全教育訓練要求

本機關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。

2. 本機關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，應使其充分瞭解本機關資通安全相關作業規範及其重要性。

4. 資通安全教育及訓練之政策，除適用所屬員工外，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

本機關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，及本機關各相關規定辦理之。

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，使本機關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，應與本機關之資通安全政策、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. 資通安全推動小組應配合上級機關要求執行內部稽核作業，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。

2. 辦理稽核前上級機關應擬定資通安全稽核計畫並安排稽核成員，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。

3. 其它本機關未訂者得參考引用 ISMS-02-16 資安稽核管理規範」要求事項辦理。

(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，應據此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

1. 本機關之資通安全推動小組應每年定期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) 過往管理審查議案之處理狀態。

(2) 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。

(3) 資通安全維護計畫內容之適切性。

(4) 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. 資通安全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. 內外部稽核結果。

E. 不符合項目及矯正措施。

(5) 風險評鑑結果及風險處理計畫執行進度。

(6) 重大資通安全事件之處理及改善情形。

(7) 利害關係人之回饋。

(8) 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。

壹拾陸、 資通安全維護計畫實施情形之提出

本機關依據本法第11條之規定，應於次年向上級或監督機關，提出上年度資通安全維護計畫實施情形，使其得瞭解本機關上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

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

17. 本機關資通安全事件通報及應變程序

18. 其它本機關未訂者得參考引用 ISMS」資訊安全管理系統文件

二、 附件表單

1. 臺南市政府「ISMS-04-02 文件總覽表」

臺南市善化區小新國民小學

學校資通安全事件通報及應變管理程序

目錄

壹、 目的

臺南市善化區小新國民中/小學(以下簡稱本校)為遵照資通安全管理法第14條及本校資通安全維護計畫之規定，建立資通安全事件之通報及應變機制，以迅速有效獲知並處理事件，特制定本資通安全事件通報及應變管理程序(以下稱本管理程序)。

貳、 適用範圍

發生於本校之事件，系統、服務或網路狀態經鑑別而顯示可能有違反資通安全政策或保護措施失效之狀態發生，影響資通系統機能運作，構成資通安全政策之威脅者。

參、 責任

一、本校於發現資通安全事件時，應依本程序或權責人員之指示，執行通報及應變事務。

二、本校應視必要性，與受託機關約定，使其制定其資通安全事件通報及應變管理程序，並於知悉資通安全事件後向本部進行通報，於完成事件之通報及應變程序後，依本校指示提供相關之紀錄或資料。

三、本校應於知悉資通安全事件後，應依本程序之規定，儘速完成損害控制、復原與事件之調查及處理作業。完成後，應依教育部指定之方式進行結案登錄作業，並送交調查、處理及改善報告。

肆、 事件通報窗口及緊急處理小組

一、臺灣學術網路資通安全事件委託由臺灣學術網路危機處理中心之教育機構資安通報應變小組(簡稱通報應變小組)負責，聯繫資訊如下：

(一) 聯絡電話：(07)525-0211

(二) 網路電話：98400000

(三) 電子郵件：service@cert.tanet.edu.tw

二、本校應至少指派二位以上資安聯絡人員，並於「教育機構資安通報應變平台」(https://info.cert.tanet.edu.tw)登錄相關聯絡資料，如有異動亦應立即上網更新。

三、本校之資通安全事件通報窗口及聯繫專線為：

聯絡人姓名	職稱	電話	E-mail
蘇育志	教師	06-5837019	suyuch@tn.edu.tw
吳忠泰	教師	06-5837019	tnwct951@tn.edu.tw
莊牧軒	職員	06-5837019	mushiuan@tn.edu.tw
鄭登文	教師	06-5837019	dayinone8153@tn.edu.tw

四、本校應以適當方式使相關人員明確知悉本機關之通報窗口及聯絡方式。

五、本校所屬人員知悉資通安全事件後，應立即至教育機構資安通報平台(https://info.cert.tanet.edu.tw)通報登錄資安事件細節、影響等級及支援申請等資訊。

六、本校應確保通報窗口之聯絡管道全天維持暢通，若因設備故障或其他情形導致窗口聯絡管道中斷，該中斷情況若持續達一小時以上者，應即將該情況告知相關人員，並即提供其他有效之臨時聯絡管道。

七、負責事件處理之單位(該事件發生之單位)權責人員應與相關單位密切合作以進行事件之處理，並使通報窗口適時掌握事件處理之進度及其他相關資訊。

八、事件經初步判斷認為可能屬重大(第「三」級、第「四」級)資安事件或事態嚴重時，應即向資通安全長報告，由資通安全長成立緊急處理小組，立即協助進行處理；接獲本校所屬分校或受託廠商所通報之資通安全事件時，亦同。

九、緊急處理小組成員由資通安全長指派機關之資通安全相關技術人員擔任，或亦得由其他機關資通安全相關技術人員或外部專家擔任之。

十、各相關權責人員應紀錄事件處理過程，並檢討事件發生原因，著手進行改善，並留存必要之證據。

伍、 通報程序

一、通報作業程序

(一)判定事件等級之流程及權責

本校之權責人員或緊急處理小組應依據以下事項，於知悉資通安全事件後，依規定完成「資通安全事件通報及應變辦法」之資通安全事件等級判斷：

1. 事件涉及核心業務或關鍵基礎設施業務之資訊與否。

2. 事件導致業務之資訊或資通系統遭竄改之影響程度，屬嚴重或輕微。

3. 事件所涉資訊是否屬於國家機密、敏感資訊或一般公務機密。

4. 機關業務運作若遭影響或資通系統停頓，是否可容忍中斷時間內能回復正常運作。

5. 事件其他足以影響資通安全事件等級之因素。

(二)本校因網路或電力中斷等事由，致無法依前項規定方式為通報者，應於確認資安事件條件成立後1小時內，與所隸屬區縣市網路中心及通報應變小組聯繫，先行提供該次資安事件應通報之內容及無法通報依規定方式通報之事由，並於事由解除後，依原方式補行通報。

(三)資通安全事件等級如有變更，本校權責人員或通報應變小組應告知通報單位，使其續行通報作業。

(四)本校於委外辦理資通系統之建置、維運或提供資通服務之情形時，應於合約中訂定委外廠商於知悉資通安全事件時，應即向委託單位所屬之權責人員通知，以指定之方式進行通報。

(五)本校於知悉資通安全事件後，如認該事件之影響涉及其他機關或應由其他機關依其法定職權處理時，權責人員或通報應變小組應於知悉資通安全事件後一小時內，將該事件依教育部或行政院所指訂或認可之方式，通知該機關。

(六)本校執行通報應變作業時，得視情形向所隸屬區縣市網路中心人員提出技術支援或其他協助之需求。

陸、 應變程序

一、事件發生前之防護措施規劃

本校應於平時妥善實施資通安全維護計畫，並以組織營運目標與策略為基準，透過整體之營運衝擊分析，規劃業務持續運作計畫並實施演練，以預防資安事件之發生。

二、損害控制機制

(一)負責應變之權責人員或緊急處理小組，應完成以下應變事務之辦理，並留存應變之紀錄

1. 資安事件之衝擊及損害控制作業。

2. 資安事件所造成損害之復原作業。

3. 重大(第「三」級、第「四」級)資安事件相關鑑識及其他調查作業。

4. 重大(第「三」級、第「四」級)資安事件之調查與處理及改善報告之方

式。

5. 重大(第「三」級、第「四」級)資安事件後續發展及與其他事件關聯性之監控。

6. 資訊系統、網路、機房等安全區域發生重大事故或災難，致使業務中斷時，應依據本機關事前擬定之緊急計畫，進行應變措施以恢復業務持續運作之狀態。

7. 其他資通安全事件應變之相關事項。

(二)對於第一級、第二級資通安全事件，本校應於知悉事件後七十二小時內完成前項事務之辦理，並應留存紀錄；於第三級、第四級資通安全事件，本校應於知悉事件後三十六小時內完成損害控制或復原作業，並執行上述事項，及留存相關紀錄。

(三)本校完成資安事件處理後，須至教育機構資安通報平台填報資安事件處理辦法及完成時間。

(四)本校於知悉受託廠商發生與受託業務相關之資通安全事件時，應於知悉委外廠商發生第一、二級資通安全事件後七十二小時內，確認委外廠商已完成損害控制或復原事項之辦理；於知悉委外廠商發生第三、四級資通安全事件後三十六小時內，確認委外廠商完成損害控制或復原事項之辦理。

柒、重大(第「三」級、第「四」級)資安事件後之復原、鑑識、調查及改善機制

一、本校若發生重大(第「三」級、第「四」級)資通安全事件時，於完成資通安全事件之通報及應變程序後，應針對事件所造成之衝擊、損害及影響進行調查及改善，並應於事件發生後一個月內完成資通安全事件調查、處理及改善報告。

二、重大(第「三」級、第「四」級)資通安全事件調查、處理及改善報告應包括以下項目：

(一)事件發生、完成損害控制或復原作業之時間。

(二)事件影響之範圍及損害評估。

(三)損害控制及復原作業之歷程。

(四)事件調查及處理作業之歷程。

(五)為防範類似事件再次發生所採取之管理、技術、人力或資源等層面之措施。

(六)前款措施之預定完成時程及成效追蹤機制。

三、本校應向所隸屬之上級機關及教育部提出前項之報告，以供監督與檢討。

捌、 紀錄留存及管理程序之調整

一、本校應將資通安全事件之通報與應變作業之執行、事件影響範圍與損害程度以及其他通報應變之執行情形，於「教育機構資安通報平台」上填報完整之紀錄，該平台事件通報應變紀錄由通報應變小組於年度彙整後，提交至本部資訊及科技教育司覆核備查。

二、本校於完成資通安全事件之通報及應變程序後，應依據實際處理之情形，於必要時對本管理程序、人力配置或其他相關事項進行修正或調整。

玖、 演練作業

一、本校應配合教育部依資通安全事件通報應變辦法之規定所辦理之社交工程演練、資通安全事件通報及應變演練。

二、本校應配合行政院依資通安全事件通報應變辦法之規定所辦理之下列資通安全演練作業：

(一)社交工程。

(二)資安事件通報及應變

(三)網路攻防

(四)情境演練

(五)其他資安演練