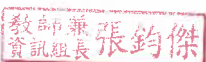


臺南市南新國民中學


資通安全維護計畫

115年度

機密等級：一般

承辦人簽章：

單位主管簽章：

資安長簽章：

校長簽章：

五、	業務持續運作演練.....	17
六、	執行資通安全健診.....	17
七、	資通安全防護設備.....	17
壹拾、	資通安全事件通報、應變及演練相關機制.....	17
壹拾壹、	資通安全情資之評估及因應.....	17
一、	資通安全情資之分類評估.....	18
二、	資通安全情資之因應措施.....	18
壹拾貳、	資通系統或服務委外辦理之管理.....	19
壹拾參、	資通安全教育訓練.....	19
一、	資通安全教育訓練要求.....	19
二、	資通安全教育訓練辦理方式.....	19
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.....	20
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.....	20
一、	資通安全維護計畫之實施.....	20
二、	資通安全維護計畫實施情形之稽核機制.....	20
三、	資通安全維護計畫之持續精進及績效管理.....	21
壹拾陸、	資通安全維護計畫實施情形之提出.....	22
壹拾柒、	相關法規、程序及表單.....	22
一、	相關法規及參考文件.....	22
二、	附件表單.....	23

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，並辦理特殊教育及親職教育等事項。	國中輔導心測系統(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
--	----------------	--------------------	-------------	-----------

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	由上級管理單位訂之

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，如差勤服務、郵件服務、用戶端服務等。(請依機關實際情形列出)
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。

伍、資通安全推動組織

一、資通安全長

依本法第11條之規定，本機關擇請教務主任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：

- 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。

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。

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。

- (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。

(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

(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。

(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。

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」