臺南市立新化國民中學資通安全管理辦法

經 102 年 1 月 18 日校務會議通過

經 103 年 2 月 10 日校務會議修正

經 107 年 6 月 29 日校務會議修正草案

一、依據

- 教育部 103 年 02 月 07 日函頒國中、小學資通安全管理系統實施原則。
- 個人資料保護法
  中華民國 101 年 9 月 21 日行政院院臺法字第 1010056845 號令發布除第 6、54 條條文外，其餘條文定自一百零一年十月一日施行。
- 個人資料保護法施行細則
  中華民國 101 年 9 月 26 日法務部法令字第 10103107360 號令修正發布名稱及全文 33 條；並自一百零一年十月一日施行。

二、目的

確保臺南市立新化國民中學（以下簡稱本校）所屬之資訊資產機密性、完整性及可用性，並符合相關法規之要求，使其免於遭受內、外部的蓄意或意外之威脅。

三、適用範圍

本校校內電腦、資訊與網路服務相關的系統、設備、程序及人員，包含合約廠商及其它經授權使用之人員。

四、實施原則

1 網路安全

1.1　網路控制措施

1.1.1 本校與外界連線，僅限於經由教育局(處)網路管理。

1.1.2 禁止私人架設網路（如：電話線、2G 或 3G 網路等）連結機房內之主機電腦或網路設備。

1.1.3 本校網段區分為伺服器、教學、行政、教師個人上網、網路電話、無線網路基地台、等。

1.1.4 避免外部連入，若有需要存取時，使用保留 ip 並限制使用者之來源 IP 及網路連線埠(Port)，以及開放時間。

1.2 無線網路存取

1.2.1 禁止使用者私自將無線網路存取設備介接至校園網路；若有需要必須向資訊組申請同意並設定帳號通行碼或加密金鑰。

1.2.2 本校提供無線網路存取服務:

- 特定辦公室提供無線網路熱點供公務使用，使用前需向資訊組登記網路實體位址 MAC Address。
- 於教學區域、會議室可使用 TN_Teacher、TN_Shjhs、TANetRoaming。
- 校外人士可使用 TANetRoaming 無線上網服務。
- TN_Teacher、TN_Shjhs、TANetRoaming 等熱點統一由本市教育局資訊中心協助管理。

2 系統安全

2.1 設備區隔

伺服器主機可依個別應用系統之需要，設置專屬主機/vm，以避免未經授權之存取。

2.2 對抗惡意軟體、隱密通道及特洛依木馬程式

2.2.1 個人電腦應:

- 本校提供 officeScan 毒軟體，可由伺服器端進行病毒碼更新的管理。自行安裝防毒軟體請將軟體設定為自動定期更新病毒碼。
- 作業系統及軟體應定期更新，以防範系統漏洞。

2.2.2 個人電腦所使用的軟體應有授權。

2.2.3 新伺服器系統啓用前，應執行相關程序(如：確認適合該作業系統之掃毒工具、預設通行碼更新、系統更新等，並記錄於啓用與報廢紀錄單)，以防範可能隱藏的病毒或後門程式。（啓用與報廢紀錄單格式，文件編號 A-1）

2.3 桌面淨空與螢幕淨空政策

2.3.1 個人電腦辦公桌面應避免存放機敏性文件，結束工作時，應將其所經辦或使用具有機密或敏感特性的資料（如公文、學籍資料等）妥善存放。

2.3.2 當個人電腦或終端機不使用時，應使用鍵盤鎖或其他控管措施保護個人電腦及終端機安全個人電腦應設定螢幕保護機制。

2.4 資料備份

本校系統管理人員需針對本校重要系統（例如系統檔案、應用系統、資料庫等）定期進行備份工作，或採用自動備份機制；週期為每週進行一次。

2.5 資訊工作日誌

2.5.1 系統管理人員需針對重要電腦系統進行檢查、維護、更新等動作時，應針對這些活動填寫日誌予以紀錄，作為未來需要時之查核。（文件編號 A-2）

2.5.2 系統每日自動執行一次校時。

2.6 資訊存取限制

1 共用的個人電腦（如：電腦教室電腦、教師休息室電腦等）僅提供教師教學準備或支援部份教學活動之使用，寒暑假將定期還原與更新。

2.7 使用者註冊

2 人員報到或離退職應會辦電腦系統帳號管理人員，執行電腦系統的使用者註冊及註銷程序，透過該註冊及註銷程序來控制使用者資訊服務的存取，該作業應包括以下內容:

- 本校新進人員，資訊人員將會以教育局資訊中心郵件系統之帳號，註冊至本校各應用系統上，再由使用者自訂其密碼。若使用者有其特殊需求，也可另行單獨申請變更。
- 本校人員離職後，資訊人員應立即註銷該員在各應用系統的帳號及使用權。
- 本校資訊人員，必須妥善管理各應用系統之使用者帳號。
  - 每人使用唯一的使用者識別碼（ID）。
  - 檢查使用者是否經過系統管理單位之授權使用資訊系統或服務。
  - 保存一份包含所有識別碼註冊的記錄。
  - 使用者調職或離職後，應移除其識別碼的存取權限。
  - 定期（建議每學期）檢查並取消多餘的使用者識別碼和帳號。

2.8 特權管理

3 電腦與網路系統資訊具有存取特權人員清單、及其所持有的權限說明，應予以文件化記錄或有系統統整檢視。（參考系統特權帳號清單格式，文件編號 A-4）

2.9 密碼（**Password**）之使用

2.9.1 本校各資訊系統與服務應避免使用共同帳號及密碼。

2.9.2 使用者應該對其個人所持有通行碼盡保密責任。

2.9.3 設定各應用系統的帳號密碼時，請遵循以下原則:

- 混合大寫與小寫字母、數字，特殊符號。
- 密碼越長越好，最短也應該在 8 個字以上。
- 至少每三個月改一次密碼。
- 使用技巧記住密碼
  - 使用字首字尾記憶法:

a. My favorite student is named Sophie Chen，取字頭成為 mFSinsC

b. There are 26 lovely kids in my English class，取字尾成為 Ee6ysnMEc

- 中文輸入按鍵記憶法：

  a. 例如「密碼」的注音輸入為「wj/ vu/6a83」

2.9.4 設定時注意事項

- 嚴禁不設密碼、與帳號相同或與主機名稱相同。
- 不要使用與自己有關的資訊，例如學校或家裡電話、親朋好友姓名、身份證號碼、生日等。
- 不重覆電腦鍵盤上的字母，例如 6666rrrr 或 qwertyui 或 zxcvbnm。
- 不使用連續或簡單的組合的字母或數字，例如 abcdefgh 或 12345678 或 24681024
- 避免全部使用數字，例如 52526565。
- 避免使用字典找得到的英文單字或詞語，如 TomCruz 、superman
- 不要使用電腦的登入畫面上任何出現的字。
- 不分享密碼內容給任何人，包括男女朋友、職務代理人、上司等。

2.10 通報安全事件與處理

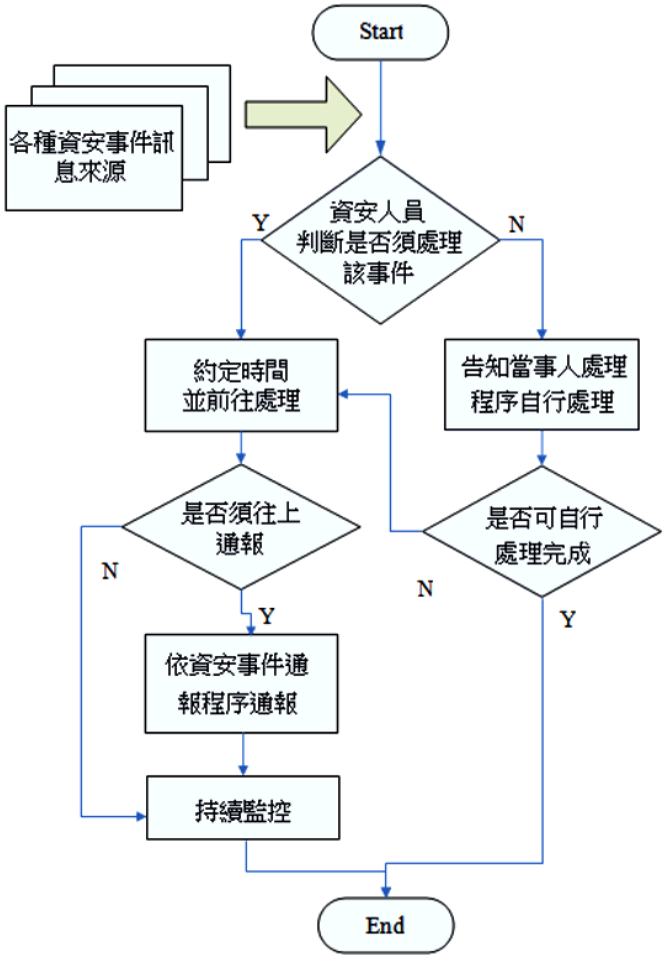
2.10.1 資訊安全事件包括：系統被入侵、對外攻擊、針對性攻擊、散播惡意程式、中繼站、電子郵件社交工程攻擊、垃圾郵件、命令或控制伺服器、殭屍電腦、惡意網頁、惡意留言、網頁置換、釣魚網頁、個資外洩等。

2.10.2 資訊安全事件等級，由輕微至嚴重區分等級如下：

- 符合下列任一情形者，屬 0 級事件：

(1) 未確定事件或待確認工單：來自不同計畫所使用新型技術 (A-SOC， miniSOC, …)所產生之工單，但其正確性有待確認。

(2) 其他單位所告知教育部所屬單位所發生未確定之資安事件。



(3) 教育部及區、縣網路中心檢舉信箱通告之資安事件。

- 符合下列任一情形者，屬 1 級事件：

(1) 非核心業務資料遭洩漏。

(2) 非核心業務系統或資料遭竄改。

(3) 非核心業務運作遭影響或短暫停頓。

- 符合下列任一情形者，屬 2 級事件：

(1) 非屬密級或敏感之核心業務資料遭洩漏。

(2) 核心業務系統或資料遭輕微竄改。

(3) 核心業務運作遭影響或系統效率降低，於可容忍中斷時間內回復正常運作。

- 符合下列任一情形者，屬 3 級事件：

(1) 密級或敏感公務資料遭洩漏。

(2) 核心業務系統或資料遭嚴重竄改。

(3) 核心業務運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作。

- 符合下列任一情形者，屬 4 級事件：

(1) 國家機密資料遭洩漏。

(2) 國家重要資訊基礎建設系統或資料遭竄改。

(3) 國家重要資訊基礎建設運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作。

2.10.3 本校任何人於校內發現異常情況或疑似資安事件，應立即向資安業務承辦人通報，資安業務承辦人應儘速進行處理並研判事件等級。

2.10.4 資安業務承辦人當發生研判事件等級 3（含）以上之事件，應立即通報資訊業務主管及校長，並以電話聯絡教育局(處)資訊安全管理單位，由校長儘快召集會議研商處理的方式。(參考資安事件通報程序，文件編號：A-6)

2.10.5 當發生無法處理之資通安全事件，應通報教育局(處)資訊安全管理單位協助處理。

2.10.6 教育機構資安通報平台（網址：https://info.cert.tanet.edu.tw/），帳號為學校 OID： 。

2.10.7 資安通報依情報來源分為「告知通報」與「自行通報」，若收到「告知通報」事件通知，由資安業務承辦人登入教育機構資安通報平台，完成通報及應變作業。

2.10.8 資安事件若為校內人員自行發現，由資安業務承辦人登入教育機構資安通報

平台進行「自行通報」完成通報及應變作業。

2.10.9 資安事件須於發生後 1 小時內進行通報，0、1、2 級事件於事件發生後 72 小時內處理完成並結案(包括通報與應變)，3、4 級事件於事件發生後 36 小時內完成並結案。

2.10.10 如有收到教育機構資安通報平台「資安預警事件」通知，由資安業務承辦人登入教育機構資安通報平台，進行資安預警事件單處理作業。

2.10.11 相關通報應變流程請依照「教育機構資安通報應變手冊」規定辦理。

3 實體安全

3.1 設備安置及保護

3.1.1 主機機房及電腦教室宜設置偵煙、偵熱或滅火設備（氣體式滅火器），並禁止擺放易燃物或飲食。

3.1.2 主機機房及電腦教室的電源線插頭應有接地的連結或有避雷針等裝置，避免如雷擊事件所造成損害情況。

3.1.3 主機機房及電腦教室應實施門禁管制。

3.2 溫濕度控制

重要的資訊設備（如：主機機房等）宜有溫濕度控制措施(溫度建議控制在 20℃~25℃，濕度建議控制在相對濕度 50%R.H.~70%R.H.)，以防止資訊設備意外損壞。機房內應有溫濕度顯示裝置，以觀察實際之溫濕度情況。

3.3 電源供應

重要的資訊設備（如：主機機房等）應有適當的電力保護設施，例如設置 UPS、電源保護措施(如：穩壓器、接地等)，以免斷電或過負載而造成損失，並設置緊急照明設備以作為停電照明之用。

3.4 纜線安全

主機機房及電腦教室內線路應考量設置保護設施(如：高架地板、線槽、套管等)。

3.5 設備與儲存媒體之安全報廢或再使用

所有包括儲存媒體的設備項目，在報廢前應填寫「啓用與報廢紀錄單」，確認已將任何敏感資料和授權軟體刪除或覆寫。（文件編號 A-1）

3.6 財產攜出

3.6.1 禁止資訊設備在未經授權之情況下攜離所屬區域，若需將設備攜出，應遵守財產管理相關規定並填寫「設備進出紀錄表」。（文件編號 A-7）

3.6.2 當有必要將設備移出，應檢視相關授權，並實施登記與歸還記錄。

4 可攜式電腦設備與媒體

4.1 公務用可攜式電腦設備(如：筆記型電腦、平板電腦、智慧型手機等)應設定保護機制，如設定通行碼、圖形辨識、臉孔辨識或指紋辨識等。

4.2 公務用可攜式電腦設備應執行安全相關程序（如：掃毒、預設通行碼更新、系統更新等），以防範可能隱藏的病毒或後門程式。

4.3 公務用可攜式儲存媒體(如：隨身碟、光碟、磁帶等)應依儲存資料的機敏性實施安全控管措施，如檔案加密儲存或將該儲存媒體存放於上鎖儲櫃或安全處所。

5 人員安全

5.1 人員安全責任

4 非正式人員、約聘(僱)人員者，因業務需要，而接觸公務機密、個人權益及學校機敏資料者須填寫保密切結書。（文件編號 A-8）

5.2 資訊安全教育與訓練

5.2.1 每學期資安業務承辦人應參加資安管理系統相關教育訓練 **12** 小時以上。

5.2.2 每學期所有教職員應參與資訊安全教育訓練或宣導活動 **3** 小時以上，以提昇資訊安全認知。

6 資訊業務委外管理

6.1 服務委外廠商合約之安全要求

6.1.1 在資訊業務委外合約中，應訂定委外廠商的資訊安全責任及保密規定。

6.1.2 應要求委外廠商簽訂安全保密切結書。(文件編號 A-9)

6.1.3 委外廠商人員到校服務時，應請其簽署委外廠商人員保密切結書。(文件編號 A-10)

6.2 委外廠商服務異動或終止時，應中止或刪除其系統上的帳號與權限。（參考帳號申請單格式，文件編號 A-3）

7 個資保護要求

7.1 本校應就法律允許下，因公務需求所蒐集、處理及保存的個人資料，公佈以下項目至學校網站上。

- 個人資料檔案名稱。
- 保有機關名稱及聯絡方式。
- 個人資料檔案保有之依據及特定目的。
- 個人資料之類別。

7.2 本校教職員工必須遵守個資法規定，不得以任何理由，在沒有法源依據或違反當事人的意願下任意蒐集或洩露他人個資。

7.3 個資法實施後，本校辦理各項活動之因應措施。

- 本校在辦理任何公開活動，會有蒐集、處理甚至公佈部份個資（例：姓名）時，必須在活動辦法及報名表中，陳述「本校之機關名稱」、「蒐集用途」及「使用

地區和期限」，在經「當事人同意」並報名後始得蒐集。若有公佈的需求時，必須加註「將會公佈本活動優勝人（學）員名單」字樣。所蒐集的個資，必須於宣告期限後予以銷毀。

- 本校承辦業務人員，必須妥善保護各項個人資料，並在活動辦法及報名表中註明「本校將會善盡保管之責」字樣。

8 利用各集會場合對全校師生口頭宣導各項相關法令。

8.1 智慧財產權
著作權法

8.2 個人資訊的資料保護及隱私
個人資料保護法及施行細則

8.3 刑法電腦犯罪專章