臺南市立關廟國民中學105學年度資通安全管理辦法

102年10月09日擴大導師會議通過
103年1月20日期末校務會議修訂通過
103年6月30日期末校務會議修訂通過

一、依據

- 教育部 96 年 5 月 30 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。
- 教育部資訊及科技教育司 100 年度教育機構個人資料保護工作事項暨檢核表。

二、目的

確保臺南市立關廟國民中學（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、組織與職權

為強化本校資通安全暨個資保護需求，健全資通安全管理制度，特設立「臺南市關廟國民中學資通安全委員會」(以下簡稱本委員會)，以推動本校資通安全管理業務之運作。本委員會之成員為校長、各處室主任及行政組長，由校長兼任召集人，資訊組長（網管）為資通安全長，行政及技術相關事宜由資訊組負責。

本委員會權責如下：

1. 訂定本校資通安全政策及資通安全管控機制。
2. 督導資通安全政策之實施。
3. 資通安全事件通報、緊急應變及危機處理。
4. 規劃並督導資通安全教育訓練。
5. 督導個人資料保護工作之落實。

本委員會每年開會一次，必要時得召開臨時會議。會議須有應出席委員半數(含)以上

五、資安政策

維護本校資訊之機密性、完整性與可用性，保障使用者資料隱私。

1. 保護本校網路資訊，避免未經授權的存取與修改。
2. 本校業務執行須符合相關法令及法規之要求。
3. 建立資訊業務永續運作計畫，確保本校業務永續運作。

六、實施規定

1. 網路安全

1.1 本校與外界連線，應僅限於經由教育局(處)網路管理單位之管控，以符合一致性與單一性之安全要求。

1.2 網路安全管理服務委外廠商合約之安全要求，委外開發或維護廠商必須簽訂安全保密切結書。

1.3 應禁止以私人架設網路（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。

1.4 宜依業務性質之不同，區分不同內部網路網段，例如：教學、行政、宿網等，以降低未經授權存取之風險。

1.5 對於開放提供外部使用者或廠商存取之服務，必須限制使用者之來源 IP 及網路連線埠(Port)，以確保安全。

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，以避免未經授權之存取，例如網路服務主機(電子郵件、網站主機)、教學系統主機(例如隨選視訊主機)等。

2.2 本校內的個人電腦應

2.2.1 裝置防毒軟體，將軟體設定為自動定期更新病毒碼；或由伺服器端進行病毒碼更新的管理。

2.2.2 作業系統及軟體應定期更新，如「Windows Update」之程式更新作業，以防範作業系統之漏洞。

2.2.3 本校電腦所使用的軟體應有授權。

2.2.4 屬於「電腦與主機類別」的動支請示單，其中的會辦單位「其他」欄由資訊組長負責蓋章確認，並請申購單位於貨到時通知資訊組長。新系統啟用前，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，並記錄於啟用與報廢紀錄單)，以防範可能隱藏的病毒或後門程式。

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

2.4.1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；建議週期為每週進行一次，並使用設備執行異地備份或使用光碟、隨身碟或外接式硬碟執行異地存放。

2.4.2每年應定期檢查備份資料之可用性與完整性。

2.5 資訊存取限制

共用的個人電腦（如：電腦教室電腦、教師休息室電腦等）應以特定功能為目的，並設定特定安全管控機制（如：限制從網路非法下載檔案行為、限制自行安裝軟體行為、限制特定資料的存取等）。

2.6 操作員日誌

2.6.1本校系統管理人員需針對敏感度高、或包含特殊資訊的電腦系統進行檢查、維護、更新等動作時，應針對這些活動填寫日誌予以紀錄，作為未來需要時之檢查。

2.6.2系統管理人員應至少每季執行一次校時。

2.6.3日誌內容可包含以下各項：

- 系統例行檢查、維護、更新活動的起始時間
- 系統錯誤內容和採取的改正措施。
- 紀錄日誌項目人員姓名與簽名欄

2.7 使用者註冊

2.7.1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。

2.7.2本校人員離職後，由人事主任知會相關名單給資訊人員，應立即於各應用系統中註銷該員的帳號及使用權。

- 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。
- 保存一份包含所有帳號註冊的記錄。
- 使用者調職或離職後，應移除其帳號的存取權限。
- 每學期應檢查使用者帳號，以確保帳號的有效性。

2.8 特權管理

本校的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，應予以文件化記錄備查。

2.9 通行碼（Password）之使用

2.9.1管制使用者第一次登入系統時，必須立即更改預設通行碼，預設通行碼應設定有效期限。

2.9.2資訊系統與服務應避免使用共用帳號及通行碼。

2.9.3由學校發佈通行碼制定與使用規則給使用者(參考優質通行碼設定原則與使用原則文件，文件編號：A-5)，內容應包含以下各項：

- 使用者應該對其個人所持有通行碼盡保密責任。
- 要求使用者的通行碼設定，應該包含英文字及數字，長度為 8 碼（含）以上。

2.9.4 應該避免的作法

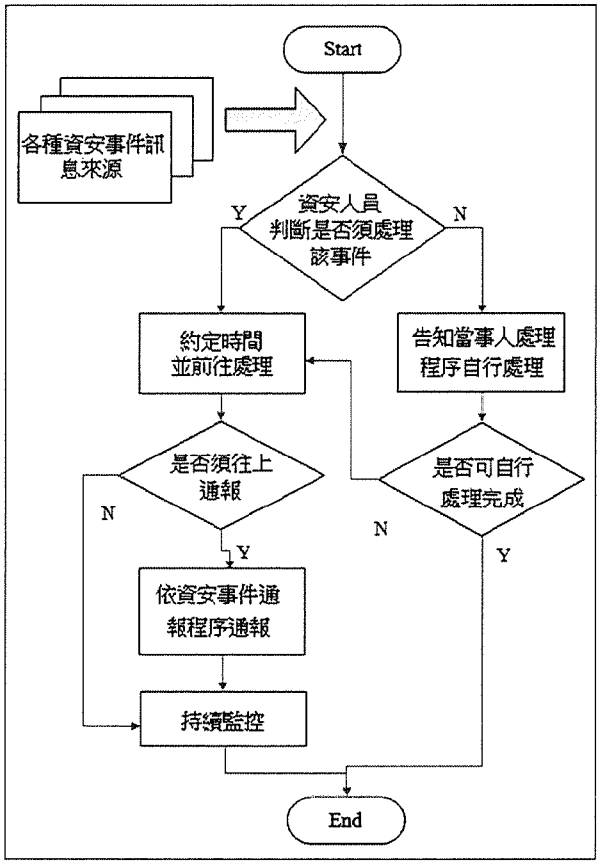
- 嚴禁不設密碼、與帳號相同或與主機名稱相同。
- 不要使用與自己有關的資訊，例如學校或家裡電話、親朋好友姓名、身份證號碼、生日等。
- 不重覆電腦鍵盤上的字母，例如 6666rrrr 或 qwertyui 或 zxcvbnm。
- 不使用連續或簡單的組合的字母或數字，例如 abcdefgh 或 12345678 或 24681024
- 避免全部使用數字，例如 52526565。
- 不使用難記以至必須寫下來的密碼。
- 避免使用字典找得到的英文單字或詞語，如 TomCruz 、superman
- 不要使用電腦的登入畫面上任何出現的字。
- 不分享密碼內容給任何人，包括男女朋友、職務代理人、上司等。
- 因特殊需要擁有多個帳號時，可考慮使用一組複雜但相同的密碼。

2.10 原始程式庫之存取控制

學校與系統廠商間的合約應加註對原始程式庫安全之要求，並防範資料庫隱碼(SQL-injection)問題，針對存取資料庫程式碼之輸入欄位進行字元合理性檢查。

2.11 通報安全事件與處理

2.11.1 本校發生資安事件之處理流程如右圖所示。



2.11.2 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。

2.11.3 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。

2.11.4 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。

2.11.5 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)

2.11.6 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。

2.11.7 教育機構資安通報平台（網址：https://info.cert.tanet.edu.tw/），帳號為學校 OID：2.16.886.111.90028.100060.2。

2.11.8 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。

2.11.9 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。

2.11.10 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。

2.11.11 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。

2.11.12 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。

2.10 無線網路存取

2.10.1 應禁止使用者私自將無線網路存取設備介接至校園網路;若有介接之必要應經權責管理人員同意並設定帳號通行碼或加密金鑰以防未經許可之盜用。

2.10.2 校園內應提供無線網路存取服務，並採取適當安全管控措施：

- 專供行政使用之無線網路熱點建議設定加密金鑰防護，並避免使用開放之無線網路存取重要資訊系統及處理敏感性資料。
- 於教學區域、會議室等場所佈建之無線網路熱點應具有使用者身分認證機制，並經由校園無線路漫遊服務系統提供外校來賓使用。
- 專供師生教學活動使用之無線網路熱點，若採用其他管理方式確有不便時，應採取限定開放時間及限制開放區域等管理措施，減少遭受不當利用之機會。
- 開放校外人士出入之公共空間可視需要提供民眾無線上網服務，其網段應與校園網路隔離，或委由網路服務業者提供。

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「啟用與報廢紀錄單」，確認已將任何敏感資料和授權軟體刪除或覆寫。

3.6 設備維護

3.6.1 應與設備廠商建立維護合約。

3.6.2 廠商進入安全區域需簽訂安全保密切結書。

3.7 財產攜出

3.7.1 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」。

3.7.2 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。

3.8 桌面淨空與螢幕淨空政策

3.8.1 結束工作時，所有學校教職員工應將其所經辦或使用具有機密或敏感特性的資料(例如公文、學籍資料等）及資料的儲存媒體（如 USB 隨身碟、磁碟片、光碟等），妥善存放。

3.8.2 本校職員工使用的個人電腦應設定個人密碼以及螢幕保護措施，螢幕保護啟動時間必須 10 分鐘或是更少。

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 正式人員、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，填寫後統一歸檔至人事室。

5.2 資通安全教育與訓練

5.2.1 鼓勵資安業務承辦人參加資安管理系統相關教育訓練。

5.2.2 鼓勵所有教職員參與資訊安全教育訓練或宣導活動，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。

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。

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

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。

7.1.1 個人資料檔案名稱。

7.1.2 保有機關名稱及聯絡方式。

7.1.3 個人資料檔案保有之依據及特定目的。

7.1.4 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 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。

7.4 若需於單位管理之網站或網頁公布個人資料時，須經所屬單位主管核准，並依相關法律及規範處理。

7.5 個人資料檔案使用完畢後，應立即退出應用程式。

7.6 學校在交換紙本個人資料時，須採取彌封或其他具備保密機制之傳遞方式，並記錄轉交或傳輸行為的流向。

7.7 含個資之紙本文件不得放置於公共區域明顯處，或回收再使用。

7.8 學校應於法律允許之範圍內提供資料當事人下列權益：查詢或請求閱覽、請求製給複製本、請求補充或更正、請求停止蒐集、處理或利用及請求刪除。

7.9 外部團體或個人更新或維修儲存個人資料檔案之電腦設備時，須指派專人在場確保資料安全。

7.10 儲存個人資料檔案之電腦或相關設備如需報廢或移轉他用，應刪除其所儲存之個人資料檔案。

8. 應對以下各項相關法令有基礎之認知，並利用各集會場合對全校師生口頭宣導(至少一學期一次)。

8.1 智慧財產權

- 經濟部智慧財產局
  http://www.tipo.gov.tw/
- 著作權法
  http://law.moj.gov.tw/LawClass/LawContent.aspx?PCODE=J0070017

8.2 個人資料保護及隱私

- 個人資料保護法
  http://law.moj.gov.tw/LawClass/LawAll.aspx?PCode=I0050021
- 個人資料保護法施行細則
  http://law.moj.gov.tw/LawClass/LawAll.aspx?PCode=I0050022

8.3 電子簽章法

- 電子簽章法
  http://law.moj.gov.tw/LawClass/LawContent.aspx?PCODE=J0080037
- 電子簽章法施行細則
  http://law.moj.gov.tw/LawClass/LawContent.aspx?PCODE=J0080039
- 核可憑證機構名單
  http://gcis.nat.gov.tw/eclaw/bbs.asp

8.4 刑法電腦犯罪專章

- 刑法第 36 章妨害電腦使用罪
  http://law.moj.gov.tw/LawClass/LawParaDeatil.aspx?Pcode=C0000001&LCNOS=%20358%20%20%20&LCC=2

承辦人：教師兼資訊組長曾昭賢　　單位主管：教師兼代教務主任林嘉瑜　　校長：關廟國中校長鍾國雲