臺南市立永仁高中資通安全管理辦法

經 2013 年 8 月 29 日校務會議通過

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

確保臺南市立永仁高中（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「臺南市立永仁高中資通安全委員會」(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)以上出席始得開會，並得邀請相關人員列席。

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。

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

六、實施原則

1. 網路安全

1.1 本校與外界連線，僅限於經由教育局資訊中心之管控，以符合一致性與單一性之安全要求。並禁止以電話線連結主機電腦或網路設備。

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。

2. 系統安全

2.1 本校內的個人電腦應

- 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。
- 定期（至少每個月）進行如「Windows Update」之程式更新作業，以防範作業系統之漏洞。
- 新系統啟用前，應經過掃毒與更新系統密碼程序，以防範可能隱藏的病毒或後門程式。

2.2 本校內個人電腦所使用的軟體應有授權，嚴禁安裝各種非法軟體。

2.3 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；建議週期為每週進行一次。

2.4 操作員日誌

- 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。
- 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

2.5 使用者註冊

- 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。
  - 定期（建議每學期）檢查新增之帳號，若有莫名帳號產生，應關閉帳號權限，並依通報程序請求處理。

2.6 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。

2.7 密碼（Password）之使用

- 本校各資訊系統與服務應避免使用共同帳號及密碼。
- 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」
- 應該避免的作法
  a. 嚴禁不設密碼、與帳號相同或與主機名稱相同。
  b. 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。
  c. 不重覆電腦鍵盤上的字母，例如 6666rrrr 或 qwertyui 或 zxcvbnm。
  d. 不使用連續或簡單的組合的字母或數字，例如 abcdefgh 或 12345678 或 24681024
  e. 避免全部使用數字，例如 52526565。
  f. 不使用難記以至必須寫下來的密碼。
  g. 避免使用字典找得到的英文單字或詞語，如 TomCruz 、superman
  h. 不要使用電腦的登入畫面上任何出現的字。
  i. 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。
  j. 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。

2.8 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。

2.9 通報安全事件與處理

- 本校發生資安事件之處理流程如右圖所示。
- 資通安全事件包括：任何來自網路的駭客攻擊、病毒感染、垃圾郵件、資料或網頁遭竄改、以及通訊中斷等。

3. 實體安全

3.1 設備安置及保護

- 本校重要的資訊設備（如主機機房）應置於設有空調空間。
- 本校資訊設備主機機房、電腦教室區域，應設置滅火設備，並禁止擺放易燃物、或飲食。
- 本校資訊設備主機機房、電腦教室區域內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。
- 本校資訊設備主機機房、電腦教室區域，應至少於入出口處加裝門鎖或其他同等裝置。

3.2 電源供應

本校重要的資訊設備（如主機機房）應有適當的電力設施，例如設置 UPS、電源保護措施，以免斷電或過負載而造成損失。

3.3 纜線安全

本校資訊設備主機機房、電腦教室區域內應避免明佈線。

3.4 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，應先確保已將任何敏感資料和授權軟體刪除或覆寫。

3.5 設備維護

- 應與設備廠商建立維護合約。
- 廠商進入安全區域需簽訂安全保密切結書。

3.6 財產攜出

- 未經授權不應將學校的資訊設備、資訊或軟體攜出所在地。
- 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。

3.7 桌面淨空與螢幕淨空政策

- 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。
- 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. 人員安全

4.1 每學年至少要於校務會議上宣導一次本管理辦法，以及重要資通安全消息，以加強教職員工的資安意識。

4.2 資通安全教育與訓練

- 本校資通安全長，每年至少要有六小時的資通安全相關教育訓練，使其有足夠能力執行日常基礎之資安管理系統維護工作，並使其瞭解資安事件通報之程序。
- 其他教職員工每年至少要有三小時，參與資通安全教育訓練或宣導活動，以提昇資通安全認知。

5. 個資保護要求

5.1 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。

5.2 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。

5.3 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。

5.4 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。

5.5 個人資料檔案使用完畢後，應立即退出應用程式。

5.6 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。

5.7 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。

5.8 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。

5.9 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。

5.10 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。

6. 應對以下各項相關法令有基礎之認知

6.1 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

6.2 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

6.3 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