臺中市私立衛道高級中學資通安全管理系統實施細則

民國 113 年 04 月 02 日行政會議訂定

一、依據：

教育部 103 年 02 月 07 日頒布的「國中、小學資通安全管理系統實施原則」訂定本細則。

二、目的：

增進學校資訊作業之安全性，確保學校資料之機密性、完整性與可用性。

三、適用：

校內電腦、資訊與網路服務相關的系統、設備、程序及人員。

四、實施細則：

（一）網路安全

1.網路控制措施

（1）學校與外界連線，應僅限於經由區網中心管控，以符合一致性與單一性之安全要求。

（2）學校內特殊系統（例如會計系統、學生學籍、成績原始資料系統等）之資料，當有必要透過網路進行傳輸時，應透過虛擬私有網路（Virtual Private Network, VPN）或同等連線方式進行；若無透過網路進行傳輸需求，則應區隔於網路之外。

（3）應禁止以電話線連結主機電腦或網路設備。

2.網路安全管理服務委外廠商合約之安全要求。

3.委外開發或維護廠商，必須簽訂「安全保密切結書」(參考切結書範本，文件編號 A-1)。

（二）系統安全

1.職責區隔

（1）學校主機電腦可依個別應用系統之需要，設置專屬電腦，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）。

（2）學校的行政系統主機（例如財務、人事、公文系統等）電腦，建議由學校專責單位統籌管理。

2.對抗惡意軟體、隱密通道及特洛依木馬程式

（1）學校內的個人電腦應：

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。

（2）學校內個人電腦所使用的軟體應有授權。

（3）新系統啟用前，應經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。

3.資料備份

（1）學校(或委託)系統管理人員需針對學校重要系統（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）操作員日誌

①學校(或委託)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。[參考日誌範本，文件編號 A-2]
- 紀錄日誌項目人員姓名與簽名欄。

4.資訊存取限制

學校內所共用的個人電腦應以特定功能為目的，並設定特定安全管控機制（例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）。

5.使用者註冊

學校應制定電腦系統使用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：

（1）使用唯一的使用者識別碼（ID）。

（2）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。

（3）保存一份包含所有識別碼註冊的記錄。

（4）使用者調職或離職後，應移除其識別碼的存取權限。

（5）定期（建議每學期）檢查並取消多餘的使用者識別碼和帳號。

（6）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（參照本文件 2.10 段落）。

6.特權管理

學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。

7.通行碼之使用

（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）資訊系統與服務應避免使用共同帳號及通行碼。

（3）由學校發佈通行碼（Password）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，文件編號 A-3]，內容應包含以下各項：

① 使用者應該對其個人所持有通行碼盡保密責任。

② 要求使用者的通行碼設定，避免使用易於猜測之數字或文字，例如生日、名字、鍵盤上聯繫的字母與數字（如 12345678 或 asdfghjk），以及過多重複字元等。或建議通行碼應該包含英文字大小寫、數字、特殊符號等四種設定中的三種。

③ 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通行碼。

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。

9.通報安全事件與處理

（1）資訊安全事件包括：任何來自網路的駭客攻擊、病毒感染、垃圾郵件、資料或網頁遭竄改及通訊中斷等。

（2）學校應建立資訊安全事件通報程序[參照安全事件通報程序，編號 A-4]以及安全事件通報單[參考安全事件通報單範本，文件編號 A-5]；通報程序應包括學校內部通報，以及學校與所屬縣市教育網路中心的通報。

（3）當學校內部無法處理之資通安全事件，應通報其所屬縣市網路中心。

（4）所訂出資訊安全事件通報程序，應公布於校園內使用電腦與網路之場所，提供使用者瞭解。

（三）實體安全

1.設備安置及保護

（1）學校重要的資訊設備（如主機機房）應置於設有空調空間。

（2）學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。

（3）學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。

（4）學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。

2.電源供應

學校重要的資訊設備（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.纜線安全

學校資訊設備主機機房、電腦教室區域內應避免明佈線。

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。

5.設備維護

（1）應與設備廠商建立維護合約。

（2）廠商進入安全區域須簽訂安全保密切結書。

6.財產攜出

（1）未經授權不得將學校資訊設備、資訊或軟體攜出所在地。

（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）相關財產之攜出，應依教育部或學校既有之相關規定處理。

7.桌面淨空與螢幕淨空政策

（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。

（2）學校提供教職員工或學生使用的個人電腦應設定保護裝置，如個人鑰匙、個人密碼以及螢幕保護。

（四）人員安全

1. 將安全列入工作執掌中

應將資訊安全納入教職員手冊說明中，以強化工作上之資訊安全意識。

2. 資訊安全教育與訓練

（1）使學校(或委託)系統管理人員有足夠能力，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。

（2）學校鼓勵或安排資訊組長/老師/系統管理人員以及所有教職員，參與資訊安全教育訓練或宣導活動，以提昇資訊安全認知。

3. 應對以下各項相關法令有基礎之認知

（1）智慧財產權

①經濟部智慧財產局 http://www.tipo.gov.tw/

②著作權法

http://www.tipo.gov.tw/copyright/copyright_law/copyright_law_92.asp

（2）個人資訊的資料保護及隱私

①個人資料保護法 https://law.moj.gov.tw/LawClass/LawAll.aspx?PCode=I0050021

②個人資料保護法施行細則

https://law.moj.gov.tw/LawClass/LawAll.aspx?PCode=I0050022

（3）電子簽章法

①電子簽章法 http://www.moea.gov.tw/~meco/doc/ndoc/s5_p05.htm

②電子簽章法施行細則 http://www.moea.gov.tw/~meco/doc/ndoc/s5_p05_p01.htm

③核可憑證機構名單

http://www.moea.gov.tw/~meco/doc/ndoc/s5_p07_p03.htm

五、本細則經行政會議討論通過，陳請校長核定後公布實施，修正時亦同。

文件編號：A-1

資訊服務委外單位服務暨保密切結書

_____公司(以下簡稱為本公司)為配合臺中市私立衛道高級中學（以下簡稱為貴校）之資訊應用業務需求，進行相關資訊系統或軟體開發、測試、建置及維護等工作。本公司提供資訊服務項目如下：

一、

二、

三、

本公司願意在對貴校提供上述服務項目範圍內之服務時，保證因提供業務服務需存取貴校資訊系統中所存放，凡屬與公文機密、個人及事業單位權益相關之資料，無論其內容之一部或全部，均負保密之責；相關資料均以留在貴校內部範疇內處理，倘須由本公司攜至校外處理，應簽奉貴校核可。

本公司亦不私自蒐集貴校所擁有之任何資訊。若所提供之資訊業務服務，不符合上述之規定或經營之服務項目超出上述範圍，或違犯法令，本公司同意無異議接受接受法律制裁與及其訴訟費用，並負責所引發之各項損失賠償。此致

臺中市私立衛道高級中學

申請單位及負責人蓋章：

日期：　　年　　月　　日

本服務暨保密切結書一式兩份，分別由_____公司以及臺中市私立衛道高級中學保存

文件編號：A-2

操作員日誌

填寫日期：　　民國___年___月___日
系統操作起始時間：　上（下）午___時___分
系統操作結束時間：　上（下）午___時___分

操作事項	☐ 系統例行檢查 ☐ 系統維護 ☐ 系統更新操作
系統錯誤說明	
採取改正措施說明	

操作人員：＿＿＿＿＿＿＿＿＿＿　簽名欄＿＿＿＿＿＿＿＿＿＿

日誌填寫人員：＿＿＿＿＿＿＿＿＿＿　簽名欄＿＿＿＿＿＿＿＿＿＿

文件編號：A-3

優質通行碼設定原則與使用原則

一、 良好的通行碼設定原則

1. 混合大寫與小寫字母、數字，特殊符號。
2. 通行碼越長越好，最短也應該在 8 個字以上。
3. 至少每三個月改一次密碼。
4. 使用技巧記住通行碼
   - 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「通行碼」的注音輸入為「wj/ vu/6a83」

二、 應該避免的作法

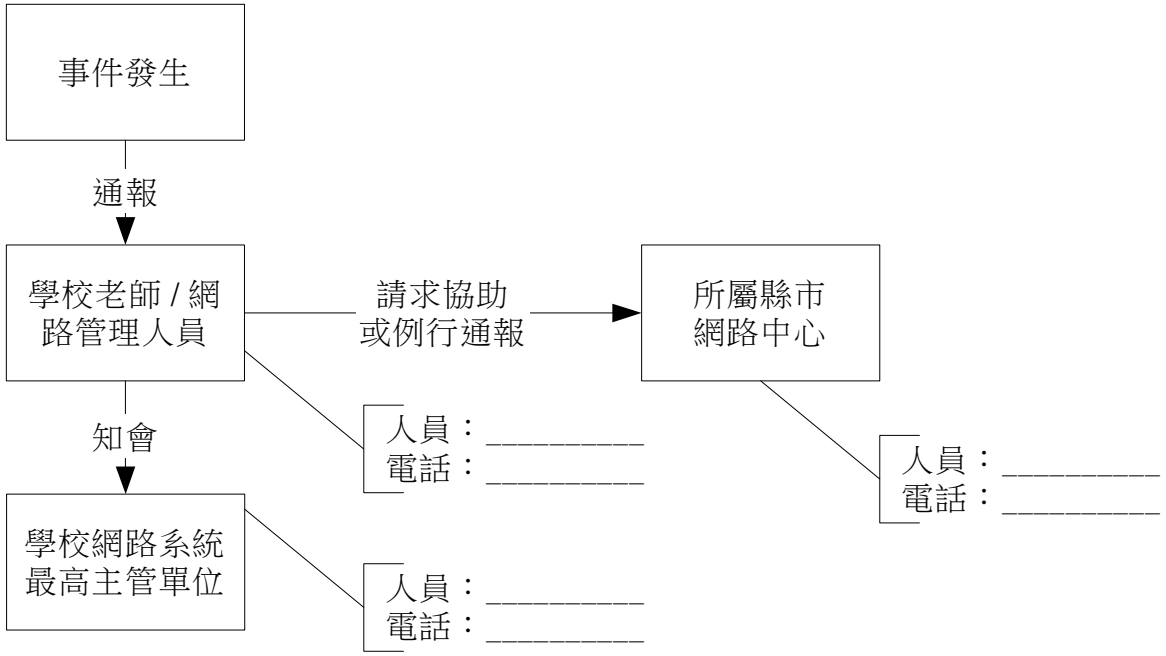
1. 嚴禁不設通行碼
2. 通行碼嚴禁與帳號相同
3. 通行碼嚴禁與主機名稱相同
4. 不要使用與自己有關的資訊，例如學校或家裡電話、親朋好友姓名、身份證號碼、生日等。
5. 不重覆電腦鍵盤上的字母，例如 6666rrrr 或 qwertyui 或 zxcvbnm。
6. 不使用連續或簡單的組合的字母或數字，例如 abcdefgh 或 12345678 或 24681024
7. 避免全部使用數字，例如 52526565
8. 不使用難記以至必須寫下來的通行碼。
9. 避免使用字典找得到的英文單字或詞語，如 TomCruz 、superman
10. 不要使用電腦的登入畫面上任何出現的字。
11. 不分享通行碼內容給任何人，包括男女朋友、職務代理人、上司等。

延伸參考：

“Password Management Guideline”, by department of defense computer security center, 12 April 1985
http://www.radium.ncsc.mil/tpep/library/rainbow/CSC-STD-002-85.pdf

文件編號：A-4

安全事件通報程序範本



文件編號：A-5

_____學校資通安全事件通報單

編號：_____

填報時間：_____年_____月_____日_____時 _____分

洽詢電話：_____ 傳真：_____

E-mail：_____

或逕送：_____

一、發生資通安全之機關(機構)聯絡資料：

機關(機構)名稱：_____聯絡人：_____

E-mail：_____

電話：_____ 傳真：_____

二、資通安全事件通報事項：

1.事件發生時間：_____年____月____日_____時_____分

2.主機(伺服器)資料：

◎ IP 位址(IP Address)：_____

◎ 網域名稱(Domain name)：_____

◎ 主機(伺服器)廠牌、機型：_____

◎ 作業系統名稱、版本、序號：_____

◎ 網際網路資訊位址(Web URL)：_____

◎ 已裝置之安全機制：_____

3.資通安全事件資料：

◎影響等級：□『A』級：影響公共安全、社會秩序、人民生命財產。

□『B』級：系統停頓，業務無法運作。

□『C』級：業務中斷，影響系統效率。

□『D』級：業務短暫停頓，可立即修復。

◎ 事件說明：

◎ 應變措施：

三、期望支援項目：

四、解決辦法：

五、已解決時間：_____年_____月_____日_____時_____分

校長： **資訊安全長：** **承辦人員：**

_____學校資通安全事件解除單

編號：_____

填報時間：_____年_____月_____日_____時 _____分

洽詢電話：_____ 傳真：_____

E-mail：_____

或逕送：_____

一、發生資通安全之機關(機構)聯絡資料：

機關(機構)名稱：_____聯絡人：_____

E-mail：_____

電話：_____ 傳真：_____

二、資通安全事件通報事項：

1.事件發生時間：_____年____月____日_____時_____分

2.主機(伺服器)資料：

◎ IP 位址(IP Address)：_____

◎ 網域名稱(Domain name)：_____

◎ 主機(伺服器)廠牌、機型：_____

◎ 作業系統名稱、版本、序號：_____

◎ 網際網路資訊位址(Web URL)：_____

◎ 已裝置之安全機制：_____

3.資通安全事件資料：

◎影響等級： □『A』級：影響公共安全、社會秩序、人民生命財產。

□『B』級：系統停頓，業務無法運作。

□『C』級：業務中斷，影響系統效率。

□『D』級：業務短暫停頓，可立即修復。

◎ 事件說明：

◎ 應變措施：

三、已解決時間：_____年_____月_____日_____時_____分

填寫人：_____