高雄市立莒光國小
資通安全管理系統(ISMS)實施辦法

中 華 民 國 104 年 4 月 23 日

高雄市立莒光國小資通安全管理系統(ISMS)實施辦法

一、 文件目標

為避免校園內部使用相關資訊設備時，因個人操作及其他因素導致重要資料外洩及設備毀損，特訂立此實施辦法。。

二、 適用範圍

學校內電腦、資訊與網路服務相關的系統、設備、程序、及人員。

三、 實施原則

1. 網路安全

1.1 網路控制措施

- 學校與外界連線，應僅限於經由高雄市教育網路中心之管控，以符合一致性與單一性之安全要求。
- 學校內特殊系統（例如會計系統、人事系統、公文系統、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，建議透過虛擬私有網路（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，則建議區隔於網路之外。
- 應禁止以電話線連結主機電腦或網路設備。

~~1.3~~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（文件編號 A-1(合約商廠商) 、 A-5(合約商員工)）。

~~1.4~~1.3 無線網路存取

- 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。
- 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。

2. 系統安全

2.1 職責區隔

- 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）。
- 學校的行政系統主機（例如財務、人事、公文系統等）電腦，建議由高雄市教育網路中心或教育局等單位統籌管理。

2.2 對抗惡意軟體、隱密通道及特洛依木馬程式

- 學校內的個人電腦應：
  - 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
  - 對於電腦作業系統及相關應用程式之漏洞，定期安裝修補之程式。
- 電腦教室若已安裝還原系統（需設定為開機還原），為因應教學特殊需求，可不安裝防毒軟體。學校內個人電腦所使用的軟體應有授權。
- 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。
- 具備存取權限之終端機不得安裝檔案分享軟體。

2.3 資料備份

- 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；(建議週期為每月進行一次。)

2.4 操作員日誌

- 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。
- 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。（文件編號 A-2）

- 紀錄日誌項目人員姓名與簽名欄

2.5 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）。

2.6 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：
  - 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（參照本文件 2.10 段落）。

2.7 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。

2.8 通行碼之使用

- 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。
- 資訊系統與服務應避免使用共同帳號及通行碼。
- 由學校發佈通行碼（Password）制定與使用規則給使用者，（文件編號 A-3），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，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），以及過多的重複字元等。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。
- 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。

2.9 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。

2.10 通報安全事件與處理

- 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、以及通訊中斷等。
- 學校應建立資訊安全事件通報程序（文件編號 A-4），並列印通報平台通報單呈報主管核章；通報程序應包括學校內部通報，以及學校與高雄市教育網路中心的通報。
- 當學校內部無法處理之資通安全事件，應通報高雄市教育網路中心。
- 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。

3. 實體安全

3.1 設備安置及保護

- 學校重要的資訊設備（如主機機房）應置於設有空調空間。
- 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。
- 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。
- 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。

3.2 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。

3.3 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。

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（文件編號 A-1 、 A-5）。

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。
- 相關財產之攜出應依教育部或學校既有之相關規定處理。

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。
- 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。

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

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。
- 具有學校電腦與網路系統資訊存取特權之人員，應簽訂安全保密切結書[文件編號 A-6]。

5.1 資訊安全教育與訓練

- 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。
- 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。

6. 資訊業務委外管理

6.1 服務委外廠商合約之安全要求

- 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。
- 應要求委外廠商簽訂安全保密切結書。(文件編號 A-1(合約商廠商) 、A-5(合約商員工))

- 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。(參考切結書格式，文件編號 A-7)

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. 應對以下各項相關法令有基礎之認知

7.1 智慧財產權

- 經濟部智慧財產局 http://www.tipo.gov.tw/
- 著作權相關法規
  http://www.tipo.gov.tw/ch/Download_DownloadPage.aspx?path=2173&Language=1&UID=9&ClsID=35&ClsTwoID=71&ClsThreeID=0
- 著作權法
  http://www.tipo.gov.tw/ch/AllInOne_Show.aspx?path=1362&guid=a71977ea-6478-4e37-a46a-15497ba7c275&lang=zh-tw

7.2 個人資訊的資料保護及隱私

- 電腦處理個人資料保護法
  http://law.moj.gov.tw/LawClass/LawContent.aspx?PCODE=I0050021

7.3 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/Scripts/newsdetail.asp?no=1J0080039
- 核可憑證機構名單
  http://www.moea.gov.tw/~meco/doc/ndoc/s5_p07_p03.htm

文件編號：A-1

資訊服務委外單位服務暨保密切結書範本

_____公司(以下簡稱為本公司)為配合_____學校（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、

(註：列出貴公司將會在健保資訊網上提供予醫事服務機構之服務項目)

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

XXX 學校

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_____學校保存

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

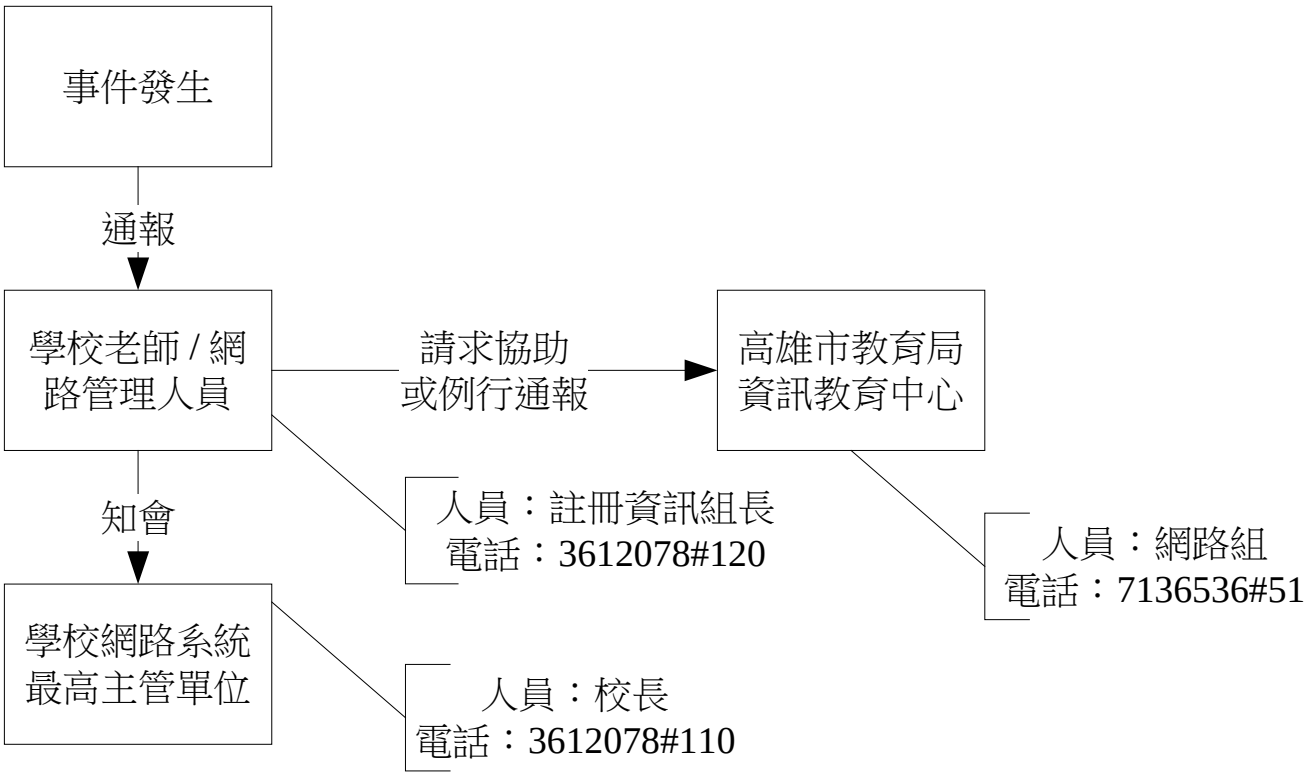
1. 嚴禁不設通行碼
2. 通行碼嚴禁與帳號相同
3. 通行碼嚴禁與主機名稱相同
4. 不要使用與自己有關的資訊，例如學校或家裡電話、親朋好友姓名、身份證號碼、生日等。
5. 不重覆電腦鍵盤上的字母，例如 6666rrrr 或 qwertyui 或 zxcvbnm。
6. 不使用連續或簡單的組合的字母或數字，例如 abcdefgh 或 12345678 或 24681024
7. 避免全部使用數字，例如 52526565
8. 不使用難記以至必須寫下來的通行碼。
9. 避免使用字典找得到的英文單字或詞語，如 TomCruz 、superman
10. 不要使用電腦的登入畫面上任何出現的字。
11.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



文件編號：A-5

合約商員工保密切結書

紀錄編號：

本人　　承攬高雄市 XX 區 XX 國民中/小學(以下簡稱貴校)「　　」業務，保證自　貴校取得之資訊（不論技術或商業資訊)，除已經公開流通之資訊外，應嚴格保密；且除因遵循法令或相關主管機關規定外，非經　貴校同意，不得向第三人披露。如因本人故意或過失，違反上開情事而為洩漏、交付或使用，致損及　貴校權益時，本人願負法律責任。

此致

高雄市楠梓區莒光國民中/小學

立 同 意 書 人：

身 分 證 字 號：

隸 屬 承 包 廠 商：

中　　華　　民　　國　　年　　月　　日

本服務暨保密切結書一式兩份，分別由_____公司以及_____學校保存

文件編號：A-6

保密切結書

紀錄編號：　　日期：　　年　　月　　日

本人 _____ 將嚴守工作保密規定與國家相關法令對業務機密負完全保密之責，並尊重智慧財產權。絕不擅自洩漏、傳播職務上任何業務相關資料及任職期間經辦、保管或接觸之所有須保密訊息資料；絕不擅自複製、傳播任何侵害智慧財產權之任何程式、軟體，違者願負法律責任。

此致

資訊教育推動小組

立 同 意 書 人：_____

所 屬 單 位 別：_____

文件編號：A-7

委外廠商人員保密切結書(範本)

_____ (以下簡稱為本人)任職於_____(委外公司名稱)，因執行_____工作，於 貴校執行服務期間，願遵守 貴校資訊安全相關規範，並對所知悉　貴校機密或任何不公開之文書、電子資料、圖畫、消息、物品或其他資訊，將恪遵保密規定，未經 貴校書面授權，不得以任何形式利用或洩漏、告知、交付、移轉予任何第三人，如有違誤願負法律上之責任。此致

〇〇學校

切結人：

任職公司：

公司統一編號：

日期：　　年　　月　　日

本保密切結書一式兩份，分別由切結人以及_____學校保存