

高雄市立海青高級工商職業學校

學校資訊安全政策及管理辦法



中 華 民 國 106 年 9 月 1 日

高雄市立海青高級工商職業學校

學校資訊安全政策及管理辦法

一、適用範圍

高雄市立海青工商內電腦、資訊與網路服務相關的系統、設備、程序及人員。

二、實施原則

1. 網路安全

1.1 網路控制措施

- 本校與外界連線，以經由高雄市教育網路中心之管控線路為主，並輔以其他 ISP 線路以提供當主要線路故障時，作為備援線路之用，以符合安全性及可用性之要求。
- 本校內特殊系統（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，需透過虛擬私有網路（Virtual Private Network, VPN）或同等連線方式進行。
- 本校不提供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（文件編號 A-1）。

2. 系統安全

2.1 職責區隔

- 本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）。
- 本校的行政系統主機（例如財務、人事、公文系統等）電腦，需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、隱密通道及特洛伊木馬程式

- 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。

- 定期（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
- 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，但教室管理人員至少每學期需更新一次各種系統及漏洞修補程式（如 Windows Update）。
- 本校內個人電腦所使用的軟體需有授權。
- 新系統啟用前，需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。

2.3 資料備份

- 本校(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。

2.4 資訊存取限制

- 本校內所共用的個人電腦以特定功能為目的，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）。
 - 安裝還原系統，並設定系統碟為開機還原。
 - 如需使用公用電腦，需向管理相關單位申請帳號密碼，權限為限制安裝軟體權限（如 WindowsXP 系統的 Users 群組）。
 - 禁止安裝 P2P 軟體。

2.5 使用者註冊

- 本校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，需移除其識別碼的存取權限。
 - 定期（每學期）檢查並取消多餘的使用者識別碼和帳號。
 - 定期（每學期）檢查新增之帳號，若有莫名帳號產生，需關閉帳號權限，並依通報程序請求處理（參照本文件 2.10 段落）。

2.6 通行碼之使用

- 由本校相關管理單位發佈通行碼(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]，內容需包含以下各項：
 - 使用者對其個人所持有通行碼盡保密責任

- 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。通行碼宜包含英文字大小寫、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。

2.7 原始程式庫之存取控制

- 本校與系統廠商間的合約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。

2.8 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。
- 本校需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]，通報程序包括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，需通報高雄市教育網路中心。

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）置於設有空調空間。
- 本校資訊設備主機機房、電腦教室區域，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，於出入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）有適當的電力設施，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，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

- 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-7）。

3.6 財產攜出

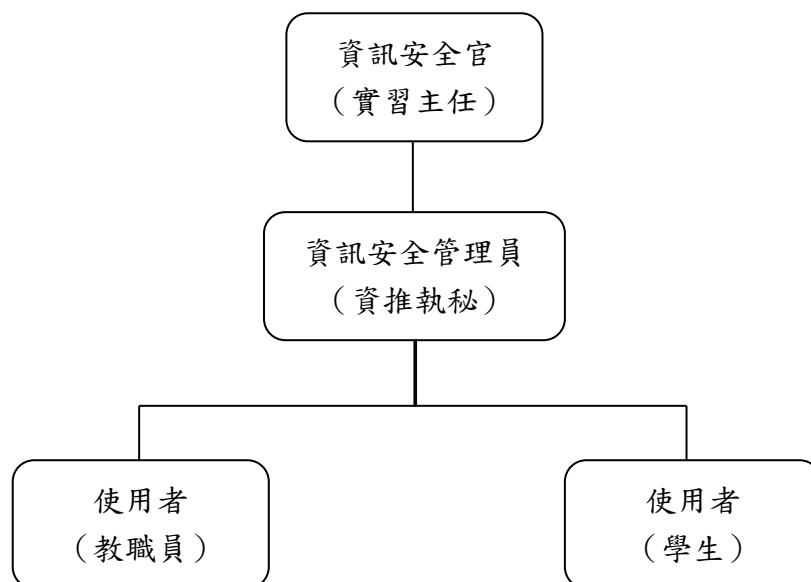
- 未經授權不得將本校的資訊設備、資訊或軟體攜出所在地。
- 當有必要將設備移出，需檢視相關授權，並實施登記與歸還記錄。
- 相關財產之攜出需依教育部或本校既有之相關規定處理。

3.7 桌面淨空與螢幕淨空政策

- 結束工作時，所有本校教職員工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。
- 本校提供教職員工或學生使用的個人電腦需設定保護裝置，如個人鑰匙、個人密碼以及螢幕保護。

4. 人員安全

4.1 組織架構圖



資訊安全組織成員表詳如（文件編號 A-6）

4.2 將安全列入工作執掌中

- 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。
- 具有本校電腦與網路系統資訊存取特權之人員，簽訂安全保密切結書[文件編號 A-8]。

4.3 資訊安全教育與訓練

- 使本校(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。
- 本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。
- 將資訊安全教育納入本校計算機概論電腦課程中。

5. 宜對以下各項相關法令有基礎之認知

5.1 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

5.2 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>

5.3 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

三、 本實施原則經校務會議通過並呈校長核定後實施，修正時亦同。



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)為配合高雄市立海青高級工商職業學校(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

高雄市立海青高級工商職業學校

申請單位及負責人蓋章：



日期： 年 月 日

--

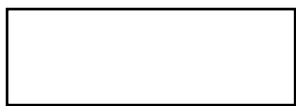
操作員日誌範本

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 _____



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. 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」

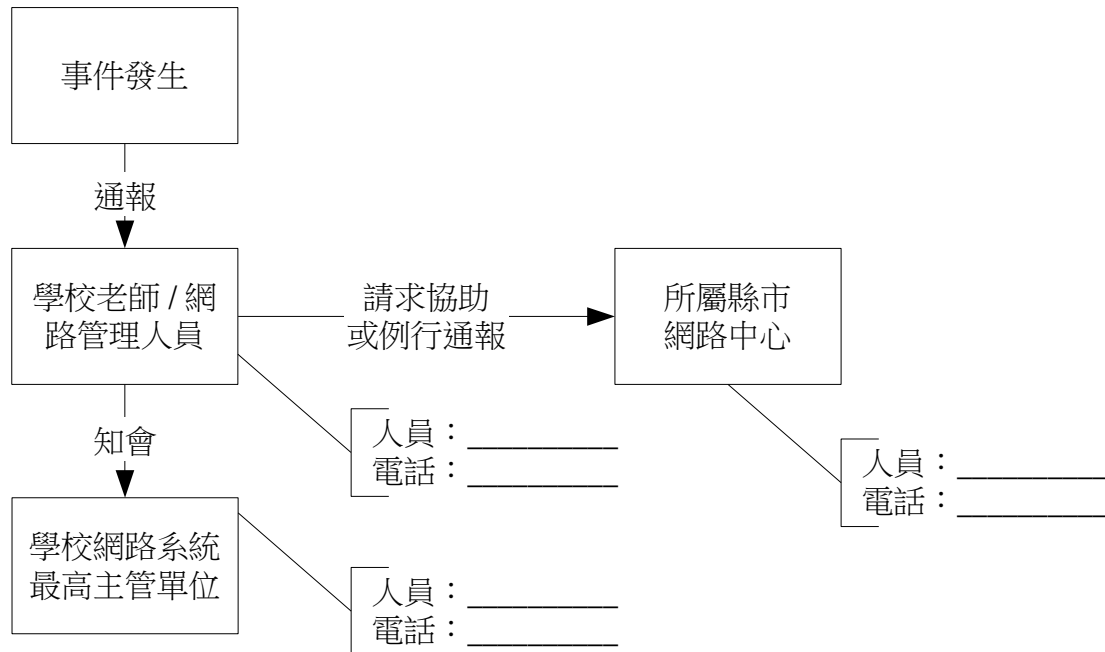
二、應該避免的作法

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. 不重覆電腦鍵盤上的字母，例如 6666rrrr 或 qwertyui 或 zxcvbnm。
5. 不使用連續或簡單的組合的字母或數字，例如 abcdefgh 或 12345678 或 24681024
6. 避免全部使用數字，例如 52526565
7. 不使用難記以至必須寫下來的通行碼。
8. 避免使用字典找得到的英文單字或詞語，如 TomCruz 、superman
9. 不要使用電腦的登入畫面上任何出現的字。
10. 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>

安全事件通報程序範本





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。

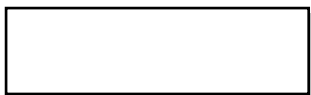
☐『D』級：業務短暫停頓，可立即修復。

◎ 事件說明：

◎ 應變措施：

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

填寫人：_____

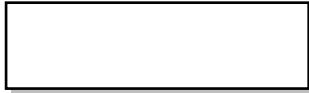


資訊安全組織成員表

記錄編號：

日期： 年 月 日

職 務	職 稱	姓 名	電 話	手 機	電 子 郵 件
資訊安全委員會					
委員兼 召集人					
委員					
委員					
資訊安全官					
資安官					
資訊安全小組					
組長					
組員					
組員					
組員					
組員					
資訊安全稽核小組					
組長					
組員					
組員					
緊急處理組					
召集人					
組員					
組員					
組員					
組員					



合約商員工保密切結書

紀錄編號：

本人 承攬高雄市立海青工商職校（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

高雄市立海青工商職校

立同意書人：

身分證字號：

隸屬承包廠商：

中 華 民 國 年 月 日

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

資訊安全管理小組

立同意書人： _____

身分證字號： _____

所屬單位別： _____

中 華 民 國 年 月 日