

# 彰化縣私立精誠高級中學資通安全帳號密碼管理辦法

114年9月17日資訊安全管理委員會議通過

1. 彰化縣私立精誠高級中學(以下簡稱本校)為提昇資通系統及設備資安強度及有效管理本校教職員工生之帳號與密碼，特訂定資通安全帳號密碼管理辦法(以下簡稱本辦法)。
2. 本辦法相關用詞，均依據資通安全管理法定義辦理。
3. 本校提供資訊服務存取所需之作業相關資訊系統與網路，包括作業平台、資料庫、應用系統、校園網路、遠距存取服務及各種資通設備等，公務用之資通產品，包含軟體、硬體、及服務均適用之。
4. 帳號安全管理原則：
  - 4.1 應有帳號授權之申請與審查機制；若單位內無相關表單時，可採用「資訊服務申請表」進行申請。
  - 4.2 系統管理者帳號存取權限應依據工作職務授予，並以所需之最小權限與最少資訊為原則；惟考量實際風險，最小化需大於等於兩個人，並應使用不同帳號登錄。
  - 4.3 每年至少進行一次帳號權限清查作業，以確保所有帳號之合法使用；清查方式得採用電子紀錄或書面審查，若單位內無相關表單時，可參考「帳號清查紀錄表」。
  - 4.4 應儘量避免共用帳號，其帳號與密碼應妥善保管。
  - 4.5 新購置或自行開發之應用軟體、系統、設備等，安裝完成後應立即更新預設之密碼(不得使用原廠預設密碼)，並刪除、關閉、停用不必要之帳號。
  - 4.6 重要系統、應用程式、設備等應開啟登出入稽核功能，並至少留存六個月紀錄(系統日誌)。
  - 4.7 伺服器主機、個人電腦、筆記型電腦、公務用行動裝置等，應設定 15 分鐘內不使用或離開後鎖定畫面，或自動清除螢幕上的資訊並登出。
  - 4.8 本校資通訊設備需維護或服務時，以到場進行為原則，若有實際需求須進行遠端連線操作時，須採「原則禁止、例外開放」方式，應經權責主管核准後方可執行，並遵守本校資訊安全相關作業要求。
  - 4.9 若無公務上需求，請勿開啟網路芳鄰分享目錄與檔案，並停用 Guest 帳號，個人機敏資料禁止存放於網路芳鄰分享目錄。
  - 4.10 應將重要系統、設備進行隔離或加裝硬體式防火牆等適當方式控管。
5. 密碼安全管理原則：
  - 5.1 密碼設定原則：
    - 5.1.1 使用者密碼長度須至少 8 字元。
    - 5.1.2 系統管理者密碼長度須至少 12 字元。
    - 5.1.3 密碼複雜度設定至少需由英文大小寫、數字或特殊符號的其中 3 個組成。
    - 5.1.4 密碼最長使用期限為 180 天，最短使用期限為 1 天。
    - 5.1.5 密碼不可與前 3 次密碼相同。
    - 5.1.6 密碼驗證失敗達 5 次後，至少 15 分鐘內不允許該帳號繼續嘗試登入。
    - 5.1.7 「忘記密碼」功能不可直接寄送密碼給予使用者，需以超連結或其他方式進行通知；且通知的 email 或簡訊需有時間限制。
  - 5.2 請勿將個人密碼張貼於個人電腦、螢幕或其它容易洩漏秘密之場所。
  - 5.3 避免使用紀錄密碼功能，造成開機時自動登入系統。
  - 5.4 使用者發現密碼可能遭破解時，應立即更改密碼。
  - 5.5 應以宣導方式或程式控制，於系統畫面上提醒使用者密碼安全原則。
6. 帳號密碼管理與違規處理(學生適用)：
  - 6.1 學生應負起帳號與密碼的妥善保管責任，嚴禁將帳號密碼隨意交付、張貼、寫於明顯處或告知他人。

- 6.2 學生因疏忽導致密碼遺失或帳號遭冒用，可向圖書館資訊媒體組提出申請，由資訊媒體組協助完成密碼重設作業，並應予以紀錄。
- 6.3 同一學期內，若學生累計達三次（含）以上申請密碼重設，將視為未盡妥善管理個人帳號密碼之責任，依下列方式處理：
  - 6.3.1 首次與第二次紀錄：進行口頭輔導，宣導並強化學生資通安全觀念。
  - 6.3.2 第三次（含）以上：除協助重設密碼外，學生須依校方規定完成愛校服務2小時以示警惕，並將紀錄送交學務處。
- 6.4 帳號密碼遺失申請、重設處理過程及懲處紀錄等，均應完整留存至少六個月，以供後續追蹤查核。
7. 本辦法經資訊安全管理委員會議通過後，陳請 校長核可後公布實施，修正時亦同。