

# 國立嘉義高級商業職業學校人員資訊安全守則

- 1 目的：為落實國立嘉義高級商業職業學校（以下簡稱本校）資訊通訊安全作業，維護資訊及處理設備之機密性、完整性及可用性，特訂定此守則。
- 2 範圍：本守則適用於正職人員與約聘（僱）人員。
- 3 作業守則
  - 3.1 公務電腦應設定登入密碼並確實保密。
  - 3.2 使用校內各項資訊系統時，禁止共用帳號密碼。
  - 3.3 電腦應使用螢幕保護程式(鎖定畫面)，設定螢幕保護密碼(勾選繼續執行後，顯示登入畫面)，並將啟動時間設定為 10 分鐘以內。
  - 3.4 電腦之作業系統應設定為自動更新，漏洞應即時更新修補。
  - 3.5 電腦應安裝防毒軟體，設定即時更新病毒碼，並定期執行電腦掃描。
  - 3.6 應定期將重要資料備份存放，避免硬體損毀及防範勒索病毒的威脅。
  - 3.7 除管理需求及經授權外，禁止使用密碼破解、網路監聽工具軟體，並不得突破他人帳號，中斷系統服務。
  - 3.8 開啟來路不明之電子郵件及其附件或下載檔案時應謹慎小心，利用防毒軟體或惡意軟體清除工具檢查，以防電腦中毒或駭客入侵。
  - 3.9 當有跡象顯示系統可能中毒時，應儘速通知相關人員。
  - 3.10 禁止私自架設或變更校內網路設備，禁止私自連接網路。
- 4 資料保護
  - 4.1 個人辦公桌面應避免存放機敏性文件，工作結束後，應妥善收藏保密。
  - 4.2 應遵守「個人資料保護法」規範，保護個人資料使用之合法性及機密性。
  - 4.3 不得在任何公開的新聞群組、論壇、或公佈欄中透露任何有關本校資訊細節。
  - 4.4 在丟棄任何曾經儲存本校資訊之電子媒介前，應將電子媒介中的資訊刪除，並徹底消磁或銷毀至無法解讀之程度。
  - 4.5 敏感等級（含）以上資訊之紙本文件若不再使用時，應以碎紙機銷毀該份紙本文件，並刪除電子檔。
  - 4.6 重要機密文件或合約，應妥善保存；若為電子檔案應設定保護密碼。
- 5 密碼使用原則
  - 5.1 應保護通行密碼，維持通行密碼的機密性；應至少每 6 個月更換一次密碼，並禁止重複使用相同的密碼。
  - 5.2 應避免將通行密碼記錄在書面上，或張貼於個人電腦、螢幕或其它容易

洩漏秘密之場所。

- 5.3 當有跡象顯示系統及通行密碼可能遭破解時，應立即更改密碼。
- 5.4 通行密碼的長度最少應有 8 位長度，且應符合密碼設置原則。
- 5.5 密碼設置原則，應包含大小寫字母、數字、符號，並儘量避免使用易猜測或公開資訊為設定：
  - 5.5.1 個人姓名、出生年月日、身分證字號、電話號碼。
  - 5.5.2 機關或單位名稱識別代碼或是其他相關事項。
  - 5.5.3 使用者識別碼、使用者姓名、群體使用者之識別碼或是其他系統識別碼。
  - 5.5.4 電腦主機名稱、作業系統名稱、或電腦上使用者的名稱。
  - 5.5.5 空白、專有名詞、英文或是其他外文字典的字彙。

## 6 電腦軟體版權之使用與管理

- 6.1 禁止濫用系統及網路資源，複製與下載非法軟體。
- 6.2 禁止使用未經授權之電腦軟體，遵守智慧財產權相關規定，有些軟體僅授權家用，不可安裝於學校電腦，請務必詳讀軟體授權說明。
- 6.3 本校電腦所使用之電腦軟體均須具有合法版權，人員不得私自安裝非法電腦軟體。
- 6.4 本校人員若有安裝機房伺服器軟體需求時，需填寫「資訊服務申請表」，經權責主管以上核准後，始得執行安裝。

## 7 資通安全教育訓練

- 7.1 依「資通安全管理法」子法「資通安全責任等級分級辦法」規定，每人每年應接受三小時以上之資通安全通識教育訓練。

## 8 保密協定

- 8.1 本校人員應填具「資訊安全保密切結書」，承諾任職期間，因職務上所獲悉之任何資訊或持有之資料、檔案、技術、財務或業務上之機密，非經主管授權不得對外透露或加以濫用。

## 9 公告與實施

- 9.1 本守則由本校資訊安全委員會通過後公告實施，修訂時亦同。
- 9.2 本校員工若未遵守上述規定或資訊安全政策及程序者，得依相關懲戒程序處置違紀人員。

簽署人：\_\_\_\_\_

中 華 民 國 年 月 日