中華醫事科技大學

**人員資訊安全守則**

1. 目的：為落實中華醫事科技大學（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. 保密要求
   1. 報到時應詳閱並簽署「IS-04-013保密切結書」
   2. 任職期間，於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。
   3. 不得任意翻閱非管業務文件，且不得將業務文件出示與業務無關之人員。
   4. 開場所不得談論機密性業務，避免洩漏重要資訊。
4. 安全要求事項
   1. 個人電腦使用安全
      1. 電腦應設定螢幕保護程式（10分鐘）並設定密碼保護。
      2. 電腦之作業系統及使用之軟體漏洞應定期更新修補，如發現過久未更新(超過一個月)或發現更新失敗，應立即通知資訊中心協助處理。
      3. 電腦應安裝防毒軟體並即時更新病毒碼，如發現過久未更新(超過一個月)或發現更新失敗，應立即通知資訊中心協助處理。
      4. 操作電腦系統如發現病毒時應立即清除，如無法自行清除病毒時，需通知資訊中心協助處理。
      5. 電腦應開啟個人防火牆並關閉網路芳鄰。
      6. 個人電腦嚴禁安裝P2P軟體。
      7. 應定期將重要資料備份存放。
   2. 使用通行密碼應注意下列要點：
      1. 應保護通行密碼，維持通行密碼的機密性：
         1. 密碼設定原則
            1. 一般使用者通行密碼的長度最少應有8位長度，管理者最少應有12位長度，且應符合複雜度原則(英文大小寫、數字、特殊符號4項原則至少取3項)。
            2. 應至少每180天更換通行密碼一次，並禁止重複使用與前3次相同的密碼。
            3. 密碼輸入5次錯誤鎖定15分鐘。
            4. 每日只能變更一次密碼。
         2. 妥慎保管個人持有之帳號、密碼，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之場所。
         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。
         4. 密碼設置應儘量避免使用易猜測或公開資訊為設定：
            1. 個人姓名、出生年月日、身分證字號。
            2. 機關或單位名稱識別代碼或是其他相關事項。
            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。
            4. 電腦主機名稱、作業系統名稱、或電腦上使用者的名稱。
            5. 電話號碼。
            6. 英文或是其他外文字典的字彙。
            7. 專有名詞。
            8. 簡單懶人密碼，如Aa123456
            9. 空白。
   3. 網路安全使用原則
      1. 使用網路時應於授權範圍內存取網路資源，遵守本校網路安全管理之相關規定，以保護本校網路之安全。
      2. 禁止瀏覽含有色情與賭博…等不當網站。
      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機密資訊細節。
      4. 嚴禁開啟來路不明電子郵件及其附件或連結，以防電腦中毒。
      5. 機密性公文及資料，避免以電子郵件或其他電子形式於網路傳遞，如有於網路傳輸的必要時，應施以加密措施。
      6. 禁止濫用系統及網路資源，複製與下載非法軟體。
      7. 利用微軟視窗作業系統網路芳鄰的檔案分享功能提供他人存取檔案時，應僅針對必要對象開放使用權限，避免將權限完全開放。
      8. 與外部交換資料時，使用資料前應啟動病毒防護軟體偵測。
   4. 電腦軟體版權之使用與管理
      1. 本校資訊機房伺服器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。
   5. 使用即時通訊軟體注意事項
      1. 本校人員使用即時通訊軟體，應以傳送溝通訊息為主。
      2. 使用即時通訊軟體傳遞訊息，內容不得涉及學校機密性資料或洩漏個人資料。
      3. 各單位建立聯絡群組，應指定群組管理人員（以下簡稱管理員），管理員應定期清查群組成員。
      4. 管理員應適時向群組成員宣達使用注意事項，發現問題應立即處理。成立群組目的消失，應即時刪除。
      5. 群組成員發現誤傳或內容不當者，應即時主動通報管理員處置。
      6. 於執行法定義務必要範圍內，得依相關法令蒐集、處理或利用所屬群組訊息內容及備份檔案。
      7. 不當使用即時通訊軟體涉及違法或違紀情事，由秘書室會同相關專業人員進行調查，追究相關人員責任。
   6. 其他安全要求事項
      1. 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。
      2. 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。
      3. 限閱等級（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. 重要機密文件或合約，應妥善保存；若為電子檔案應考慮設定保護密碼。
      5. 應遵守「個人資料保護法」相關規定，保護個人資料使用之合法性及機密性。
5. 本校員工若未遵守上述規定或資訊安全及個資保護政策與程序者，得陳報校方，依本校相關懲戒程序處置違紀人員。

本守則由資通安全長核准後公告實施，修訂時亦同。

宣導人： 被宣導人：