

文件編號	IS-D-017	機密等級	一般	版本	2.0
------	----------	------	----	----	-----

中山醫學大學 資安宣導單

- 1 目的：為落實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、可用性、適法性，特訂定規範。
- 2 依據教育部 109 年 09 月 25 日臺教資(五)字第 1090135390 號函修訂。
- 3 適用範圍：本校專任教職員工(含約雇人員)、借調人員、計畫人員、工讀人員與委外人員（以下簡稱業務人員）。
- 4 資安宣導：密碼換新、程式更新、下載要當心。
- 5 業務人員應遵守「資通安全管理法」及「個人資料保護法」規範，保護資通安全及個人資料保護使用之合法性及機密性。
- 6 電腦應設定密碼確實保密。業務人員離開座位時，電腦應進行作業系統登出或設定具密碼保護之螢幕保護程式(不得超過 15 分鐘)。
- 7 電腦應安裝防毒軟體並即時更新病毒碼，電腦之作業系統漏洞應即時更新修補。
- 8 當有跡象顯示電腦可能中毒或發現異常連線時，應儘速通知網路通訊組(緊急應變暨技術支援組)
- 9 應定期將重要資料備份存放。
- 10 使用通行密碼應注意下列要點：
 - 10.1 應保護通行密碼，維持通行密碼的機密性；一般資訊系統之系統管理者應至少每六個月更換通行密碼一次，並禁止重複使用相同的密碼。
 - 10.2 避免將通行密碼記錄在書面，或張貼於個人電腦、螢幕或其它容易洩漏秘密之場所。
 - 10.3 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，並通知資安窗口。
 - 10.4 通行密碼的長度最少應有 8 位長度，且符合密碼設置原則。
 - 10.5 密碼設置原則，應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、電話號碼
 - (2) 機關、單位名稱或其他相關事項
 - (3) 使用者 ID、其他系統 ID
 - (4) 電腦主機名稱、作業系統名稱
 - (5) 空白
- 11 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。
- 12 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。
- 13 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。
- 14 敏感等級（含）以上資訊之紙本文件若不再使用時，應以碎紙機銷毀該文件，並刪除電子檔。
- 15 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。
- 16 禁止濫用系統及網路資源，複製與下載非法軟體。
- 17 公共區域的設備：公用電腦、網路印表機、網路攝影機、門禁設備、無線網路基地台、無線路由與環控系統等，應有具體的加密保護機制、遵守上述通行密碼要點及漏洞更新修補，網路印表機應避免連上公開網路。

文件編號	IS-D-017	機密等級	一般	版本	2.0
------	----------	------	----	----	-----

中山醫學大學 資安宣導單

18 電子郵件管理

- 18.1 來路不明之電子郵件及其附件應謹慎勿開啟，以防電腦中毒。
- 18.2 禁止發送匿名信，或偽造他人名義發送電子郵件騷擾他人，導致他人之不安與不便。
- 18.3 機密等級和敏感等級資料或文件，應避免以即時通訊軟體、電子郵件傳送。
- 18.4 不得傳遞大量且非必要的資訊，避免網路壅塞及資源浪費。
- 18.5 電子郵件附加之檔案應加密，事前檢視內容有無錯誤後方可傳送。
- 18.6 轉寄他人郵件至外部單位時避免直接使用全部回覆信件功能，以免洩露單位內部個人重要資訊。
- 18.7 個人電子郵件帳號資訊勿隨意透露或註冊給不認識之人員及網站。
- 18.8 關閉電子郵件信件預覽視窗、自動下載圖片及自動回覆功能，以防電子郵件社交工程攻擊。
- 18.9 不得使用公務電子信箱帳號登記做為非公務網站的帳號，如社群網站、電商服務等。
- 18.10 公務資料傳遞及聯繫必須使用公務電子郵件帳號，不得使用非公務電子郵件傳送或討論公務訊息。

19 電腦軟體版權之使用與管理

- 19.1 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。
- 19.2 業務人員若有安裝伺服器軟體需求時，須經單位主管核准並填寫「伺服器軟體安裝紀錄表」。
- 19.3 業務人員應遵循合法軟體授權使用範圍進行安裝並檢視個人電腦中所安裝的軟體是否為正版授權軟體，以避免觸犯著作權法，影響本校聲譽或造成電腦病毒侵害而影響電腦作業之進行。校級授權軟體以外之軟體版權之管理，由各單位自行負責。使用者需自負正版軟體舉證責任，應自行約束不得使用非法軟體，並遵守智慧財產權等相關法令，違者應自負法律責任。

20 保密協定

本校人員應恪遵人事單位所訂之聘約上所規範之條款並配合各單位業務需求填具「個人保密切結書」，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。

- 21 為避免涉及個人隱私資料或機敏業務文件，遭未經授權之使用者存取，應避免使用網路芳鄰分享資料夾的方式進行資料傳輸；如必須使用分享資料夾，應對欲分享文件進行加密並於用畢後立即關閉分享。
- 22 業務人員若未遵守上述規定或資通安全管理政策及程序者，得依相關懲戒程序處置違紀人員。
- 23 主動通報資安事件或可能資安風險者，依規定獎勵。
- 24 有資安疑慮或異常時，應即時通報網路通訊組（緊急應變暨技術支援組）。
- 25 本校資通安全管理制度專區之各項規範：中山醫學大學首頁-公開資訊-法規與宣導-資通安全暨個人資料保護管理專區
- 26 圖書資訊處網路通訊組（緊急應變暨技術支援組）：
電子郵件信箱：cs1515@csmu.edu.tw 聯絡電話：04-36097295。