中山醫學大學

資安宣導單

<table>
<tr><th>分類</th><th>宣導事項</th></tr>
<tr><td>目的</td><td>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、可用性及適法性，特訂定規範。</td></tr>
<tr><td>依據</td><td>教育部 109 年 09 月 25 日臺教資(五)字第 1090135390 號函修訂。</td></tr>
<tr><td>適用範圍</td><td>本校正職人員、約聘（僱）人員與委外人員（以下簡稱業務人員）</td></tr>
<tr><td>資安宣導</td><td>密碼換新、程式更新、下載要當心。</td></tr>
<tr><td>通則</td><td>1. 業務人員應遵守「資通安全管理法」及「個人資料保護法」、本校「資通安全管理政策」、「個人資料保護管理政策」之規範，保護資通安全及個人資料保護使用之合法性及機密性。參閱本校資通安全管理專區（政策與法規）。
2. 業務人員若未遵守資安宣導單或本校政策及程序者，得依相關懲戒程序處置違紀人員。
3. 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-資通安全管理專區。</td></tr>
<tr><td>資安分級</td><td>本校依據教育部 111 年 9 月 5 日臺教資(四)字第 1112703805 號「111 年全國大專校院資安長會議」紀錄及「高教深耕計畫資安專章 QA」之要求，依循 C 級特定非公務機關之規定推動本校資通安全維護與管理。</td></tr>
<tr><td>教育訓練時數</td><td>
<table>
<tr><th>身分</th><th>時數及課程</th><th>身分類型</th></tr>
<tr><td>主管人員</td><td>● 每人每年 3 小時以上資通安全通識教育訓練
● 每人每年 1 小時以上個人資料保護議題課程</td><td>指擔任主管職務相關人員，如校長、副校長、處室主管（含資訊主管）等</td></tr>
<tr><td>資通安全專職人員以外之資訊人員</td><td>● 每人每 2 年 3 小時以上資安專業課程或資安職能訓練，且每年 3 小時以上資通安全通識教育訓練
● 每人每年 1 小時以上個人資料保護議題課程</td><td>指負責資訊作業相關人員，如系統分析設計人員、系統設計人員、系統管理人員及系統操作人員等</td></tr>
<tr><td>資通安全專職人員</td><td>● 每人每年 12 小時以上資安專業課程或資安職能訓練
● 每人每年 1 小時以上個人資料保護議題課程</td><td>指負責資安業務相關人員，如資安管理人員、資安聯絡人員等</td></tr>
<tr><td>一般人員</td><td>● 每人每年 3 小時以上資通安全通識教育訓練
● 每人每年 1 小時以上個人資料保護議題課程</td><td>指行政、會計、總務、等單位內資通系統之使用者（含委外供應商駐點人員）</td></tr>
<tr><td>教師</td><td>● 每人每年 3 小時以上資通安全通識教育訓練(含個資)</td><td>本校教師</td></tr>
</table>
</td></tr>
<tr><td>辦公區域安全要求</td><td>1. 電腦應設定密碼確實保密。業務人員離開座位時，電腦、即時通訊軟體、資通系統應進行作業系統登出，避免被冒用入侵。
2. 電腦應設定具密碼保護之螢幕保護程式(不得超過 15 分鐘)。
3. 電腦應安裝防毒軟體並即時更新病毒碼，電腦作業系統漏洞應即時更新修補。
4. 應定期將重要資料備份存放。
5. 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；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。
(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。
(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，並通知網路通訊組（緊急應變暨技術支援組）。</td></tr>
</table>

中山醫學大學

資安宣導單

分類	宣導事項
	(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。 (5) 密碼設置原則，應避免使用易猜測或公開資訊為設定： A. 個人姓名、出生年月日、身分證字號、電話號碼 B. 機關、單位名稱或其他相關事項 C. 使用者 ID、其他系統 ID D. 電腦主機名稱、作業系統名稱 E. 空白 6. 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。 7. 除管理需求及經授權外，禁止濫用系統及網路資源或使用密碼破解、網路監聽工具軟體；不得複製與下載非法軟體，亦不得突破他人帳號，中斷系統服務。 8. 不要點擊網頁彈出的奇怪視窗、來源不明之超連結。 9. 桌面淨空：下班或不使用時，存有個資之紙本與可攜式儲存媒體（如隨身碟）應放置於上鎖之抽屜或儲櫃內。 10. 設備巡檢：每日應檢查公用印表機、傳真機或多功能事務機，確認無個資文件遺留。
電腦軟體版權之使用與管理	1. 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。 2. 伺服器所使用之電腦軟體均須具有合法版權。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」。 3. 經教育部、區網中心來信通知，本校所屬 IP 發生違法下載受智慧財產權保護之遊戲、音樂、軟體等或嘗試入侵散發病毒等涉及侵害之行為，均屬網路侵權。相關事項可查閱本校「學術網路疑似侵權處理辦法」。
電子郵件管理	1. 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。 2. 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。 3. 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。 4. 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並留意信件來源，以防電子郵件社交工程攻擊。 5. 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。 6. 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。 7. 不得傳遞大量且非必要的資訊，避免網路壅塞及資源浪費。 8. 機密等級和敏感等級資料或文件，應避免以電子郵件傳送。 9. 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。 10. 使用電子郵件傳送個人資料：所有傳輸行為必須事前完成自我檢核並經單位主管核准。寄送或傳輸前完成自我檢核，且包含個資之附件應採取壓縮並設定密碼之加密措施。加密之檔案之解密資訊，須透過不同管道分開傳送（如另寄獨

中山醫學大學

資安宣導單

分類	宣導事項
	立電子郵件、以安全通訊軟體傳遞或以口頭通知），不得與加密檔案於同一郵件或訊息中同時傳送。 11. 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。 12. 教育部每年辦理社交工程演練，相關宣導可參閱本校社交工程演練宣導網站。凡受誘騙者應配合執行以下項目： (1) 逐一發信通知單位主管與受誘騙者，受誘騙者應詳閱本校社交工程演練宣導網站。 (2) 強制參與社交工程防範宣導教職員內訓課程，並須完成課程測驗，未完成者列提主管會議。
網路即時通訊	1. 如非必要請避免在公務用電腦或共用電腦登入個人即時通訊帳號，且使用後應即刻登出。 2. 應在 Google Play 或 APP Store 平台等正規合法管道下載，不得下載來源不明或非官方認證應用程式。確認軟體為最新版本，並定期更新。 3. 避免非授權人員取得機密性資料；具機密性、敏感性或安全與隱私之議題，不應使用於即時通訊軟體傳遞。 4. 未確認傳遞者身分前，不得點選訊息超連結，並注意釣魚、惡意或高風險之網站服務。 5. 不得傳遞隱私或非經證實之訊息，但未經證實之訊息需釐清或有其他業務需求者不在此限。 6. 人員異動時，應退出原任機關各即時通訊群組，並自行刪除對話紀錄，對前揭資料及帳號資訊，應予以保密。
禁止危害國家資通安全產品	1. 危害國家資通安全產品：指經主管機關認定，對國家資通安全具有直接或間接造成危害風險，影響政府運作或社會安定之資通系統、服務或產品。 2. 依行政院秘書長 109 年 12 月 18 日院臺護長字第 1090201804A 號函規定，禁止使用及採購危害國家資通安全之資通訊設備，例如，大陸廠牌資通訊產品（含軟體、硬體及服務）。 3. 依資通安全管理法第 11 條，不得下載、安裝或使用危害國家資通安全產品。但因業務需求且無其他替代方案者，經資通安全長核可，函報教育部核定後，得以專案方式使用，並列冊管理。 4. 詳細規範請參照本校資通安全管理專區。
網路安全	1. 依據本校「校園網路使用辦法」，對外連結以學術網路為主，所有使用者必須遵守臺灣學術網路規定及履行。 2. 嚴禁使用校園網路做為傳遞具威脅性、猥褻性、不友善性之資訊，並愛惜使用網路頻寬。 3. 嚴禁使用校園網路做為干擾或破壞網路上其它使用者或節點之軟硬體系統。 4. 嚴禁以破解、盜用或冒用他人帳號及密碼等方式，未經授權使用網路資源或無故洩漏他人之帳號密碼，並禁止使用者之帳號相互轉借。 5. 謹慎使用公開之無線網路，並留意藍芽、衛星定位系統及近場通訊等連線安全。

中山醫學大學

資安宣導單

分類	宣導事項
	6. 無線網路使用規範: （1）無線網路基地台之使用應經適當控管。 （2）無線網路設備之安裝設定應經核准。 （3）無線網路設備之使用應取得授權，禁止於內部網路私自使用任何無線網路產品。 （4）無線網路設備之使用應有適當管理機制，例如：授權使用之 IP 數量、連接埠、網卡位址（Mac address）過濾等。 （5）無線網路之資料傳輸應使用加密機制，並就安全與資訊風險之考量，增加適當之防護機制以避免資料外洩。
物聯網(IoT)設備	1. 物聯網(IoT)設備(含網路印表機、網路攝影機、門禁設備、環控系統、無線基地台、無線路由器等)各類硬體設施。 2. 物聯網(IOT)設備的系統管理者應變更設備預設密碼、密碼不得使用弱密碼、密碼宜符合密碼設置原則、定期更新與修補設備。若接獲相關威脅情資應依本校「安全事件管理程序書」之規範進行漏洞修補或防火牆防護等設定。 3. 物聯網(IoT)設備應避免連上公開網路。
個人行動裝置、可攜式媒體	1. 可攜式媒體定義，如磁片、磁碟、磁帶、IC 卡、匣式磁帶、外接式硬碟、光碟、隨身碟、記憶卡、錄影帶、錄音帶、筆記型電腦、掌上型電腦、行動電話等。 2. 校內可攜式設備與媒體管理： （1）使用可攜式設備與媒體時，資料攜入或攜出，應自我要求謹慎防範資訊洩漏或妨害組織利益等情節發生，評估可能面臨的風險。 （2）將機密資料存放於可攜式設備與媒體時，應採取適當加密處理或保護措施，避免遺失時洩漏資訊。 （3）可攜式設備與媒體之互相借用時，借用人應負保管責任，不得將設備擅自轉借他人使用；借用完成後應刪除設備內之資料。 （4）可攜式設備與媒體僅限於公務使用，禁止使用於非法用途。 3. 安全區域可攜式設備與媒體管理： （1）應審慎評估外部人員於安全區域(例如：資訊機房、檔案庫房)使用可攜式設備與媒體使用需求之必要性。 （2）私人可攜式設備與媒體，應評估風險後方可存取公務資料。 （3）外部人員使用可攜式設備與媒體連接內部網路，依「存取控制管理程序書」規範遵循。
雲端服務應用	1. 使用公有雲端服務前，宜先對雲端服務供應商的資安能力進行評估，如透過網路查詢雲端服務供應商資安標準取得(如，ISO27017、ISO 27018)、相關法規遵守情況及服務可用性等資訊。 2. 針對公有雲端服務方面，各使用單位應注意以下事項： （1）宜有電子/書面化的協議（如合約、服務條款、訂單等）確保雲端服務供應商應盡責任及使用期限建立有效溝通管道。

中山醫學大學

資安宣導單

分類	宣導事項
	（2）定期維護雲端服務並進行安全管理機制，如：帳號權限清查、事件日誌紀錄檢視、系統更新維護、刪除不需保存之敏感個資或作遮蔽/加密保護機制。 （3）如有使用上級或主管機關之雲端服務，應依其規範辦理相關作業。 3. 從雲端服務供應商撤出時應確保： （1）雲端服務內的資料及系統可正常移轉，如:移轉到新的雲端服務供應商或本校內的基礎設施。 （2）雲端服務內的資料及系統可被完整刪除，以免系統或資料因未完整刪除造成外洩之資安事故。 4. 依據教育部 110 年 09 月 08 日臺教資(四)字第 1100122001 號函「學校使用資通系統或服務蒐集及使用個人資料注意事項」： 學校為行政目的使用資通系統或雲端資通服務(如 Google 表單、Microsoft Forms 等問卷調查服務)蒐集個人資料時應注意事項： （1）資料蒐集最小化：僅蒐集適當、相關且限於處理目的所必要之個人資料，處理及利用時，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯。 （2）存取控制：應注意檔案存取權限設定，應採最小權限原則，僅允許使用者依目的，指派任務所需之最小授權存取。 （3）使用雲端資通服務者，應詳閱設定內容，不宜使用者共同編輯個人資料檔案清冊，並應注意避免設定允許顯示其他使用者作答內容，避免使用者能瀏覽其他使用者資料，造成個人資料外洩。公佈前應確實做好相關設定檢查，並實際操作測試，確認無誤後再行發布。 （4）傳輸之機密性：網路傳輸應採用網站安全傳輸通訊協定（HTTPS）加密傳輸，並使用 TLS 1.2 以上版本傳輸。 （5）資料儲存安全：如涉及蒐集個人資料保護法第 6 條之個人資料或其他敏感個人資料，應以加密方式儲存。 （6）應訂定個人資料保存期限，並於期限或業務終止後將蒐集之個人資料予以刪除或銷毀，避免個人資料外洩。
資料保護與保密協定	1. 傳輸個人資料必須遵循以下三大原則： （1）事前授權：所有個資傳輸，都必須經過單位主管審核與授權。 例如，未經授權不得將機敏文件攜出辦公環境區域。若有需要應提出申請，須經單位主管核准方可執行。 （2）最小化原則：僅傳輸業務必需的最少資料，避免過度傳送。 （3）適當加密：必須採取有效的安全措施，確保資料在傳遞途中不被竊取。 例如，重要文件或合約，應妥善保存；若為電子檔案應設定保護密碼。 2. 個人資料檔案保存與銷毀 各單位應至少每年定期檢視所保有之個資，確認其特定目的（如活動辦理完畢）是否消失或保存期限是否屆滿，若已無保存必要，應主動辦理刪除或銷

中山醫學大學

資安宣導單

分類	宣導事項
	毀。執行銷毀程序時，必須填寫「個人資料紀錄銷毀申請單」，並經單位主管核准後始得執行。 3. 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. 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。 5. 本校人員應恪遵人力資源室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。 6. 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。
個人資料蒐集控管原則	1. 告知義務先行： 蒐集個資前（如辦理活動、問卷），應明確告知當事人本校名稱、蒐集目的、類別、利用期間及地區，以及當事人可行使之五大權利。 2. 蒐集最小化： 僅蒐集執行業務所必要之個人資料，並應與蒐集目的具備正當合理關聯。 3. 未成年人保護： 蒐集未成年人個資時，應加註須由當事人告知其法定代理人或監護人。 4. 間接蒐集之告知： 若資料非由當事人提供，應於處理或利用前，確認是否已取得當事人同意並完成相關告知。
事件通報應變	1. 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) 2. 主動通報資安事件或可能資安風險者，依規定獎勵。 3. 發現或知悉疑似資通安全事件時，應即刻通知本校緊急應變暨技術支援組，後續通報及相關作業，由本校緊急應變暨技術支援組依規定時限(知悉後 1 小時內)辦理。 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。 4. 發現疑似個資外洩事件，應即刻通知本校秘書室，後續通報及相關作業由本校個資保護申訴窗口依規定時限(知悉起 72 小時內完成)辦理。 個資保護申訴窗口（秘書室林小姐）： 電子郵件信箱：cs1021@csmu.edu.tw、聯絡電話：04-24730022# 11021。