中國醫藥大學個人資料安全保護管理規範

中華民國 104 年 12 月 21 日 104 學年度第 1 次個人資料保護執行小組會議修訂通過
中華民國 105 年 1 月 18 日文資字第 1050000710 號函公布
中華民國 107 年 11 月 19 日 107 學年度第 1 次資訊安全暨個人資料保護推動委員會會議修訂通過
中華民國 107 年 12 月 10 日文資字第 1070017246 號函公布

壹、目的

為使各單位進行內部相關作業程序所產生或經手之各種形式（含書面或電子）之個人資料，能有遵循之準據以達保護之責，特依據教育部所頒佈之「教育體系個人資料安全保護基本措施及作法」訂定本規範。

貳、人員管理

一、 本校教職員工職務如有異動，其保管之個人資料（以下簡稱個資）檔案應列入移交，相關資訊系統存取權限應重新設定。

二、 單位接觸個資檔案人員應依照本校個資政策要求，執行相關規定之程序，簽署保密切結書，負擔個資保密義務，並於離職或合約終止時停用接觸的相關個資及系統使用者識別帳號。

三、 未經許可禁止使用任何形式傳輸或公開業務所知悉之個資。

參、作業管理

一、 個資蒐集應秉持「適當、相當且不過度」只蒐集必要個資，以降低個資外洩風險。

二、 針對所保有之個資，部份甚為敏感的欄位內容，譬如：密碼、身分證號等，於蒐集、處理或利用時，加上適宜之遮蔽措施。

三、 個資檔案使用完畢後，應立即退出應用程式。

四、 個資檔案禁止存放網路共用目錄及校外儲存空間。

五、 網路傳送個資檔案時，應對資料檔案加密，並再確認傳送對象無誤及請對方收到後回覆確認。

六、 使用可攜式電腦儲存媒體時，遵循以下的使用規範：

1.確定電腦安裝之防毒程式及病毒碼都有定時更新，足以偵測隱藏之病毒後，方可讀取可攜式電腦儲存媒體內的檔案。

2.暫存的個資檔案，使用後應確認刪除。

3.電腦使用應設登入密碼且符合密碼複雜難度要求。

七、 影印、列印、傳真使用後須確認設備內並未遺留個資資料及原稿。

八、 應定期備份含有個資的系統，及確認備份資料的可用性與安全性。

九、 個人電腦報廢或移作他用時，應確認資料刪除並無法復原再進行處理。

十、 報廢之個資文件須確實銷毀；電子檔須確實刪除與清空資源回收桶。

十一、 委託他人執行上述行為時，需對受委託人依個資法施行細則第八條規定為適當之監督，並明確約定相關事項、方式、義務及責任。

肆、物理環境管理

一、 保有個資之檔案室與主機房

1.為確保相關設施及個資安全，非權責單位指定之人員不得擅自進入，必要時可加裝監視設備，若無人在內需上鎖。

2.若外部人員或未具進出權限之人員，因執行業務需求進入時，必須指派人員隨行並填寫「人員進出登記表」後方可進出，並遵守相關設備管理之規定。

3.門禁紀錄及人員進出登記表，應適當保存與定期審閱。

二、 保有個資之辦公室

1.無人或下班最後一人離開時，需將辦公室關門上鎖。

2.敏感之文件與可攜式資訊設備存放於儲存櫃並上鎖。

3.辦公室內需隨時注意身分不明或可疑的人員。發現不明身分之人員時，需主動詢問並儘速通知相關部門進行處理。

三、 個人資料儲存媒體的保管

1.應對儲存媒體內重要的個資檔案加強安全管控，例如加密。

2.應有備份機制，避免重要資料遺失。

3.隨身碟只適宜儲存暫時性檔案，重要的個資檔案使用後應儘快刪除，避免因隨身碟遺失造成個資檔案外洩。

伍、技術管理

一、 重要資訊系統主機應做防火牆設定。

二、 重要資訊系統應適宜的限制存取 IP。

三、 電腦作業系統及相關應用程式之漏洞，應常做修補。資訊系統主機必要時需定時做弱點掃描，讓主機維持在不易入侵狀態。

四、 公務個人電腦應安裝防毒程式並設定自動更新病毒碼及 Windows Update。

五、 存有個資的個人電腦及伺服器，應設定登入密碼，且其密碼要符合安全之複雜度，至少 8 碼以上，且定期需更換密碼一次。

六、 個人電腦應設定螢幕保護密碼，且螢幕保護啟動時間定在 10 分鐘以內。

七、 應維持個資存取權限的正確性，且原則上不得共用存取權限，並留意個資被存取的情形。

八、 於入侵偵防設備上，設定禁止人員使用點對點(P2P)軟體提供分享檔案。

九、 每年執行個資盤點，檢查個資之使用狀況及存取情形。

陸、認知宣導及教育訓練

一、 本校教職員工應參與校內外資訊安全與個資保護之教育訓練，並定期宣導個資保護之重要性。

二、 每年本校校內至少舉辦 1 場(含)以上的個資保護相關宣導及教育訓練，以養成教職員工生個資保護的警覺性。

三、 本校個資窗口負責單位應時常注意個資保護相關知識與訊息，並摘要彙整於「個人資料保護專區」網站，以作為教職員工生獲取個資保護資訊的重要管道。

柒、紀錄機制

一、 個資交付、傳輸之紀錄

1.以 E-mail 方式，交付人應保留相關紀錄。

2.系統提供授權人連線下載方式，系統應有連線紀錄可供查閱。

二、 確認個人資料正確性及更正紀錄

1.資訊系統設計上應提供個人查核本人的基本資料，並允許做適宜之資料更新，以維-持個資正確性。

2.個人以異於上述的其它方式請求更正時，如電話、E-mail、信函等，處理人員除做必要的查核身份程序外，尚應設法留存事件紀錄。

三、 提供當事人行使權利之紀錄本校「個人資料保護專區」網站中「提供當事人行使權利」應清楚說明，依據個人資料保護法第三條，當事人得行使之相關權利，例如請求閱覽等，並提供本校個資窗口之詳細連絡資訊，例如連絡電話、E-mail 及郵寄地址。

四、 工作人員權限新增、變動及刪除紀錄人員工作異動時，重要資訊系統負責人應即對系統使用權限重新做設定，並保留相關紀錄。

五、 執行個資盤點與風險評鑑時，個資保管人應對已超過保留期限的部份銷毀並紀錄於盤點表中。

捌、本規範由資訊安全暨個人資料保護推動委員會會議審議通過，陳請校長核准後公佈實施，修正時亦同。