中國醫藥大學資訊安全管理作業規範

中華民國104年6月10日103學年度第2學期第5次行政會議訂定
中華民國104年6月22日文資字第1040007798號函公布
中華民國106年1月11日105學年度第1學期第6次行政會議修訂
中華民國 106 年 1 月 26 日文資字第 1060001105 號函公布
中華民國107年9月12日107學年度第1學期第2次行政會議修訂
中華民國 107 年 10 月 16 日文資字第 1070014519 號函公布

一、 依據『教育部所屬機關及各級公私立學校資通安全工作事項』制定「中國醫藥大學資訊安全管理作業規範」(以下簡稱本規範)，以維護本校網路、電腦設備及網站應用軟體使用之安全。

二、 本規範適用全校行政與學術單位及學生宿舍。

三、 使用本校提供之網路資源，應需遵守「中國醫藥大學校園網路使用規範」。

四、 除無線網路外，各單位電腦設備採固定網路 IP 位址，未經申請者，不得擅自設定、異動 IP 位址。

五、 防火牆管理：

(一)本校防火牆外部連接內部連接埠，原則禁止，例外開放；內部連接外部連接埠，原則開放，例外禁止，以維護校內設備安全。

(二)如因教學、研究或行政作業上需求，欲申請對外開放連接埠，依資訊中心「資訊安全管理系統(ISMS)」規定之程序辦理。

六、 無線網路管理：

(一)本校無線網路提供本校教職員生及跨校漫遊連線單位登入使用，非本校教職員生如因舉辦活動需使用本校無線網路，採線上申請方式。

(二)因教學、研究或行政作業上需求設立之無線網路基地台，須設定連線加密或帳號密碼身分過濾機制，且不得影響公用無線訊號。

七、 帳號管理：

(一)凡本校專、兼任教師、員工、及本校學生，均可申請帳號。

(二)各項帳號申請需填寫「網路帳號使用申請單」。學生則依據在學期間給予網路帳號。

(三)帳號有效起於申請生效日，止於辦理離校手續，退休人員保留電子郵件帳號，主機內信件及檔案等私人資料，需於帳號失效前自行備份完成。

(四)帳號只限於申請者本人使用，不得借予他人，或告知他人密碼，帳號一經建立，即不接受更改帳號名稱。

八、 密碼設定管理：

(一)第一次登入系統時，應立即更改系統預設通行碼，並定期更換密碼。

(二)避免將密碼記錄在書面上或張貼在個人電腦或終端機螢幕或其他容易洩漏秘密之場所。

(三)避免以個人資訊有關之資料(如生日、電話號碼或使用者帳號等)做為密碼；密碼應 8 碼以上，需為英文字母、數字或特殊字元的組合。

九、 電腦設備安全管理：

(一)應安裝防毒軟體、進行病毒資料庫、軟體更新、修補系統漏洞。

(二)應設定開機密碼，以防範未經授權使用。

(三)應開啟螢幕保護程式，啟動時間設定 10 分鐘以內，並設定密碼保護。

(四)下班或公出離開辦公室前，需關閉電腦設備，避免遭竊取機密資料或侵入系統。

十、 軟體使用管理：

(一)禁止安裝或使用來路不明、未經授權或影響電腦網路環境安全之電腦軟體。

(二)各單位採購之軟體，需妥善保存授權證明、原始程式或使用手冊等。

十一、電子郵件與通訊軟體：

(一)傳送機敏性資料需加密處理或於加密管道進行。

(二)留意社交工程攻擊(如:惡意電子郵件、釣魚網站)，勿開啟不明人士寄來的電子郵件、郵件附件及連結。

十二、儲存媒體管理：

(一)存放機敏資料之可攜式儲存媒體應納入管理，並存放在安全環境，未經單位主管核可，不得攜離辦公場所。

(二)不再繼續使用、逾保存年限或報廢時，應以安全的方式將儲存的內容消除，例如燒毀、以碎紙機處理、或將資料從媒體中完全清除。

(三)個人電腦或含有儲存媒體的設備，應在報廢處理前詳加檢查，以確保機密性、敏感性之資料及有版權之軟體已被移除。

十三、系統存取控制：

(一)執行業務及職務所必要時，得賦予使用者適當的系統存取權限。但工作調整時，使用者權限應立即異動；人員離職或退休應中止其使用權限。

(二)人員因故離開座位暫停作業時，必須登出系統或使用畫面鎖定保護，防止帳號被盜用或資料被竊取。

(三)校外存取校內未公開之資源需進行申請，禁止使用各種方法破解、入侵使用校內資源。

十四、作業系統及網站應用軟體進行遠端操作時，應於加密管道進行，並管制維護來源 IP。

十五、網站應用程式所有輸入欄位應進行字元檢查，排除不必要特殊字元，以防止資料庫隱碼攻擊(SQL-injection)。

十六、本規範經行政會議通過，陳請校長公佈後實施，修正時亦同。