嘉南藥理大學電腦設備安全管理作業規範

民國 97 年 5 月 21 日資訊安全委員會議制訂通過
民國 109 年 5 月 5 日資訊安全委員會議修正通過

第1條　目的及依據

嘉南藥理大學(以下簡稱本校)為確保電腦資料、系統、設備及網路之安全，並依據教育部台電字第 0960196582 號函辦理，特制定「嘉南藥理大學電腦設備安全管理作業規範」(以下簡稱本規範)。以避免因人為疏失、蓄意破壞或自然災害等風險，遭致資訊資產不當使用、洩漏、竄改、破壞等情事，而影響電腦系統正常運轉。

第2條　適用範圍

(一) 人員：本校教、職員工(含約聘僱人員)、學生等使用本校資訊資源，或資訊業務委外服務之廠商人員。

(二) 硬體設備：各類主機、工作站、伺服器及個人電腦等。

第3條　管理及使用單位

(一) 圖書資訊館為本校電腦設備安全管理之督導單位。

(二) 各單位為業務使用的電腦設備之使用單位，實際負責單位內的電腦設備資訊安全稽核及保護事宜。

第4條　人員安全與管理

(一) 本校教、職員工(含約聘僱人員)必須遵守本規範，任何因違規導致之資訊安全意外事件將依相關人事法規懲處。

(二) 本校資訊業務委外服務之廠商人員，應於簽訂契約時同時簽署保密切結書，切結遵守本規範。

(三) 本校同仁離職時，須依規定辦理離職手續，並由各管理單位更改使用者密碼或刪除各業務使用帳號後，始完成離職程序。

(四) 如因職務異動成為非授權使用者時，隸屬單位應主動通知各單位更改使用者密碼或刪除該使用者帳號。

第5條　電腦系統安全管理

(一) 資料庫或個人重要資料應定時執行備份，並異地存放，以確保資料的安全。

(二) 處理含個人資料時，應依據「電腦處理個人資料保護法」及相關規定審慎處理，不得私自蒐集或洩漏業務資訊，非公務用途不得調閱使用。

(三) 各單位之個人資料索取或調閱，須經單位主管核准，依據「電腦處理個人資料保護法」及相關規定審查後，始可提供資料。

(四)　病毒防護軟體及系統回復軟體由督導單位每年定期統一規劃、評估與建置。

(五) 應使用合法版權軟體，避免上網下載來路不明之軟體。

(六) 與外部交換機密敏感資料時，需依據安全查核機制，確定無安全疑慮，方可進行。

(七) 應安裝防毒軟體，隨時更新病毒碼，並下載系統漏洞修補程式。

第6條　電腦儲存媒體之安全管理

(一) 儲存應保密資料之可攜帶移動的儲存裝置(如磁帶、磁碟等)、電腦列印之各式報表、作業程序目錄、及系統文件等應納入管理。

(二) 電腦儲存媒體應依保存規格要求，存放在安全的環境，未經主管核准，不得攜離辦公場所。

(三) 電腦媒體儲存的資料,不再繼續使用或逾保存年限時,應將儲存的內容消除；報廢時，應由專人以安全的方式處理，例如燒　毀、以碎紙機處理、或將資料從媒體中完全清除。

(四) 電腦媒體運送過程，應有妥善的安全措施，以防止資料遭竄改破壞、誤用或未經授權的取用。

第7條　系統存取控制

(一) 因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，使用者名稱須立即異動。

(二) 應用系統使用者各自擁有自己的使用者名稱和密碼，不同的使用者各有不同的作業範圍和權限。密碼必須加以保密，避免洩密遭人盜用，並應定期更改通行密碼。

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

第8條　資訊資產之安全管理

(一) 建立資訊系統有關資訊資產目錄，明列資訊資產的項目、管理(負責)人及安全等級分類，如有變更應詳細記載。

(二) 分類依據國家機密保護、電腦處理個人資料保護及政府資訊公開等相關法規，區分為機密性、敏感性及一般性等三類。

(三) 資訊資產實體設備故障應通知資產管理(負責)人，並由管理(負責)人依規定提出請修申請。

(四) 資訊資產實體設備報廢，由財產管理人員依規定辦理。

(五) 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。

第9條　系統發展與維護之安全管理

(一) 本校行政系統由督導單位負責開發、採購與維護。

(二) 各單位要求開發新系統時,須填具申請表,經審核後,由督導單位規劃開發、測試、上線時程。

(三) 系統規劃開發過程中應對惡意碼與行動碼建立控制措施。

(四) 系統規劃開發過程中應針對原始碼建立資料庫隱碼攻擊檢核機制。

(五) 資訊業務委外時，應於事前審慎評估可能的潛在安全風險，並與廠商簽定適當的資訊安全協定，及課以相關的安全管理責任，納入契約條款，必要時並應不定期派員監督、管理委外廠商實際作業情形。

(六) 委外作業承包之工作人員，如需進入相關系統作業，由委外業務之主管單位依規定申請使用者名稱，並於委外業務完成後立刻依規定刪除。

(七) 委外作業輸入之資料由主管單位指派專人核對以確保資料之正確性，委外資訊廠商除安全管理責任外，尚應落實保密作為。

(八) 系統委外開發承包商應提供系統建置(含規格及軟體程式)之完整、詳細說明文件。

第10條　實體及環境安全管理

(一) 電腦設備安全管理

1. 專人負責，並制訂電腦設備開關機操作程序。
2. 定期維護保養，確保設備的完整性及可以持續使用。
3. 電腦設備、資料或軟體，未經管理人員同意下，不得攜離辦公室。

(二) 電力供應系統的管理

1. 相關電腦設備之電源使用應依據製造廠商提供規格設置，並需防止斷電或電力不正常導致的傷害。
2. 緊急供電系統暨不斷電系統應由專人負責管理及制訂開關機操作程序，並定期維護保養及測試。

(三) 電腦機房消防系統的設置管理

1. 專人負責管理。
2. 定期維護保養及測試，確保設備的完整性及可以持續使用。

(四) 其他安全管理

1. 電腦機房實施門禁安全控管。
2. 資訊支援或維護服務人員需由管理人員陪同並經登記後，始得進出管 制區域。
3. 電腦機房及各項電腦軟、硬體設備應強化設(放)置處、所防護措施，避免遭致水患、風災、火災等災害，造成損失。

第11條　資訊安全稽核

(一) 資訊機密維護及稽核使用管理事項，由資訊安全委員會及相關單位組成安全稽核小組負責辦理。

(二) 稽核之結果應填寫紀錄表完整記錄。

(三) 資訊安全稽核之結果，應彙整相關單位之優缺點及綜合改進建議，可提供相關單位改進，並列入下年度稽核時追蹤。

(四) 每年應進行資訊安全風險評估及作業檢討，並據以修正本規範，確保資訊安全實務作業之有效性。

第12條　本規範經資訊安全委員會議通過，陳請校長核定後公布實施，修正時亦同。