嘉南藥理大學網路安全管理作業規範

民國 97 年 5 月 21 日資訊安全委員會議制定通過
民國 109 年 5 月 5 日資訊安全委員會議修正通過
民國 110 年 7 月 29 日第 6 次行政會議修正通過

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「嘉南藥理大學網路安全管理作業規範」(以下簡稱本規範)。以避免因電腦病毒或駭客攻擊、人為疏失、蓄意破壞或自然災害等風險，遭致發生網路安全事件等情事，而影響網路系統正常運轉。

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。

三、　網路及其設施：本校校園網路(含無線網路)、網際網路之數據專線及相關網路設備。

第3條　網路服務之管理

一、　專人負責管理與存放網路安全相關的記錄檔案。

二、　定期審閱網路安全相關的記錄檔案。

三、　定期檢討網路安全控管事項之執行。

四、　設置網路系統管理人員，負責網路安全相關管理。

五、　網路系統管理人員應負責系統安全規範的擬訂，執行系統管理工具之設定與操作，確保系統與資料的安全性與完整性。

六、　系統管理人員應依程序撤銷離(休)職人員之使用帳號，以取消其存取之權利。

七、　網路系統管理人員除依相關法令或機關規定，不得閱覽使用者之私人檔案；但如發現有可疑的網路安全情事，網路系統管理人員得依授權規定，使用自動搜尋工具檢查檔案。

八、　網路系統管理人員未經使用者同意，不得增加、刪除及修改私人檔案。如有特殊緊急狀況須刪除私人檔案，應事先知會檔案擁有者。

九、　如有發現任何網路安全事件，應及時通知相關網路系統管理人員進行處理，向主管報告，並通報圖書資訊館數位資訊組處理。

十、　系統管理人員不得新增、刪除、修改記錄檔(LOG)，以避免違反資安事件發生時，造成追蹤查詢的困擾。

十一、 網路設備均應設置不斷電裝備以防止不正常的斷電狀況，並應定期維護。

第4條　網路使用者之管理

一、　利用網路使用任何電腦資源，均需遵守本校校園網路使用規範。

二、　所有人員應主動了解本校網路安全相關規定，並確實瞭解其應負的責任，以免發生違反網路安全情事，遭致懲處。

三、　不得將自己的登入身份識別與登入網路的密碼交付他人使用。

四、　不得以任何方法竊取他人登入網路的身份識別與通行碼。

五、 不得以任何儀器設備或軟體工具竊聽網路上的通訊。

六、 不得將色情檔案建置在校園網路，亦不得在網路上散播色情文字、圖片、影像、聲音等不法或不當的資訊。

七、 不得發送電子郵件騷擾他人，導致其他使用者不安與不便；亦不得發送匿名信，或偽造他人名義發送電子郵件。

八、 不得以任何手段蓄意干擾或妨害網路系統的正常運作。

九、 非本校教職員工需經授權後才得使用網路及電腦資源，並須遵守本校使用網路之一切規定。

十、 應辦理資訊安全宣導講習(含防毒、備份及一般機密保護規定)。

第5條 主機安全之防護

一、 機密性及敏感性資料之主機或伺服器主機，應防制非法使用者假冒合法使用者身分登入主機進行偷竊、破壞等情事。

二、 為提升主機或伺服器主機連線作業之安全性，應視需要使用 VPN 等各種安全控管技術，以建立安全及可信賴的通信管道。

第6條 防火牆之安全管理

一、 內部網路與外部網路連接需加裝防火牆，以控管外界與內部網路之間的資料傳輸與資源存取。

二、 防火牆之記錄檔(LOG)應由防火牆管理人員檢視分析有無異常狀況並定期備份。

三、 防火牆主機需使用帳號密碼登入，以確保安全。

四、 防火牆之安全控管設定應經常檢討，並作必要之調整，以確定發揮應有的安全控管目標。

五、 防火牆系統應定期作好資料備份，且只能做單機備份，不可採用網路等其他方式備份資料。

六、 防火牆系統軟體，應經常更新版本，以因應各種網路攻擊。

第7條 軟體使用與控制

一、 不得經由網際網路下載非制式軟體使用。若需要下載制式軟體，亦應注意預防電腦病毒感染。

二、 不得使用來路不明之軟體，亦不得測試來路不明之軟體，以免引入電腦病毒。

三、 於網路下載軟體使用之初期，應勤於掃瞄病毒，以確定下載軟體安全無虞。

四、 應全面使用防毒軟體並即時更新病毒碼。

五、 軟體需妥善保存授權證明、原版程式、使用手冊。

六、 使用適當稽查軟體工具檢查所有個人電腦內使用之軟體，確定個人電腦中只載入合法軟體。

第8條 網路資訊之管理

一、 對外開放的全球資訊網(web)資訊系統，所提供之資料內容由各業務單位決定其適當性，並協調電腦系統管理人員作安全權限之設定。

二、 對外開放資訊系統的主機，應以防火牆與內部網路區隔，提高內部網路的安全性。

三、 對外開放全球資訊網資訊系統的主機，不得對外開放遠端登入與遙控的功能。

四、 對外開放全球資訊網資訊系統的主機，應針對蓄意破壞者可能以發送作業系統指令或傳送大量資料(如電子郵件、註冊或申請資料)導致系統作業癱瘓等情事，預作有效的防範，以免影響服務品質。

五、 機密性及敏感性的資料或文件，不得存放在對外開放的資訊系統中。

六、 對外開放的全球資訊網資訊系統，如存放私人資料檔案，應以加密方式處理，並妥善保管，以防止被竊取或移作他途之用。

七、 對外開放全球資訊網資訊系統的主機，須妥善規劃資料備份作業並確實執行。

第9條 網路入侵之處理如發現網站遭入侵，應處理下列事宜：

一、 關閉對外之連線。

二、 通報所屬主管及圖書資訊館資訊服務組。

三、 備份被入侵主機當時之系統，作為日後檢驗之用。

四、 修護系統，及移除惡意程式或檔案。

五、 全面檢討網路安全措施及修正防火牆的設定，以防禦類似入侵與攻擊。

六、 提出入侵檢討報告。

第10條 電子郵件之安全管理

一、 用戶端的郵件軟體設定不建議系統直接記憶密碼，而須採用每次連接郵件伺服器時，再登錄密碼方式為之。

二、 禁止轉信(open relay)功能，防止有心人士利用本校郵件伺服器做非法信件的轉寄，而增加追查作業的複雜度。

三、 非本校教職員工不得申請建立本校教職員工電子郵件帳號。

四、 需定時進入垃圾郵件系統，檢視是否有誤判之垃圾郵件。

五、 需定期進行個人郵件備份，以防止郵件遺失造成損失。

第11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。