法鼓文理學院 網路安全管理作業規範

中華明國 97 年 9 月 25 日 97 學年度第 1 次行政會議修訂通過
中華民國 105 年 3 月 16 日 104 學年度第 3 次行政會議修訂通過

一、依「教育部所屬機關及各公私立學校資通安全工作事項」，為規範網路安全管理作業，訂定本規範。

二、網路安全之管制

(一) 本校網路安全管理人員由圖書資訊館資訊與傳播組(以下簡稱本組)指派合格且適任之人員擔任。

(二) 與外界網路連接之網點，應以防火牆及其他必要安全設施，控管外界與內部網路之資料傳輸與資源存取。

(三) 聯外網路應安裝入侵偵測系統，網路安全管理人員須定時檢視入侵監測系統之紀錄，以監控非法入侵之犯罪行為，並收集入侵證據以作為法律控訴之證物。

(四) 本校教職員生如因教學研究或其他特殊需求，需於防火牆對外開放特殊服務（如遠端登入 Telnet 或檔案傳輸 FTP 等），在不影響本校網路安全條件下（如採用 VPN tunnel 技術），經本組核可後，由本組設定開放權限。

(五) 開放外界連線作業之資訊系統，應視資料及系統之重要性及價值，採用資料加密、身分鑑別、電子簽章、防火牆及安全漏洞偵測等不同安全等級之技術或措施，防止資料及系統被侵入、破壞、竄改、刪除及未經授權之存取。

(六) 對校內網路建立警示系統，於特定網路安全事件發生時，能立即產生警示訊號通知網路系統管理人員，俾採取有效的防護措施，降低安全事件所產生的危害。

(七) 校內之機密性資料及文件不得以電子郵件或其他電子方式對外傳送。若需對校內以電子化方式傳送機密文件及資料時，必須搭配適當加密處理或或電子簽章等安全技術處理後方可傳送。

(八) 若因為單位業務性質特殊，須利用電子郵件或其他電子方式對外傳送機密性資料及文件者，得採用權責主管機關認可之加密或電子簽章等安全技術處理。

(九) 為避免網路使用者不慎違反本校相關網路安全規定，網路管理人員可考慮以相關網路技術以不干擾正常網路使用為原則下，主動管制違反本校相關網路規定之使用者。

三、網路入侵之處理

(一) 立即拒絕入侵者任何存取動作，防止災害繼續擴大；當防護網被突破時，系統應設定拒絕任何存取；並於事後全面檢討網路安全措施及修正防火牆的設定，以防禦類似的入侵與攻擊。

(二) 為達到追查入侵者的目的，可考慮讓入侵者做有條件的連接，一旦入侵者危害到內部網路安全，則必須立即切斷入侵者的連接。

(三) 對入侵者的追查，除利用稽核檔案提供的資料外，得使用系統指令執行反向查詢，並連合相關單位(如網路服務公司)，追蹤入侵者。

(四) 入侵者之行為若觸犯法律規定，構成犯罪事實，應立即告知檢警憲調單位，請其處理入侵者之犯罪事實調查。

四、本規範經行政會議通過，陳請校長核定後公布施行，修正時亦同。