景文科技大學網路安全管理作業規範

（圖 036）

民國 103 年 7 月 1 日 102 學年度第 21 次行政會議通過

一、景文科技大學（以下簡稱本校）為進行網路管理時能有所依據，建立網路對外服務申辦作業及安全檢查，特訂定本校網路安全管理作業規範（以下簡稱本規範）。

二、範圍：行政單位與學術單位。

三、固定 IP 管理：

（一）各單位個人電腦均採行 DHCP（Dynamic Host Configuration Protocol）方式取得 IP，未經申請者，不得擅自設定固定 IP。

（二）為避免影響網路正常運作，未經圖書資訊處（下簡稱本處）核准，勿擅自架設 DHCP 服務。

（三）如因教學、研究或行政作業上需求，欲申請固定 IP，須填具「固定 IP/網域名稱申請表」，逕向本處申請，經審查核准，配發 IP 後始可設定。

（四）為避免 IP 資源配置不當，申請之固定 IP 如經查於一年內無使用紀錄，本處可清除申請資訊，重新進行 IP 配置。

四、防火牆管理：

（一）本校防火牆對外連接埠（Port），原則禁止，例外開放。

（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，須填具「固定 IP/網域名稱申請表」，逕向本處申請，經審查核准後開放。

（三）本校防火牆政策，應依資訊安全等需求，進行必要之調整。

五、無線網路管理：

（一）本校無線網路僅提供本校教職員生及跨校漫遊連線單位登入使用。

（二）如因舉辦活動需使用本校無線網路，於 3 個工作天前填具「圖資處支援單」，逕向本處申請，經審查核准後，開放無線網路參訪者（Guest）使用。

（三）為避免干擾無線網路之正常運作及保障本校資訊安全，校內不得私設無線網路基地台。如因教學、研究或行政作業上需求，需向本處申請核可。

六、軟體使用管理：

（一）禁止下載、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）使用外來檔案，應先進行掃毒，勿任意移除或關閉防毒軟體。

（三）本校校園合法軟體授權版本、使用範圍可諮詢本處資源管理組。

（四）各單位逕行採購之軟體，需妥善保存授權證明、原始程式或使用手冊等。

七、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。

（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）輸入密碼時應謹防他人偷窺。

（四）應保持高度之警戒心，防範不法人士以社交工程（Social Engineering）騙取帳號及密碼入侵。

（五）密碼應 8 碼以上，同時需為英文字母、數字或特殊字元的組合。

（六）儘量避免以時間、個人資訊、單位識別代碼、電話號碼或使用者帳號等做為密碼。

（七）應定期更換密碼，同一密碼使用期限最長應不超過 6 個月，並應儘量避免重複或循環使用舊的密碼。

八、主機安全管理：

（一）本校對外提供服務之主機，均需遵守本校校園伺服器管理要點。

（二）主機密碼管理同第七點。

（三）應配合進行軟體更新，修補漏洞。

（四）應設定螢幕保護密碼，螢幕保護啟動設定為 10 分鐘。

（五）應安裝防毒軟體，並更新病毒定義檔。

（六）禁止使用點對點互連（P2P）軟體及 Tunnel 相關工具下載或提供分享檔案。如因教學、研究或行政作業上需求，需向本處申請核可。

九、管理者責任：

（一）管理者負責建立及維護系統使用者帳號，並記錄系統異常狀況及相關維護書面資料。

（二）管理者未經單位主管人員許可，不得閱覽、增加、刪除或修改其他使用者上傳之私人檔案。如發現有可疑之網路安全情事(如病毒、惡意程式或檔案等)，得使用適當的工具追蹤檢查相關檔案，採取必要處理措施，事後再行知會該檔案使用者。如確定為感染病毒，為避免病毒擴散，得逕行掃毒、隔離或刪除檔案再行知會該檔案使用者。

（三）管理者登入系統時應保留所有登出入系統紀錄，不得新增、刪除或修改稽核資料檔案，避免於安全事件發生後造成追蹤查詢之困擾。

（四）管理者應定期檢查及撤銷閒置不用的帳號，不得將其重新配賦給其他的使用者，且須確認不得有非必要的帳號存在（如 Guest、Anonymous…等）。

（五）每位使用者僅得核發一個使用者帳號，如有特殊情形(如系統測試等用途)，經單位主管核定，始得建立匿名或多人共享的帳號。

十、使用者責任：

（一）使用者利用本校提供網路資源，均需遵守本校學術網路使用準則。

（二）使用者密碼管理同第七點。

（三）使用者不得以任何不法手段蓄意干擾或妨害網路的正常運作。

（四）非本校教職員生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。

十一、 網路入侵處理程序：

（一）關閉對外網路連線。

（二）通報單位主管與本處資訊網路組。

（三）備份被入侵主機作業系統、應用系統及 log 等。

（四）修復作業系統，重新安裝應用系統，移除惡意程式或檔案。

（五）為防止類似的入侵與攻擊再次發生，檢討主機網路安全，調整防火牆設定、系統漏洞修補及安裝防毒軟體等。

十二、 本規範經行政會議通過，校長核定後公布實施。