景文科技大學電腦設備安全管理作業規範

（圖 037）

民國 104 年 1 月 20 日 103 學年度第 11 次行政會議通過
民國 104 年 4 月 14 日 103 學年度第 16 次行政會議修正通過

一、景文科技大學（以下簡稱本校）為規範伺服主機與個人電腦系統建置安全，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」，訂定電腦設備安全管理作業規範（以下簡稱本規範）。

二、範圍：行政單位與學術單位。

三、智慧財產權管理：

（一）各電腦設備應安裝合法取得授權之軟體，勿任意下載或安裝來路不明、有違反法令疑慮或與業務無關的電腦軟體。

（二）各電腦設備嚴格禁止裝設點對點（P2P）下載軟體，以防資料外洩。

（三）各電腦設備禁止對外提供下載或張貼受著作權保護之內容，包含文字、檔案、影像、圖片及軟體。

四、資訊安全管理：

（一）應安裝防毒軟體，並適時更新病毒資料庫。

（二）應開啟作業系統之防火牆。

（三）應適時進行作業系統漏洞修補與更新軟體。

（四）應設定 8 碼以上，同時須為英文字母、數字或特殊字元組合的密碼。

（五）應設定至少等候 10 分鐘啟用螢幕保護裝置功能，並需用密碼啟動解除。

五、個人資料安全管理：

（一）個人資料之建檔、增修、存放、刪除程序之管理與紀錄，應遵循「個人資料保護法」等相關對個人資料保護之規範。

（二）電腦設備進行報廢或汰換前，應逕行將機密性、敏感性及個人資料予以刪除，以確保任何機密性、敏感性、個人隱私之資料不外流。

六、可攜式儲存媒體之安全管理：

（一）可攜式儲存媒體需連接本校設備或網路時，應先進行防毒軟體掃描，確認無問題後始可使用。

（二）機敏性資料儲存於可攜式儲存媒體時，應進行加密技術或其他加強安全控管，並於使用完畢後刪除。

（三）非公務需求不得將載有機敏性資料之可攜式儲存媒體攜出辦公場所。

（四）含機敏性資料之可攜式儲存媒體遞送，應以專人或密件方式傳送。

七、遠端維護管理：

本校防火牆對外連接埠（Port）因教學、研究或行政作業上需求，需於防火牆對外開放特殊服務（如遠端登入或檔案傳輸等），在不影響本校網路安全條件下（如採用 VPN tunnel、SSH 技術），填具「固定 IP/網域名稱申請表」逕向圖書資訊處申請核可後始得開放。

八、電腦設備應置於通風良好之適當空間，散熱孔不得任意阻擋或封住。

九、電腦設備若無特殊需求，應於下班後，關閉電源以節能減碳。

十、各單位電腦設備之維護須重新安裝時，必須由授權之維護人員執行，並填具「景文科技大學電腦設備安裝完成檢測清單」，交付至圖書資訊處留存備查。

十一、 各單位新購電腦設備交付前，應進行檢測，並填具「景文科技大學電腦設備安裝完成檢測清單」，交付至圖書資訊處留存備查。

十二、 本規範對於伺服主機之管理，應依據本校「校園伺服器管理要點」辦理。

十三、 本規範經行政會議通過，校長核定後公布實施。