伺服器資訊安全管理

（一）、各行政及教學單位對外開放網際網路服務之伺服器，應符合「國立雲林科技大學伺服器管理辦法」之規定。

（二）、設定防火牆以控管外界與單位內網路間之資料傳輸與資源存取，應符合「國立雲林科技大學防火牆系統管理規範」，並關閉不使用的通訊埠，以避免病毒感染及駭客攻擊。

（三）、開放外界連線作業之伺服器主機，應避免外界直接進入資訊系統或資料庫存取資料。

（四）、伺服器主機管理之安全性，應視需要之使用情況，加密通道（如 VPN、SSH）等各種安全控管技術。

（五）、各單位開發之系統及網站(含委外開發)，應於完成後，先執行弱點掃描與完成修補風險弱點始可上線；運作中網站亦請定期進行必要的系統及網站弱點掃瞄，相關檢測事項請依「網站應用程式弱點檢測管理要點」辦理。

（六）、每次掃描完成後應產出弱點掃描報告與進行相關漏洞修補，並填寫「弱點處理報告單」(表單編號：YUNTECH-ISPI-D-002)，修補後應進行複掃，確保弱點均已處理無遺漏。弱點若因故無法修補，應於「弱點處理報告單」說明無法修補之原因與防禦因應方法。

（七）、伺服器管理者應於每工作日時依「系統與網路巡查紀錄表」(表單編號：YUNTECH-ISPI-D-003)所列項目檢查重要系統主機狀況，以確保系統正常運作。

（八）、重要系統設定檔、網頁資料、伺服器檔案、資料庫及機敏性檔案資料均應訂定備份週期，並依據週期執行系統排程或手動備份。備份宜以加密方式保護，備份狀況記錄於「備份狀況紀錄表」(表單編號：YUNTECH-ISPI-D-004)。

（九）、伺服器結束遠端系統維護作業後，應關閉應用系統及網路連線，並清除螢幕上的資訊，將作業系統登出。

（十）、檢視各設備中系統之時間是否一致，並進行校正及同步作業。