

國立臺灣師範大學校園伺服器管理要點

民國 97 年 5 月 14 日第 35 次行政主管會議通過

民國 112 年 6 月 28 日 111 學年度第一次資訊安全暨個人資料保護委員會修正通過

民國 113 年 12 月 30 日 113 學年度第一次資訊安全暨個人資料保護委員會修正通過

壹、總則

- 一、為提昇本校伺服器之資訊安全管理，依據「資通安全管理法」訂定本要點。
- 二、本要點所指之伺服器，係為對外提供服務之伺服器，如網站(Website)、電子郵件(E-mail 與 Webmail)、檔案傳輸(FTP)與網路硬碟(NAS)等。
- 三、本校各單位伺服器之管理，應符合「資通安全管理法」、「教育部校園網路使用規範」、「臺灣學術網路使用規範」及「國立臺灣師範大學校園網路使用與管理要點」，並參照本校資訊安全管理制度(ISMS)及資安相關法規。

貳、人員

- 四、各單位伺服器應設置專人負責維護管理，並配合本校相關資訊安全作業之輔導。伺服器管理者應每年參加資訊安全講習。

參、放置地點

- 五、各單位伺服器應建置於校內，並優先選擇雲端虛擬主機，申請方式詳「國立臺灣師範大學資訊中心虛擬主機服務管理暨收費辦法」；因特殊因素須自購硬體設備者，則以申請主機代管服務集中放置為原則，申請方式詳「國立臺灣師範大學主機代管服務要點」。

肆、伺服器管理

- 六、各單位伺服器一律納入管控。如需對外開放服務者，須向資訊中心申請，未經申請者，將限制由校外連線。另進行校外遠端維護時，須使用 VPN 連線。
- 七、各單位伺服器若疑遭駭客入侵、網路流量發生異常、濫發廣告信等相關行為或有重大資安漏洞，經查證屬實者，得停止該伺服器之網路使用權。

伍、稽核

- 八、各單位伺服器之管理應落實「伺服器資安管控措施檢核表」之各項規範；資安暨個資保護執行推動小組每年將對單位伺服器進行資訊安全稽核，各單位針對稽核缺失應於期限內完成改善，並送資安暨個資保護執行推動小組備查。

陸、訂定及修正

- 九、本要點經資訊安全暨個人資料保護委員會通過後實施，修正時亦同。

國立臺灣師範大學伺服器資安管控措施檢核表

填寫日期：____年____月____日

單位：_____ 管理人員：_____ 電話：_____ 電子郵件：_____

伺服器種類：網頁伺服器 FTP DNS Webmail NAS 其他：_____

IP：_____ 網址：_____

編號	檢核項目	自我檢核			複核		
		通過	未通過	不適用	通過	未通過	不適用
1	不得使用預設密碼，所有帳號之密碼須符合複雜性原則（數字、小寫英文、大寫英文或特殊符號這4種中必須要有3種，且至少10碼以上），並停用訪客帳號，每半年變更密碼乙次，密碼變更不得與前3次一樣	<input type="checkbox"/>					
2	伺服器須設定時間校時(註1)	<input type="checkbox"/>					
3	伺服器禁止顯示版本信息(如 apache、php 等版本)及其他預設資訊	<input type="checkbox"/>					
4	啟用防火牆保護機制並設定僅開放許可的服務	<input type="checkbox"/>					
5	使用遠端連線工具（遠端桌面、VNC、SSH 等）進行維運管理，應確認僅限制管理 IP 可連線存取，並限制遠端可連線時間	<input type="checkbox"/>					
6	管理者登入頁面須限制可連線 IP	<input type="checkbox"/>					
7	敏感等級以上之業務資料或文件不得存放於對外開放之資訊系統中，若因特殊業務功能之需求，必須採取安全管控機制	<input type="checkbox"/>					
8	系統登入須設定帳號鎖定機制，如輸入錯誤5次封鎖30分鐘等，並開啟稽核機制	<input type="checkbox"/>					
9	重要資料必須定期進行異機備份，如網頁、資料庫資料及系統 log	<input type="checkbox"/>					
10	定期檢視系統使用容量，避免容量不足而導致主機當機或資料毀損	<input type="checkbox"/>					
11	人員離職或調離管理作業時，應移除其系統帳號，並至少每年盤點一次管理帳號	<input type="checkbox"/>					
12	Windows 作業系統須安裝防毒軟體，並設定定時自動更新病毒碼及執行系統掃描	<input type="checkbox"/>					
13	主機須更新到最新修正檔，並進行主機弱點掃描(如 Nessus)，確保無高、中等級之漏洞	<input type="checkbox"/>					
14	Windows 伺服器需導入 VANS(弱點通報機制)	<input type="checkbox"/>					
15	遵守教育部「各級學校使用資通系統或服務蒐集及使用個人資料注意事項」，涉及蒐集個人資料者，注意資料蒐集最小化、存取控制及詳閱設定內容(雲端資通服務)等項目	<input type="checkbox"/>					
16	伺服器管理人員每二年須接受至少3小時資安專業課程	<input type="checkbox"/>					
網頁伺服器檢核項目							
17	網頁伺服器禁止設定目錄瀏覽功能，避免駭客竊取資料。可於 Google 搜尋"index of / site:xxx.ntnu.edu.tw"	<input type="checkbox"/>					
18	伺服器錯誤網頁不得顯示程式碼等敏感資訊	<input type="checkbox"/>					

19	公告之資訊，應確認未含有敏感等級以上資訊、違反資訊安全管理相關資訊，以及違反智慧財產權或法令所明訂之禁止資訊	<input type="checkbox"/>					
20	定期檢視留言板內容，注意網頁內容之合法性，不得有猥褻性、攻擊性、及商業性之資料，或涉及侵害智慧財產權之行為	<input type="checkbox"/>					
21	網站必須使用 https 連線，並停用 http 連線	<input type="checkbox"/>					
22	資料庫儲存之機敏資料必須加密儲存(如密碼、身分證字號等)	<input type="checkbox"/>					
23	系統網站內容遭竄改時，應備妥應變機制，以利於發現網頁遭竄改後 10 分鐘內切換為維護公告頁面，並進行演練	<input type="checkbox"/>					
24	網站應用系統已完成弱點掃描(如 Appscan)，並完成資安漏洞處理	<input type="checkbox"/>					

註 1:校內可使用校時主機為 time.stdtime.gov.tw、tick.stdtime.gov.tw、time.windows.com、time.asia.apple.com、ntp.ubuntu.com、0.debian.pool.ntp.org、1.debian.pool.ntp.org、2.debian.pool.ntp.org、3.debian.pool.ntp.org、0.centos.pool.ntp.org、1.centos.pool.ntp.org、2.centos.pool.ntp.org、0.rhel.pool.ntp.org、1.rhel.pool.ntp.org、2.rhel.pool.ntp.org，若要使用校內 NTP server，校本部及公館可使用 140.122.8.254、林口校區可使用 140.122.240.190

填寫人：_____ 連絡電話：_____ 單位主管：_____

※ 請單位先自行檢核，並將佐證資料以電子檔傳送資訊中心複核，確認後再送交紙本資料。

※ 虛擬主機管理人員：李良谷先生，電話：3735，E-mail:jacklee@ntnu.edu.tw

※ 主機代管管理人員：林柏宏先生，電話：8627，E-mail:stevenlin@ntnu.edu.tw

※ 資安聯絡窗口：柯文傑先生，電話:3733，E-mail:genieke@ntnu.edu.tw

資訊中心複核意見：

收件日期：_____年____月____日 複核日期：_____年____月____日

複核人：_____ 單位主管：_____