國立臺灣科技大學
架設伺服器資訊安全參考規範

110.3.22 資訊安全委員會議通過

1. 根據「資通安全責任等級分級辦法」，本校為資通安全責任等級 C 級之公務機關，全機關之公務資通訊設備均須符合資通安全管理法及其相關法規之資安規定。

2. 建議設置硬體防火牆，外部網路對內部網路，除了提供網路服務及管理的通訊埠(PORT)外，一律設定封鎖。內部網路對外部網路，除了允許的伺服器 IP 及通訊埠(PORT)外，一律設定封鎖。

3. 若須從遠端(校外)進行伺服器管理時，請務必以 VPN 連線進行管理。
VPN 可使用電子計算機中心之 VPN 服務或防火牆內建之 VPN 功能皆可。

4. 超級使用者的帳號與密碼，知悉者最小化為原則，但考量實際風險，最小化需大於等於兩個人；並應使用不同帳號登錄。請將超級使用者的帳號與密碼以紙本或電子形式封存於所屬長官或指導教授處，以備不時之需。
嚴禁將帳號密碼書寫或黏貼在伺服器上、螢幕上、公開的地方。

5. 請定期(建議每周一次)備份伺服器內之重要資料、程式碼、資料庫、電子郵件等至備份裝置。

6. 需定期(建議每周至少一次)執行系統更新。Windows 系統執行 Windows Update；Apple、Linux(Red Hat、Ubuntu、Fedora、OpenSUSE、Debian、CentOS 等)、其他作業系統亦須定期(建議每周至少一次)審視是否進行系統更新。

7. 需定期(建議每周至少一次)進行應用軟體安全性更新(Java、Adobe Flash Player、Adobe Reader、其他軟體)

8. 安裝防毒軟體，並至少每一星期(含)以內執行更新病毒碼的動作。

9. 請依本校 GCB 規範導入政府組態基準(GCB：Government Configuration Baseline)。
參考網址：https://www.nccst.nat.gov.tw/GCB

10. 將「網際網路時間設定」伺服器欄位設為 ：140.118.31.199，校正伺服器及

防火牆系統日期時間。

11. 定期(建議每天或每周)審視伺服器內部事件紀錄及防火牆的 Log 紀錄，若有發現異常，應立即採取防範措施。

12. 若有不提供服務的時段(下班、假日、連續長假等)，請關機!!!

13. 因任務結束、計畫結束、其他原因，伺服器不再提供服務時，請關機；並移除網路線及電源。

14. 定期將伺服器及防火牆狀況告知主管或指導教授。若伺服器管理者要離職或畢業，請務必將伺服器及防火牆之帳號、密碼、文件、相關資料移交給主管或指導教授指派之同仁或同學；受指派的同仁或同學必須確實了解相關交接的內容。

15. 使用適當的網路工具軟體，不定期的監看網路進出 IP 是否正常及每天網路進出流量，發現異常需立即通知主管或指導教授。

16. 至少每半年進行一次伺服器弱點掃描；並針對掃描結果採取相關因應措施。

17. 若有關自設伺服器資訊安全的相關問題，請向電子計算機中心洽詢。

18. 本規範經「資訊安全委員會」審議通過後施行，修正時亦同。