國立清華大學 對外網路服務管理規則(草稿)

中華民國115年X月X日資安管理委員會115學年度第一次會議通過

第一條　為強化本校對外網路服務管理與安全控管，降低常見資安風險，並確保符合法規與稽核要求，特訂定此管理規則。

第二條　依據資通安全管理法(以下簡稱資安法)及資通安全事件通報及應變辦法、資通安全責任等級分級辦法、「國立大專校院資通安全維護作業指引」、「臺灣學術網路管理規範」第七條第(六)項辦理。

第三條　本規則適用於本校所有提供對外服務之資訊設備與系統。視法規或稽核需求，得逐步擴大至其他協定與設備。

第四條　適用範圍之資訊設備辦理"資訊設備盤點"及"網路應用服務管理"。

第五條　以使用 HTTP/HTTPS 協定並對外提供服務之資訊設備為第一階段盤點目標，後續得依需求擴大範圍。盤點程序如下：

一、系統管理者須於本校「開放網站服務申請表單」完成登記（含系統負責單位、系統名稱、對外 IP、服務協定、管理聯絡人等必要欄位）。

二、單位網管確認申請內容（包含 IP 與系統資訊）後回覆計通中心。

三、計通中心在確認後，將該對外服務 IP 加入管制排除清單，並列入定期檢視名單。

第六條　盤點資料由計通中心彙整並保存，並配合資安稽核與法規查核需求提供相關紀錄。

第七條　為確保校園網路安全，計通中心將透過第七層防火牆功能對下列網路應用協定予以管制（阻斷），並提供替代方案與使用建議：

一、禁用校外往校內 HTTP 服務的連線。

- 風險：HTTP 資料以明文傳輸，易遭竊聽或中間人攻擊。
- 建議：申請 SSL/TLS 憑證，設定強制 HTTPS 轉導，實施 HSTS 以防止降級攻擊。

二、禁用校外往校內 FTP 服務的連線。

- 風險：FTP 明文傳輸，易遭竊聽或中間人攻擊。
- 建議：改用 SFTP 或 FTPS，停用匿名登入，採強密碼策略、登入限制與日誌監控。

三、全面禁用校外往校內 TELNET 連線。

- 風險：TELNET 明文傳輸，易遭竊聽或中間人攻擊。
- 建議：改用 SSH，採用強密碼或金鑰驗證、登入限制與日誌監控。

四、考量下列網路應用服務主要用於區域網路環境，且通常無須對校外網路開放，故預設禁用這些服務的對外連線，以強化網路安全：

- 印表機服務：Print-service (Port:9100)、IPP (Port:631)
- UPnP 協定：SLP (Port:427)、SSDP (Port:1900)
- 網路芳鄰：NetBIOS-* (Port:137-139)、SMBv* (Port:445)

第八條　若設備因特殊需求確需使用受管制服務之對外連線，系統管理者或負責單位應以電子郵件向計通中心提出申請，內容應包含：設備IP、業務必要性說明、可行替代方案檢視結果、預期使用時段與風險緩解措施。計通中心審查後，於確認無其他可行方案且風險可被接受時，得將該設備 IP 暫時或條件性加入管制排除清單，並訂定必要之監控與稽核條件。所有例外核准案應記錄於例外登記表，並列入定期覆核。

第九條　例外核准之設備若發生資安事件或違反核准條件，計通中心得撤銷例外並回復管制。

第十條　規則變更或重大例外應由計通中心提出，並經資安暨個資管理委員會核定。

第十一條　本規則如有未盡事宜，得依相關法規或上級機關指示辦理。本規則自公告施行日起生效。