大 仁 科 技 大 學
Tajen University

管 制 文 件 訂 修 廢 履 歷 表

文件編號	資訊-程序-32	文件名稱	防火牆管理程序書
使用部門	圖書資訊館	機密等級	普通

版次	頁數	文件修訂摘要	實施日期
A.0	5	初版	99/05/24
B.0	5	修改資訊-程序-30-01 防火牆通訊埠申請單，增加指導老師簽章。	100/06/01

訂修廢者	單位主管	資訊安全長

※管制文件不得擅自塗改及做記號並禁止影印。

1.目的

為促使本校資訊機房防火牆於安裝建置、管理與維護之安全指導有一明確之規範，以有效強化防火牆之安全角色，特制定本程序書。

2.適用範圍

凡資訊機房防火牆之管理，均適用本程序書。

3.參考文件

3.1 資訊-程序-13 帳號密碼及存取控制管理程序書

3.2 資訊-程序-23 資訊安全事件通報及危機處理管理程序書

3.3 資訊-程序-08 矯正及預防管理程序書

4.名詞定義

4.1 ACL

4.1.1 防火牆規則正面表列：依允許進入的方式作存取控制，其內定設定為禁止。

4.1.2 防火牆規則負面表列：依禁止進入的方式作存取控制，其內定設定為開放。

5.作業內容

5.1 防火牆管理流程圖

流程	權責	相關文件
提出防火牆服務需求	圖書資訊館	
設定防火牆	圖書資訊館	防火牆通訊埠申請單
設定安全管理規定	圖書資訊館	資訊機房檢查表
使用及維護	全校各單位	防火牆通訊埠申請單
查核（異常／正常）	圖書資訊館	資訊機房檢查表
異常處理	圖書資訊館	
記錄保存	圖書資訊館	

5.2 提出防火牆服務需求

為避免來自網際網路外部的入侵攻擊事件,降低被非授權的使用者或駭客入侵的機會,確保本校各項資訊系統能持續運作及提供穩定的服務,故需架設防火牆啟動安全防禦機制,以降低威脅及風險所造成的營運衝擊。

5.3 設定防火牆系統

本校防火牆系統之設定、維護及更新,由圖書資訊館負責規劃,並呈送圖書資訊館數位學習中心主任審核。

5.4 設定防火牆安全管理規定

5.4.1 防火牆管理原則

5.4.1.1 內部員工皆需透過適當設置之防火牆連接網際網路。

5.4.1.2 提供外部存取服務之主機,為降低暴露之風險,得將此類主機群建置於獨立網段區。

5.4.1.3 來自於網際網路之外部連線,除特殊限制因素外,僅允許連接至經申請核可的網站主機,降低內部網路遭受外部入侵之風險。

5.4.1.4 自內部網路對網際網路之任何連線與存取,應以業務需求不同為主要考量,分別給予適當的限制。一般使用者端除特殊需求者外,應適當限制其可連外之服務通訊埠,以杜絕內部主機嘗試入侵位於網際網路之主機。

5.4.2 防火牆過濾規則設定管理

5.4.2.1 除由指定 IP 及特定的連接埠登入管理外,應限制來自任何網路對防火牆管理的連線,並以此作為防火牆之基本過濾原則。

5.4.2.2 應避免以過大範圍之群組設定來源或目標位址和協定。

5.4.2.3 優先考慮使用正面表列,並應於規則最後設置拒絕全部服務的規則(Implicit Denied All),以預防因前述規則的

疏漏，導致來自網際網路之入侵與非法連線，進而產生防火牆於網路防護上之漏洞與風險。

5.4.2.4 防火牆於建置完成後，需每年定期檢視並修改或移除相關不適用之規則。

5.4.2.5 為避免邏輯上重複與繁瑣之過濾原則，導致防火牆效能低落以及負載過重，需詳細審查與檢視過濾規則，並考慮效能以及邏輯重複問題。

5.4.3 防火牆規則新增及異動(刪除、修改)管理

5.4.3.1 對校外網路服務新增或異動時，申請人應先填寫「資訊-程序-32-01 防火牆通訊埠申請單」，提出對校外網路存取使用與異動需求，經權責主管核可後方可執行。

5.4.4 防火牆備份與修正管理

5.4.4.1 由系統管理者定期或於防火牆變更時，進行防火牆資料、規則與設定之備份作業，並保存至少三個月以上。

5.4.4.2 系統管理者發現有新的修正程式發佈時，在不影響正常營運的前提下，經原廠工程師確認無誤後，更新防火牆修正程式。若老舊系統無法提供此功能，待版本升級或更新系統時改善。

5.4.5 防火牆帳號管理

5.4.5.1 防火牆管理員帳號、權限除因代理人制度外，應限制及控管帳號保管人之數目，以不超過 3 人(含)為限。

5.4.5.2 防火牆系統管理員帳號應遵循「資訊-程序-13 帳號密碼及存取控制管理程序書」之規定進行密碼管理，定期變更密碼，並保有適當密碼強度。

5.5 使用及維護

5.5.1 防火牆的使用與管理規定，則依據本程序書 5.4 設定防火牆

安全管理規定之章節辦理。

5.6 查核

5.6.1 圖書資訊館執行資訊機房例行檢查時,檢視防火牆是否正常運作，並定期由防火牆系統管理者將檢查結果記載於「資訊-程序-20-03 資訊機房檢查表」。

5.6.2 防火牆發現異常狀況，應即時通知系統管理者、權責主管及相關單位，並立即執行異常處理作業。

5.7 異常處理

5.7.1 防火牆發生異常狀況，先檢視日誌紀錄並作故障排除，無法及時處理解決時，應依據「資訊-程序-23 資訊安全事件通報及危機處理管理程序書」進行事件通報與緊急處理。

5.7.2 異常狀況依「資訊-程序-23 資訊安全事件通報及危機處理管理程序書」緊急處理完畢後，需依據「資訊-程序-08 矯正及預防管理程序書」之規定執行矯正措施，進行問題矯正，避免異常情況再度發生。

6.附件

6.1 資訊-程序-20-03 資訊機房檢查表

6.2 資訊-程序-32-01 防火牆通訊埠申請單。