電算中心資訊安全與防駭作法

一、一般性防範：

1. 依循 ISO27001 防範綱要，實作各項資訊安全要項，並固定每年聘請認證公司稽核相關做法，以落實資訊安的具體防範作業。

2. 重要資料定期進行備份。

3. 配合教育部不定期舉辦本校社交工程演練與相關教育訓練。

二、具體性防範：

1. 網路面

防範問題	解決方式
防制駭客掃描服務之弱點	各主機只開啟需要提供服務的 port
防制駭客跳板攻擊	中心主機統一放置於 server foundry
防治木馬程式與 IP 盜用	紀錄各 user 的目的與流量
防制駭客竊聽、連線劫持	遠端桌面等危險 port 只針對特定 IP 開放

2. 系統開發面

防範問題	解決方式

防止注入式(Injection)攻擊	欄位傳送後須經過字串過濾程序
防止注入式(Injection)攻擊	在使用者輸入相關頁面不使用字串聯結方式組合 SQL 指令
身分驗證功能缺失	除登入、公告、關於等首頁相關頁面外，應經過 session 檢查才可放行
不安全的參數傳輸	減少使用 get 方式傳遞參數資料，改用 post 方式
防止未授權的入侵行動	全面啟動輸入驗證碼機制與錯誤登入 3 次以後暫停使用網站 10 分鐘之機制
防止未授權的入侵行動	資料庫不使用最高權限帳號 sa 連線
防止未授權的入侵行動	避免開放的資料庫帳號權限過大
防止跨網站腳本攻擊	所有欄位設定可輸入的最大長度
未來開發系統新增做法	
防止遭竄改與紀錄追查	老師或學生上繳資料之後應發送確認的電子郵件，防範資料庫遭竄改

防止遭竄改與紀錄追查	對於重要資料(個資、成績、金額)啟動紀錄機制
防止遭竄改與紀錄追查	資料表每筆紀錄應增加新增與修改日期 2 欄位

3.伺服器面

防範問題	解決方式
防範字典式攻擊	啟用密碼需符合複雜度規定
防範字典式攻擊	啟用帳號登入紀錄
減少駭客攻擊的目標	關閉不需要之伺服器服務
防範惡意程式攻擊	關閉外接裝置與 CDROM、USB 的自動執行
修補系統弱點	定期進行必要之軟體與作業系統更新
減少駭客盜用身分進行攻擊	刪除(停用)過時及不必要之帳號
防範駭客植入有害程式	檢查網頁伺服器針對目錄的寫入權限設定是否合理

三、中長期精進作法：

1. 加強工具與教育訓練

2. 建置 Web 應用程式防火牆

3. 使用工具進行滲透測試

4. 規劃資訊安全知識庫分享經驗與成果