淡江大學資訊處電腦網路資安紀錄管理要點

99.9.24 資訊處 99 學年度第 1 學期第 1 次業務會議通過
100.9.23 資訊處 100 學年度第 1 學期第 1 次業務會議修正通過

一、為規範資訊處電腦網路資安使用紀錄(以下簡稱資安紀錄)之管理，以為各電腦伺服器與網路紀錄、管理資安紀錄之準則，特訂定本要點。

二、資安紀錄範圍

資安紀錄應包含資安軟體(Security Software)、作業系統(Operating System)及應用軟體(Application Software)等所產生之資安相關事件。

(一)資安軟體類：

1、反惡意軟體(Antimalware)：包含反惡意(Antimalware)、反毒軟體(AntiVirus)之標準紀錄、執行掃描及病毒碼更新時間等。

2、入侵偵測及防禦系統(Intrusion Detect and Intrusion Prevention)：包含系統產生之資安紀錄、系統更新時間等。

3、遠端存取軟體(Remote Access Software)：包含登入成功、失敗、資料存取量。

4、網頁代理(Web Proxies)：應記錄伺服器及客戶端所有網址(URL)通聯紀錄。

5、認證伺服系統(Authentication Servers)：包含目錄伺服器及單一認證伺服器，應記錄所有登入紀錄，如使用者、來源位址、成功、失敗、時間等。

6、路由器(Routers)：如來源及目的位址、存取紀錄等。

7、防火牆(Firewalls)：如違犯防火牆政策之來源及目的位址、存取紀錄等。

(二)作業系統類：

1、系統事件(System Events)：如作業系統啟動(Startup)時間、關閉(Shutdown)時間、服務啟動關閉時間、系統失敗(Failure)紀錄及其他重要系統狀態(Status)與錯誤(Error)事件。

2、稽核紀錄(Audit Records)：如使用者認證、帳號新增、刪除紀錄、使用特權(Privilege)帳號等不論成功或失敗之紀錄。

(三)應用軟體類：

1、客戶端請求(Client Requests)與伺服器端回應(Server Responses)：如網頁伺服器必須記錄請求網址(URL)及提供之回

應，資料庫應用伺服器必須記錄使用者存取之紀錄，其他類型伺服器資安相關紀錄。

2、帳號資訊(Account Information)：如帳號之新增、刪除紀錄，使用特權帳號指令紀錄，其他可辨識之資安相關紀錄。

3、統計使用資訊(Usage Information)：如交易量(Number of Transaction)、交易大小(Size)等對資訊安全監控有幫助之資訊。

4、重要操作行為(Significant Operational Action)：如應用軟體啟始時間、關閉時間、系統失敗(Failure)及組態(Configuration)變更紀錄。

三、資安紀錄儲存

伺服器、應用軟體或網路設備等軟、硬體管理者應建置獨立資安紀錄儲存空間，並依類型設定資安紀錄儲存循環日期與周期，除當前紀錄外，不得存放於產生紀錄之本機，紀錄儲存時間以6個月以上為原則。

四、資安紀錄管理

資安紀錄管理者須訂定安全規則限制其存取，並依紀錄之重要性決定備份之需求，原則以一份備份為原則。紀錄資訊檢索以使用者要求、資安事件處理或系統必要之處理(如統計)為原則，除本校「淡江大學網路使用管理辦法」中羅列事項外，不得將紀錄流出、損毀、竄改或私下運用處理，違者經資訊處業務會議決議後依校規處理。

五、本要點經資訊處業務會議通過，報請校長核定後，自公布日實施；修正時亦同。