東方設計學院
資訊網路或硬體相關緊急應變處理程序

九十七年四月二日圖資委員會議通過

九十九年九月二十九日圖資委員會議修訂通過

一、目的

針對違反資安規範，可能造成重大影響者，得於事發或跡象產生時之第一時間內立即處理，以降低災情或防範於未然。

二、對象

本校資訊設備管理人員及其相關人員。

三、需求

所謂緊急處理程序異於一般之作業程序，為控制災情持續擴大，得應用非常措施。如以網路運作而言，為免全面癱瘓得將某一部份之網路設備停機等，

針對各種突發狀況訂定緊急處理程序：

- 網路運作
- 大規模感染病毒
- 火警
- 地震
- 實體環境入侵事件

四、程序

偵測

針對緊急處理程序所設定之偵測點之及啟動條件

通報

針對緊急處理程序所設定之通報規則，通報負責人作進一步的判斷，或處理

判斷

負責人判斷目前狀況決定是否進一步處理及處理方式

處理

針對緊急處理程序所設定之程序處理

優先順序

訂定緊急處理時之優先順序，以保護核心系統

記錄

從偵測開始之每個步驟皆需記錄，

警戒

狀況並不明顯及不會造成災害，或處理後的後續監控

檢討與改善

針對已發生之事件處理及偵測之記錄進行檢討，以期改善處理程序或改善預防措施。除了各子程序文件註明外，須於資訊安全委員會定期會議中報告。若事關重大，得由資訊安全長召開「資訊安全委員會臨時會議」進行檢討。

狀況演練

定期針對狀況進行演練，以增進處理之熟練度及時效，並找出緊急處理程序之盲點。

演練計劃擬定需考量下列項目：

- 演練時間
- 參加人員及任務編組
- 訊息發佈
- 設備及工具
- 狀況
- 真實場景或模擬（測試）場景
- 記錄
- 檢討

五、記錄

緊急應變處理程序記錄表

六、參考文件

緊急應變處理程序－網路運作

緊急應變處理程序－機房火警

七、本程序經圖資委員會議通過後實行，修正時亦同。