國 立 臺 灣 海 洋 大 學

文件類別	作業程序	編號	圖-網-09	頁次	1/8
文件名稱	資訊安全事件管理程序	生效日期	106.08.07	版次	1.0
單位	圖書暨資訊處校園網路組	承辦人	梁滌宏	分機	2113

1. 目的

建立快速、有效、有秩序的資訊安全事件管理流程，以降低或消除可能之資訊安全事件所帶來的衝擊與傷害，並強化資訊安全事件處理能力，從中吸取經驗，據以防範未來可能再發生的資訊安全事件。

2. 適用範圍

適用於本校各單位。

3. 定義

3.1 資訊安全事件

任何可能會侵害資訊資產價值、影響業務正常運作、威脅或破壞資訊安全之事件、狀態或訊息。

3.2 資訊安全長

本程序「資訊安全長」由「資訊安全暨個人資料保護委員會」主席擔任。

4. 權責

4.1 全體同仁

4.1.1 了解資訊安全事件之通報程序。

4.1.2 對於已觀察到或懷疑可能發生的資訊安全事件，必須儘速通報校園網路組。

4.2 校園網路組

4.2.1 接受全體同仁已觀察到或懷疑可能發生的資訊安全事件回報。

4.2.2 判定資訊安全事件種類、等級、影響範圍、所需資源。

4.2.3 判定資安事件是否需要通報，是否需要外力支援。

4.2.4 評估資安事件處理所需時間，是否可能及時完成。

4.2.5 判定資訊安全事件是否需要執行業務持續運作計畫。

4.2.6 協助資安事件應變與處理作業。

4.2.7 資安事件協調、任務管制、與進度追蹤。

4.2.8 指派相關人員回應此事件。

4.2.9 執行政府機關資安事件通報作業，並於事件結束後回覆結案。

4.2.10 彙整資訊安全事件之風險等級，以採取相對應措施。

4.2.11 彙整資訊安全事件資訊予以統計分析，並將資訊提供給資訊安全長。

4.3 業務負責人／管理員

4.3.1 依授權執行損害管制作業。

4.3.2 執行資安事件應變與處理作業。

4.3.3 對負責之範圍執行復原作業。

4.4 資訊安全長

4.4.1 授權執行損害管制作業。

4.4.2 利用資訊安全事件資訊定期或不定期修訂資訊安全管理系統。

5. 作業說明

5.1 執行時機

5.1.1 資訊安全事件發生時。

5.1.2 當發生符合威脅與脆弱點所列之任何現象，或發生不在清單中但可能危害資訊資產安全之現象時。

5.1.3 校園網路組統計分析資訊安全事件資訊時。

5.1.4 資訊安全長改善資訊安全管理系統時。

5.2 資訊安全事件管理流程

程序	說明	標準	負責人
開始			
發生資訊安全或疑似資訊安全事件	當發生疑似威脅與脆弱點所列之各種現象，或發生不在列示中但可能危害資訊資產安全之現象時		全體同仁
回報資訊安全事件	儘速通報校園網路組		全體同仁
判斷資安事件類別與嚴重性	● 判定事件之等級、類別，並填寫「資安事件通報單」 ● 判定事件影響範圍，以及範圍內之資訊資產負責人 ● 事件發生後，判定是否需要外力支援		校園網路組

文件類別	作業程序	編號	圖-網-09	頁次	3/8
文件名稱	資訊安全事件管理程序	生效日期	106.08.07	版次	1.0

通報資訊安全事件	● 依據事件種類與等級，決定事件內部通報對象 ● 如資安事件屬於需要外部通報之類別，依照資安事件通報等級，於一定的時間內向通報網站辦理通報作業 ● 如需外力支援，向通報應變組請求支援	行政院及所屬各機關資安事件通報應變作業規範	校園網路組
是否需要執行業務持續運作（是）	依據事件種類與等級，決定事件的處理方式		校園網路組
否 依矯正與預防程序 是： 否：	● 校園網路組會同技術顧問小組、相關資產負責人，依照「矯正與預防措施管理程序」進行事件處理 ● 如未能及時完成修復，則進行損害管制，並執行業務持續運作計畫	矯正與預防措施管理程序 行政院及所屬各機關資安事件通報應變作業規範	校園網路組
執行業務持續運作計畫	依照「業務持續運作管理程序」進行緊急應變	業務持續運作管理程序	資訊安全長
通報結案	資安事件處理完畢後，向通報網站進行「通報結案」作業	行政院及所屬各機關資安事件通報應變作業規範	校園網路組
整理/分析資訊安全事件	校園網路組定期將資訊安全事件處理紀錄彙整與統計分析報告，交予資安代表。		資安代表
結束			

5.3 資訊安全事件管理說明

5.3.1 資訊安全事件類別

資安事件依發生之位置及區域分為三大類：

5.3.1.1 系統類資安事件

發生在網路環境、主機系統、個人電腦的資安事件，軟體、硬體與資訊紀錄相關者均屬之。例如系統故障、網路斷線、硬碟損毀、程式錯誤、機密檔案

外洩等。

5.3.1.2 實體環境類資安事件

發生於實體環境內之資安事件，與實體環境相關者均屬之。例如門禁故障、門窗未關、過載跳電、闖空門、火災等。

5.3.1.3 人員類資安事件

與人員相關之資安事件，例如人員意外事故、商業間諜混入偷竊、罷工暴動、作業疏失等。

5.3.2 資訊安全事件等級

將資訊安全事件分為五個等級，說明於後：

5.3.2.1 『4』級：影響中心安全、員工生命財產，或影響公共安全、社會秩序、人民生命財產。例如：

5.3.2.1.1 法定傳染病肆虐，例如 SARS、禽流感等。

5.3.2.1.2 天然災害，例如地震、水災、颱風、土石流等。

5.3.2.1.3 環境災害，例如火災、爆炸、建築物倒塌等。

5.3.2.1.4 恐怖攻擊，例如武裝脅持人質、炸彈恐嚇等。

5.3.2.2 『3』級：系統全面停頓，業務長時間無法運作，且無法短時間恢復。例如：

5.3.2.2.1 辦公場所受損。

5.3.2.2.2 電力設備受損。

5.3.2.2.3 電信通訊受損。

5.3.2.2.4 主機系統/網路設備受損。

5.3.2.2.5 關鍵人員遭遇重大變故。

5.3.2.3 『2』級：系統短暫停頓，業務中斷，例如電力，電信設備、辦公場所， 網路設備、主機系統中斷造成業務中斷之事件。

5.3.2.3.1 區域網路遭受侵入、破壞、竄改、刪除或未經授權之存取事故。

5.3.2.3.2 惡意程式大規模感染破壞。

5.3.2.3.3 網路設備故障。

5.3.2.3.4 電腦硬體設備故障。

5.3.2.3.5 系統故障(Crash)。

5.3.2.3.6 無預警斷電。

5.3.2.4 『1』級：系統效能降低，業務受到影響，可立即修復。例如：

5.3.2.4.1 資訊系統處理錯誤或不當變更。

5.3.2.4.2 使用者錯誤。

5.3.2.4.3 惡意程式碼肆虐，例如病毒或後門程式。

5.3.2.4.4 網路流量滿載。

5.3.2.4.5 軟體運作失效：開發系統錯誤、功能錯誤。

5.3.2.4.6 電腦當機。

5.3.2.4.7 辦公事務設備故障。

5.3.2.4.8 失竊及門禁警報。

5.3.2.4.9 電力瞬斷，電壓不穩。

5.3.2.5 『0』級：疑似或可能發生，但尚未造成任何影響。例如：

5.3.2.5.1 系統發現新漏洞，且未有修補程式。

5.3.2.5.2 資訊交換的威脅，例如使用 HUB 可能會被竊聽。

5.3.2.5.3 遠端作業的弱點，例如缺乏適切資安訓練的遠端工作者。

5.3.2.5.4 系統監控異常警示，例如 CPU 溫度過高，磁碟空間不足。

5.3.2.5.5 發現不知名人士於辦公區內獨自活動。

5.3.2.5.6 機密級以上文件、資訊紀錄未妥善保存。

5.3.2.5.7 機房或機櫃溫度過高。

5.3.2.5.8 防毒軟體病毒碼過期未更新。

5.3.3 需進行外部通報之資安事件

當資安事件等級為「1」級以上，並屬於以下類別，將進行外部通報：

5.3.3.1 電腦當機及中斷服務

因負荷太重、軟體異常、或其他因素導致電腦當機及服務中斷。

5.3.3.2 惡意的程式碼

指的是因不良意圖而設計，會影響主機的程式，通常指的是：

5.3.3.2.1 電腦病毒(Virus)。

5.3.3.2.2 蠕蟲(Worm)。

5.3.3.2.3 特洛伊木馬(Trojan)。

5.3.3.2.4 邏輯炸彈(Logic bomb)。

5.3.3.2.5 間諜軟體(Spyware)。

5.3.3.2.6 惡意的可攜性程式(Mobile code)，例如巨集病毒。

5.3.3.2.7 廣告軟體(Ad-ware)。

5.3.3.2.8 其他會干擾使用者作業之程式

5.3.3.3 阻斷服務

攻擊者利用消耗資源的方式，阻止或降低合法使用者使用其網路、系統、應用程式等服務。

5.3.3.4 業務資料不完整，或是資料不正確導致的作業錯誤

使用者使用不完整或不正確的資料運行資訊系統所導致的作業錯誤。

5.3.3.5 機密性資料遭侵犯

未經授權取得機密性資料的讀取、修改、及刪除等存取權限。

5.3.3.6 資訊系統的不當使用

不符合資訊系統作業流程之行為。如在資訊系統的主機上安裝、執行、或備份軟體程式與文件。

5.3.4 資安事件通報

資安事件通報分為循行政程序上報之內部通報，以及向通報網站進行通報之外部通報：

5.3.4.1 內部通報

5.3.4.1.1 判別事件種類及嚴重性後，將事件狀況、應變措施等相關資訊向資訊安全長報告。

5.3.4.1.2 聯絡相關業務負責人及相關系統管理員，並視事件種類及等級，聯絡校園網路組協助。

5.3.4.1.3 視事件範圍、種類及等級，聯絡相關維護廠商或委外管理廠商協助應變處理與復原。

5.3.4.2 外部通報

5.3.4.2.1 依據「教育機構資安通報平台」之要求，事件級別為0、1、2級之資安事件於72小時內通報並結案，事件級別為3、4級之資安事件於36小時內通報並結案。

5.3.4.2.2 於資安事件處理完畢，系統恢復正常運作，須至通報網站進行「通報結案」作業。

5.3.5 資訊安全事件處理方式

依據資安事件等級，判斷事件的處理方式：

5.3.5.1 **2** 級(含)以下：依本程序以及「矯正與預防程序」處理。

5.3.5.2 **3** 級(含)以上：經評估業務中斷時間將超過資安事件處理時限，或超過可接受中斷時限，則依「業務持續運作管理程序」處理。

5.3.6 請求外力支援

5.3.6.1 當校園網路組準備進行事件處理時，發現如下情況，可由資訊安全長判定請求外力支援：

5.3.6.1.1 人力不足

5.3.6.1.2 技術能力不足

5.3.6.1.3 未處理過，也不會處理此類資安事件

5.3.6.1.4 效率不足或不熟悉，無法及時將資安事件處理完畢

5.3.6.1.5 處理資安事件需使用的專業軟硬體設備不足

5.3.6.2 可能的外力支援管道：

5.3.6.2.1 國家資通安全會報技術服務中心(ICST)：
http://www.icst.org.tw

5.3.6.2.2 台灣電腦網路危機處理暨協調中心(TWCERT/CC)：
http://www.cert.org.tw

5.3.6.2.3 政府網路危機處理中心(GSN-CERT)：
http://www.gsn-cert.nat.gov.tw/

5.3.6.2.4 專業資安顧問

5.3.6.2.5 資安設備與服務廠商

5.3.6.2.6 資安相關專家學者

5.3.6.2.7 其他政府機關資安負責人員

5.3.7 資訊安全事件通報應變作業實施原則

5.3.7.1 若於非工作時間(例假日)發現資安事件，仍應依循程序通報。

5.3.7.2 資安事件發生時，應保持電腦稽核軌跡，避免重新啟動或刪除資料，造成電腦稽核軌跡(audit trail)及系統紀錄資訊毀損，影響日後證據蒐集。

5.3.7.3 識別事件所影響之資源與系統，供復原作業時參考。

5.3.7.4 數位證據蒐集完畢後，可執行損害管制防範事件繼續擴大。

5.3.7.5 進行損害管制時，系統管理人員應依授權實施網路中斷、系統關閉或其他處理措施以控制資安事件影響範圍之擴大。

5.3.8 資訊安全事件處理作業實施原則

5.3.8.1 資安事件處理作業依照「矯正與預防措施管理程序」執行，並對資安事件受影響範圍依照「矯正-復原-檢討」的順序處理。

5.3.8.2 處理作業時間應於指定時間完成，作業內容應記錄備查，並經由權責人員審視確認。

5.3.8.3 資安事件處理前，應先備份數位證據（例如系統紀錄、稽核軌跡），確實做好證據保存工作。

5.3.8.4 應鑑別資安事件發生根本原因，以利事件處理作業，如為外來攻擊事件，應適當鑑別攻擊來源。

5.3.8.5 系統漏洞或脆弱點，應透過網站資訊、技術支援單位（如廠商、技服中心等）查詢獲得解決方案，並執行修復動作。如暫時無解決方案，應先停用或封鎖脆弱點之相關功能或元件，避免脆弱點再度遭受利用。

5.3.8.6 若無法鑑別入侵系統之所有惡意行為（病毒感染、駭客入侵、木馬後門等），無法確保完全清除並排除惡意程式或行為造成的影響，應嘗試重建一個乾淨之系統，避免惡意程式持續影響系統運作。

5.3.8.7 受影響之範圍經測試確認已恢復正常，並完成安全控制項目，確認脆弱點無法再被利用，系統才可上線運作，並視實際需求觀察系統運行一段時間，以確認系統持續正常運作。

5.3.9 資訊安全事件彙總與分析

校園網路組每月收集彙整資訊安全事件，統計資安事件之數量、類別、等級、影響範圍、發生部門/系統等，並分析其中的異常變化，以便掌握矯正及預防措施之有效性，發掘資訊安全管理系統可能的脆弱點。常見的交叉分析類別如下：

5.3.9.1 資安事件類別與數量

5.3.9.2 資安事件等級與數量

5.3.9.3 資安事件發生部門/系統與數量

5.3.9.4 資安事件發生部門/系統與平均等級

5.3.9.5 資安事件影響範圍資產負責人與數量

6. 相關作業

略

7. 使用表單

7.1 資安事件通報單

國立臺灣海洋大學
資安事件通報單

□**通報單**
□**協助研判申請單**

一、發生資通安全之單位聯絡資料：					
單位名稱		E-MAIL			
聯絡人		電　話		傳　真	

二、資安事件通報事項：

1、事件發生時間：　年　月　日　時　分

2、主機(伺服器)資料：

◎IP 位址(IP Address)：

◎網域名稱(Domain name)：

◎主機(伺服器)廠牌、機型：

◎作業系統名稱、版本、序號：

◎網際網路資訊位址(Web URL)：

◎已裝置之安全機制：

3、資安事件資料：

事件類別：□『1』系統類；□『2』實體環境類；□『3』人員類

事件等級：□『4』級；□『3』級；□『2』級；□『1』級；□『0』級

◎事件說明：

◎可能影響範圍及損失評估：

◎應變措施：

三、期望支援項目：

四、解決辦法：

五、已解決時間：　年　月　日　時　分

申請單位		圖資處校園網路組	
承辦人	主管	承辦人	主管

備註：
一、「資安事件管理中心」緊急連絡電話:(02)2462-2192 轉 2113,傳真電話:(02)2463-1208
二、 安全事件等級列表

等級	說明
『4』	影響中心安全、員工生命財產，或影響公共安全、社會秩序、人民生命財產，例如： ● 法定傳染病肆虐，例如 SARS、禽流感等。 ● 天然災害，例如地震、水災、颱風、土石流等。 ● 環境災害，例如火災、爆炸、建築物倒塌等。 ● 恐怖攻擊，例如武裝脅持人質、炸彈恐嚇等。
『3』	系統全面停頓，業務長時間無法運作，且無法短時間恢復。例如： ● 辦公場所受損。 ● 電力設備受損。 ● 電信通訊受損。 ● 主機系統/網路設備受損。 ● 關鍵人員遭遇重大變故。
『2』	系統短暫停頓，業務中斷，例如電力，電信設備、辦公場所， 網路設備、主機系統中斷造成業務中斷之事件。 ● 區域網路遭受侵入、破壞、竄改、刪除或未經授權之存取事故。 ● 惡意程式大規模感染破壞。 ● 網路設備故障。 ● 電腦硬體設備故障。 ● 系統故障(Crash)。 ● 無預警斷電。
『1』	系統效能降低，業務受到影響，可立即修復。例如： ● 資訊系統處理錯誤或不當變更。 ● 使用者錯誤。 ● 惡意程式碼肆虐，例如病毒或後門程式。 ● 網路流量滿載。 ● 軟體運作失效：開發系統錯誤、功能錯誤。 ● 電腦當機。 ● 辦公事務設備故障。 ● 失竊及門禁警報。 ● 電力瞬斷，電壓不穩。
『0』	疑似或可能發生，但尚未造成任何影響。例如： ● 系統發現新漏洞，且未有修補程式。 ● 資訊交換的威脅，例如使用 HUB 可能會被竊聽。 ● 遠端作業的弱點，例如缺乏適切資安訓練的遠端工作者。 ● 系統監控異常警示，例如 CPU 溫度過高，磁碟空間不足。 ● 發現不知名人士於辦公區內獨自活動。 ● 機密級以上文件、資訊紀錄未妥善保存。 ● 機房或機櫃溫度過高。