國 立 臺 灣 海 洋 大 學

（首 頁）

文件類別	標準作業流程	編　號	圖-網-08	頁　次	1/3
文件名稱	資通安全事件 管理、通報處理流程	公布日期	111.07.20	版　次	1.1
單　位	圖書暨資訊處校園網路組	承 辦 人	梁滌宏	分　機	2113

1　目的與範圍

1.1　為遵照資通安全管理法第 14 條及本校「資通安全維護計畫」之規定，建立本校資通安全事件之通報及應變機制，以迅速有效獲知並處理事件，特制定「資通安全事件管理、通報處理流程」。

1.2　發生於本校之事件，系統、服務或網路狀態，經鑑別而顯示可能有違反資通安全政策或保護措施失效之狀態發生，影響資通系統機能運作，構成資通安全政策之威脅者。

2　參考文件（法規／依據）

2.1　全國性法規

2.1.1　資通安全事件通報及應變辦法

2.1.2　臺灣學術網路各級學校資通安全通報應變作業程序第三章第一條第六款

2.2　校內相關法規

2.2.1　國立臺灣海洋大學校園網路使用規範

3　權責單位

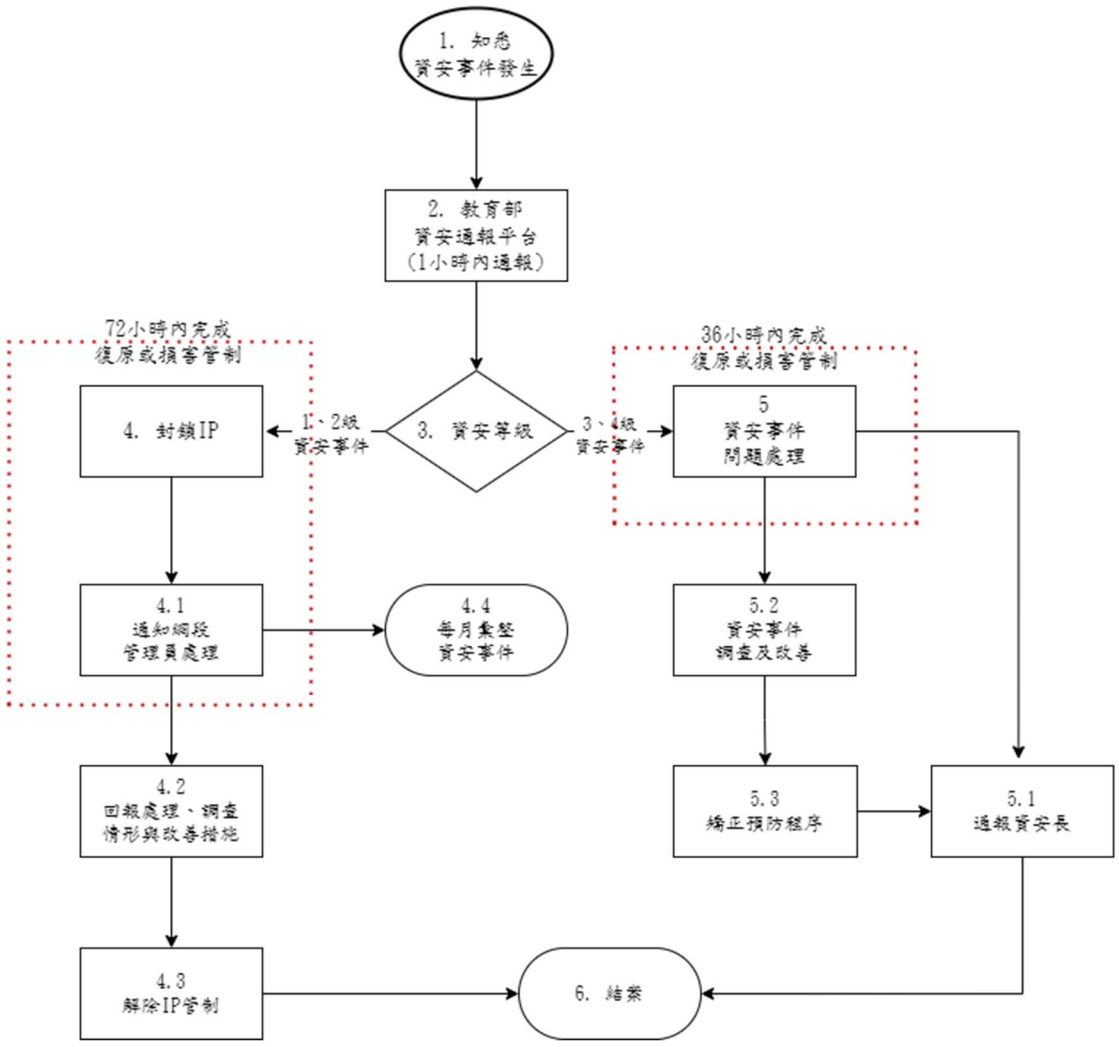
3.1　圖書暨資訊處校園網路組

4　對象

4.1 使用本校 IP 之各類資訊設備。

文件類別	標準作業流程	編　號	圖-網-08	頁　次	2/3
文件名稱	資通安全事件 管理、通報處理流程	公布日期	111.07.20	版　次	1.1

5　流程圖



文件類別	標準作業流程	編　號	圖-網-08	頁　次	3/3
文件名稱	資通安全事件 管理、通報處理流程	公布日期	111.07.20	版　次	1.1

6　作業內容（對應程流圖，敘明作業內容）

6.1 接獲本校所屬資訊設備發生資通安全事件時(以下簡稱資安事件)，開始進行本流程。

6.2 知悉資安事件時，應於1小時內至「教育機構資安通報平台」進行通報，並取得事件單編號。

通報網址：https://info.cert.tanet.edu.tw

6.3 判斷資安事件等級。

6.4 當資安等級為1、2級時，應於72小時內完成復原或損害管制。並在「不當使用公告平台系統」封鎖該資訊設備的IP，將事件單編號登入於系統原始案號。

6.4.1 系統自動發mail通知發生資安事件所屬資訊設備IP網段之管理者信箱。

6.4.2 網管人員回報內容需包含相關處理方式(如電腦重灌、移除病毒等)、調查原因(如作業系統受否更新、防毒防火牆是否有安裝、共用電腦還是個人使用、帳號權限有無控管、密碼強度與長度是否足夠等)、及改善措施(如要安裝防毒軟體、要定期Update、不任意下載不明非法軟體)。

6.4.3 確認回報內容均符合 6.4.2 之要求後，再於「不當使用公告系統」解除該設備的IP管制。

6.4.4 依據「臺灣學術網路各級學校資通安全通報應變作業程序」,每月彙整1、2級資安事件，並提報單位主管。

6.5 當資安等級為3、4級時，應於36小時內完成復原或損害管制。

6.5.1 通報資安長，讓資安長了解發生3、4級資安事件。

6.5.2 發生資安事件後，需進行事件調查、處理及改善報告，該報告應包含：

6.5.2.1 事件發生、完成損害控制或復原作業之時間。

6.5.2.2 事件影響之範圍及損害評估。

6.5.2.3 損害控制及復原作業之歷程。

6.5.2.4 事件調查及處理作業之歷程。

6.5.3 將調查過程中發現缺失與潛在之風險，依「I-02-05 矯正預防管理程序」提報資安長審核。

6.6 結案

7　附件（相關表單或文件）

7.1　I-02-05 矯正預防管理程序書

承辦人	二級單位主管	一級單位主管

國立臺灣海洋大學內部控制制度作業層級自行評估表

___年度

自行評估單位：圖資處校園網路組　　評估期間：　年　月　日至　年　月　日

作業類別(項目)：資通安全事件管理、通報處理流程

檢查重點	自行評估情形					控制措施
	落實	部分落實	未落實	不適用	其他	
一、作業程序說明表及作業流程圖之製作是否與規定相符						
二、內部控制制度是否有效設計及執行。						
三、知悉資安事件發生,於一小時內完成通報。						
四、每月彙整1、2級資安事件，並提報單位主管。						
五、發生 3、4 級資安事件需通知資安長						
六、發生 3、4 級資安事件後的調查、處理及改善報告應包含 6.5.2.1~6.5.2.4 所有事項。						

填表人：　　複核：　　單位主管：