

## 臺灣學術網路各級學校資通安全事件通報單 (人工通報流程)

### 一. 教育機構資通安全事件單人工通報流程

依臺灣學術網路各級學校資通安全通報應變作業程序，各連線單位發現資安事件後可先進行事件確認，經確認為資安事件後，須於 1 小時內，至教育機構資安通報應變網站 (<https://info.cert.tanet.edu.tw>) 通報登錄資安事件細節、影響等級及是否申請支援等資訊，並評估該事件是否影響其他連線單位運作。

如因網路或電力中斷等事由，致使無法上網填報資安事件，可先填具附件一教育機構資通安全事件單，以 TACERT 備用通報信箱或傳真方式送至臺灣學術網路危機處理中心(TACERT)，惟待網路連線恢復後，仍須至通報應變網站補登錄通報。

TACERT 備用通報信箱：TACERT-service@ids.mis.nsysu.edu.tw

諮詢專線：(07)5250211

傳真專線：(07)5251535

### 二. 學術網路 DDoS 攻擊流量清洗服務事件單人工通報流程

依據臺灣學術網路(TANet)分散式阻斷服務(DDoS)通報應變作業指引，當連線單位遭受分散式阻斷服務攻擊 (Distributed Denial of Service, DDoS) 時，連線單位可申請學術網路 DDoS 攻擊流量清洗服務並進行資安事件通報。

如因網路或電力中斷等事由，致使無法上網申請 DDoS 攻擊流量清洗服務事件單，可先填具附件二學術網路 DDoS 攻擊流量清洗服務申請單，以 TACERT 備用通報信箱或傳真方式送至臺灣學術網路危機處理中心(TACERT)，惟待網路連線恢復後，仍須至教育機構資安通報報表系統(<https://portal.cert.tanet.edu.tw/>)補申請 DDoS 攻擊流量清洗服務事件單。

TACERT 備用通報信箱：TACERT-service@ids.mis.nsysu.edu.tw

諮詢專線：(07)5250211

傳真專線：(07)5251535

## 附件 一．教育機構資通安全事件通報單

\*注意事項：「◎」為必填項目

◎ 填報時間：\_\_\_\_年\_\_\_\_月\_\_\_\_日\_\_\_\_時\_\_\_\_分

### STEP1. 請填寫事件相關基本資料

#### 一、發生資通安全事件之機關(機構)聯絡資料：

- ◎ 單位名稱：
- ◎ 通報人：
- ◎ 電話
- ◎ 傳真：
- ◎ 電子郵件信箱：

### STEP2. 事件發生時間

#### 二、事件發生時：

- ◎ 事件發生時間：\_\_\_\_年\_\_\_\_月\_\_\_\_日\_\_\_\_時\_\_\_\_分
- ◎ 確認(知悉)為資安事件時間：\_\_\_\_年\_\_\_\_月\_\_\_\_日\_\_\_\_時\_\_\_\_分

### STEP3. 設備資料

#### 三、設備資料事件發生時：

- ◎ IP 位置 (IP address)：
- ◎ 網際網路位置 (web-url)：
- ◎ 設備廠牌、機型：
- ◎ 作業系統 (名稱/版本)：
- ◎ 受駭應用軟體 (名稱/版本)：
- ◎ 已裝置之安全防护軟體：
  - 防毒軟體 (名稱/版本)：
  - 防火牆 (名稱/版本)：
  - IPS/IDS (名稱/版本)：
  - 其它 (名稱/版本)：
- ◎ 受駭設備類型：
  - ☐ 個人電腦
  - ☐ 伺服器
  - ☐ 大型主機
  - ☐ 網路通訊設備
  - ☐ SCADA(資料採集與監視系統)
  - ☐ 控制器(PLC、PAC)
  - ☐ 人機介面(HMI)

☐ 其他：

◎ 受害設備說明(150字內)：

◎ 損害類別說明：

☐ 可用性損害

☐ 資料外洩

☐ 資料竄改

☐ 硬體損害

☐ 金錢損失

☐ 其他：

◎ 攻擊手法：

☐ 社交工程

☐ 人為疏失

☐ 設定錯誤

☐ 設備異常/毀損

☐ 電力供應異常

☐ 作業系統/平台漏洞

☐ 弱密碼或密碼遭暴力破解

☐ 應用程式漏洞

☐ 網站設計不當

☐ 行動裝置不當使用

☐ 事件發生原因不明

☐ 其他：

◎ 調查說明(150字內)：

◎ 情資類型：

☐ 惡意內容

☐ 惡意程式

☐ 資料蒐集

☐ 入侵嘗試

☐ 入侵攻擊

☐ 阻斷服務

☐ 資訊內容安全

☐ 詐欺攻擊

☐ 系統弱點

☐ 其他：

#### STEP4. 資通安全事件：基本資料

##### 四、事件分類：

###### ◎ INT (入侵型態)：

- ☐ 系統被入侵
- ☐ 對外攻擊
- ☐ 針對性攻擊
- ☐ 散播惡意程式
- ☐ 中繼站
- ☐ 電子郵件社交工程攻擊
- ☐ 垃圾郵件(Spam)
- ☐ 命令與控制伺服器(C&C)
- ☐ 殭屍電腦(Bot)

###### ◎ DEF (網頁型態)

- ☐ 惡意網頁
- ☐ 惡意留言
- ☐ 網頁置換
- ☐ 釣魚網頁
- ☐ 資料外洩

###### ◎ FAC (設施問題)

- ☐ 設備故障/毀損
- ☐ 電力異常
- ☐ 網路服務中斷
- ☐ 設備遺失
- ☐ 阻斷服務

###### ◎ 破壞程度(文字勿超過200中文字)：

###### ◎ 事件與處置說明(文字勿超過200中文字)：

#### STEP5. 資通安全事件：影響等級說明

#### 五、資安事件判斷：

- 1、事件等級：取底下三個欄位中最高等級當成最後之事件等級
- 2、第3、4級事件係屬於重大資安事件，教育部各長官需親自督導進度
- 3、若有3、4級事件，請立刻電話告知您所屬的主管機關
- 4、如果您無法確定如何填寫時，請電話連絡您所屬的主管機關請求協助

◎ 請分別評估資安事件造成之機密性、完整性以及可用性衝擊：

\*資安事件影響等級為機密性、完整性及可用性衝擊最嚴重者(數字最大者)\*

##### (1). 機密性衝擊：(單選)

- ☐ 1級-非核心業務資訊遭輕微洩漏
- ☐ 2級-非核心業務資訊遭嚴重洩漏，或未涉及關鍵基礎設施維運之核心業務資訊遭輕微洩漏
- ☐ 3級-未涉及關鍵基礎設施維運之核心業務資訊遭嚴重洩漏，或一般公務機密、敏感資訊或涉及關鍵基礎設施維運之核心業務資訊遭輕微洩漏
- ☐ 4級-一般公務機密、敏感資訊或涉及關鍵基礎設施維運之核心業務資訊遭嚴重洩漏，或國家機密遭洩漏
- ☐ 無系統或設備受影響

##### (2). 完整性衝擊：(單選)

- ☐ 1級-非核心業務資訊或非核心資通系統遭輕微竄改
- ☐ 2級-非核心業務資訊或非核心資通系統遭嚴重竄改，或未涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭輕微竄改
- ☐ 3級-未涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭嚴重竄改，或一般公務機密、敏感資訊、涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭輕微竄改
- ☐ 4級-一般公務機密、敏感資訊、涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭嚴重竄改，或國家機密遭竄改
- ☐ 無系統或設備受影響

##### (3). 可用性衝擊：(單選)

- ☐ 1級-非核心業務之運作受影響或停頓，於可容忍中斷時間內回復正常運作，造成機關日常作業影響
- ☐ 2級-非核心業務之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作，或未涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，於可容忍中斷時間內回復正常運作

- ☐ 3級-未涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作，或涉及關鍵基礎設施維運之核心業務或核心資通系統之運作影響或停頓，於可容忍中斷時間內回復正常運作
- ☐ 4級-涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作
- ☐ 無系統或設備受影響

◎ 可能影響範圍及損失評估(文字勿超過200中文字)：

#### STEP6. 是否需要支援

六、是否需要支援：

- ☐ 是，期望支援方式：
  - ☐ 電話告知
  - ☐ Email 告知
- ☐ 否：通報單位自行解決

#### STEP7. 應變流程

七、應變流程：

◎ 緊急應變措施：

- ☐ 已中斷網路連線，待處理完成後再上線
- ☐ 已停止伺服器之服務，待處理完成後再上線
- ☐ 直接處理完成，解決辦法詳見【解決辦法】
- ☐ 其它

◎ 解決辦法(文字勿超過200中文字)：

◎ 完成損害控制時間：\_\_\_\_年\_\_\_\_月\_\_\_\_日\_\_\_\_時\_\_\_\_分

◎ 損害控制狀態：

- ☐ 是：完成損害控制
- ☐ 是：完成損害控制與復原

備註：1、2級事件簽核至單位主管，3、4級事件簽核至資通安全長。

**STEP8. 改善措施**

八、改善辦法：

◎ 改善辦法(文字勿超過200中文字)：

◎ 改善時間：\_\_\_\_年\_\_\_\_月\_\_\_\_日\_\_\_\_時\_\_\_\_分



## 附件二. 學術網路 DDoS 攻擊流量清洗服務事件單

| 學術網路 DDoS 攻擊流量清洗服務事件單                |                                 |
|--------------------------------------|---------------------------------|
| <b>STEP1. 請填寫事件相關基本資料</b>            |                                 |
| 發生資通安全事件之機關(機構)聯絡資料：                 |                                 |
| ◎ 單位名稱：                              | <input type="text"/>            |
| ◎ 通報人：                               | <input type="text"/>            |
| ◎ 電話：                                | <input type="text"/>            |
| 傳真：                                  | <input type="text"/>            |
| ◎ 電子郵件信箱：                            | <input type="text"/>            |
| <b>STEP2. 請填寫申請 DDoS 清洗服務的 IP 資訊</b> |                                 |
| ◎ 清洗 IP：                             | <input type="text"/>            |
| DNS IP：                              | <input type="text"/>            |
| ◎ 通訊協定：                              | <input type="text"/>            |
| ◎ 服務說明：                              | <input type="text"/> 例如：WEB、FTP |
| ◎ 通訊埠：                               | <input type="text"/> 例如：80      |
| ◎ 申請理由：                              | <input type="text"/>            |