臺灣學術網路各級學校資通安全事件通報單

學術網路所屬單位應至教育機構資安通報平台（https://info.cert.tanet.edu.tw）通報資安事件，若因故無法上網填報，可先填具本通報單以郵寄方式寄送至臺灣學術網路危機處理中心，惟待網路連線恢復後仍需上網補登通報。

諮詢專線：(07)5250211

郵寄地址：高雄市鼓山區蓮海路 70 號 臺灣學術網路危機處理中心

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

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)：

◎ 已裝置之安全防護軟體:

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):

STEP4. 資通安全事件：基本資料

四、事件分類：

◎ INT（入侵攻擊）：

- ☐ 系統被入侵(資訊設備遭惡意使用者入侵)
- ☐ 對外攻擊(對外部主機進行攻擊行為)
- ☐ 針對性攻擊(針對特定個人的資訊洩漏與身分盜取)
- ☐ 散播惡意程式(主機對外進行惡意程式散播)
- ☐ 中繼站(主機成駭客之中繼站，接收惡意程式連線)
- ☐ 電子郵件社交工程攻擊(帳號遭盜用對外發動社交工程攻擊)
- ☐ 垃圾郵件(Spam)(資訊設備從事 Spam Mail 散播行為)
- ☐ 命令與控制伺服器(C&C)(主機疑似為駭客之 Botnet C&C Server)
- ☐ 殭屍電腦(Bot)(資訊設備疑似成為駭客所控制之 Botnet 成員)
- ☐ 其它類型的入侵攻擊：

◎ DEF（網頁攻擊）

- ☐ 惡意網頁(網頁遭駭客置換或放置不當內容)
- ☐ 惡意留言(網頁遭駭客放上惡意留言)
- ☐ 網頁置換(網頁遭駭客置換)
- ☐ 釣魚網頁(主機遭駭客置入釣魚網頁)
- ☐ 個資外洩(主機遭個資外洩)
- ☐ 其它類型的網頁攻擊

◎ 破壞程度：

◎ 事件說明：

STEP5. 資通安全事件：影響等級說明

五、資安事件判斷：

◎ 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)

－機密性衝擊：(單選)

- ☐ 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(4 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(3 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(2 級)
- ☐ 非核心業務資訊遭輕微洩漏(1 級)

－完整性衝擊：(單選)

- ☐ 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(4 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(3 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(2 級)
- ☐ 非核心業務資訊或非核心資通系統遭輕微竄改(1 級)

－可用性衝擊：(單選)

- ☐ 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(4 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(3 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(2 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(1 級)

◎ 可能影響範圍及損失評估：

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：

◎ 解決時間：_____年____月____日____時____分

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。