國立臺灣大學資通安全事件報告單					
文件編號	NTU-IS2-15-F01	機密等級	限閱	版本	2.3

紀錄編號：_____ 填報時間：_____年_____月_____日

各單位因受外在因素所產生資通安全事件時通報事項：

1. 以下表單各欄位若為紅色◎標示，則為必填欄位。
2. 本表填寫完畢，請繳交至計算機及資訊網路中心 資安承辦人。

一、 ◎發生資通安全事件之單位聯絡資料：

單位名稱：_____ 通報人：_____

電話：_____傳真：_____E-mail：_____

二、 資通安全事件通報事項：

** 表述式有誤 **.◎事件發生時間：_____年_____月_____日_____時__分

2.受影響系統：_____

3.設備資料

◎IP 位址（IP Address）：_____

◎網際網路位址（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）：_____

◎已裝置之安全機制：如：防毒軟體、防火牆、IPS/IDS_____

◎已裝置之安全防護軟體：

防毒軟體（名稱/版本）：範例：Avira 10.0.0.561_____

防火牆（名稱/版本）：範例：iptables，此為不確定版本的範例

_____

◎受駭設備類型（請擇一填寫）：

□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、□人機介面、□其他_____

◎受害設備說明：範例：同仁桌機_____

◎損害類別說明（請擇一填寫）：

□資料外洩、□資料竄改、□硬體損害、□金錢損失、□其他_____

◎攻擊手法（請擇一填寫）：

□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/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：範例：同仁誤執行惡意程式_____

◎情資類型（請擇一填寫）：

□惡意內容、□惡意程式、□資訊蒐集、□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_____

◎IPS/IDS（名稱/版本）：範例：snort 2.8.3_____

◎其它（名稱/版本）：_____

4.資通安全事件：基本資料

◎事件分類（請擇一填寫）：

□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份盜取）

□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 Sever）

□殭屍電腦（Bot）（資訊設備疑似成為駭客所控制之 Botnet 成員）

□其他類型的入侵攻擊_____

□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）

□其他類型的網頁攻擊_____

□OTHER（其它）

□設備故障/毀損

□電力異常

□網路服務中斷

□設備遺失

□其它類型攻擊_____

◎破壞程度(文字勿超過 200 中文字，標點符號請用全形)

◎事件與處置方式說明：(詳細事件調查報告可檢附於後，文字勿超過 200 中文字，標點符號請用全形)

◎業務衝擊評判等級（請參考業務衝擊分析表）：□高級；□中級；□普級

◎資通安全事件判斷：

機密性衝擊	□0 級：資訊無洩漏 □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
完整性衝擊	□0 級：資訊未遭竄改 □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
可用性衝擊	□0 級：基礎設施或設備異常，但不影響服務運作（例如：發電機、UPS、主機、磁碟陣列等，在 H/A 備援模式下，單一元件/系統故障。） □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受影響或停頓，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

◎資安事件綜合評估等級：(由上表之機密性、完整性、可用性衝擊取最高等級)

□0 級　□1 級　□2 級　□3 級　□4 級

◎可能影響範圍及損失評估(文字勿超過 200 中文字，標點符號請用全形)

三、　期望支援項目：(含會辦單位及業務支援內容，標點符號請用大寫)

四、　◎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【五、解決辦法】

□其他_____

五、　◎解決辦法：(文字勿超過 200 字，標點符號請用全形)

六、　◎解決時間：_____年_____月_____日_____時_____分

業務單位承辦人	業務單位權責主管	會辦單位承辦人	會辦單位權責主管

以下由計算機及資訊網路中心填寫

是否對主管機關通報：（請交由資安承辦人填寫）

☐是。

_____年_____月_____日通報 TACERT(臺灣學術網路危機處理中心)教育機構資安通報平台，事件單編號_____。

☐否，無需通報。原因：

資安負責人	**權責主管**		**資安長**（3 級以上資安事件須請資安長核章）
	二級單位主管	**一級單位主管**	