臺灣學術網路各級學校
資通安全通報應變作業程序
修正草案

教育部

中華民國 110 年 4 月

目錄

第 1 章 前言

本部為求有效掌握臺灣學術網路（以下簡稱 TANet）各級學校、教育及研究機構之資通系統發生資通安全事件（以下簡稱資安事件）時，能迅速通報及緊急應變處置，以確保臺灣學術網路各級學校之正常運作，並符合「資通安全管理法」相關規範，使各單位人員能快速掌握處理原則，特訂定「臺灣學術網路各級學校資通安全通報應變作業程序」（以下簡稱本作業程序）。本作業程序不適用本部及所屬機關(構)。

本作業程序分為 6 章，除前言外，依整體作業、通報作業、應變作業、資安演練作業、獎懲及減責標準等逐項規範或說明。其中「整體作業」包括臺灣學術網路通報應變架構暨各單位角色職掌、資安事件等級定義及作業流程，明確規範資安事件發生時之通報應變作業程序；「通報作業」含各級學校、教育及研究機構之通報作業方式及要求；「應變作業」說明各級學校、教育及研究機構之事前安全防護、事中緊急應變、事後復原作業之具體機制及相關應變作業檢討等；「資安演練作業」敘述通報應變小組應辦理之相關資通安全演練作業，據以檢驗區、縣（市）網路中心及所屬連線單位之資安通報機制及應變能力；「獎懲及減責標準」則規範提報獎勵標準、懲處規定及減責規定等。

第 2 章 整體作業

一、適用範圍

臺灣學術網路轄下各級學校、學術機構及連線單位。但不包括國立大學附設醫療院所。

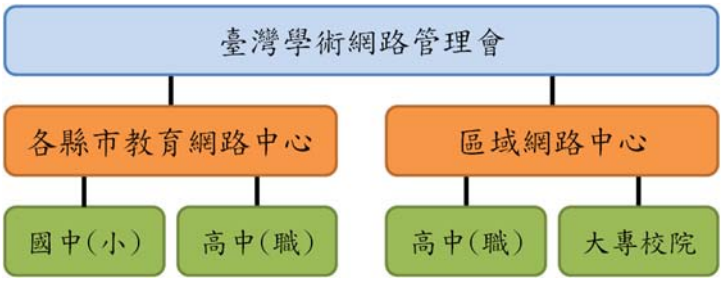
二、臺灣學術網路通報應變架構

臺灣學術網路以支援全國各級學校、研究機構間之教學與學術研究活動及教育行政應用服務為目的，其管理組織依序分為下列三個層級，架構如圖一所示。

（一）臺灣學術網路管理會：設立於本部，其幕僚作業由本部資訊及科技教育司辦理。

（二）縣（市）教育網路中心及區域網路中心：由各直轄市、縣（市）政府設立縣（市）教育網路中心，十三所大學則分別設立區域網路中心。

（三）連線臺灣學術網路各級學校（以下簡稱連線單位）。



圖一、臺灣學術網路通報應變架構

本作業程序各單位角色及執掌說明如下：

（一）第一線人員：指各連線單位之網管、資安人員，其職掌範圍為其所管轄單位之資安事件通報與處理。各單位應配置 2 名人員以求資安事件處理之有效。

（二）第二線人員：指各縣（市）教育網路中心及區域網路中心之網管、資安人員，職掌範圍為審核連線單位之資安事件、協助第一線人員資安事件之處理。區、縣（市）網人員應配置 2 名人員以求資安事件處理之效果。

（三）各級學校資安通報應變小組(以下簡稱通報應變小組)：指臺灣學術網路危機處理中心（TACERT），職掌範圍為負責各級學校資安通報平台之營運，審核所有資安事件，協調資安事件通報、處理與支援事項。

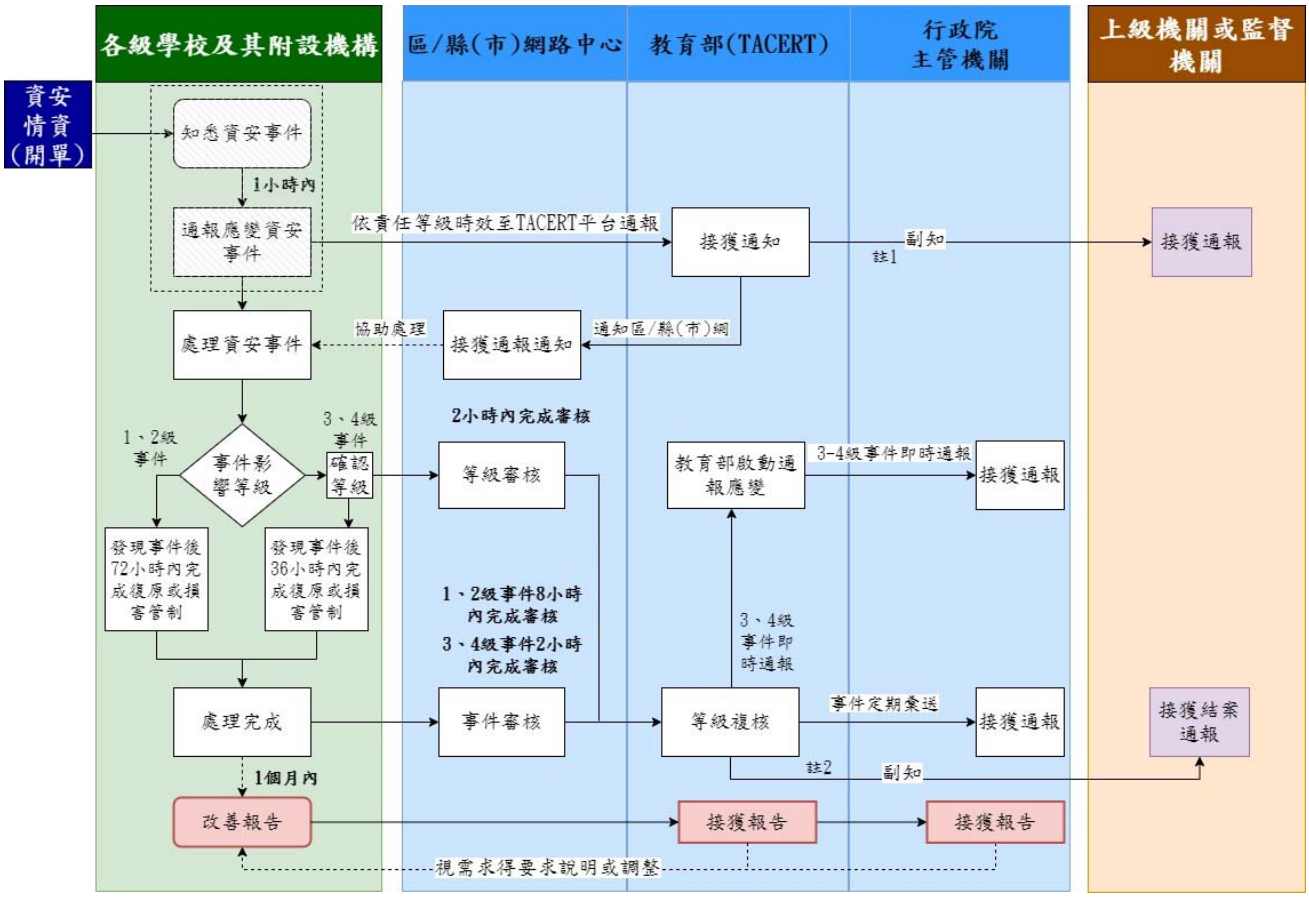
（四）教育部人員：指教育部資訊及科技教育司(以下簡稱本部資科司)，職掌範圍為指揮與監督重大資安事件之通報應變。

三、資通安全事件等級

本作業程序將資通安全事件分為四級，由重至輕分別為「4 級」、「3 級」、「2 級」及「1 級」，其等級定義依據「資通安全事件通報及應變辦法」第 2 條之規定。

四、通報及應變作業流程

資通安全事件通報及應變流程如圖二所示，相關作業程序請參見「第 3 章 通報作業」及「第 4 章 應變作業」。



註 1:國立高級中學(含)以下學校發生資通安全事件 TACERT 主動副知教育部國民及學前教育署

註 2:國立高級中學(含)以下學校發生資通安全事件經 TACERT 審核後主動副知結案至教育部國民及學前教育署

圖二、各級學校通報及應變流程

各單位通報資安事件或進行結案，以及區域網路中心及縣市教育網路中心審核所屬連線單位資安事件通報或結案時，均須至各級學校資安通報平台(以下簡稱通報應變網站)登錄作業，該網站營運維護、資安事件通報管理、技術諮詢及支援等服務，由本部委託臺灣學術網路危機處理中心負責，聯繫資訊如下：

（一）網址：https://cert.tanet.edu.tw

（二）聯絡電話：(07)525-0211

（三）網路電話：98400000

（四）電子郵件：service@cert.tanet.edu.tw

第 3 章 通報作業

一、臺灣學術網路轄下各級學校、學術機構及連線單位

（一）各連線單位通報範圍應包含自建或委外之資通系統。

（二）各連線單位知悉資通安全事件一小時內進行資通安全事件通報，至通報應變網站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。其資通安全事件定義依據「資通安全管理法」第 3 條第 4 項之規定。

（三）如因網路或電力中斷等事由，致使無法上網填報資安事件，須於知悉資安事件後 1 小時內，與所屬區、縣（市）網路中心及通報應變小組聯繫，先行提供事件細節，待網路通訊恢復正常後，仍須至通報應變網站補登錄通報。

（四）「4」、「3」級資安事件須於 36 小時內完成損害控制或復原；「2」、「1」級資安事件須於 72 小時內完成損害控制或復原。

（五）完成資安事件處理後，須至通報應變網站通報結案，並登錄資安事件處理過程及完成時間。

（六）「2」、「1」級資安事件通報應變完成後，應至通報應變網站列印單件，每月彙整送呈單位主管；「4」、「3」級資安事件需於事件發生後 36 小時內，通報送陳單位資通安全長。

（七）「4」、「3」級資安事件依本項規定完成損害控制或復原作業後，應持續進行資通安全事件之調查及處理，並於一個月內將調查、處理及改善報告函送本部，由本部彙送主管機關。

（八）各單位如因網路問題無法通報，可填寫「臺灣學術網路各級學校資通安全事件通報單」以傳真或電子郵件方式送至「臺灣學術網路危機處理中心」進行通報。

二、區、縣（市）網路中心

（一）區、縣（市）網路中心在接獲所屬連線單位通報後，應主動掌握事件狀況、協助所屬連線單位進行資安事件應變處理，並督導事件處理過程。

針對「4」、「3」級資安事件，區、縣（市）網路中心將主動通知通報應變小組，以利通報應變小組評估事件影響及通報本部資科司。

（二）區、縣（市）網路中心須至通報應變網站審核所屬連線單位通報之資安事件，並評估該事件是否影響其他連線單位運作以及事件影響等級之合理性，視需要申請技術支援。若資安事件屬「4」、「3」級事件，須於通報後 2 小時內完成審核；「2」、「1」級事件，則須於通報 8 小時內完成審核。

（三）若各連線單位完成資安事件處理，應至通報應變網站通報結案。針對「4」、「3」級資安事件，區、縣（市）網路中心於接獲所屬連線單位結案申請，除至通報應變網站審核所屬連線單位資安事件結案內容外，尚需對於該資安事件填寫應配合辦理事項或規劃相關作業。

三、通報應變小組

（一）通報應變小組依據各連線單位及其區、縣（市）網路中心通報之資訊，評估通報內容及事件等級合理性，並得視需要變更事件等級，如區、縣（市）網路中心未能於規定時限內完成通報審核，得逕行通知完成審核。

（二）區、縣（市）網路中心申請技術支援時，通報應變小組須於完成複核後，聯繫區、縣（市）網路中心確認技術支援事項，並通報本部資科司及協調提供技術支援方式。

（三）通報應變小組應彙整各級資安事件，定期提供至本部資科司；如接獲「4」、「3」級資安事件，應通報本部資科司。經本部知悉級別後一小時內，依行政院指定方式及對象，進行資通安全事件通報，俾供研析相關因應作為。

（四）「4」、「3」級資安事件，本部資科司得依事件情形邀集相關處理單位，召開緊急應變會議；必要時逐級陳報至本部資通安全長，召開資安防護會議。

（五）若行政院主管機關認為資安事件等級需調整時，通報應變小組應至國家資通安全通報應變網站申請等級變更調整，並依後續相關資安事件等級進行因應作為。

第 4 章 應變作業

一、各級學校、學術機構及連線單位

各連線單位應建立資安事件之「事前安全防護」、「事中緊急應變」及「事後復原」作業之具體機制，並至少包含下列各項：

（一）事前安全防護

1. 核心資訊系統應依「資通安全責任等級分級辦法」第 11 條或本部訂定之相關資安規定進行盤點作業,判定資訊系統安全防護等級,並據以落實資安防護基準。
2. 應規劃建置資通安全整體防護環境，做好內部資料存取控制，對於機敏文件、資料及檔案等應採取加密或實體隔離等防護措施。
3. 應訂定災害預防、緊急應變程序、復原計畫等防護措施並定期演練，以建立緊急應變能量。
4. 應依資通安全防護需要，執行入侵偵測、安全檢測及弱點掃描等安全檢測工作，並訂定系統與資料備份管理辦法，以做好事前防禦準備。
5. 應實施資通安全稽核、網路監控及人員安全管理等機制，以強化資通安全整體防護能力，降低安全威脅及災害損失。
6. 應保留資安紀錄與備份，如資訊系統屬委外建置管理者，應於合約內要求承商保留相關資安紀錄。
7. 應針對上述建立資通安全防護環境及相關措施，列入年度定期稽核項目，定期實施內部稽核，以儘早發現系統安全弱點並完成修復補強。
8. 應建置並保存相關設備之系統日誌。
9. 應每年定期規劃辦理資安認知教育訓練。

（二）事中緊急應變

1. 應就資安事件發生原因、影響等級、可能影響範圍、可能損失及是否需要支援等項目逐一檢討與處置，並保留被入侵或破壞相關證據。

2. 依訂定之緊急應變程序，實施緊急應變處置，並持續監控與追蹤管制。
3. 查詢臺灣學術網路危機處理中心網站、系統弱點(病毒)資料庫或聯絡技術支援單位(廠商)等方式，以尋求解決方案；如無法解決，應儘速向所屬區、縣（市）網路中心及通報應變小組反應，請求提供相關技術支援。
4. 評估資安事件對業務運作造成之衝擊，並進行損害管制。若未納入各單位防護範圍之資訊系統發生資安事件，為防止損害擴大影響他人或正常使用者之權益，依據「臺灣學術網路管理規範」，各單位得先行中斷發生資安事件之系統網路連線，待該系統完成通報應變改善作為後，始得恢復其連線。
5. 資安事件損壞程度，請遵循各單位內部備份管理辦法，啟動備援計畫、異地備援或備援中心等應變措施，以防止事件擴大。
6. 資安事件如涉及刑責，應做好相關資料(含稽核紀錄)保全工作，以便聯繫檢警調單位協助偵查。
7. 各連線單位如發生重大(「4」、「3」級)資安事件，應主動提供相關設備系統日誌予所屬區、縣（市）網路中心及通報應變小組，俾提供相關協助。

（三）事後復原

1. 在執行復原重建工作時，應執行環境重建、系統復原及掃描作業，俟系統正常運作後，即進行安全備份及資料復原等相關事宜。
2. 在完成復原重建工作後，應將復原過程之完整紀錄(如資安事件原因分析與檢討改善方案、防止同類事件再次發生之具體方案、稽核軌跡及蒐集分析相關證據等資料)，予以建檔管制，以利爾後查考使用。
3. 全面檢討網路安全措施、修補安全弱點、修正防火牆設定等具體改善措施，以防止類似入侵或攻擊情事再度發生，並視需要修訂應變計畫。

二、區縣（市）教育網路中心

區縣（市）教育網路中心應於資安事件處理完成後，針對以下項目進行應變作業檢視。

（一）作業程序：檢視人員辦理通報作業的熟悉程度與程序是否適當。

（二）事件處理：檢視人員事件應變處理措施是否適當。

三、通報應變小組

如重大(「4」、「3」級)資安事件經資安防護會議評估資安事件涉及下列事項時，經由本部資科司提報行政院國家資通安全會報，啟動相關應變機制，以控管損害。

（一）涉及網路犯罪相關議題。

（二）對關鍵基礎設施(Critical Infrastructure, CI)造成威脅時。

（三）對國家安全造成威脅時。

第 5 章 資安演練作業

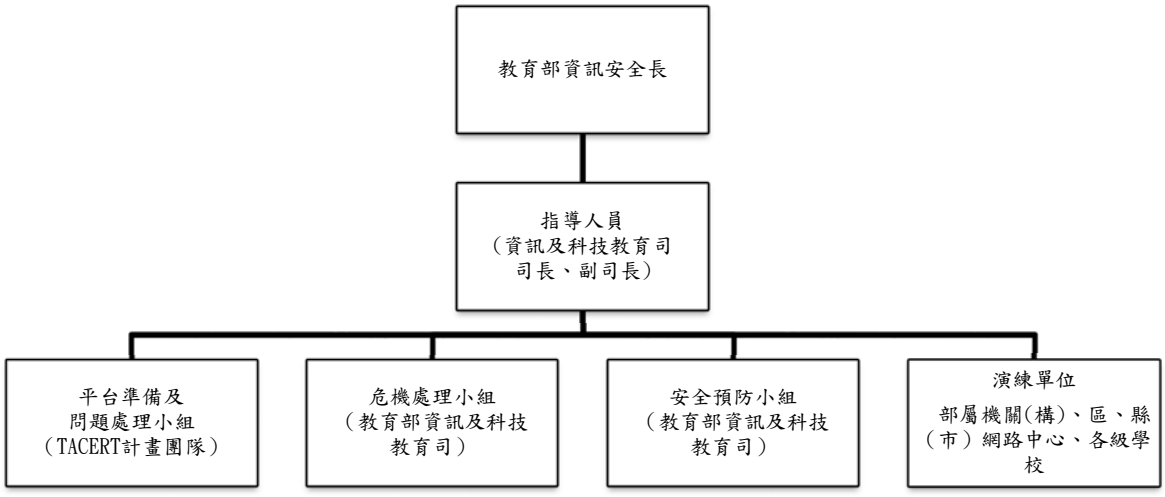
一、資通安全通報演練

（一）演練目的：檢驗「區、縣(市)網路中心」及所屬連線單位之資安通報機制及應變能力。

（二）演練時間：每年辦理 1 次，確實執行日期由通報應變小組提報演練計畫至本部資科司核定，惟須於每年 9 月底前完成。

（三）一般說明：

1. 本項演練作業，應分組分工執行各項任務。如平台準備及問題處理小組負責「各級學校資安通報演練平台」維護、規劃演練各項事宜及問題處理；危機處理小組負責規劃演練各種模擬狀況及處理突發狀況；安全預防小組負責規劃參演單位及支援演練計畫執行處理作業；演練單位針對演練模擬事件，研擬應變處理作為，並於「各級學校資安通報演練平台」回復應變處理作為，組織架構如圖三所示。



圖三、資通安全通報演練組織架構

2. 演練計畫應簽奉本部資科司核定後實施。

3. 遴選演練對象方式，由平台準備及問題處理小組提交單位清單供安全預防小組選取參與演練單位。

4. 演練前，平台準備及問題處理小組預先規劃各級資安事件之各種模擬狀況(至少 10 種以上)，提交危機處理小組複核。演練時採隨機選取方式，分配予參與演練單位。
5. 演練完成後將「演練事件紀錄」提交至本部資科司備查，並由平台準備及問題處理小組彙整統計演練成果報告，供本部資科司研商辦理獎勵及改善事宜。

二、防範惡意電子郵件社交工程演練

（一） 演練目的：提高「區、縣（市）網路中心」及其所屬連線單位對社交工程攻擊防制認知。

（二） 演練時間：每半年辦理一次社交工程演練，由本部資科司規劃及執行。

（三） 一般說明：

1. 演練對象由本部資科司決定，惟區縣（市）教育網路中心及所屬連線單位具有公務電子郵件人員，須 1/4（含）以上參與演練。
2. 演練實施前須訂定演練計畫，簽奉本部資通安全長核定。
3. 完成演練作業後，演練報告經本部資通安全長核定，並於每次演練完成後 1 個月內主動送行政院國家資通安全會報備查。

第 6 章 獎勵及減責標準

一、獎勵標準

（一）公務機關依「公務機關所屬人員資通安全事項獎懲辦法」辦理。

（二）非公務機關就其所屬人員辦理業務涉及資通安全事項之獎勵，得依「公務機關所屬人員資通安全事項獎懲辦法」之規定，自行訂定相關基準。

二、權責

具以下情事之一者，由本部資科司建議相關單位視情節輕重對所屬人員予以適度追究相關責任：

（一）校內發生資安事件，隱匿未向上級機關進行通報者。

（二）各校轄下單位之資通系統，若包含教、職、員、生可識別之個人資料，則該系統資料持有單位應確實評估風險，主動加以防護或納入校內核心系統給予應有之級別防護。若因未適當防護，致使該資通系統發生資安事件影響他人權益，資料持有單位應負相關責任。

（三）未遵循本作業程序規定落實資安事件通報應變作業及提供資安紀錄，致國家或社會受有重大損害時，依法追訴行為人涉及湮滅證據等相關刑事責任；此外另追究行為人、其主責單位及相關人員之行政責任。

三、減責標準

遵循本作業程序規定確實辦理資安事件通報及應變作業並提供資安紀錄，仍致政府或民眾權益受損時，區（縣）市教育網路中心及通報應變小組應協助提供資料予本部資科司，並建議減輕其責。

附件一 區（縣）市教育網路中心列表

編號	（縣）市教育網路中心	編號	區域網路中心
1	基隆市教育網路中心	1	臺北區域網路中心(1)
2	新北市教育網路中心	2	臺北區域網路中心(2)
3	臺北市教育網路中心	3	桃園區域網路中心
4	桃園市教育網路中心	4	竹苗區域網路中心
5	新竹縣教育研究發展暨網路中心	5	新竹區域網路中心
6	新竹市教育網路中心	6	臺中區域網路中心
7	苗栗縣教育網路中心	7	南投區域網路中心
8	臺中市教育網路中心	8	雲嘉區域網路中心
9	彰化縣教育網路中心	9	臺南區域網路中心
10	南投縣教育網路中心	10	高屏澎區域網路中心
11	雲林縣教育網路中心	11	宜蘭區域網路中心
12	嘉義縣教育網路中心	12	花蓮區域網路中心
13	嘉義市教育網路中心	13	臺東區域網路中心
14	臺南市政府教育局資訊中心		
15	高雄市政府教育局資訊教育中心		
16	屏東縣教育網路中心		
17	宜蘭縣教育網路中心		
18	花蓮縣教育網路中心		
19	臺東縣教育網路中心		
20	澎湖縣教育網路中心		
21	金門縣教育網路中心		
22	連江縣教育網路中心		

附件二 臺灣學術網路之各單位資通安全事件通報單

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. 知悉事件發生時間

二、知悉事件發生時：

◎知悉事件發生時間：_____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)

☐ 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

－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

－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：

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。