教育部 110 年度教育機構資通安全通報演練計畫

壹、依據

一、行政院發布之「資通安全管理法」及「資通安全事件通報及應變辦法」辦理。

二、教育部函頒之「臺灣學術網路各級學校資通安全通報應變作業程序」辦理。

貳、目的

一、檢驗「教育機構資安通報平台」所登錄單位資安聯絡人資料之正確性。

二、檢驗教育部、各區縣（市）網路中心通報反應、處理能力與審核機制是否完善。

三、測試教育機構分組資安聯絡人聯絡管道是否暢通。

四、測試各單位於發現資安事件時，是否可正確、快速執行通報作業。

五、測試通報網站、電子郵件、電話等各種通訊聯絡管道暢通與存活率。

參、任務編組

本次資通安全通報演練之任務編組如圖 1，

一、任務編組架構：

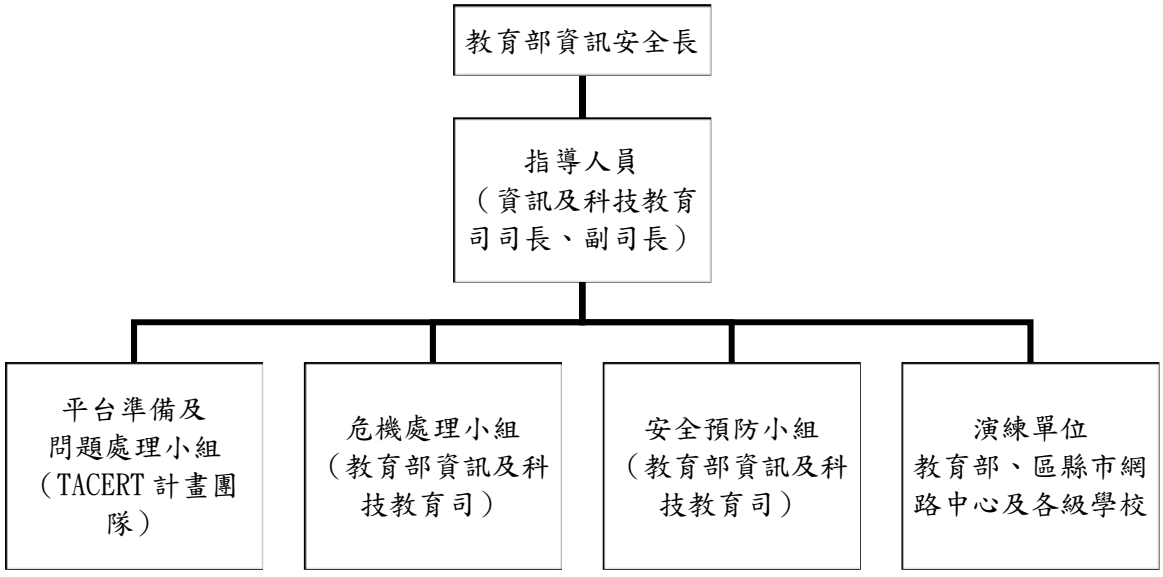

圖 1、任務編組架構圖

二、工作內容：

(一)平台準備及問題處理小組：

負責教育機構資安通報演練平台維護、規劃演練各項事宜及問題處理。

(二)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。

(三)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。

(四)演練單位：

針對演練模擬事件，研擬應變處理作為，並於教育機構通報演練平台回復應變處理作為。

肆、演練期程

一、演練資料整備作業：

自計畫頒布日至 110 年 09 月 03 日止

二、資安通報演練作業：

(一)第一梯次演練：**110 年 09 月 06 日至 110 年 09 月 10 日止**。

(二)第二梯次演練：**110 年 09 月 13 日至 110 年 09 月 17 日止**。

備註：每梯次前三日為演練事件派發作業時間，後二日為預留作業時間。

伍、演練資料整備作業

一、整備項目：

(一)確認教育機構資安通報平台帳號資料

教育機構資安通報平台係以國發會所核發之機關單位統一識別碼（OID）作為各單位登入帳號，各執行演練單位資安聯絡人若忘記登入帳號時可至該網站 https://oid.nat.gov.tw 查詢；如名稱有所異動時，請先行至國發會申辦 OID，並告知臺灣學術網路危機處理中心（TACERT）辦理帳號異動。

申請 OID 時請至該網站點選「申請組織與團體 OID 說明」選項，相關申請流程請參考網頁說明。

(二)確認教育機構資安通報平台資安聯絡人資料

各執行演練單位請於演練資料整備期間內至「**教育機構資安通報平**

台」登錄資料，各機關（構）、學校至少應填列2名資安聯絡人(第一、二連絡人)，並檢查資安聯絡人資料是否正確並完成密碼更新。

二、配合注意事項：

(一)因應通報作業需要，各機關單位統一識別碼（OID）帳號分割成多組帳號，各聯絡人以各自帳號登入進行聯絡人資料確認及密碼更新作業。

(二)第一、二連絡人為主要連絡人，建議將業務負責人員填寫於前二位連絡人，並將未使用之連絡人帳號關閉，以達風險控管目的。

(三)為各單位能於演練期間完成演練，單位於收到演練公文開始至**整備結束期間**皆可更新密碼，且至少前二位連絡人需進行密碼變更。

(四)建議使用高強度密碼，以大小寫英文、數字、符號至少擇其二種組合成8碼以上之密碼。

陸、資安通報演練作業

一、演練說明：

本次演練依據行政院函頒之「資通安全事件通報及應變辦法」及教育部頒訂之「臺灣學術網路各級學校資通安全通報應變作業程序」，以模擬事件，檢視教育機構資安事件通報是否符合「資通安全事件通報及應變辦法」之規範。藉此檢視機關（構）、學校資料更新程度，並了解教育部、各區縣（市）網路中心及機關（構）、學校反應能力。

二、執行演練單位：

(一)第一梯次執行演練單位

執行演練單位：臺北區域網路中心（1）、臺北區域網路中心（2）、桃園區域網路中心、竹苗區域網路中心、新竹區域網路中心、南投區域網路中心、宜蘭區域網路中心、花蓮區域網路中心、臺東區域網路中心、基隆市教育網路中心、臺北市教育網路中心、新北市教育網路中心、桃園市教育網路中心、新竹市教育網路中心、新竹縣教育研究發展暨網路中心、苗栗縣教育網路中心、南投縣教育網路中心、宜蘭縣教育網路中心、花蓮縣教育網路中心、臺東縣教育網路中心、金門縣教育網路中心、連江縣教育網路中心、中央研究院、教育部等，及其

所服務之連線學校、機構。

(二)第二梯次執行演練單位

執行演練單位：臺中區域網路中心、雲嘉區域網路中心、臺南區域網路中心、高屏澎區域網路中心、臺中市教育網路中心、彰化縣教育網路中心、雲林縣教育網路中心、嘉義市教育網路中心、嘉義縣教育網路中心、臺南市教育網路中心、高雄市政府教育局資訊教育中心、屏東縣教育網路中心、澎湖縣教育網路中心等，及其所服務之連線學校、機構。

三、演練方式：

(一)本次演練將以「**告知通報**」形式進行，教育部將於資安通報演練作業期間以郵件及簡訊傳送「資安演練事件通知單」。為避免與真實事件產生混淆，演練模擬事件通知簡訊及郵件上皆加註「**告知通報演練**」字樣，另事件單編號皆以「**DRILL**」開頭進行編碼。

(二)系統將以教育部模擬之 10 種情境樣本以亂數方式，於演練期間分別發送至所有演練單位，執行演練單位於收到 mail 及簡訊通知後，應於規定的時限內至**教育機構資安通報演練平台**完成事件通報流程，並依事件等級於處理時限內完成事件應變處理並結案。

演練平台網址：**https://drill.cert.tanet.edu.tw**

四、演練模擬事件類型：

演練情境由教育部依教育體系常見資安情資與事件實至加以規劃，計 10 種情境(如表 1)，進行教育部及教育機構之演練，藉此檢測演練單位能否於符合教育部規範之時限內正確地完成通報應變流程。

表 1、演練模擬資安事件情境

模擬狀況編號	攻擊事件說明
1	單位內主機被植入勒索病毒，系統資料遭到加密
2	單位內 IoT 設備未更改預設帳號密碼
3	單位人員誤將個人資料置於公開網路上，導致外部人員可下載相關資訊
4	發現單位電腦系統被植入惡意程式，並對外進行 APT 攻擊
5	單位內網站具有跨網站腳本攻擊(Cross-site scripting，簡稱 XSS)的漏洞，可能造成瀏覽者的危害
6	單位內電腦被入侵，並被利用來進行遠端桌面(RDP)暴力攻擊
7	發現單位電腦系統被入侵，並進行挖礦惡意行為
8	單位電腦被入侵，而成為 BotNet 所控制的 Bot 主機
9	單位網站被置入詐騙網頁，誘導使用者至釣魚網站
10	單位內電腦感染特洛伊木馬病毒而對外攻擊

此次演練為配合教育部內針對資訊安全 3 級與 4 級事件通報流程演練，將於各梯次抽選區縣（市）網路中心進行 3 級與 4 級事件派發，收到之單位依演練流程完成通報應變作業。

此次演練重大模擬資安事件之說明如表 2。

表 2、演練模擬重大資安事件情境

模擬狀況編號	攻擊事件說明
1	單位含有大量學生個資(姓名、身分證字號)被置於網站上，並造成資料外洩。
2	攻擊者取得合法帳號後，利用單位 VPN 主機做為跳板，取得敏感資料庫之相關帳號及密碼。

五、演練模擬事件通報方式：

各執行演練單位將於受測期限內某時間收到演練平台所寄發之簡訊及電子郵件兩種告知訊息，格式與範例如後。

(一)發送之演練簡訊格式與範例：

格式：(告知通報演練) [受測單位],[事件類型]警訊,[事件編號],請盡速至平台完成事件處理。

範例 1：(告知通報演練) [國立 XX 大學],[入侵攻擊]事件警訊,[15],請盡速至平台完成事件處理。

範例 2：(告知通報演練) [國立 YY 大學],[網頁攻擊]事件警訊,[16],請盡速至平台完成事件處理。

(二)發送之演練事件通知電子郵件主旨格式與範例：

1.郵件主旨欄格式：(事件單編號：DRILL-2021-XX)(告知通報演練) [事件類型]事件警報

範例 1：(事件單編號：DRILL-2021-15)(告知通報演練) 入侵攻擊事件警報)

範例 2：(事件單編號：DRILL-2021-16)(告知通報演練) 網頁攻擊事件警報)

2.演練事件通知單內容範例：

範例　　教育機構資安通報【演練平台】

教育機構分組資通安全演練事件通知單

演練事件類型：入侵事件警訊

演練事件單編號：DRILL-INT-2021-xx

原發布編號	DRILL-INT-2021-xxxx	原發布時間	2021-09-xx xx:xx:xx
演練事件類型	中繼站	原發現時間	2021-09-xx xx:xx:xx
演練事件主旨	單位內主機[XXX.XXX.XXX.XXX] 遭受殭屍(Bot)惡意程式感染，對外進行攻擊。		
演練事件描述	該主機可能被植入 Bot 程式而成為殭屍網路(BotNet)中的一員而受到惡意攻擊者的控制。並持續以 IRC（Internet Relay Chat）封包持續與惡意的 C&C(Command and Control)伺服器連線， 而被入侵偵測系統所偵測。		
手法研判	由於該主機具有 MS08-067 弱點，可能受到殭屍(Bot)惡意程式利用而被感染		
建議措施	建議立即採取下列步驟： 1.檢查該系統上是否有不明程式正大量對外建立網路連線(如 TCP Port 139、445)。 2.主機之管理者/使用者查明來源主機的發起攻擊行為之原因為何，若為非預定安裝程式所引發，建議直接移除該程式，並詳加檢測貴單位主機是否有任何的異常狀況。 3.進行該主機全系統病毒掃描後，安裝最新的系統安全修正程式。		
此演練事件需要進行通報，請 貴單位資安聯絡人登入資安通報演練平台進行通報應變作業			
如果您對此通告的內容有疑問或有關於此演練事件的建議，歡迎與我們連絡。			

3.演練通報應變流程說明：

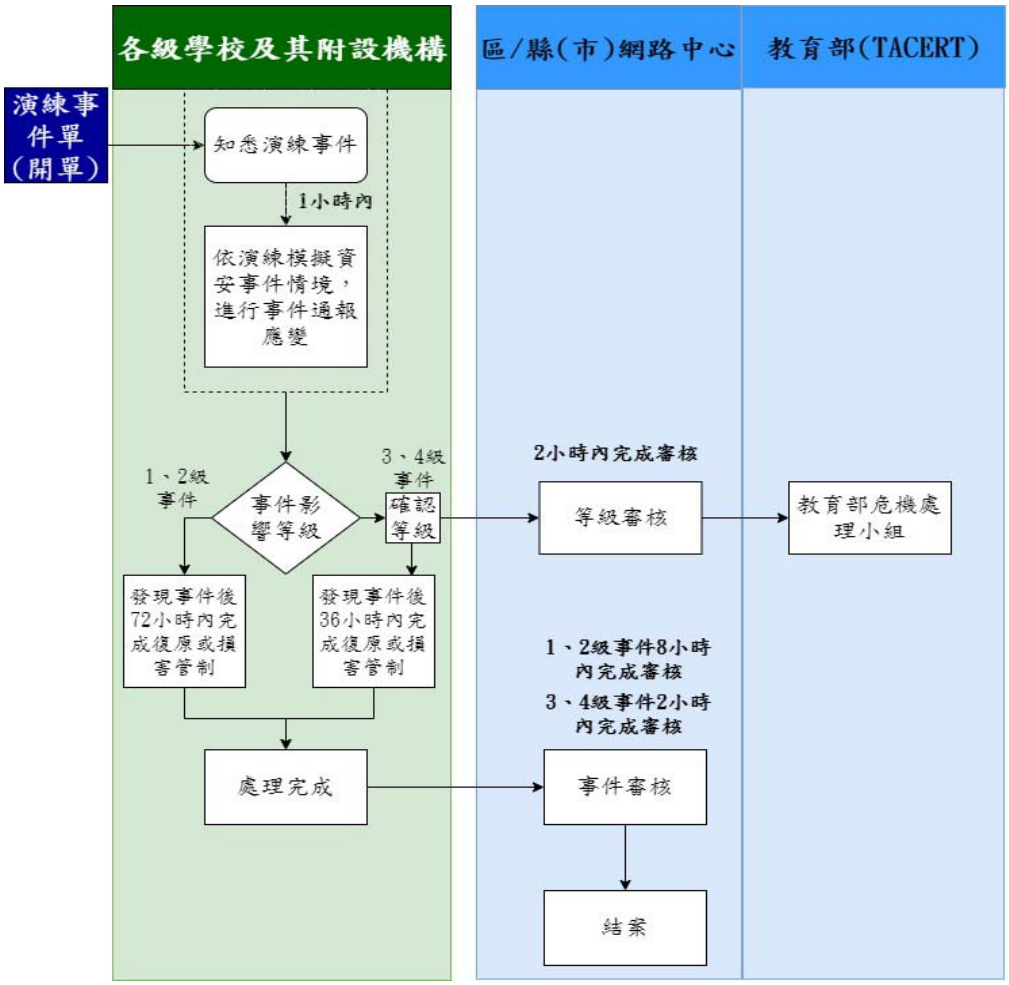

圖 2、演練通報應變流程圖

六、更新資安聯絡人資料及填報應變處理作為：

(一)請上「教育機構資安通報平台」(https://info.cert.tanet.edu.tw/) 更新資安聯絡人資料。

(二)依據教育部頒布之「臺灣學術網路各級學校資通安全通報應變作業程序」標準，進行通報應變流程，請於時限內至「教育機構資安通報演練平台」網站（https://drill.cert.tanet.edu.tw/)，填報應變處理作為。

七、評分對象：包括教育部、區縣（市）網路中心及各連線服務機關（構)、學校

(一)教育部、區縣(市)網路中心以管轄單位密碼更新比率、通報完成率、

應變完成率及是否依通報應變流程時限內完成審核作為評比標準。

(二)學校以是否依通報應變流程時限內完成通報、應變及單位聯絡人資料準確度及完整性作為評比標準。

八、評分標準說明：

(一)教育部及各區縣(市)網路中心)評分標準

1. 密碼更新率：以各區縣（市）網路中心所轄機構、學校主要資安連絡人密碼更新比率給分，該項最高 2 分。
   密碼更新率=（已更新主要資安連絡人密碼數量/轄下單位主要資安連絡人密碼總數量）* 100%。
2. 通報完成率：以各區縣（市）網路中心所轄機構、學校是否在時限內完成通報比率給分，該項最高 2 分。
   通報完成率=（轄下單位合格通報演練事件數量/轄下單位演練事件總量）*100%。
   註：合格通報演練：為符合「資通安全事件通報及應變辦法第四條規範」之演練事件單，即知悉演練事件後，應於一小時內完成通報。
3. 應變完成率：以各區縣（市）網路中心所轄機構、學校是否在時限(應變時間-發佈時間)內完成應變比率給分，該項最高 2 分。
   應變完成率=（轄下單位合格應變演練事件數量/轄下單位演練事件總量）*100%。
   註：合格應變演練：即 1、2 級演練事件，於發佈該事件後 72 小時完成應變；3、4 級演練事件，於發佈該事件後 36 小時完成應變。
4. 審核即時率：以教育部、各區縣（市）網路中心是否能於時限內完成案件審核給分，該項最高 2 分。
   審核即時率=（合格審核時限的演練事件數量/轄下單位演練事件總量）*100%
   註：合格審核時限：為符合「資通安全事件通報及應變辦法第五條規範」之演練事件單。即轄下單位通報 1、2 級演練事件後 8 小時內審核完畢，轄下單位通報 3、4 級演練事件後 2 小時內審核

完畢。

表 3、教育部、各區縣（市）網路中心評分標準說明

給分標準（每項） / 評分項目	2	1	0
密碼更新率	90%(含)以上	70%~90%	70%(含)以下
通報完成率	所轄連線單位於時限內完成通報的比率達 90%(含)。	所轄連線單位於時限內完成通報的比率達 90%~70%。	所轄連線單位於時限內完成通報的比率未達 70%。
應變完成率	所轄連線單位於時限內完成應變的比率達 90%。	所轄連線單位於時限內完成應變的比率達 90%~70%。	所轄連線單位於時限內完成應變的比率未達 70%。
審核即時率	所轄連線單位事件單審核作業於時限內完成率達 85%。	所轄連線單位事件單審核作業於時限內完成率達 85%~70%。	所轄連線單位事件單審核作業於時限內完成率未達 70%。

(二)各機關(構)及學校評分標準

1. 通報時效率：以各機關（構）、學校於知悉演練事件後，於 1 小時內進行通報作業。

   通報時效計算公式：通報時間-知悉時間

2. 應變時效率：以各機關（構）、學校依安全等級時限內完成處理。

   應變時效計算公式：應變時間-發佈時間

   註：規定的應變時限為演練事件發佈後，1、2 級事件需於 72 小時內完成應變作業，3、4 級事件需於 36 小時內完成應變作業。

3. 資料正確率：各機關（構）、學校需依序於教育機構資安通報平台登錄至少 2 名資安連絡人，並隨時保持資料最新且正確。

   註：主要資安連絡人為單位第一及第二連絡人，需於整備期間完成密碼更新。

表 4、各機關（構）及學校評分標準說明

給分標準（每項）／評分項目	2	1.5	1	0
通報即時率	30 分鐘內	45 分鐘內	1 小時內(含)完成	未於 1 小時內完成
應變時效率	30 分鐘內	45 分鐘內	於規定的應變時限內完成	未於規定的應變時限內完成
資料正確率	2 位(含)以上主要資安聯絡人所有欄位資料填寫完整（含密碼更新）		僅一位主要資安聯絡人資料填寫完整（含密碼更新）	主要資安聯絡人的資料均不完整

九、獎懲標準說明：

(一)為鼓勵積極推動資通安全防護及即時完成通報作業,教育部將依據本次演練結果挑選績優單位及改善單位，並辦理所轄機構獎懲作業。

(二)績優單位：擇取規則如表 5 定義。擇取後，由教育部發文該單位建議予以獎勵（請依權責自行敘獎）。

表 5、獎懲擇取標準說明

類別	對象	分組排名	說明
績優單位	區縣(市)網路中心	連線單位 200 個(含)以上，取演練成績最優 3 名	1. 演練成績需取得 8 分，方可進入績優單位排名。 2. 若當年未有單位取得 8 分，當年度績優單位即從缺。 3. 若分數相同,即以「通報審核率」擇優排名。 4. 若「通報審核率」相同則以通報、應變即審核之時間總和(秒)平均值做排名。
		連線單位 50(含)至 199 個，取演練成績最優 3 名	
		連線單位 10(含)以上至 50 個以下，取演練成績最優 3 名	

	機(關)構、學校	取演練成績最優 10 名	1. 演練成績需取得 6 分，方可進入績優單位排名。 2. 若當年未有單位取得 6 分，當年度績優單位即從缺。 3. 若分數相同，即以「應變時效率」擇優排名。 4. 若「應變時效率」相同則以通報及應變之時間總和（秒）平均值做排名。
需改善單位	全體	區縣（市）網路中心及學校演練成績總分在 2 分以下，函請其研提改善作為。	

十、檢討與改善作為

(一)需改善單位：區縣（市）網路中心或學校總分在 2 分以下，請該單位檢具檢討改善報告（如附件）報部備查，並列入教育部資訊安全稽核優先名單。

(二)各縣市政府參演成績將列入「110 年度統合視導地方教育事務」評分項目之一，如有待加強事項，教育部將發函至需改善單位，研提改善作為，並於統合視導單位時驗證單位改善成效。

十一、協調聯絡資訊

(一)教育機構資安通報平台網址：**https://info.cert.tanet.edu.tw**

(二)通報平台操作相關事宜洽臺灣學術網路危機處理中心服務人員協助

連絡電話：(07) 525-0211

VOIP 網路電話：98400000

E-mail： service@cert.tanet.edu.tw

附件

教育部教育部 110 年度教育機構資通安全通報演練

檢討改善情形報告

_____年_____區縣(市)網路中心機構、學校名稱_____ **檢討改善情形報告**
一、 演練整備情形說明： 說明區縣(市)網路中心機構、學校於本次資安通報演練之**整備**概況與尚待精進之處。以 500 字為限。 **二、 通報作業檢討：** 檢討本次資安**通報及演練作業**概況與尚待精進之處。以 500 字為限。 **三、 改善計畫與改善情形說明：** 了解現行作業是否符合「教育體系資安事件應變處理機制」作業及通報流程[登載於 https://cert.tanet.edu.tw]要求，提出改善計畫與改善情形說明。以 500 字為限。 **四、 通報應變作業建議：** 針對「國家資通安全事件通報應變機制」及「教育部 110 年度教育機構資通安全通報演練」，提出改善或相關建議。以 500 字為限。

填報人：_____ 主管：_____ 資訊安全長（副首長）：_____