114學年度
資通安全維護計畫撰寫
與教育體系資安通報應變處理

新北市政府教育局
教育研究及資訊發展科
余宗翰輔導員

今日議題

- 準備事項
- 資通安全維護計畫
- 資安通報應變處理
- 資安資源介紹
- 結語

❖ 簡報格式

下底線：有超連結

藍色粗體：重點、須遵守

紅色粗體：禁止、須避免

準備事項

準備事項

- 資通安全維護計畫與分工表(新北教研資字第1141541501號)
- 資通安全維護計畫附件範例(新北教研資字第1141541501號)
- 教育機構資安通報平台帳密(前手交接)
- 114學年度教育機構資安通報演練事件情境範本(新北教研資字第1141557959號)

資通安全維護計畫

資通安全維護計畫

- 期程：以**學年**為單位，每學年修訂後落實
- 修訂計畫
  - 透過備註功能找到**必須修改項目**
  - 如需列印建議刪除備註
  - 填妥**分工表**
  - 分工表核章後掃描依公文透過**校務行政系統填報模組上傳**
- 計畫與分工表上傳：**114年8月29日前完成**
- **請勿使用本學年度公文附件以外之版本**

資通安全維護計畫

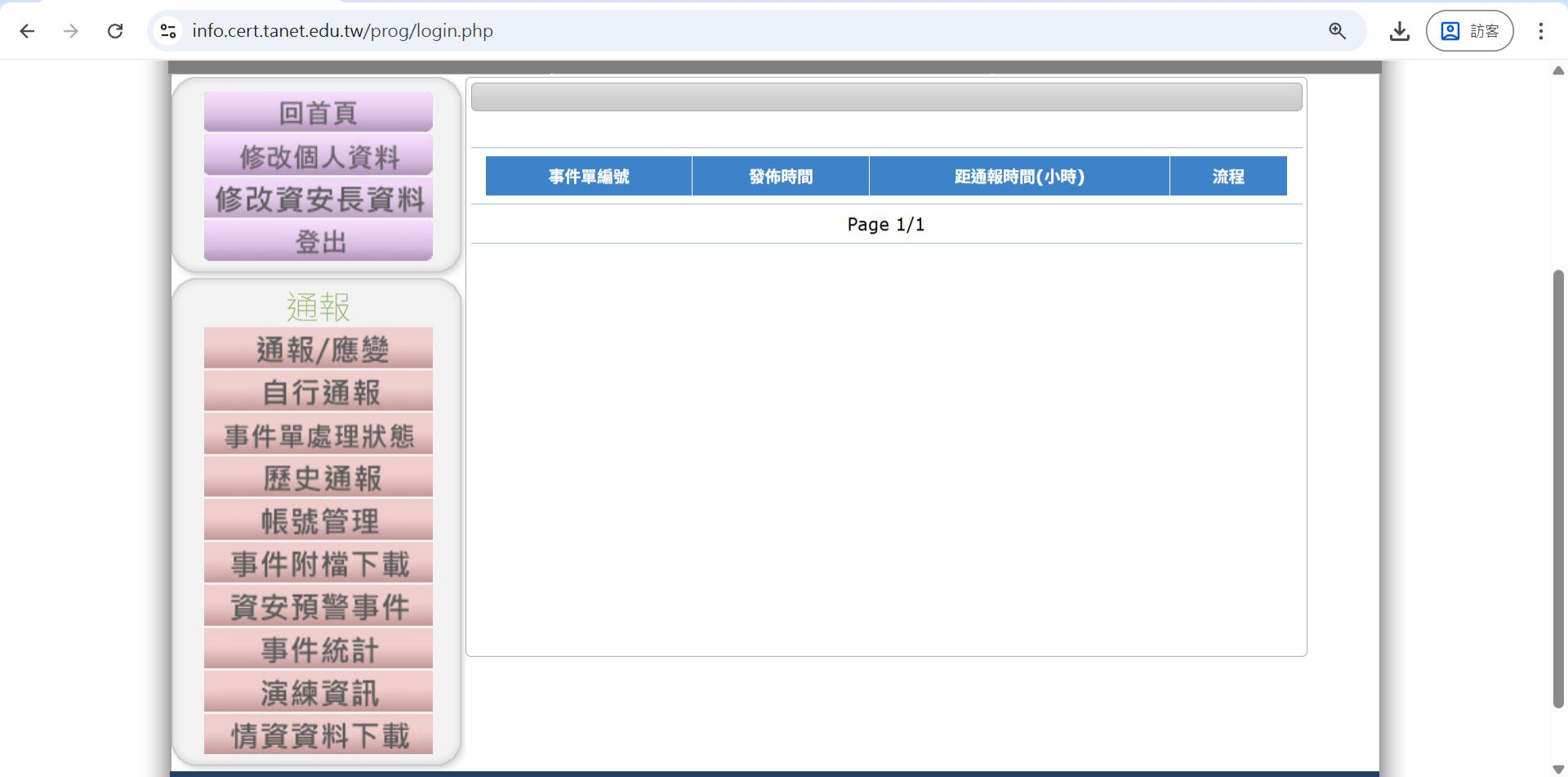
- 執行項目：
  - **校內同仁(具校務行政帳號者)資安研習時數三小時**
    - 可提供**線上資源**供老師取得時數，或**自辦研習**
  - 其餘項目請參考計畫附件
- 成果提交：
  - **學年末**繳交，另函通知
  - 資產清冊微調後亦可用於數發部管考系統填報

資安通報應變處理

資安通報應變處理

- **教育機構資安通報平台** (正式)
- 114學年資安通報演練
  - 整備期:114年7月16日-114年8月29日
  - 整備事項(正式平台資料會連動到演練平台):
    - **第一聯絡人變更密碼**
    - **第二聯絡人變更密碼**
    - **更新資安長資料**

教育機構資安通報平台(主畫面)



教育機構資安通報平台(修改個人資料、查看其他聯絡人)

教育機構資安通報平台(修改資安長資料)

資安通報應變處理(事件單)

教育機構資安通報平台

事件類型:入侵事件警訊

事件單編號:OOOOOO

原發布編號	OOOOOOOOOOOO	原發布時間	OOOOOO
事件類型	惡意程式		
事件主旨	教育部資安通告-OOOOOOOO[XXX.XXX.XXX.XXX]主機進行惡意程式連線(MALWARE-CNC Embedded.Exploit.Hoaxcalls variant outbound connection)		
事件描述	原始紀錄:MALWARE-CNC Embedded.Exploit.Hoaxcalls variant outbound connection,入侵偵測防禦系統偵測到來源IP(XXX.XXX.XXX.XXX)，包含疑似惡意程式連線行為特徵之封包，對目標IP(YYY.YYY.YYY.YYY)進行連線，原始事件觸發時間：OOOOOO。此事件來源 PORT(OOOOOO)，目標 PORT(80)。		
手法研判			
建議措施	請檢視來源IP該連線行為是否已得到合法授權。 若來源IP該連線為異常行為，可先利用掃毒軟體進行全系統掃描，並利用ACL暫時阻擋該可疑IP。同時建議管理者進行以下檢查： a.請查看來源IP有無異常動作(如：新增帳號、開啟不明Port、執行不明程式)。 b.確認防毒軟體的病毒碼已更新為最新版本，並進入系統安全模式下行進行全系統掃描作業、系統是否已安裝相關修正檔，或關閉不使用的應用軟體與相關通訊埠。 若來源IP為DNS server、NAT主機或IP分享器等設備IP時，表示有內部主機透過這些設備向外連線時而觸發偵測規則， 則需先請設備管理者透過事件單所附之資訊(目的地IP、時間、來源port)，來協助查找內部觸發偵測規則之主機，再依前述建議處理措施進行作業。		
參考資料			
如果您對此通告的內容有疑問或有關於此事件的建議，歡迎與我們連絡。			

資安通報應變處理

- 114學年資安通報演練
  - **教育機構資安通報演練平台** (整備與演練期間開放)
  - 演練期:
    - 第一梯次:**114年09月01日至114年09月05日**
    - 第二梯次:**114年09月08日至114年09月12日**
  - **演練情境範本**

資安通報應變處理

- 正式事件處理原則
  - **保持聯繫**
  - 定位設備 > 找出根本原因 > 修補/緩解
- 常見修補/緩解措施
  - 重灌系統
  - 重裝軟體
  - 移入內部網路

資安通報應變處理

- 發生時間
  - 告知通報(系統開單)：信件裡會帶有時間
  - 自行通報(學校自行產單)：學校自行填寫
- **知悉**時間
  - 會自動帶入開啟平台之時間，**建議勿更改**

資安通報應變處理

- **通報**：**知悉**後**一小時**內完成
- 損害控制或復原(應變)：
  - 第一級或第二級資通安全事件，於**知悉**該事件後**七十二**小時內
  - 第三級或第四級資通安全事件，於**知悉**該事件後**三十六**小時內
- 建議：**通報與應變一併處理，可洽教網中心尋求支援**

資安通報應變處理(預警單)

EWA事件單狀態		
誤判		
確實事件	事件單編號	
確實預警(未造成損害)		
無法判斷		
原因		

資安通報應變處理

- 教育機構資安通報平台系統操作問題
  - (07)525-0211
- 新北市政府教育網路中心資安支援
  - (02)8072-3456#534

資安資源介紹

資安資源介紹

- 新北市資訊業務入口網
  - 威脅情資
  - 法規、期程、防毒、其他資源
- MSERT
- 資安健診小助手
  - 受檢測之主機執行前建議先跑一輪MSERT(full scan更好)
  - 建議針對行政電腦，於上學期完成資安健診小助手資料回收，以利組長掌握學校行政電腦整體狀況

結語

結語

- 根:**落實法遵**，奠定資安根基
- 苗:配合教網中心情資與指引
- 花:視學校負擔施行進階補強
- 果:逐步建立可信賴資安文化