資安事件通報處理與通報平台操作

新北市政府教育局
教育研究及資訊發展科

幸福美麗大臺北 返璞歸真心教育

- 資安通報平台操作
- 資安通報演練說明

資安通報平台操作

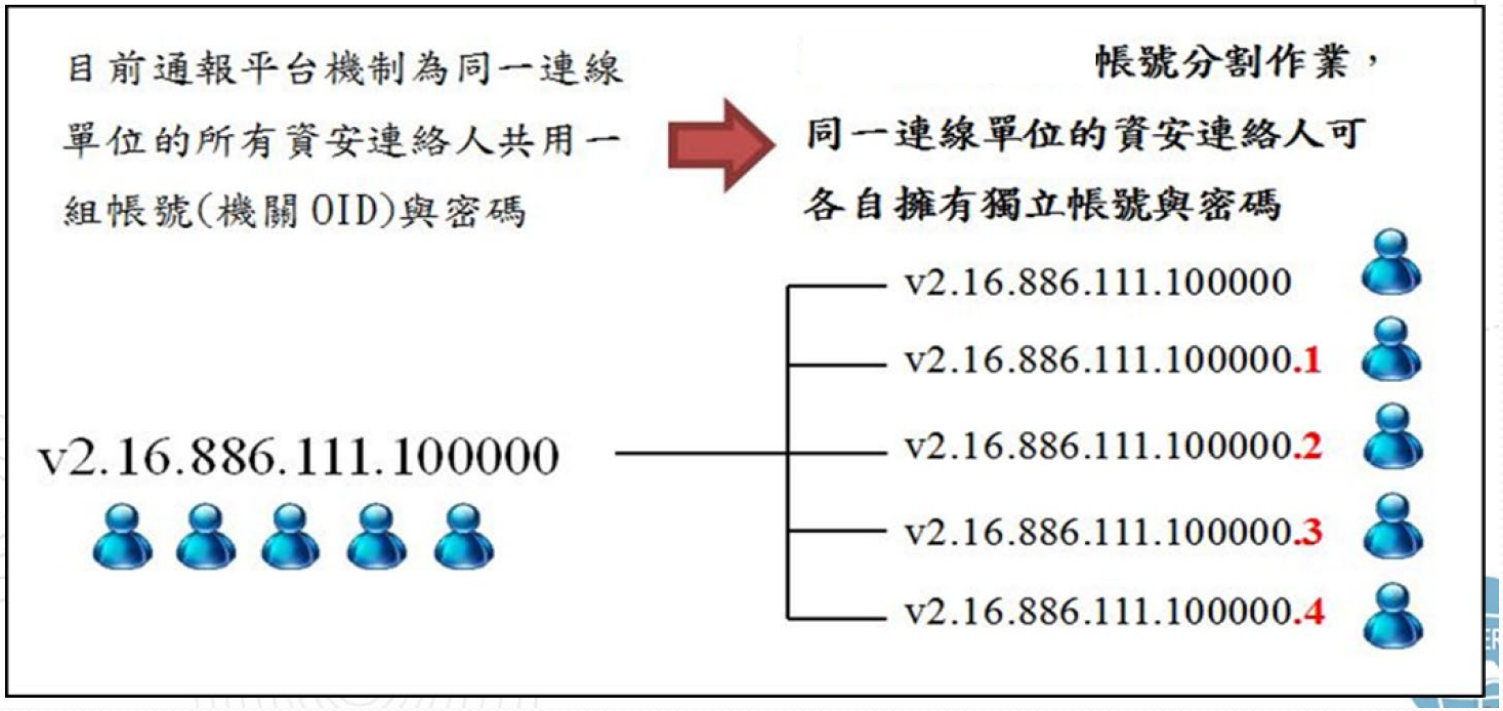
教育機構資安通報平台

教育機構資安通報平台網址:
https://info.cert.tanet.edu.tw/prog/index.php

- 會員登入
  - 使用OID帳號登入
  - 一個學校至少**兩位聯絡人**
  - 每個聯絡人OID密碼可不同

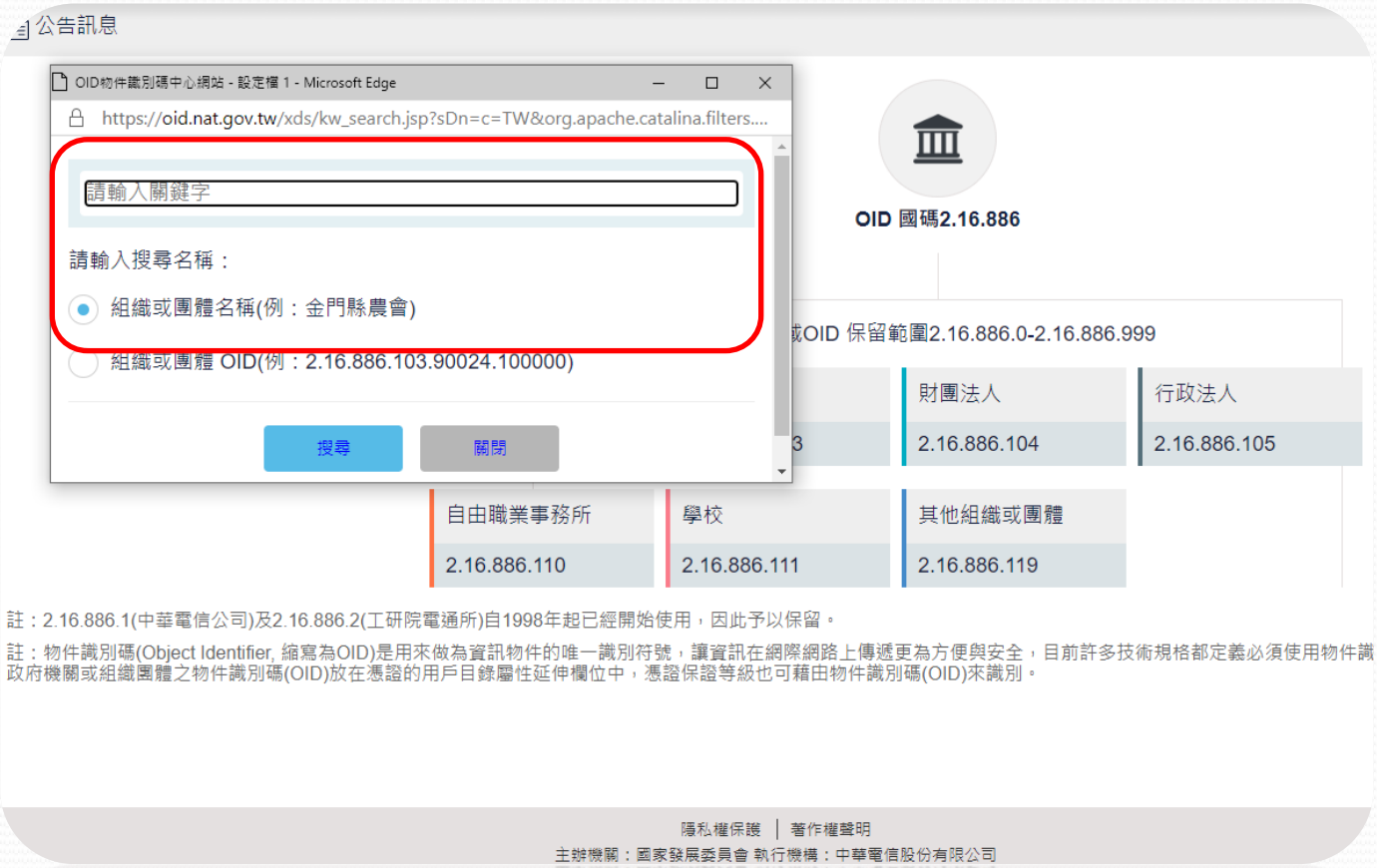
- 忘記密碼
  - 點選密碼查詢
  - 詢問前校內資安通報承辦人
  - 聯絡TACERT(臺灣學術網路危機處理中心)
    服務電話：(07)525-0211

- 使用OID及密碼登入
- 一個單位最多有五位連絡人
- 每個連絡人OID及密碼可不同



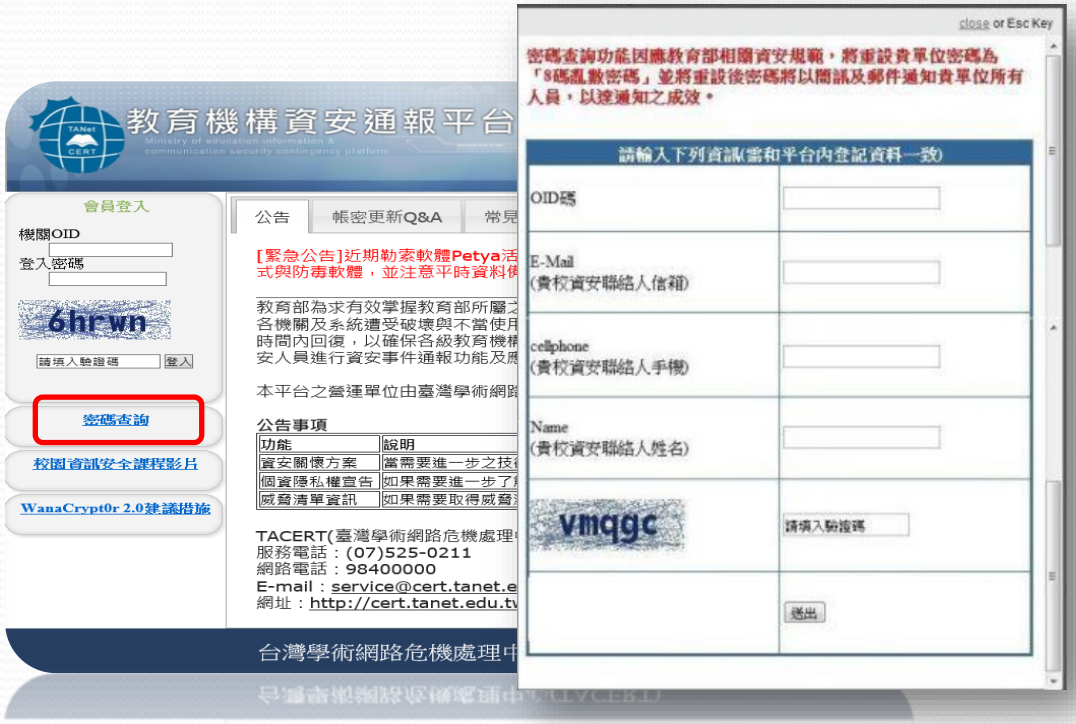
- 忘記單位(學校)OID
  - 可至**國家發展委員會**網站(https://oid.nat.gov.tw/OIDWeb/)，點選「**組織及團體物件識別碼(OID)查詢**」進行查詢
  - 可來電(信)至教育機構資安通報平台詢問

- 搜尋學校關鍵字建議輸入學校全名
  - 例如:新北市立**國民中學



密碼查詢

- 密碼查詢機制核對「單位OID」、「聯絡人姓名」、「聯絡人郵件」、「聯絡人手機」及「驗證碼」，以上資訊需和教育機構資安通報平台內聯絡人資料符合
- 以「重設8碼亂數密碼」，並以簡訊及電子郵件通知該聯絡人



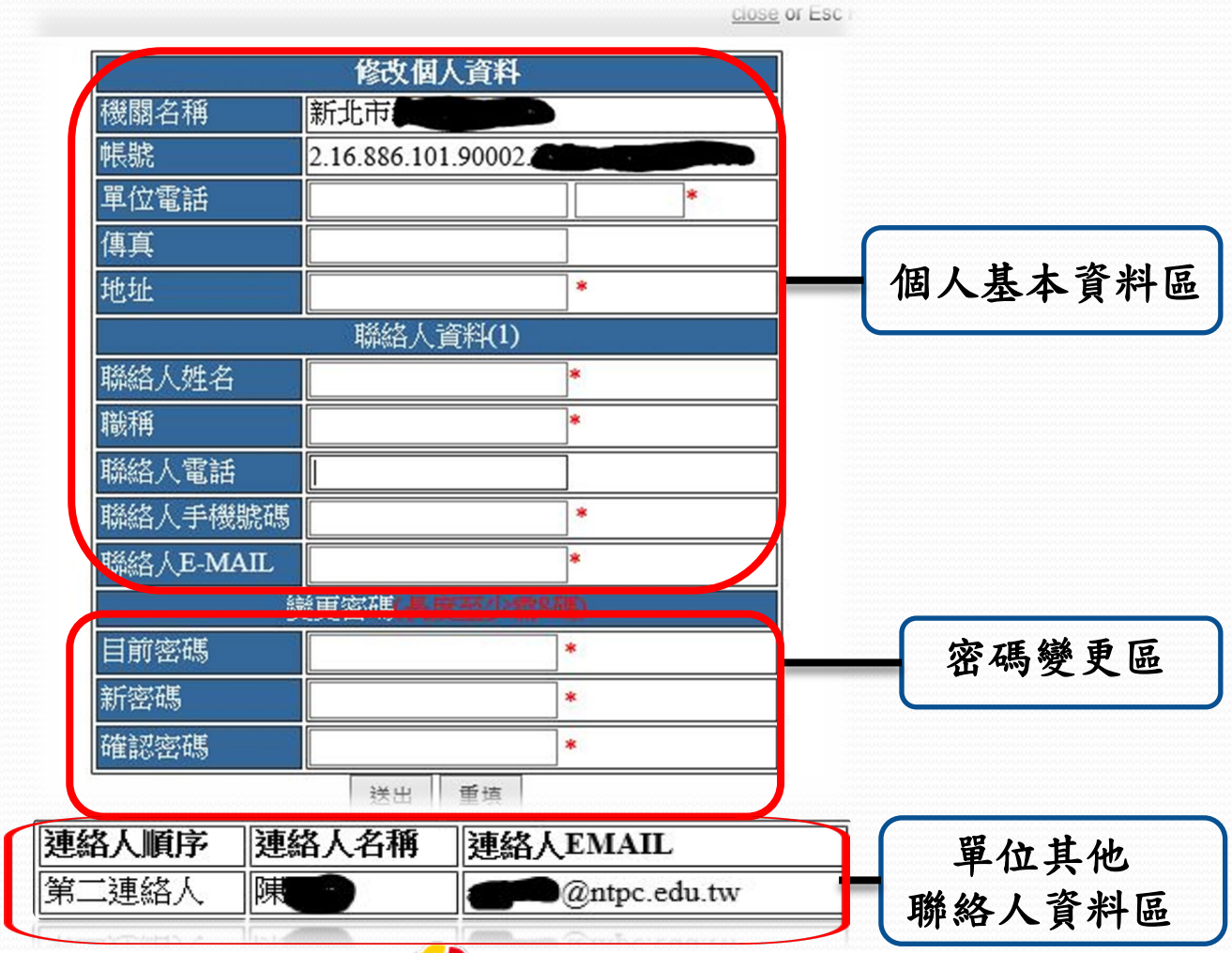
登入畫面


單位資訊
主管單位資訊
教育機構單位資訊
教育機構資安通報平台
Ministry of education information & communication security contingency platform
聯絡資訊
機關名稱:新北市[redacted]
使用者:[redacted]
主管機關:新北市教育網路中心
聯絡電話:02-8072-3456[redacted]
E-Mail:[redacted]
教育機構資安通報應變小組
聯絡電話:07-525-0211
E-Mail:service@cert.tanet.edu.tw
個人資料區
回首頁
修改個人資料
登出
通報
通報/應變
自行通報
事件單處理狀態
歷史通報
帳號管理
事件附檔下載
資安預警事件
事件統計
演練資訊
事件單處理區
事件單編號
發佈時間
距通報時間(小時)
流程
Page 1/1
台灣學術網路危機處理中心(TACERT)

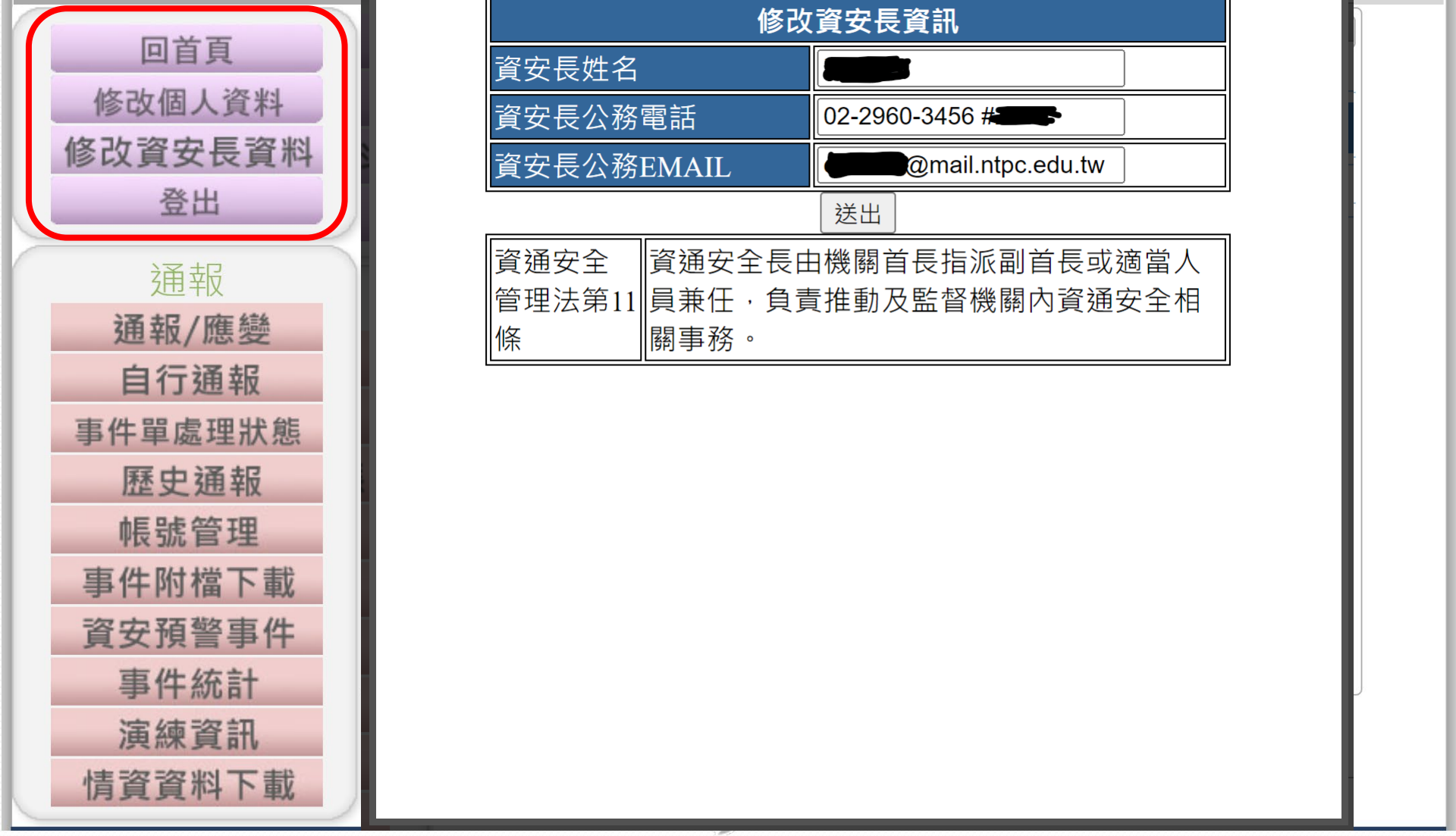
資安通報平台功能簡介

- 個人資料區各功能說明：
  - 首頁：顯示未處理完成事件
  - 修改個人資料：修改個人聯絡資料
- 事件單處理區各功能說明：
  - 通報/應變：未完成通報應變事件單表列於此，以利處理
  - 自行通報：如發現資安事件或EWA事件單確認屬實，可利用此功能完成通報應變
  - 事件單處理狀態：未結案前之事件單狀態查詢
  - 歷史通報：已結案事件單表列於此
  - 帳號管理：管理聯絡人帳號開啟關閉
  - 事件附檔下載：事件單佐證表依發佈編號查詢下載
  - 資安預警事件：**預警事件**單表列於此
- 網址:https://info.cert.tanet.edu.tw/prog/index.php

修改個人資料


close or Esc
修改個人資料
機關名稱
新北市
帳號
2.16.886.101.90002
單位電話
傳真
地址
聯絡人資料(1)
聯絡人姓名
職稱
聯絡人電話
聯絡人手機號碼
聯絡人E-MAIL
目前密碼
新密碼
確認密碼
送出
重填
連絡人順序
連絡人名稱
連絡人EMAIL
第二連絡人
@ntpc.edu.tw
個人基本資料區
密碼變更區
單位其他
聯絡人資料區

修改個人資料


回首頁
修改個人資料
修改資安長資料
登出
通報
通報/應變
自行通報
事件單處理狀態
歷史通報
帳號管理
事件附檔下載
資安預警事件
事件統計
演練資訊
情資資料下載
close or Esc Key
修改資安長資訊
資安長姓名
資安長公務電話
02-2960-3456 #
資安長公務EMAIL
@mail.ntpc.edu.tw
送出
資通安全管理法第11條
資通安全長由機關首長指派副首長或適當人員兼任，負責推動及監督機關內資通安全相關事務。

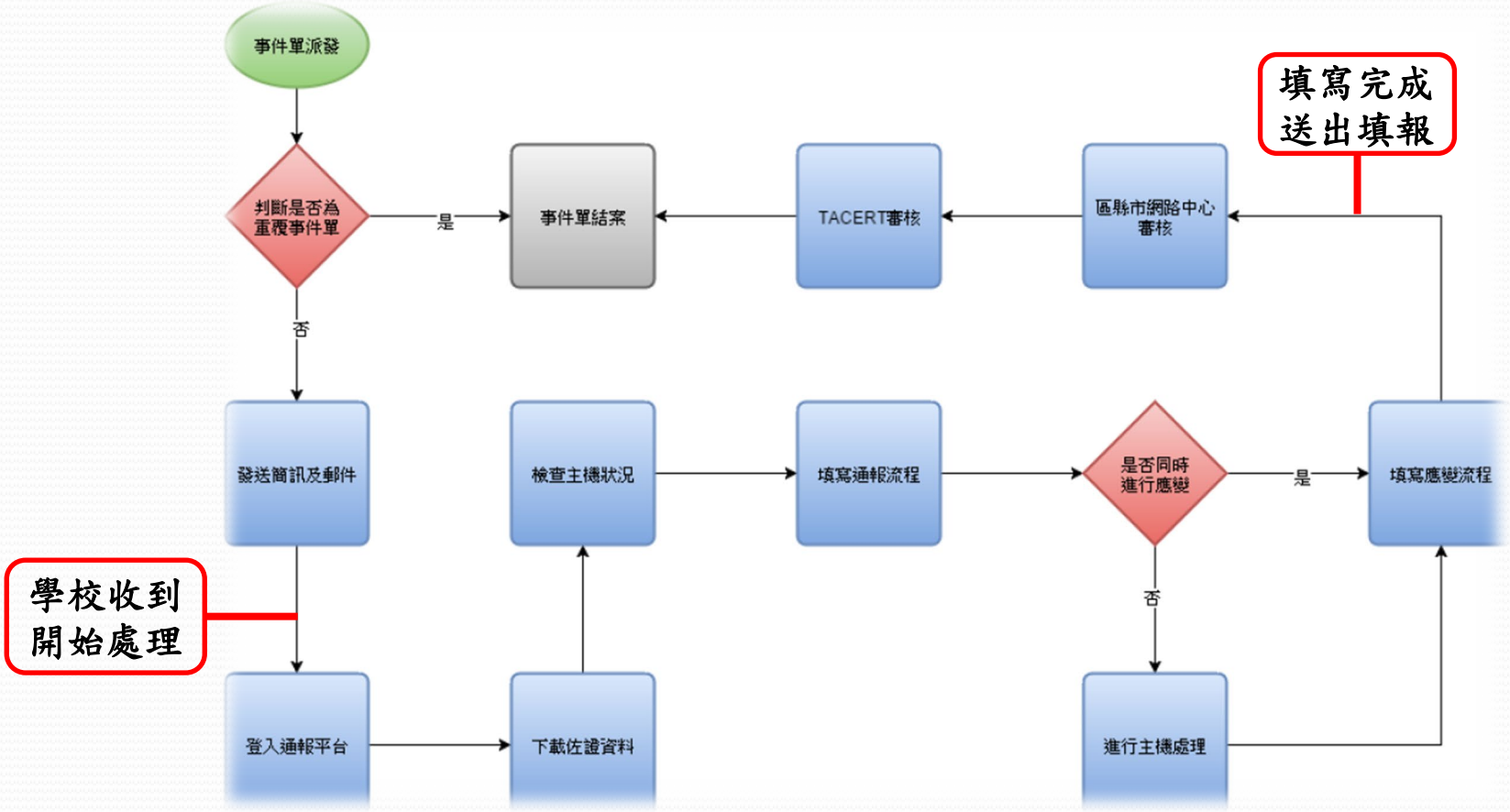
帳號管理功能


回首頁
修改個人資料
登出
通報
通報/應變
自行通報
事件單處理狀態
歷史通報
帳號管理
事件附檔下載
資安預警事件
事件統計
演練資訊
帳號名稱
帳號狀態
帳號管理
第三資安連絡人
已開啟
關閉此帳號
送出
第四資安連絡人
已開啟
關閉此帳號
送出
第五資安連絡人
已開啟
關閉此帳號
送出
帳號管理說明文件下載

連線單位資安聯絡人異動

- 確保資安事件能夠即時通知與處理，資安聯絡人發生異動時，務必確保資安事件的處理業務能妥善完成交接
  - 資安聯絡人員至少需有二位，以建立代理人制度
  - 將主要負責人員填寫於第一、二聯絡人
  - 教育機構資安通報平台的帳號密碼進行交接
  - 登入教育機構資安通報平台於「修改個人資料」進行聯絡人資訊更新

事件單處理流程


事件單派發
判斷是否為重覆事件單
是
事件單結案
TACERT審核
區縣市網路中心審核
填寫完成送出填報
否
發送簡訊及郵件
檢查主機狀況
填寫通報流程
是否同時進行應變
是
填寫應變流程
學校收到開始處理
否
登入通報平台
下載佐證資料
進行主機處理

通報應變規劃重點

- 為使通報應變流程更有效掌握，通報應變平台之流程畫分為通報流程與應變流程
- 第一線人員由於處理時間的限制，可先進行通報流程，待完成處理後再進行應變流程
- 請學校盡可能通報與應變同時進行
- 所有通報應變流程之通報，都必須審核過後才是(教育部規範)正式結束通報流程

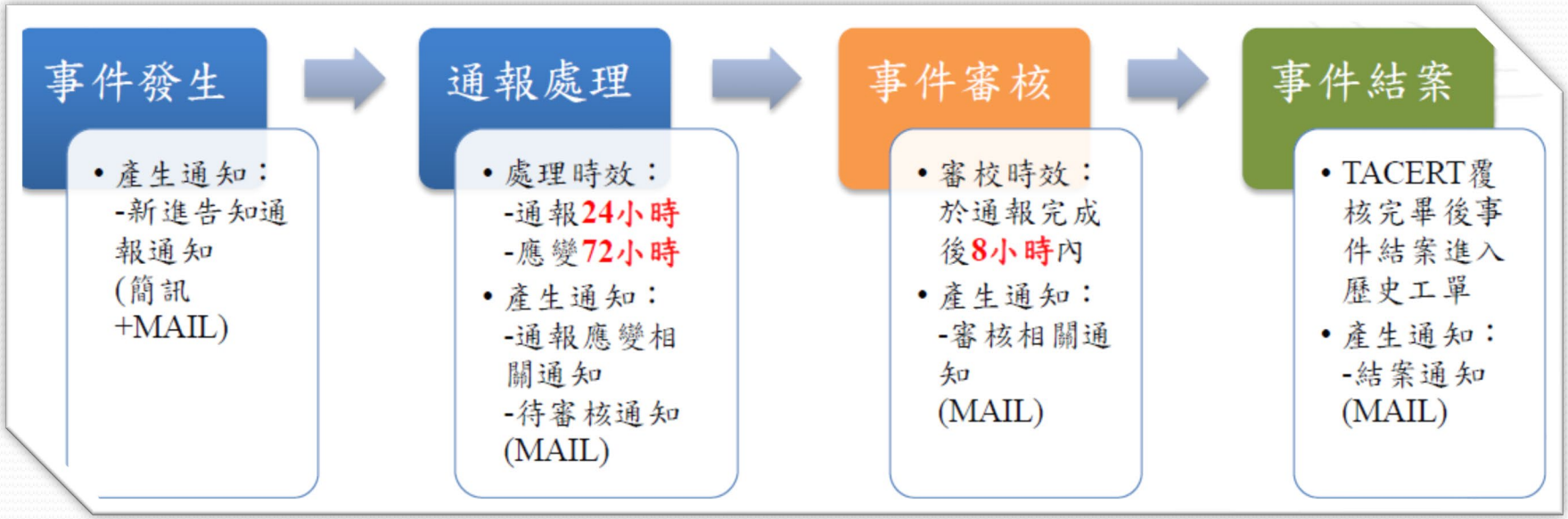
依資安等級區分

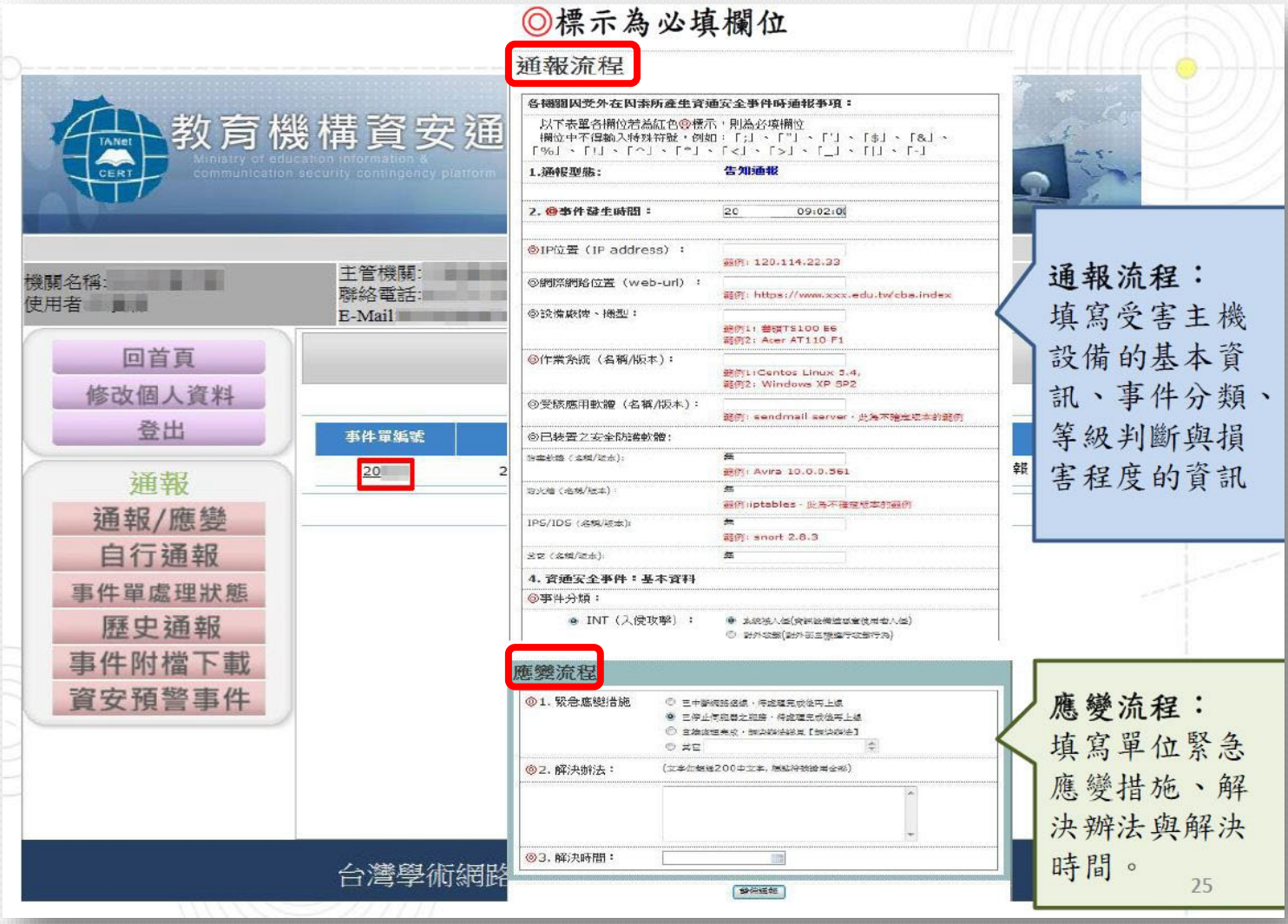
- 法規
  https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=A0030305
- 第1、2級資安事件
  - **事件處理**時間**通報**於**1小時**內完成，**應變**於**72小時**內完成(通報+應變)
  - 電子郵件通知寄發
    - 事件單成立後1個小時
    - 事件單成立後每隔12個小時通知
    - 事件單成立後72小時後每隔12個小時寄發逾時通知

依資安等級區分

- 法規
  https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=A0030305
- 第3、4級資安事件
  - 針對**政府或國家等級**之攻擊行為或其他重大資訊安全事件。
  - **事件處理**時間**通報**於**1小時**內完成，**應變**於**36小時**內完成(通報+應變)
  - 需和上級管理單位報備且建立聯絡並指定相關人員待命追蹤處理狀況
  - 電子郵件通知寄發
    - 事件單成立後1個小時
    - 事件單成立後每隔12個小時通知
    - 事件單成立後36小時後每隔12個小時寄發逾時通知

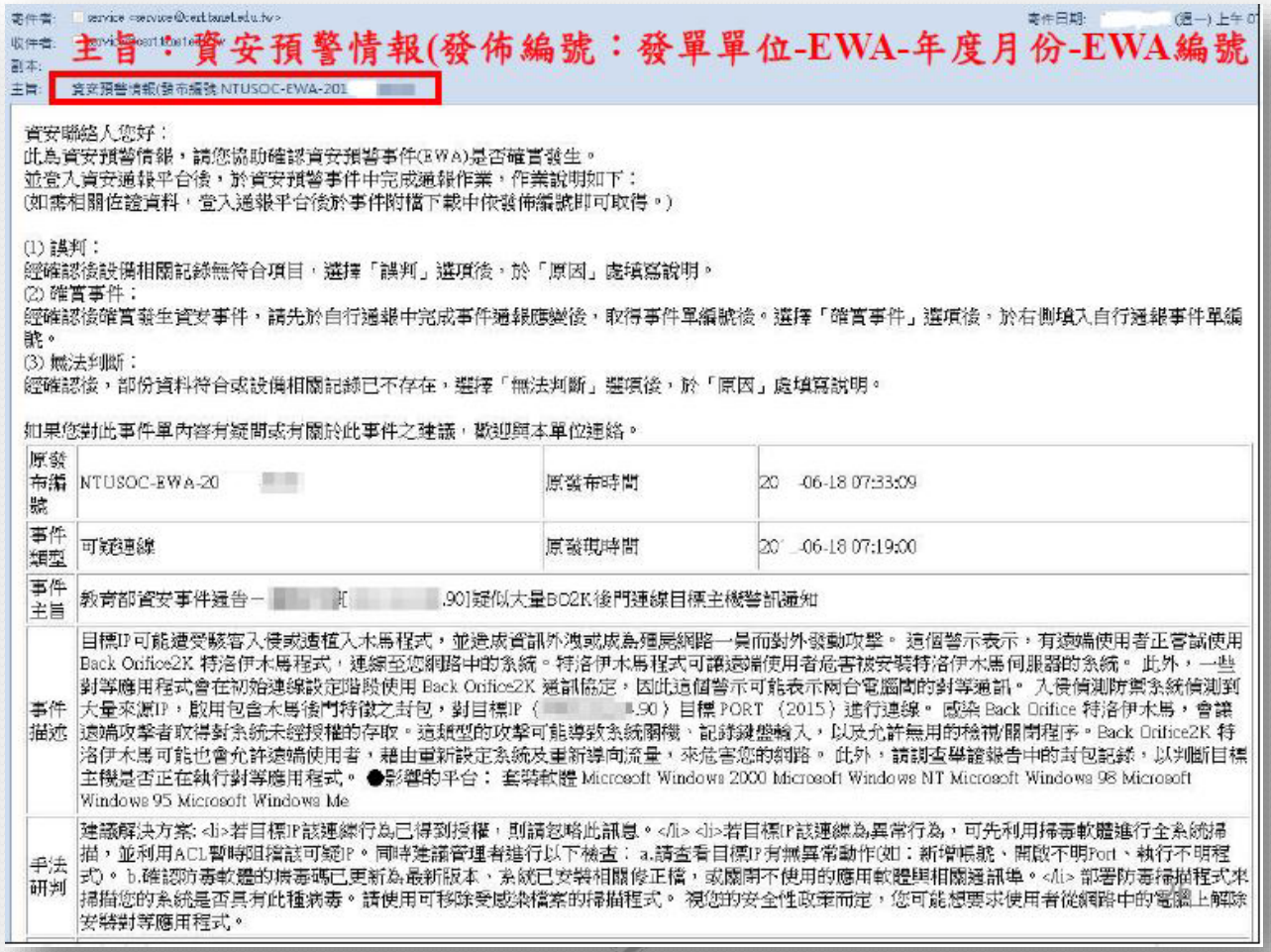
事件單處理流程


事件發生
• 產生通知：
-新進告知通報通知
(簡訊+MAIL)
通報處理
• 處理時效：
-通報24小時
-應變72小時
• 產生通知：
-通報應變相關通知
-待審核通知
(MAIL)
事件審核
• 審校時效：
於通報完成後8小時內
• 產生通知：
-審核相關通知
(MAIL)
事件結案
• TACERT覆核完畢後事件結案進入歷史工單
• 產生通知：
-結案通知
(MAIL)


◎標示為必填欄位
通報流程
教育機構資安通
Ministry of education information & communication security contingency platform
回首頁
修改個人資料
登出
通報
通報/應變
自行通報
事件單處理狀態
歷史通報
事件附檔下載
資安預警事件
事件單編號
台灣學術網路
各機關因受外在因素所產生資通安全事件時通報事項：
以下表單各欄位若為紅色◎標示，則為必填欄位
1.通報型態：
告知通報
2. ◎事件發生時間：
◎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：
4. 資通安全事件：基本資料
◎事件分類：
INT（入侵攻擊）：
應變流程
◎1. 緊急應變措施
◎2. 解決辦法：
◎3. 解決時間：
通報流程：
填寫受害主機設備的基本資訊、事件分類、等級判斷與損害程度的資訊
應變流程：
填寫單位緊急應變措施、解決辦法與解決時間。
25

預警情報事件單(EWA)

- 資安預警情報只派發MAIL通知，**不派發簡訊通知**



主旨：資安預警情報(發佈編號：發單單位-EWA-年度月份-EWA編號

資安聯絡人您好：
此為資安預警情報，請您協助確認資安預警事件(EWA)是否確實發生。
並登入資安通報平台後，於資安預警事件中完成通報作業，作業說明如下：
(如需相關佐證資料，登入通報平台後於事件附檔下載中依發佈編號即可取得。)

(1) 誤判：
經確認後設備相關記錄無符合項目，選擇「誤判」選項後，於「原因」處填寫說明。
(2) 確實事件：
經確認後確實發生資安事件，請先於自行通報中完成事件通報應變後，取得事件單編號後。選擇「確實事件」選項後，於右側填入自行通報事件單編號。
(3) 無法判斷：
經確認後，部份資料符合或設備相關記錄已不存在，選擇「無法判斷」選項後，於「原因」處填寫說明。

如果您對此事件單內容有疑問或有關於此事件之建議，歡迎與本單位連絡。

原發布編號	NTUSOC-EWA-20	原發布時間	20 -06-18 07:33:09
事件類型	可疑連線	原發現時間	20 -06-18 07:19:00
事件主旨	教育部資安事件通告－ 到 .90]疑似大量BO2K後門連線目標主機警訊通知		
事件描述	目標IP可能遭受駭客入侵或遭植入木馬程式，並造成資訊外洩或成為殭屍網路一員而對外發動攻擊。這個警示表示，有遠端使用者正嘗試使用Back Orifice2K 特洛伊木馬程式，連線至您網路中的系統。特洛伊木馬程式可讓遠端使用者危害被安裝特洛伊木馬伺服器的系統。此外，一些對等應用程式會在初始連線設定階段使用 Back Orifice2K 通訊協定，因此這個警示可能表示兩台電腦間的對等通訊。入侵偵測防禦系統偵測到大量來源IP，啟用包含木馬後門特徵之封包，對目標IP（ .90）目標 PORT（2015）進行連線。感染 Back Orifice 特洛伊木馬，會讓遠端攻擊者取得對系統未經授權的存取。這類型的攻擊可能導致系統關機、記錄鍵盤輸入，以及允許無用的檢視/關閉程序。Back Orifice2K 特洛伊木馬可能也會允許遠端使用者，藉由重新設定系統及重新導向流量，來危害您的網路。此外，請調查舉證報告中的封包記錄，以判斷目標主機是否正在執行對等應用程式。●影響的平台： 套裝軟體 Microsoft Windows 2000 Microsoft Windows NT Microsoft Windows 98 Microsoft Windows 95 Microsoft Windows Me		
手法研判	建議解決方案: - 若目標IP該連線行為已得到授權，則請忽略此訊息。 - 若目標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.請查看目標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，系統已安裝相關修正檔，或關閉不使用的應用軟體與相關通訊埠。 部署防毒掃描程式來掃描您的系統是否具有此種病毒。請使用可移除受感染檔案的掃描程式。視您的安全性政策而定，您可能想要求使用者從網路中的電腦上解除安裝對等應用程式。		

資安預警情報

- 資安預警情報(EWA)為教育部各資安計畫團隊或是其他情資來源單位，偵測到疑似網路攻擊行為時所發送的預警通知
- 由學校單位進行檢查、處理及填報作業，教育局進行追蹤作業
- 連線單位收到資安預警通知時，請檢查該主機是否有異常網路活動，並進行處理狀態回覆：
  - 確實事件：先於通報平台採『自行通報』取得事件單編號
  - 誤報：請詳填原因(以利發單單位調校規則)
  - 無法判斷：證據不足
- 處理時效：一星期內

資安預警情報回報方式


教育機構資安通
回首頁
修改個人資料
登出
通報
通報/應變
自行通報
事件單處理狀態
歷史通報
事件附檔下載
資安預警事件
EWA編號
EWA事件單
ASOC-EWA-20
low
EWA事件單狀態
誤判
確實事件
無法判斷
事件單編號
原因
送出
台灣學術網路
完整資安預警(EWA)事件單訊息
回報資安預警(EWA)事件單的處理狀況

資安通報演練說明

教育部資安通報演練計畫

- 檢驗「教育機構資安通報平台」所登錄學校**資安聯絡人資料之正確性**
- 檢驗教網中心通報反應及處理能力機制是否完善
- 測試學術機關(構)分組資安聯絡人聯絡管道是否暢通
- 測試學校於發現資安事件時，是否可正確、快速執行通報作業
- 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

資安演練期程

- 演練資料整備作業:
  - 即日起至**112年9月1日止**，112年8月22日局端執行清查作業
  - 確認教育機構資安通報平台資安聯絡人資料更新
  - 確認教育機構資安通報平台資安長資料更新
  - 演練學校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，學校依序至少應填列2名資安聯絡人，並檢查資安聯絡人資料是否正確並完成密碼更新

資安演練期程

- 資安通報演練作業:
  - 112年9月4日至112年9月8日
  - 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。
  - 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，學校收到mail及簡訊通知後，於**1小時**內至教育機構資安通報演練平台完成事件通報及應變處理

教育機構通報演練平台網站

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

演練模擬事件類型

演練模擬資安事件情境

模擬狀況編號	攻擊事件說明
1	單位電腦被入侵，而成為 BotNet 所控制的 Bot 主機
2	單位內主機被植入勒索病毒，系統資料遭到加密
3	單位電腦系統被入侵，並進行挖礦惡意行為
4	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
5	單位內 IoT 設備使用預設帳號密碼，遭駭客入侵
6	單位電腦被入侵，並利用散佈垃圾郵件
7	單位內電腦被入侵，並被利用來進行遠端桌面(RDP)暴力攻擊
8	單位網站遭網頁置換，誘導使用者連線至詐騙網站
9	單位電腦系統被植入惡意程式，並對外進行 APT 攻擊
10	單位電腦遭入侵成為中繼站，接收惡意程式連線

・演練子類型會依前一年較常發生之類型進行更新，以演練計畫核定內容為主

演練模擬事件類型

模擬狀況編號	攻擊事件說明
1	學校單位於網站發布之公告中，因附件檔案含有學生個資(姓名、身分證字號等)未做遮蔽，造成個資外洩。
2	於 google 搜尋中的庫頁暫存檔，發現學校單位含學生個資檔案可供他人搜尋瀏覽，造成個資外洩。

資安通報聯絡人資訊

- 填報或行政諮詢:教育局阮小姐，(02)8072-3456#523
- 技術或網路查詢:資安駐點工程師鄧先生，(02)8072-3456#534
- 技術問題或忘記密碼:臺灣學術網路危機處理中心，(07)525-0211

Q&A