教育機構

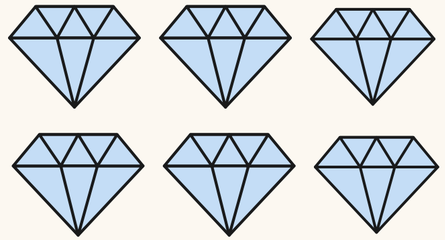
資安通報平台操作

#TACERT#2024.08.13
#新任資訊組長#基礎知能培訓研習

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

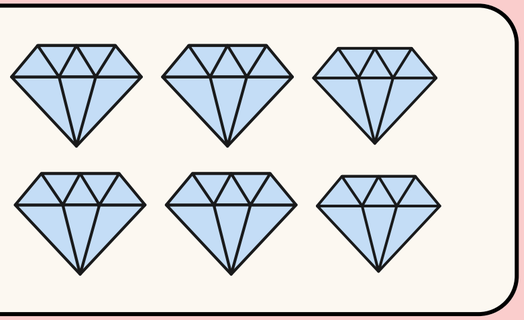
會員登入



- 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

如果忘記密碼怎麼辦??

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）

TACERT服務電話：(07)525-0211
如果忘記OID，也需同樣去電TACERT

密碼查詢功能因應教育部相關資安規範，將重設貴單位密碼為「8碼亂數密碼」並將重設後密碼將以簡訊及郵件通知貴單位所有人員，以達通知之成效。

請輸入下列資訊(需和平台內登記資料一致)	
OID碼	
Name (貴校資安聯絡人姓名)	
E-Mail (貴校資安聯絡人信箱)	
cellphone (貴校資安聯絡人手機)	
b49vx	請填入驗證碼
	送出

密碼查詢

以「重設8碼亂數密碼」，並以簡訊及電子郵件通知該聯絡人

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

教育機構資安通

會員登入

機關OID

登入密碼

qp2rg

請填入驗證碼 登入

密碼查詢

重大資安事件通報需知

學術網路危機處理中心

公告 帳密更新Q

教育部為求有效掌握及系統遭受破壞與不以確保各級教育機構通報功能及應變處理

公告事項

功能
新增通報應變欄位說
其它類型欄位說明
資安長欄位說明
資安通報審核確認欄
資安通報情資欄位說
資安通報平台通報應
個資隱私權宣告

登入畫面

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

登入畫面

事件單處理區

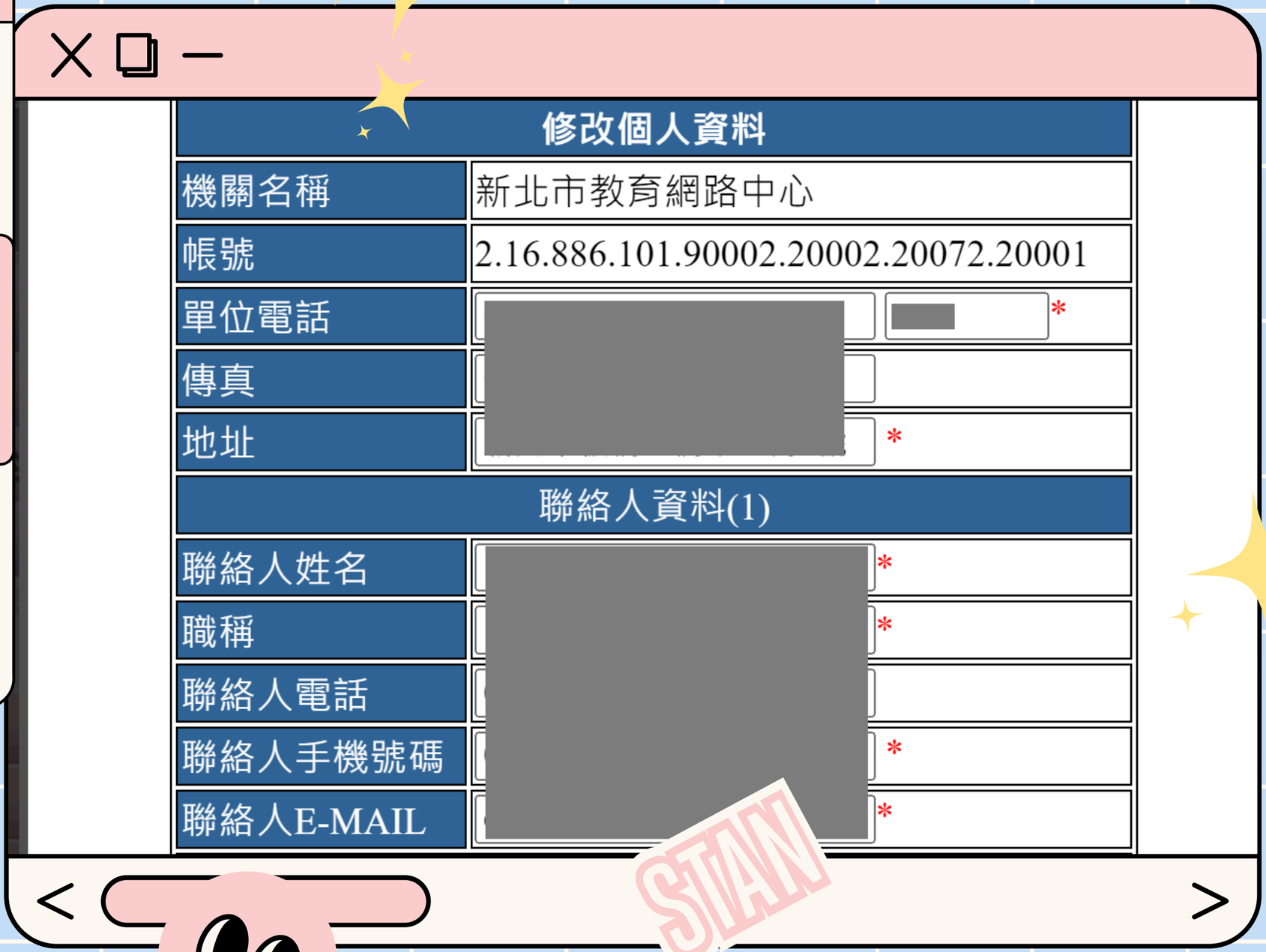
各功能說明

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

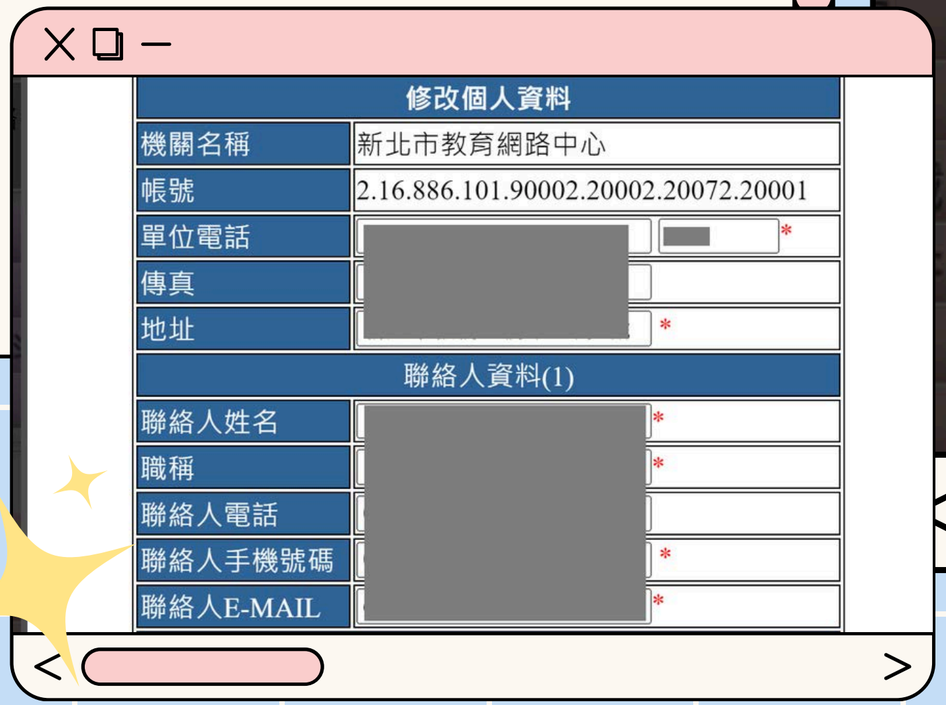
修改個人資料

- 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

- 個人基本資料區
- 密碼變更區
- 單位其他聯絡人資料區



LIKE

聯絡資訊

機關名稱:新北市教育網路中心
使用者:
主管機關:新北市教育網路中心
聯絡電話:
E-Mail:

回首頁
修改個人資料
修改資安長資料
登出

通報

事件單編號	發佈時間	距通報時間

Page 1/1

close or Esc Key

修改資安長資訊

資安長姓名	
資安長公務電話	
資安長公務EMAIL	

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。

修改資安長資訊

帳號管理功能

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

將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

注意事項

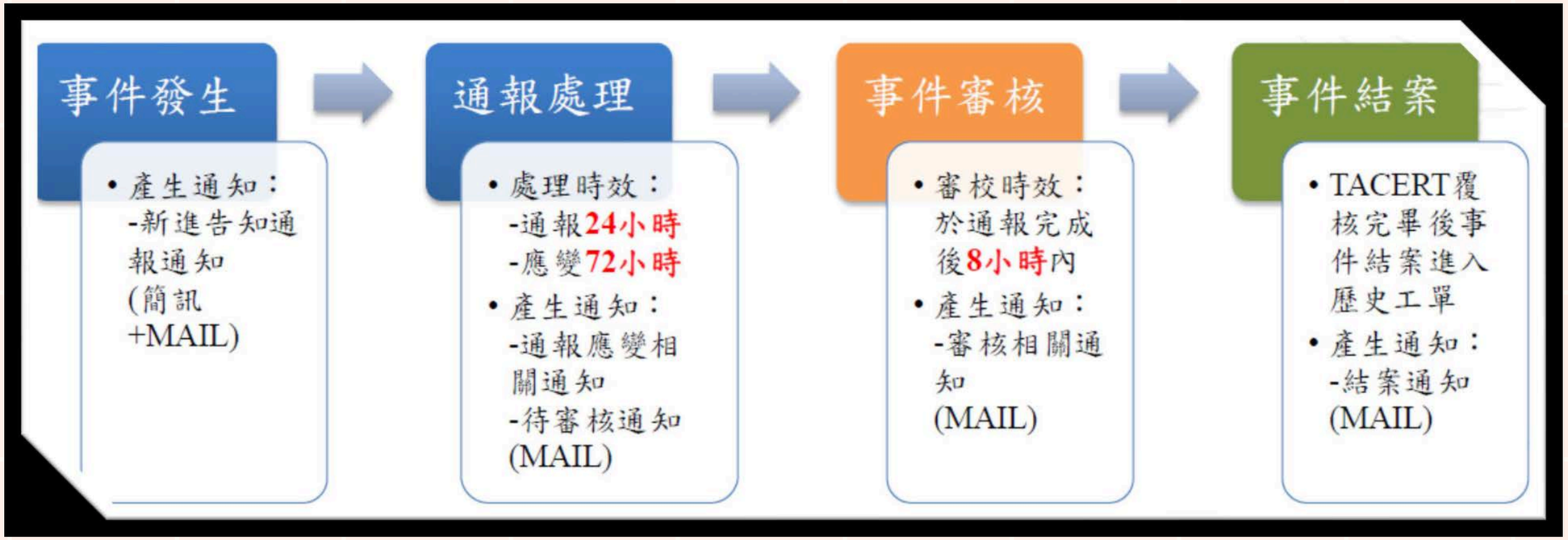
關於聯絡人資料

由於TACERT後台無法紀錄到兩位聯絡人各自的辦公室分機，因此辦公室分機的部分，請留第一聯絡人的分機即可。

事件單處理流程

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，請學校盡可能通報與應變同時進行。



資安等級1,2

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，請學校盡可能通報與應變同時進行。

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

資安等級3,4

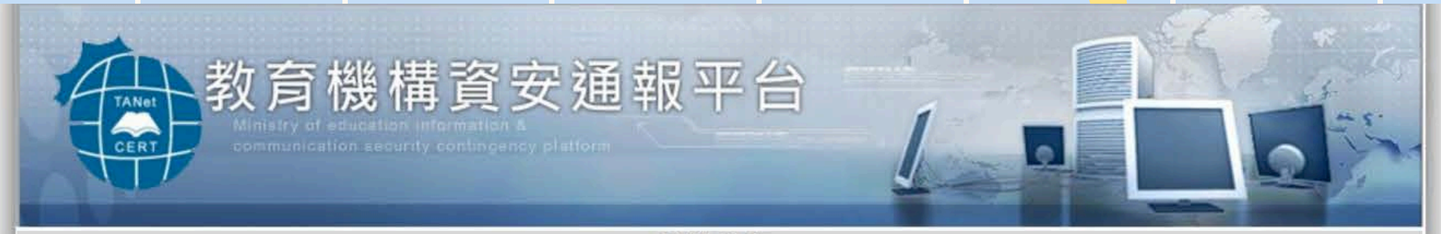
通報應變規劃重點

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，請學校盡可能通報與應變同時進行。

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
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

第3、4級資安事件	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)
	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

通報流程



聯絡資訊

機關名稱:新北市教育網路中心 使用者:	主管機關:新北市教育網路中心 聯絡電話: E-Mail:	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

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

填報時間為:2024-8-9 13:53:58

通報流程

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
欄位中不得輸入特殊符號，例如：「;」、「"」、「'」、「$」、「&」、「%」、「!」、「^」、「*」、「<」、「>」、「_」、「|」、「-」

1. 通報型態:	■主動通報(各單位自行發現資安事件)
2.◎確認(知悉)為資安事件時間:	2024-08-09 13:51:58
3. ◎事件發生時間：	
◎IP位置（IP address）：	範例: 120.114.22.33
◎網際網路位置（web-url）：	範例: https://www.xxx.edu.tw/cba.index
◎設備廠牌、機型：	範例1: 華碩TS100 E6 範例2: Acer AT110 F1
◎作業系統（名稱/版本）：	範例1:Centos Linux 5.4, 範例2: Windows XP SP2
◎受駭應用軟體（名稱/版本）：	範例: sendmail server，此為不確定版本的範例

通報流程

◎受駭應用軟體（名稱/版本）：

範例: sendmail server，此為不確定版本的範例

◎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：個人電腦

◎受害設備說明(150字內)：

範例: 同仁桌機

◎損害類別說明(150字內)：可用性損害

◎攻擊手法(150字內)：社交工程

◎調查說明(150字內)：

範例: 同仁誤執行惡意程式

◎情資類型：惡意內容

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：

INT（入侵型態）：
- 系統被入侵
- 對外攻擊
- 針對性攻擊
- 散播惡意程式
- 中繼站
- 電子郵件社交工程攻擊
- 垃圾郵件(Spam)
- 命令與控制伺服器(C&C)
- 殭屍電腦(Bot)

DEF（網頁型態）：
- 惡意網頁
- 惡意留言
- 網頁置換
- 釣魚網頁
- 資料外洩

FAC（設施問題）：
- 設備故障/毀損
- 電力異常
- 網路服務中斷
- 設備遺失
- 拒絕服務

通報流程

○ 資料外洩

○ FAC（設施問題）：
- 設備故障/毀損
- 電力異常
- 網路服務中斷
- 設備遺失
- 拒絕服務

◎破壞程度：(文字勿超過200中文字)

◎事件與處置說明：(文字勿超過200中文字)

5. 資通安全事件：影響等級及說明

1. 事件等級：取底下三個欄位中最高等級當成最後之事件等級
2. 第3、4級事件係屬於重大資安事件，教育部各長官需親自督導進度
3. 若有3、4級事件，請立刻電話告知您所屬的主管機關
4. 如果您無法確定如何填寫時，請電話連絡您所屬的主管機關請求協助
5. 等級0之資安事件教育部另有規範，請至少填入等級1

◎資安事件判斷：

(1) 機密性衝擊 -
- ◉ 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

(2) 完整性衝擊 -
- ◉ 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

通報流程

(2) 完整性衝擊 -

- (●) 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

(3) 可用性衝擊

- (●) 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

資安事件綜合評估等級：1級

◎可能影響範圍及損失評估　（文字勿超過200字）

6. ◎是否需要支援?

- ( ) 是
  你的上層機關負責人為: [redacted]
  聯絡電話: [redacted]
  E-mail: [redacted]
  期望支援方式:
  (●)電話告知 ( )Email告知
- (●) 否:通報單位自行解決

7. ◎是否同時進行通報流程與應變流程?

- (●) 是
  (請繼續完成 II.應變流程之作業)
- ( ) 否
  (會先完成 I.通報流程 並結束，後續時間請儘快完成 II.應變流程)

應變流程

通報流程

○ 是
你的上層機關負責人為: [redacted]
聯絡電話: [redacted]
E-mail: [redacted]
期望支援方式:
◉電話告知 ○Email告知

◉ 否:通報單位自行解決

7. ◎是否同時進行通報流程與應變流程?

◉ 是
(請繼續完成 II.應變流程之作業)

○否
(會先完成 I.通報流程 並結束，後續時間請儘快完成 II.應變流程)

應變流程

◎1. 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

◎2. 解決辦法： (文字勿超過200中文字)

◎3.完成損害控制時間：

◎4. 損害控制狀態： 是：完成損害控制

改善措施

◎改善辦法： (文字勿超過200中文字)

依資通安全相關管理規範進行改善措施

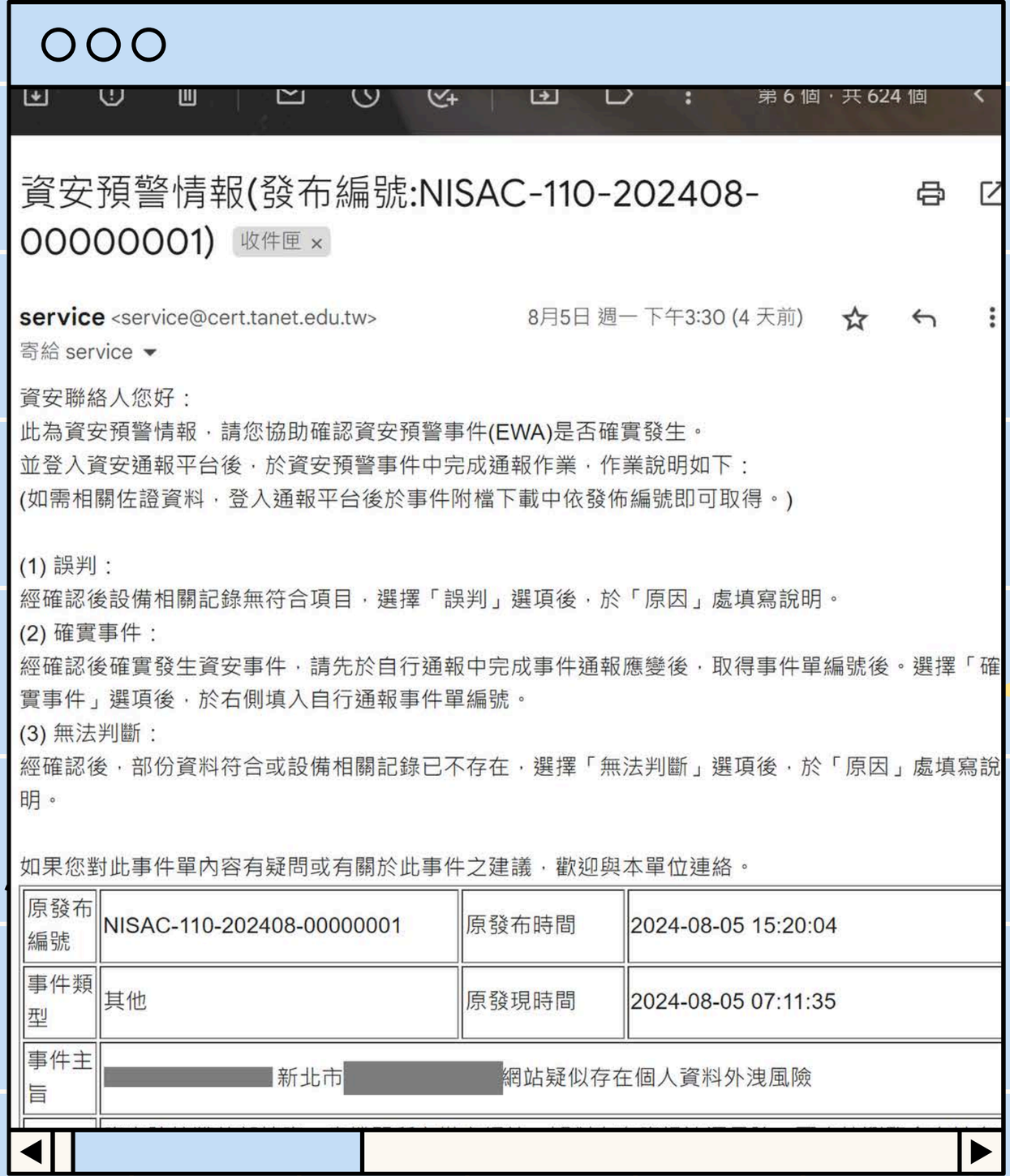
◎ 改善時間： 2024-08-23 13:51:58

發佈通報

台灣學術網路危機處理中心(TACERT)

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
- 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



第 6 個，共 624 個

資安預警情報(發布編號:NISAC-110-202408-00000001) 收件匣 ×

service <service@cert.tanet.edu.tw> 8月5日 週一 下午3:30 (4 天前)

寄給 service

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	NISAC-110-202408-00000001	原發布時間	2024-08-05 15:20:04
事件類型	其他	原發現時間	2024-08-05 07:11:35
事件主旨	[redacted] 新北市 [redacted] 網站疑似存在個人資料外洩風險		

登入畫面

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

資安預警情報

處理時效:一星期內

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:

誤判

確實事件:先於通報平台採『自行通報』取得事件單編號

確實預警(未造成損害)

無法判斷:請詳填原因(以利發單單位調校規則)

佈時間	2024-08-05 11:00:11
發生時間	2024-08-05 02:50:08
受害IP	[redacted]
受害網址	
事件分類	系統弱點
主旨	[新北市[redacted]]貴單位所屬IP([redacted])網路印表機OTHER login by default password
說明	ASOC發現貴單位(新北市[redacted])所屬[redacted]網路印表機KYOCERA Command Center RX TASKalfa 4052ci(J) OTHER login by default password
手法研判	

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:

誤判

確實事件:先於通報平台採『自行通報』取得事件單編號

確實預警(未造成損害)

無法判斷:請詳填原因(以利發單單位調校規則)

主旨	IP([redacted])網路印表機OTHER login by default password
說明	ASOC發現貴單位(新北市[redacted])所屬[redacted]網路印表機KYOCERA Command Center RX TASKalfa 4052ci(J) OTHER login by default password
手法研判	
應變措施	請確認該裝置是否需要讓外部IP存取，並檢視防火牆規則，避免非經授權之系統存取；若否，則建議移至內部網路並限制特定IP才可管理該系統與使用服務。 評估系統上非必要的服務或程式建議移除或關閉。
參考資訊	

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		

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:

誤判

確實事件:先於通報平台採『自行通報』取得事件單編號

確實預警(未造成損害)

無法判斷:請詳填原因(以利發單單位調校規則)

8月23日前
更新資安通報平台資訊、密碼
8月26-30日局端檢查
9月2日開始資安演練