

教育機構資安通報平台 通報應變流程修正說明



前言

- 資通安全管理法經立法院於107年5月三讀通過後，行政院對外公告於**108年1月1日**施行。
- 為符合資通安全管理法相關規定，TACERT團隊執行「教育機構資安通報平台」內容相關修正。
- 下列將針對相關修正項目進行說明



修正重點

新增「確認時間」

- 於通報流程中新增「**確認時間**」欄位，以利記錄事件確認時間。

新增「改善措施」

- 於應變流程中新增「**改善措施**」欄位，以利處理人員填寫事件改善措施。

新增「事件列印」

- 於事件通報應變完成後，於「**歷史通報**」中新增「**事件列印**」功能，以利處理人員列印事件內容送呈單位主管

修正時程

- 此次修正項目預計於**108年09月01日(日)**上線，上線後依據相關修正進行通報應變作業。



修正依據

資通安全事件通報及應變辦法

- 依據資通安全管理法之資通安全事件通報及應變辦法**第二章第四條**規定：
 - 公務機關**知悉**資通安全事件後，應於**一小時**內依主管機關指定之方式及對象，進行資通安全事件之通報
- 依據資通安全法之資通安全事件通報及應變辦法**第三章第十一條**規定：
 - 特定非公務機關**知悉**資通安全事件後，應於**一小時**內依中央目的事業主管機關指定之方式，進行資通安全事件之通報

臺灣學術網路各級學校資通安全通報應變作業程序

- 依據臺灣學術網路各級學校資通安全通報應變作業程序第三章第一節第二條規定：
 - 各連線單位發現資安事件後可先進行事件確認，經確認為資安事件後，須於**一小時**內，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。



相關修正說明



確認時間修正說明

新增「確認時間」

- 於現行通報流程填寫欄位新增「**確認時間**」欄位
- 確認時間指各連線單位發現資安事件後可先進行事件確認，經確認資安事件條件成立之時間
- 事件通報流程需於確認時間後**1小時內**完成
- 事件通報應變時效不因新增確認時間而改變，
「1」、「2」級事件需於**72小時內**完成；
「3」、「4」級事件需於**36小時內**完成。



現行通報應變時程

事件發生
時間

事件發佈
時間

通報完成
時間

應變完成
時間

通報時間
(通報完成時間-
事件發佈時間)

應變時間
(應變完成時間-
通報完成時間)

事件處理時間



修正後通報應變時程

事件發生
時間

事件發佈
時間

**事件確認
時間**

通報完成
時間

應變完成
時間

確認時間

通報時間
(於1小時內)

應變時間

事件處理時間



確認時間畫面

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: 告知通報

2.⊙事件發生時間: 2019-04-30 14:47:31

3.⊙確認時間: 2019-05-30 09:17:50

140.117.101.171 顯示

為因應資安法的規定，需於確認時間後一小時內通報

確定

提示訊息



改善措施修正說明

新增「改善措施」

- 於現行應變流程填寫欄位新增「**改善措施**」欄位
- 改善措施指各連線單位於完成通報應變後，針對事件發生提出相關改善措施，以完備事件處理流程及預防事件重覆發生
- 改善措施包含「**改善辦法**」及「**改善時間**」欄位



改善措施畫面

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，標點符號請用全形)

◎3. 解決時間：

改善措施

◎改善辦法： (文字勿超過200中文字，標點符號請用全形)

依資通安全相關管理規範進行改善措施

◎改善時間：

2019-05-24 14:37:36



事件列印修正說明

新增「事件列印」

- 依據臺灣學術網路各級學校資通安全通報應變作業程序第三章第一節第六條規定：
 - 「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。
- 於登入「教育機構資安通報平台」後，左側「**歷史通報**」中即可套表列印貴單位事件單以利送呈簽核



事件列印畫面


教育機構資安通報平台
Ministry of education information & communication security contingency platform

聯絡資訊

[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](#)
[情資資料下載](#)

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)



事件列印畫面


教育機構資安通報平台
Ministry of education information & communication security contingency platform

聯絡資訊

[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](#)
[情資資料下載](#)

開始日期: 結束日期:

第一頁 | 上一頁 | 下一頁 | 最尾頁

事件單編號	單位	來源	等級	IP	發佈時間	結束時間
120553		列印	1級		2017-09-03 13:40:19	2017-09-05 16:00:48
119749		列印	1級		2017-08-22 14:10:24	2017-08-23 14:38:13
53335		列印	N-ASOC 1級		2015-04-24 10:11:12	2015-04-24 16:29:07
39053		列印	N-ASOC 1級		2014-06-10 10:38:05	2014-06-10 11:58:30
32023		列印	N-ASOC 1級		2014-01-02	2014-01-02

台灣學術網路危機處理中心(TACERT)



事件列印畫面

◎緊急應變措施：

已中斷網路連線，待處理完成後再上線

解決辦法：

中斷機器對外連線，待處理完成後再上線。

解決時間：

2019-04-22 12:55:56

◎改善措施：

改善辦法：

改善時間：

1999-01-01 00:00:00

套表簽核欄位

承辦人：

單位主管：

資安長官：



重點整理

新增「**確認時間**」並於事件確認後**一小時內**完成通報流程

新增「**改善措施**」以完備事件處理流程

新增「**事件列印**」以利送呈簽核

修正項目於**108年09月01日(日)**上線



重點提醒

因應「**資通安全管理法**」及其相關辦法
與「**臺灣學術網路各級學校資通安全通
報應變作業程序**」進行相關修正作業

各單位務必掌握時效依照相關規定完成
通報應變作業，以避免相關刑事、民事
及行政相關責任。

