福和國中資安通報應變手冊

壹、 事件等級說明及處理原則

底下針對教育部所使用的事件等級加以說明。

（一）4 級事件:

符合下列任一情形者，屬 4 級事件：

1. 國家機密資料遭洩漏。
2. 國家重要資訊基礎建設系統或資料遭竄改。
3. 國家重要資訊基礎建設運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作。

（二）3 級事件

符合下列任一情形者，屬 3 級事件：

1. 密級或敏感公務資料遭洩漏。
2. 核心業務系統或資料遭嚴重竄改。
3. 核心業務運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作。

案例 1：98 年 x 月 y 日某中學，發現兩名學生撬開教務處窗戶入侵，盜用各辦公室電腦， 利用燒片、拷貝等方式，竊走全校學生詳細個資及全校教職員個資與帳號密碼， 並利用此帳號密碼入侵學務系統，竄改學籍資料與成績，犯罪行為持續年餘，因 該生已影響學校學務系統並涉及個資法，具符合上述條款(1).密級或敏感公務資 料遭洩漏範圍擴及全校與(2).核心業務系統或資料遭嚴重竄改，故判定為 3 級資 安事件

案例 2:96 年 x 月 y 日某大學，因空調水塔缺水，使得機房溫度升高，造成伺服器及網 路設備當機，機房營運中斷，此符合上述條款(3)核心業務運作遭影響或系統停 頓，無法於可容忍中斷時間內回復正常運作，故判定為 3 級資安事件。

（三）2 級事件

符合下列任一情形者，屬 2 級事件：

1. 非屬密級或敏感之核心業務資料遭洩漏。
2. 核心業務系統或資料遭輕微竄改。
3. 核心業務運作遭影響或系統效率降低，於可容忍中斷時間內回復正常運

作。

案例 1:99 年 x 月 y 日某大學資料庫主機中教職員工帳號資料表，疑似遭 SQL Injection 值入 javascript 字串，導致部份系統無法正常登入，調用備份之資料，還原資料表，僅 影響數筆資料，此符合上述(2).核心業務系統或資料遭輕微竄改與(3).核心業務運作遭 影響或系統效率降低，於可容忍中斷時間內回復正常運作，故判定為 2 級資安事件。

案例 2:98 年 9 月 12 日某大學，遭到入侵並安裝惡意程式，得暫時關閉 web，影響部份 網頁收信功能，此符合上述(3).核心業務運作遭影響或系統效率降低，於可容忍中斷時 間內回復正常運作，故判定為 2 級資安事件。

（四）1 級事件

符合下列任一情形者，屬 1 級事件：

1.非核心業務資料遭洩漏。

2.非核心業務系統或資料遭竄改。

3.非核心業務運作遭影響或短暫停頓。

案例 1:99 年 x 月 y 日某國小，發現科任教室教學電腦被植入惡意程式，經修復後移除 惡意程式無損失，此符合(2).非核心業務系統或資料遭竄改，故判定為 1 級資安事件。

案例 2:99 年 x 月 y 日某大學，發現學務處一般行政用主機，使用者電腦有異常的情形 發生且無法使用防毒軟體移除病毒，於資料備份後重新安裝作業系統，已上線使用中， 此符合上述條件(1).非核心業務資料遭洩漏、(2).非核心業務系統或資料遭竄改與(3). 非核心業務運作遭影響或短暫停頓，故判定為 1 級資安事件。

（五）0 級事件(資安預警) 凡屬於下列工單皆屬於 0 級事件

1.未確定事件或待確認工單:來自不同計畫所使用新型技術所產生之工單，但其正確性有待確認。

2.其他單位所告知教育部所屬單位所發生未確定之資安事件。

3.教育部及區、縣網路中心檢舉信箱通告之資安事件。

貳、 學校通報教育機構原則

1.通報作業：若發現資安事件後需於 1 小時內通報完成。

2.應變處理作業：

(1)事件級別為 0、1、2 級資安事件需於 72 小時內處理完成並結案(包括通報流程與應 變流程)。

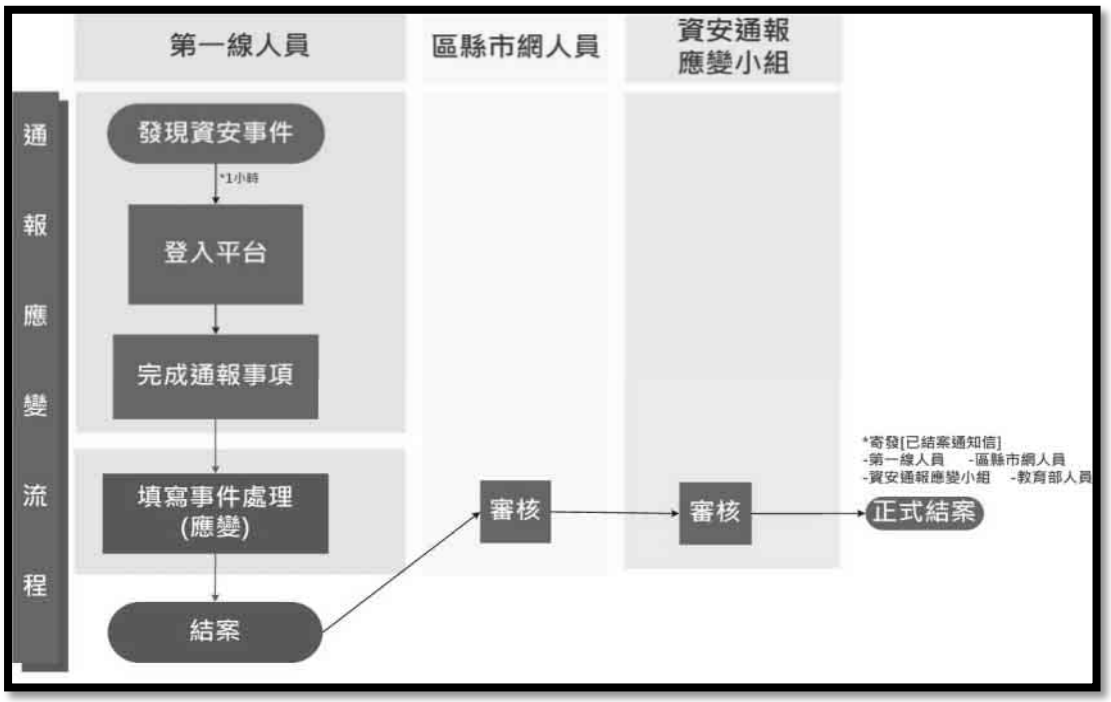
(2)事件級別為 3、4 級資安事件需於 36 小時內處理完成並結案(包括通報流程與應變流程)。

參、 學校通報教育機構自行通報流程

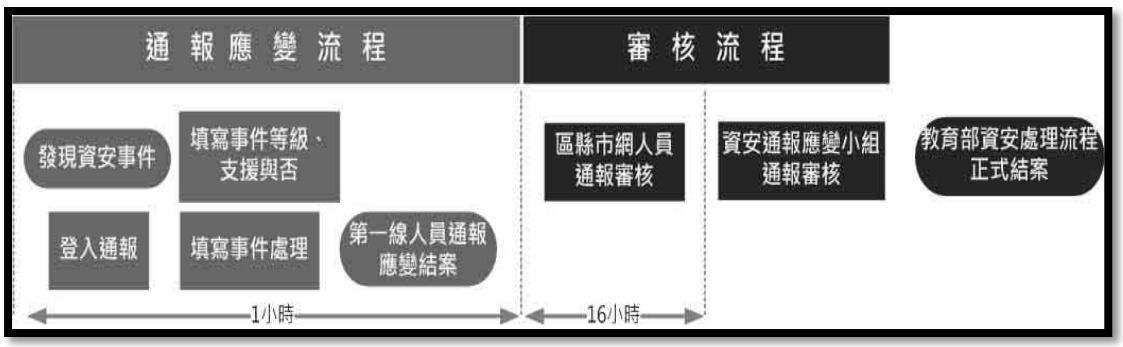
通報流程參考 TANet 自行通報處理流程之標準作業程序,首先自行通報可以是【第一線人員:資訊組長】自行發現問題時必主動向上級報告。不管是那一級資安事件，當第一線人員發現事件時須於 1 小時 內登入通報平台完成通報此事件。若為 3-4 級因事態嚴重，須電話通知上層管理(教務及總務主任、校長、教研中心)，落實緊急通報。

一、 【自行通報】(1、2 級)處理流程

處理流程圖如下：



處理時限如下:



通報流程說明：

登入通報平台進行通報應變作業

【第一線人員:資訊組長】自行發現資安事件時，先通報教務及總務主任，登入通報平台進行資安處理作業。

通報平台網址為：https://info.cert.tanet.edu.tw/prog/index.php

▸注意事項

第一線人員:資訊組長發現資安事件時,須於 1 小時內登入通報平台完成通報此資安事件。

▸說明事項

1. 資安事件說明包含受害之系統 IP 等基本資料

(1)事件等級: 因係 1-2 級通報，故無須電話告知【市網人員】。

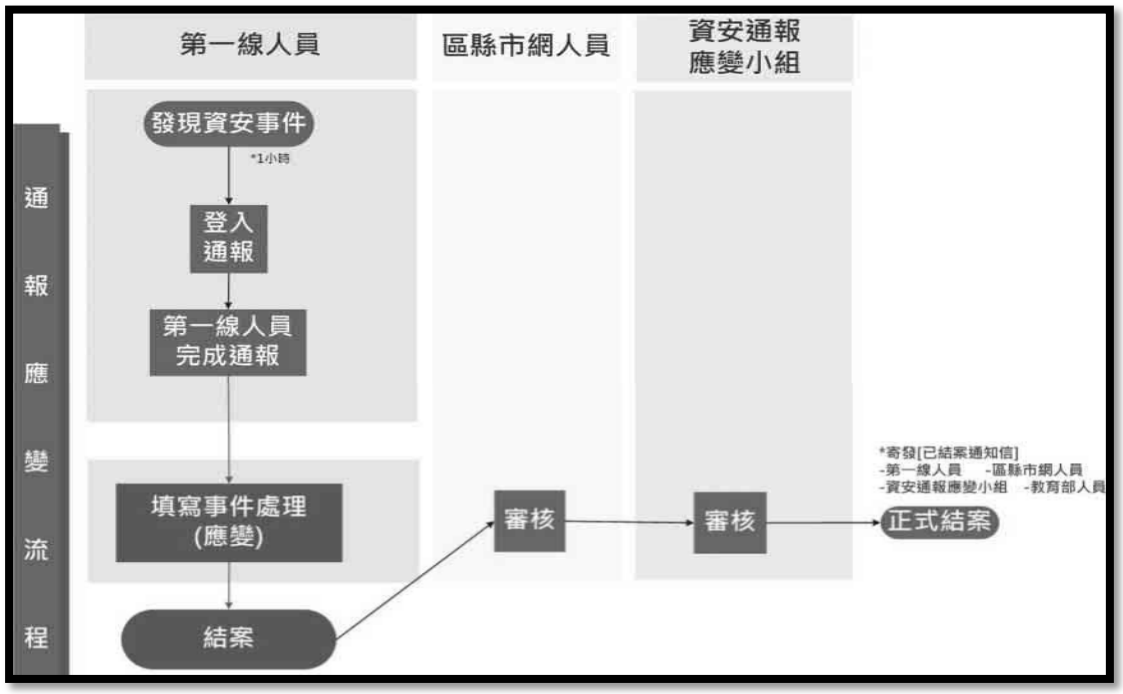
(2)是否需支援:若需支援，則主動電話聯繫市網人員請求協助。

2.【第一線人員:資訊組長】填完成通報流程後，繼續填寫應變流程，按發佈通報 結案，便已完成【第一線人員:資訊組長】之通報應變，此時間即為通報應變完成時間。

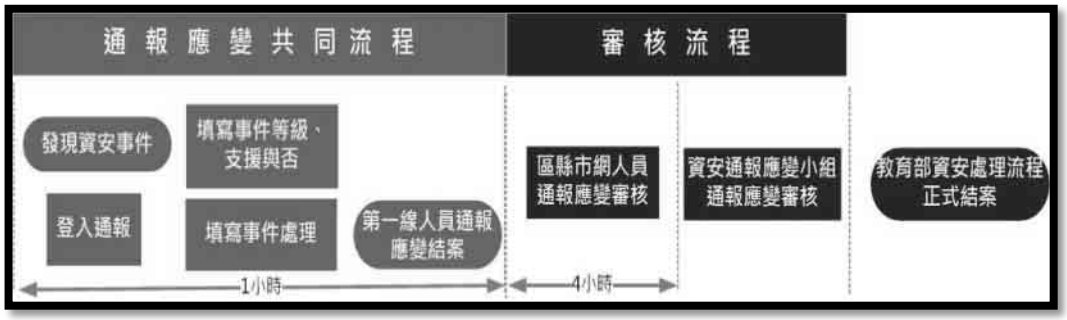
3. 完整之通報仍待【市網人員】與【教育機構資安通報應變小組】審核結果。

二、 【自行通報】(3、4 級)處理流程

處理流程圖如下：



處理時限如下:



通報流程說明：

登入通報平台進行通報應變作業

【第一線人員:資訊組長】自行發現資安事件時，先通報教務及總務主任，登入通報平台進行資安處理作業。

通報平台網址為：https://info.cert.tanet.edu.tw/prog/index.php

▸注意事項

第一線人員:資訊組長發現資安事件時,須於 1 小時內登入通報平台完成通報此資安事件。

▸說明事項

1. 資安事件說明包含受害之系統 IP 等基本資料

(1)事件等級: 因係 3-4 級通報須電話告知【市網人員】及【教育機構資安通報應變小組】。

(2)是否需支援:若需支援，則主動電話聯繫市網人員請求協助。

2.【第一線人員:資訊組長】填完成通報流程後，繼續填寫應變流程，按發佈通報 結案，便已完成【第一線人員:資訊組長】之通報應變，此時間即為通報應變完成時間。

⇨【第一線人員:資訊組長】完成通報應變流程之時間即為回報給行政院之通報完成時間與應變完成時間(兩時間相同)。

肆、學校內部通報流程

學校內部的通報程序，由本校網站經由校務行政帳號認證後，至「修繕登記」區登錄，資訊組即會派人處理，若無法處理，或找不出原因，則進行前述之通報流程。

內部通報流程說明：

1. 至學校首頁點擊右上角登入按鈕

2. 選擇使用 SSO 認證登入

3. 點選修繕登記(新)

4. 進行資安及設備維修填報