《桃園縣立永豐高中發生資安事件之處理程序》

目前主要有三個途徑得知事件發生：教育部或縣網收到檢舉信件、教育部或縣網自行發現封鎖並通知學校、學校端自行發現處理後回報。以下依回報方式分兩類說明步驟：

一、 需回報「教育機構資安通報平台」：

主要有這四項：遭植入惡意程式碼、網路釣魚(網路詐騙)、遭植入惡意程式、遭受惡意入侵。在得知相關情形後，請依下列程序處理：

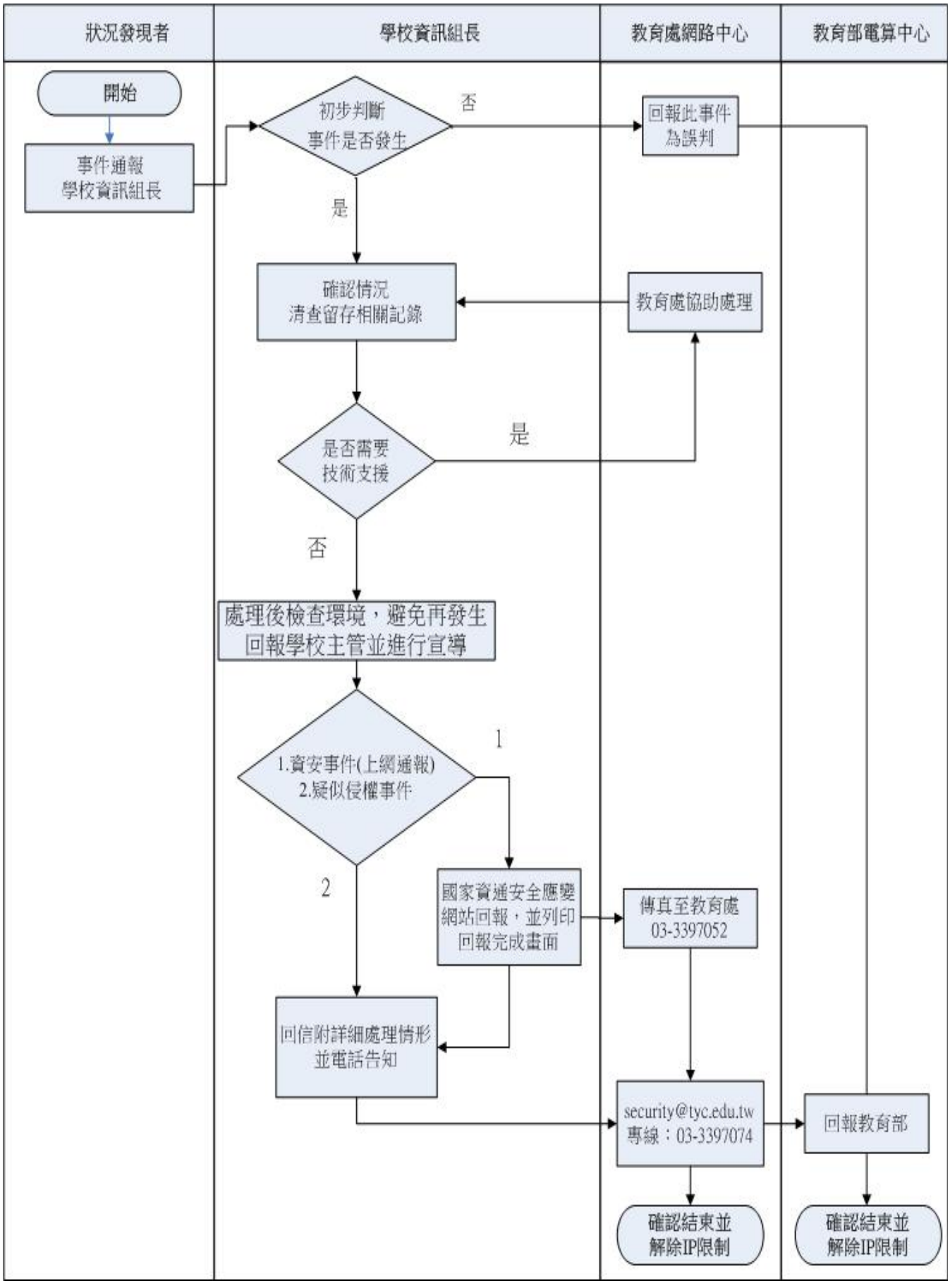
1. 保存相關檔案：第一時間了解情況，清查並留存相關記錄(惡意程式檔案或相關網頁原始碼，以及相關登入記錄，足以證明者)。
2. 修復並檢查系統環境：移除檔案以及修正有問題的帳號密碼、登入方式，檢查目前系統環境是否仍有同樣問題可能造成資安事件再次發生。例：帳密太簡單、網頁上傳權限問題等。
3. 回報：向學校主管回報詳細狀況。
4. 教育機構資安通報平台網站通報：請在 24hr 內，至教育機構資安通報平台網站(https://info.cert.tanet.edu.tw/)回報處理情形並結案。
5. 傳真回報完成畫面：請列印回報完成畫面傳真至縣網中心(3397052)。
6. 回信及電話通知：請回信至 security@tyc.edu.tw 並附上詳細處理經過，以及電話通知處理情形(03-3397074)，俾利本局處理人員儘快回報教育部，協助解除連網限制。
7. 資安觀念宣導：加強校內相關資安觀念宣導。

二、 疑似違反智慧財產權之事件：

主要有這三項：非法 FTP 站、非法 P2P 傳輸、非法交換平台。在得知相關情形後，請依下列程序處理：

1. 保存相關檔案：第一時間了解情況，清查並留存相關記錄(惡意程式檔案或相關網頁原始碼，以及相關登入記錄，足以證明者)。
2. 修復並檢查系統環境：移除檔案及相關軟體，或修正相關帳號密碼，並檢查目前環境是否仍有問題可能造成資安事件再次發生。
3. 回報：向學校主管回報詳細狀況。
4. 回信及電話通知：請回信至 security@tyc.edu.tw 並附上詳細處理經過，以及電話通知處理情形(03-3397074)，俾利本局處理人員儘快回報教育部，協助解除連網限制。
5. 資安及智慧財產權觀念宣導：加強校內相關資安觀念及智慧財產權觀念宣導。

資安事件處理流程圖：


狀況發現者
學校資訊組長
教育處網路中心
教育部電算中心
開始
事件通報
學校資訊組長
初步判斷
事件是否發生
否
是
回報此事件
為誤判
確認情況
清查留存相關記錄
教育處協助處理
是否需要
技術支援
是
否
處理後檢查環境，避免再發生
回報學校主管並進行宣導
1.資安事件(上網通報)
2.疑似侵權事件
1
2
國家資通安全應變
網站回報，並列印
回報完成畫面
傳真至教育處
03-3397052
回信附詳細處理情形
並電話告知
security@tyc.edu.tw
專線：03-3397074
回報教育部
確認結束並
解除IP限制
確認結束並
解除IP限制