私立南強高級工商職業學校網路攻擊行為處理機制

一、通報資料來源：

1.教育部電算中心網路封包偵測系統(http://192.83.166.30/?open)

2.縣網流量分析主機病毒偵測系(http://enctc.tpc.edu.tw/files/11-1000-68.php)

3.上層管理單位或其他 user 反映網路攻擊事件之通報

4.本校自行建置之網路攻擊偵測系統

二、處理方式：

1.將該主機之網路線拔除或設定 router（switch、firewall）之 ACL 以限制其進出校園網路。

2.查明是校內正常服務之主機，還是一般使用者的電腦。

（1）服務主機之處理方式：

查明是否中毒

修補系統漏洞

查明是否遭到入侵

查明是否主機內帳號密碼被盜用

（2）一般電腦之處理方式：

查明是否中毒

修補系統漏洞

查明是否遭到入侵

三、後續處理及回報：

1.處理過程中，若有困難或疑問，請求縣網中心網路組協助處理。

2.若有惡意架站者，則依「校園網路使用規範」處理。

3.完成後，插回網路線或解除校內限制，並連絡縣網中心網路組協助測試。

4.測試完成後，將發生經過與處理情形通報本校行政主管。

5.若遭到上一層網管人員限制進出 TANet，通報該上級單位處理結果，以便解除限制。

私立南強高級工商職業學校廣告信件行為處理機制

一、電子郵件主機設定：

1.建立電子郵件帳號，供使用者檢舉廣告信件。

2.關閉各伺服主機 Open-Relay 功能，使本校主機不致成為他人之廣告發信機。

3.僅提供學校行政單位公用之電子郵件，集中管理。

二、廣告信通報資料來源：

1.教育部電算中心廣告信處理網頁 (http://140.111.1.22/tanet/spam.html)

2.本縣縣網路中心資訊安全網 (http://enctc.tpc.edu.tw/files/11-1000-88.php)

3.上級管理單位或其他使用者反映廣告信件之通報

三、處理方式：

1.將該主機之網路線拔除或設定路由器(Router)以限制其進出校園網路。

2.查明是校內正常服務之郵件主機，還是一般使用者的電腦。

郵件主機之處理方式：

（1）查明發信來源是否未設限(Open Relay)，若是，則設定限制發信來源為校內。

（2）查明是否中毒

（3）查明是否主機內帳號密碼被盜用

（4）查明是否遭到入侵

（5）修補系統漏洞

非郵件主機及一般電腦之處理方式：

（1）查明 SMTP Service 是否未關閉

（2）查明是否中毒

（3）查明是否主機內帳號密碼被盜用

（4）查明是否遭到入侵

（5）修補系統漏洞

四、後續處理及回報：

1.處理過程中，若有困難或疑問，請求本縣教育網路中心協助處理。

2.本校教職員生惡意架站或發送廣告信件經調查屬實後，依據校園網路使用規範處理。

3.完成後，插回網路線或解除校內限制，並連絡本縣教育網路中心協助測試。

4.測試完成後，將發生經過與處理情形通報本校行政主管。

5.若遭到上一層網管人員限制進出 TANet，通報該上層單位處理結果，以便解除限制。