臺南市市立新泰國民小學

資訊安全線上評量結果報告

製作日期：102 年 12 月 15 日

一、目的

為加強本市各國民中小學資通安全防護作業，實施資安內部稽核，以瞭解各校資通安全工作落實現況及未來可強化之方向，並確保資料、系統、設備及網路安全無虞，符合國家資通安全作業流程。

二、依據

（一）教育部102年度教育部對各地方政府統合視導訪視紀錄表。

（二）教育部國中、小學資通安全管理系統實施原則。

三、辦理單位

主辦單位：臺南市政府教育局

四、稽核對象

臺南市市立國民中小學

五、稽核日期

自民國102年11月起至102年12月止

六、稽核項目

（一）資訊安全管理規範

（二）網路安全

（三）系統安全

（四）實體安全

（五）人員安全

（六）相關法規與施行單位政策之符合性

七、稽核方式

（一）第一階段：

將資安文件佐證資料上傳至「教育部全國國中小學資訊安全管理系統」網址：http://isas.test.ntpc.edu.tw/，進行自評。

（二）第二階段：

由資安管理制度審查小組成員進行線上審查，審查後給予各校一份稽核報告書。

審查結果有缺失及改進意見之受檢單位，分析問題發生之原因及影響程度，填寫「矯正與預防處理單」，並依據「矯正與預防處理單」上之項目，進行改善並於1個月內提供改善佐證文件，紙本經機關首長核章後，郵寄一份至本局資訊中心備查。

（三）第三階段：

抽查5-10所學校，辦理到校資安訪視（日期另訂），由資安管理制度審查小組，到校確認各校落實程度。

八、稽核程序

（一）資安管理制度審查小組得依本計畫及賦予之業務職掌，至各受檢單位進行實地資通安全稽核與文件審閱。

（二）資安管理制度審查小組於資安訪視作業完成後，應填寫資訊安全內部稽核記錄表，並由受檢人員及單位主管確認簽章後，攜回本局資訊中心。

（三）資安管理制度審查小組需持續追蹤各校改善情形，彙整資料予本局資訊中心，並作為下次檢查重點。

九、稽核結果處理

（一）作為本局系統推動評估、資訊漏洞防堵及電腦設備配置之參考。

（二）受檢單位於接獲稽核報告後，最晚於1個月內完成缺失分析原因及擬採行之矯正與預防措施，並填寫「矯正與預防處理單」並經單位主管核定後回覆資安管理制度審查小組。

（三）資訊安全內部稽核報告由本局資訊中心依相關規定歸檔備查。

十、行政支援事項

（一）實施稽核得調閱有關資料、實地測試或檢查資訊軟、硬體設備使用情形，並請受檢單位相關作業人員提出說明。

（二）受檢單位、個人對於資安管理制度審查小組實施稽核時，應充分配合執行。

十一、評定標準

訪視評定以「符合」、「部分符合」、「不符合」或「不適用」作為評比標準。

以下為評定標準定義：

（一）符合：

1.實際作業依照書面規範進行；紀錄及審核皆按照規定辦理。

2.已建立書面規範，但尚未有實際作業或紀錄。

（二）部分符合：

1.雖按照規範執行作業，但於過程中發生疏失或無相關書面紀錄。

2.作業流程尚有改善空間。

（三）不符合：

1.尚未規劃或執行相關安全管理規定。

2.違反自訂之管理規範。

3.違反教育部或本局之資安相關規範之要求。

（四）不適用：貴校之現行作業無相關作業需求。

十二、線上評量結果：

十三、學校背景資料

序	項目內容	填答
未填報		

十四、線上評量檢查表

受評量單位：臺南市新泰國小　評量人員：郭子誠　評量日期：102年12月15日
自評結果：71分　　評量結果：64.5分

評量項目	自評	評量結果	執行現況或改善建議
一、資通安全管理規範			

01.訂定學校資通安全管理規範	部分符合	符合	
二、網路安全			
02.學校與外界連線，是否僅限於經由教育局網路管理單位之管控，以符合一致性與單一性之安全要求？	符合	符合	
03.是否禁止使用私自連線（如：電話線、2G或3G網路等）以連結主機電腦或網路設備？	符合	符合	
三、系統安全			
04.學校主機電腦是否依個別應用系統之需要，設置專屬電腦，例如網路服務主機（電子郵件、網站主機）、教學系統主機（例如隨選視訊主機）？ (1)裝置防毒軟體，將軟體設定為自動定期更新病毒碼；或由伺服器端進行病毒碼更新的管理。 (2)定期（至少每個月）進行如「Windows Update」之程式更新作業，以防範作業系統之漏洞。 (3)瀏覽器之安全性設定中網際網路的安全性須設定為中安全性以上。	符合	符合	附件做的很清楚,符合。
05.學校內的個人電腦是否進行以下設定？ (1)裝置防毒軟體，將軟體設定為自動定期更新病毒碼；或由伺服器端進行病毒碼更新的管理。 (2)定期（至少每個月）進行如「Windows Update」之程式更新作業，以防範作業系統之漏洞。 (3)瀏覽器之安全性設定中網際網路的安全性須設定為中安全性以上。	符合	符合	
06.學校內個人電腦所使用的軟體是否均有授權？	符合	符合	
07.新系統啟用前，是否經過掃毒與更新系統密碼程序，以防範可能隱藏的病毒或後門程式？	符合	符合	
08.學校(或委託)系統管理人員是否針對學校重要系統（例如：系統檔案、應用系統、資料庫等）定期進行備份工作，或採用自動備份機制？（建議週期為每週至少進行一次）	符合	符合	
09.學校(或委託)系統管理人員是否針對敏感度高、或包含特殊資訊的電腦系統進	部分符合	部分符合	

行檢查、維護、更新等動作時，應針對這些活動填寫日誌（書面或系統的log）予以紀錄，作為未來需要時之檢查？ (1)系統例行檢查、維護、更新活動的起始時間。 (2)紀錄日誌項目人員姓名與簽名欄。			
10.學校內所共用的個人電腦是否以特定功能為目的，並設定特定安全管控機制（例如限制從網路非法下載檔案行為、限制自行安裝軟體行為、限制特定資料的存取等）。	符合	符合	
11.學校是否制定電腦系統的使用者註冊及註銷程序，透過該註冊及註銷程序來控制使用者資訊服務的存取？該作業是否包括以下內容？ (1)使用唯一的使用者識別碼（ID）。 (2)檢查使用者是否經過系統管理單位之授權使用資訊系統或服務。 (3)保存一份包含所有識別碼註冊的記錄。 (4)使用者調職或離職後，應移除其識別碼的存取權限。 (5)定期（建議每學期）檢查並取消多餘的使用者識別碼和帳號。 (6)定期（建議每學期）檢查新增之帳號，若有莫名帳號產生，應關閉帳號權限，並依通報程序請求處理。	部分符合	部分符合	若能附上實際處理畫面,或相關處理記錄表單會更好。
12.學校的電腦與網路系統資訊具有存取特權人員清單、及其所持有的權限說明，是否予以文件化記錄備查？	不符合	不符合	附件無法佐證。
13.管制使用者第一次登入系統時，是否立即更改預設通行碼？預設通行碼是否設定有效期限？	部分符合	部分符合	
14.資訊系統登入帳號與服務是否避免使用共同帳號及通行碼？	未填		
15.由學校發佈通行碼（Password）制定與使用規則給使用者，內容是否包含以下項目？ (1)使用者應該對其個人所持有通行碼盡保密責任。 (2)要求使用者的通行碼設定，應該包含英文字、數字、特殊符號，長度為8碼（含）以上。	部分符合	部分符合	佐證資料中未提到相關密碼強度要求。
16.因特殊需要擁有多個帳號時，是否使用一組複雜但相同的通行碼？	部分符合	部分符合	佐證資料中未提到相關密碼強度要求。

17.學校是否建立資訊安全事件（包括：任何來自網路的駭客攻擊、病毒感染、垃圾郵件、資料或網頁遭竄改、以及通訊中斷等）通報程序？通報程序是否包括學校內部通報，以及學校向教育機構通報平台通報？	不符合	不符合	無佐證
18.當學校內部發生無法處理之資通安全事件，是否有通報至教育機構通報平台？人員是否了解通報的管道？	未填		
19.所訂出資訊安全事件通報程序是否公布於校園內使用電腦與網路之場所，提供使用者瞭解？	不符合	不符合	
四、實體安全			
20.學校重要的資訊設備是否置於設有空調的空間？	符合	符合	
21.學校資訊設備放置空間與電腦教室區域，是否設置滅火設備，並禁止擺放易燃物或飲食？	符合	符合	
22.學校資訊設備主機空間與電腦教室區域內的電源線插頭是否有接地的連結、或有避雷針等裝置，避免如雷擊事件所造成損害情況？	符合	符合	
23.學校資訊設備主機空間與電腦教室區域，是否於入出口處加裝門鎖或其他同等裝置？	符合	符合	
24.學校重要的資訊設備（如：伺服器安置空間）是否有適當的電力設施，例如：設置UPS、電源保護措施，以免斷電或過負載而造成損失？	符合	符合	
25.學校資訊設備安置空間與電腦教室區域內應避免明佈線？	符合	符合	
26.所有包括儲存媒體的設備項目，在報廢前，是否先確保已將任何敏感資料和授權軟體刪除或覆寫？	部分符合	部分符合	若能留下相關處理記錄會更好。
27.是否與設備廠商建立維護合約？	不適用	不適用	
28.維護廠商進入資訊設備主機空間是否事先簽訂安全保密切結書？	不適用	不符合	
29.未經授權前是否將學校的資訊設備、資訊或軟體攜出所在地？	部分符合	不符合	

30.因業務需要將機敏資料交付委外廠商時（如辦理保險、校外教學等），廠商是否簽訂安全保密切結書？	不適用	不適用	
31.當有必要將設備移出，是否已檢視相關授權，並實施登記與歸還記錄？	不適用	不符合	
32.相關財產之攜出是否依教育部或學校既有之相關規定處理？	部分符合	不符合	
33.結束工作時，所有學校教職員工是否將其所經辦或使用具有機密或敏感特性的資料（例如公文、學籍資料等）及資料的儲存媒體（如USB隨身碟、磁碟片、光碟等），妥善存放？	符合	符合	
34.學校提供教職員工或學生使用的個人電腦是否設定保護裝置，如個人鑰匙、個人密碼以及螢幕保護？	未填		
五、人員安全			
35.是否將資訊安全納入教職員手冊說明中，以強化工作上之資訊安全意識？	不適用	不符合	
36.是否使學校(或委託)系統管理人員有足夠能力執行日常基礎之資安管理系統維護工作，並使其瞭解資安事件通報之程序？	符合	符合	
37.學校是否鼓勵或安排資訊組長/老師/系統管理人員、以及所有教職員參與資訊安全教育訓練或宣導活動，以提昇資訊安全認知？	符合	符合	
六、法令認知			
38.是否宣導師生遵守智慧財產權相關法令規定？	符合	符合	
39.是否宣導遵守電腦處理個人資料保護法及個人資料保護法修訂規定？	符合	符合	
40.是否宣導遵守校園網路使用規範？	符合	符合	