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：103 年 10 月 20 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）新北市政府教育局103年5月1日北教研字第1030767136號函辦理。

（二）教育部103年度教育部對各地方政府統合視導訪視紀錄表。

（三）教育部102年8月8日臺教資(四)字第1020099098號函辦理。

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103年09月起至103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：https://isas.moe.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。

（三）第三階段：

抽查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。

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。

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：學校之現行作業無相關作業需求。

十二、線上評量結果：

(一)優點：

35項：電腦維修時,將有機密資料之硬碟留下,資安意識良好

(二)建議：

01項：無校長簽核與公告記錄
16項：應定期進行資料還原測試
23項：21.特權管理中多位同仁共用管理者帳號,建議調整
24項：密碼長度建議修改,調整為8碼以上
41項：未說明學校是否有任何委外之資訊業務
08項：若未開放校外人士使用,可填不適用
42項：未說明學校是否有任何委外之資訊業務
43項：未說明學校是否有任何委外之資訊業務
44項：未說明學校是否有任何委外之資訊業務

十三、學校背景資料

序	項目內容	填答
01	貴校班級數(班)	21
02	貴校資訊、資訊安全人力概況(不含委外人力)(人)	1
03	貴校對外服務主機數量(台),包含實體主機、虛擬主機，不包含託管在教網的主機。	5
04	貴校行政電腦數量(台)	16
05	貴校班級電腦數量(台)	30
06	貴校電腦教室或專科教室用電腦數量(台)	48
07	貴校可攜式設備(公發的手機 平板 筆電)數量(台)	5
08	貴校對外連線頻寬(in/out，Mb)	1000
09	校內個人電腦是否使用網路位址的轉址(NAT，Network Address Translation)?	否
10	貴校是否建置入侵偵測系統(IDS，Intrusion detection system)?	是
11	貴校是否建置防火牆?	是
12	貴校是否建置防毒機制	是
13	貴校是否建置郵件過濾機制?	是
14	貴校重要的系統有哪些，請列出系統名稱	Linux Rsync備份主機

		Windows2008 office scan 防毒主機
15	貴校教職員工人數(人)	34

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：薛甘霖-正修科技大學　評量日期：103年10月20日
自評結果：74分　　評量結果：69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且經校長簽核及公告	符合	不符合	無校長簽核與公告記錄
二、網路安全			
02.【網路控制措施】 (1)與外界連線，應僅限於經由教育局(處)網路管理單位之管控，以符合一致性與單一性之安全要求。 (2)宜依業務性質之不同，區分不同內部網路網段，例如：教學、行政、宿網等，以降低未經授權存取之風險。	符合	符合	
03.【網路控制措施】 應禁止以私人架設網路（如：電話線、2G或3G網路等）連結機房內之主機電腦或網路設備。 【無線網路存取】 應禁止使用者私自將無線網路存取設備介接至校園網路；若有介接之必要應經權責管理人員同意並設定帳號通行碼或加密金鑰以防未經許可之盜用。	符合	符合	
04.【網路控制措施】 對於開放提供外部使用者或廠商存取之服務，必須限制使用者之來源IP及網路連線埠(Port)，以確保安全。	符合	符合	
05.【無線網路存取】 校園內應提供無線網路存取服務，並採取適當安全管控措施： (1)專供行政使用之無線網路熱點建議設定加密金鑰防護，並避免使用開放之無線網路存取重要資訊系統及處理敏感性資料。	符合	符合	
06.(2)於教學區域、會議室等場所佈建之	符合	符合	

無線網路熱點應具有使用者身分認證機制，並經由校園無線路漫遊服務系統提供外校來賓使用。			
07.(3)專供師生教學活動使用之無線網路熱點，若採用其他管理方式確有不便時，應採取限定開放時間及限制開放區域等管理措施，減少遭受不當利用之機會。	符合	符合	
08.(4)開放校外人士出入之公共空間可視需要提供民眾無線上網服務，其網段應與校園網路隔離，或委由網路服務業者提供。	未填	不符合	若未開放校外人士使用,可填不適用
三、系統安全			
09.【設備區隔】 伺服器主機可依個別應用系統之需要，設置專屬主機，以避免未經授權之存取，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)等。	符合	符合	
10.【對抗惡意軟體、隱密通道及特洛依木馬程式】 個人電腦應： (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)作業系統及軟體應定期更新，以防範系統漏洞。	符合	符合	
11.【對抗惡意軟體、隱密通道及特洛依木馬程式】 個人電腦所使用的軟體應有授權。	符合	符合	
12.【對抗惡意軟體、隱密通道及特洛依木馬程式】 新伺服器系統啟用前，應執行相關程序(如：確認適合該作業系統之掃毒工具、預設通行碼更新、系統更新等，並記錄於啟用與報廢紀錄單)，以防範可能隱藏的病毒或後門程式。	符合	符合	
13.【桌面淨空與螢幕淨空政策】 個人電腦辦公桌面應避免存放機敏性文件，結束工作時，應將其所經辦或使用具有機密或敏感特性的資料（如公文、學籍資	符合	符合	

料等）妥善存放。			
14.【桌面淨空與螢幕淨空政策】 當個人電腦或終端機不使用時，應使用鍵盤鎖或其他控管措施保護個人電腦及終端機安全，個人電腦應設定螢幕保護機制。	符合	符合	
15.【資料備份】 系統管理人員需針對學校重要電腦系統及資料（如:系統檔案、網站、資料庫等）應每週至少進行一次備份工作；建議使用設備執行異地備份或使用光碟、隨身碟或外接式硬碟執行異地存放。	符合	符合	
16.【資料備份】 每年應定期檢查備份資料之可用性與完整性。	未填	不符合	應定期進行資料還原測試
17.【資訊工作日誌】 系統管理人員需針對重要電腦系統進行檢查、維護、更新等動作時，應針對這些活動填寫日誌予以紀錄，作為未來需要時之查核。	符合	符合	
18.【資訊工作日誌】 系統管理人員應至少每季執行一次校時。	符合	符合	
19.【資訊存取限制】 共用的個人電腦（如：電腦教室電腦、教師休息室電腦等）應以特定功能為目的，並設定特定安全管控機制（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	
20.【使用者註冊】 人員報到或離退職應會辦電腦系統帳號管理人員，執行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，該作業應包括以下內容： (1)使用唯一的使用者帳號。 (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)保存一份包含所有帳號註冊的記錄。 (4)使用者調職或離職後，應移除其帳號的存取權限。 (5)每學期應檢查使用者帳號，以確保帳	符合	符合	

號的有效性。			
21.【特權管理】 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，應予以文件化記錄。	符合	符合	
22.【通行碼（Password）之使用】 管制使用者第一次登入系統時，必須立即更改預設通行碼，預設通行碼應設定有效期限。	符合	符合	
23.【通行碼（Password）之使用】 資訊系統與服務應避免使用共用帳號及通行碼。	符合	不符合	21.特權管理中多位同仁共用管理者帳號,建議調整
24.【通行碼（Password）之使用】 由學校發佈通行碼制定與使用規則給使用者(參考優質通行碼設定原則與使用原則文件，文件編號：A-5)，內容應包含以下各項： 使用者應該對其個人所持有通行碼盡保密責任。 要求使用者的通行碼設定，應該包含英文字及數字，長度為8碼（含）以上。	部分符合	部分符合	密碼長度建議修改,調整為8碼以上
25.【通報安全事件與處理】 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，通報程序包括學校內部通報，以及學校向教育機構通報平台通報。	符合	符合	
26.【通報安全事件與處理】 校內人員應了解通報的管道，並將資訊安全事件通報程序應公布於校園內使用電腦與網路之場所，提供使用者了解。	符合	符合	
四、實體安全			
27.【設備安置及保護】 主機機房及電腦教室宜設置偵煙、偵熱或滅火設備（氣體式滅火器），並禁止擺放易燃物或飲食。	符合	符合	
28.【設備安置及保護】 主機機房及電腦教室的電源線插頭應有接	符合	符合	

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。			
29.【設備安置及保護】 主機機房及電腦教室應實施門禁管制。	符合	符合	
30.【溫濕度控制】 重要的資訊設備（如：主機機房等）宜有溫濕度控制措施(溫度建議控制在20℃~25℃，濕度建議控制在相對濕度50%R.H.~70%R.H.)，以防止資訊設備意外損壞。機房內應有溫濕度顯示裝置，以觀察實際之溫濕度情況。	符合	符合	
31.【電源供應】 重要的資訊設備（如主機機房）應有適當的電力保護設施，例如設置UPS、電源保護措施(如穩壓器、接地等)，以免斷電或過負載而造成損失，並設置緊急照明設備以作為停電照明之用。	符合	符合	
32.【纜線安全】 主機機房及電腦教室內線路應考量設置保護設施(如：高架地板、線槽、套管等)。	符合	符合	
33.【設備與儲存媒體之安全報廢或再使用】 所有包括儲存媒體的設備項目，在報廢前應填寫「啟用與報廢紀錄單」，確認已將任何敏感資料和授權軟體刪除或覆寫。	符合	符合	
34.【財產攜出】 禁止資訊設備在未經授權之情況下攜離所屬區域，若需將設備攜出，應遵守財產管理相關規定並填寫「設備進出紀錄表」。	符合	符合	
35.【財產攜出】 當有必要將設備移出，應檢視相關授權，並實施登記與歸還記錄。	符合	符合	電腦維修時,將有機密資料之硬碟留下,資安意識良好
五、可攜式電腦設備與媒體			
36.公務用可攜式電腦設備(如：筆記型電腦、平板電腦、智慧型手機等)應設定保護機制，如設定通行碼、圖形辨識、臉孔辨識或指紋辨識等。	符合	符合	

公務用可攜式電腦設備應執行安全相關程序(如：掃毒、預設通行碼更新、系統更新等)，以防範可能隱藏的病毒或後門程式。			
37.公務用可攜式儲存媒體(如：隨身碟、光碟、磁帶等)應依儲存資料的機敏性實施安全控管措施，如檔案加密儲存或將該儲存媒體存放於上鎖儲櫃或安全處所。	符合	符合	
六、人員安全			
38.【人員安全責任】 非正式人員、約聘(僱)人員者，因業務需要，而接觸公務機密、個人權益及學校機敏資料者須填寫保密切結書。	符合	符合	
39.【資訊安全教育與訓練】 鼓勵資安業務承辦人參加資安管理系統相關教育訓練。	符合	符合	
40.【資訊安全教育與訓練】 鼓勵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	
七、資訊業務委外管理			
41.【服務委外廠商合約之安全要求】 在資訊業務委外合約中，應訂定委外廠商的資訊安全責任及保密規定。	未填	不符合	未說明學校是否有任何委外之資訊業務
42.【服務委外廠商合約之安全要求】 應要求委外廠商簽訂安全保密切結書。	未填	不符合	未說明學校是否有任何委外之資訊業務
43.委外廠商人員到校服務時，應請其簽署委外廠商人員保密切結書。	未填	不符合	未說明學校是否有任何委外之資訊業務
44.委外廠商服務異動或終止時，應中止或刪除其系統上的帳號與權限。	未填	不符合	未說明學校是否有任何委外之資訊業務
八、法令認知			
45.宣導師生遵守智慧財產權、個人資料保護法及其施行細則、刑法電腦犯罪專章等相關法令規定。	符合	符合	
九、個人資料保護法			

46.【規劃】 建立個人資料保護管理政策。	符合	符合	
47.【界定個人資料之範圍】 進行個人資料盤點後，建立「個人資料檔案清冊」，並依個資法規定於網站公布個人資料檔案大綱。	符合	符合	
48.【個人資料蒐集、處理及利用之內部管理程序】 進行個人資料之蒐集與利用時，必須符合法令規定，包含： (1)個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯。 (2)蒐集個人資料時，應依法令規定告知當事人蒐集資料之目的、利用範圍等資訊。 (3)除符合法令規定外，有關醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。 (4)當資料利用範圍超出蒐集的特定目的時，應依個資法規定取得當事人之書面同意。	未填	不符合	
49.【事故之預防、通報及應變機制】 學校須設置「個資保護聯絡窗口」，協調聯繫個資事宜，並將聯繫方式(如：電話、email)置於單位網站，以便利民眾提出申訴與救濟。	符合	符合	
50.【資料安全管理】 對於個人資料之調閱，須有申請及核准程序，並記錄保存調閱者身分及行為。	未填	不符合	