附件一：臺南市公私立國中、小學資訊安全管理內部稽核表

文件編號		機密等級	限 閱	版本	1.1

填表日期：　年　月　日

稽核單位：	
稽核地點：	
參考條款：	國中小資通安全管理系統實施原則（中華民國 96 年 5 月 30 日版）
稽核日期：	
稽核範圍：	國中、小學內電腦、資訊與網路服務相關的系統、設備、程序、及人員。

適用對象：
本稽核表之設計主要參照「國中小資通安全管理系統實施原則（以下簡稱規範）」之內涵，並沿用規範所定義之適用範圍與對象。本表適用對象為台南市國中、小學

評分標準說明：
A：相關資訊安全管理制度規範已建立，且落實執行
B：相關資訊安全管理制度規範未建立，但已實施替代性資安控管措施
C：相關資訊安全管理制度規範已建立，但未落實執行
D：相關資訊安全管理制度規範未建立，且未實施替代性資安控管措施
E：不適用

稽核項目 - 控制目標與控制項目

條款 章節	依據條文		稽核評分 A B C D E	稽核發現與說明
1	網路安全			
1.1	網路控制措施			
1.1.1	對外連線	學校與外界連線，應僅限於經由學術網路之管控，以符合一致性與單一性之安全要求。 禁止以電話線連結主機電腦或網路設備。	□ □ □ □ □	
1.1.2	學校內特殊系統連線	學校內特殊系統（例如會計系統、學生學籍、成績原始資料系統等）之資料，當有必要透過網路進行傳輸時，透過虛擬私有網路（VPN）或同等連線方式進行；若無透過網路進行傳輸需求，則建議區隔於網路之外。	□ □ □ □ □	
1.2	網路安全管理服務委外廠商合約之安全要求			
1.2.1	保密條款之簽訂	委外開發或維護廠商必須簽訂安全保密切結書，確保其了解應有之資安責任與相關限制。	□ □ □ □ □	
2	系統安全			
2.1	職責區隔			
2.1.1	主機區隔	學校主機電腦可依網路服務、行政使用與個別應用系統之需要做區隔，設置專屬電腦	□ □ □ □ □	
2.1.2	行政系統主機管理	學校的行政系統主機（例如財務、人事、公文系統等）電腦，由教育局資訊中心統籌管理	□ □ □ □ □	

條款 章節	依據條文		稽核評分 A B C D E	稽核發現與說明
2.2	對抗惡意軟體、隱密通道及特洛依木馬程式			
2.2.1	防毒軟體更新	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，定期（至少每個月）進行程式更新作業，以防範作業系統之漏洞。	□ □ □ □ □	
2.2.2	軟體授權	學校內個人電腦所使用的軟體應有授權	□ □ □ □ □	
2.2.3	新系統啟用	新系統啟用前，應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。	□ □ □ □ □	
2.3	備份作業之控管			
2.3.1	資料備份	學校(或委託)系統管理人員需針對學校重要系統（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；週期為每週進行一次。	□ □ □ □ □	
2.4	操作員日誌			
2.4.1	系統管理者與作業人員之紀錄	學校(或委託)系統管理人員需針對敏感度高、或包含特殊資訊的電腦系統進行檢查、維護、更新等動作時，應針對這些活動填寫日誌予以紀錄，作為未來需要時之檢查。 日誌內容可包含以下各項： 系統例行檢查、維護、更新活動的起始時間 紀錄日誌項目人員姓名與簽名欄	□ □ □ □ □	
2.4.2	系統錯誤事項之記錄	系統發生錯誤之事項時，應予以忠實的記錄，並進行適當的處理程序。	□ □ □ □ □	

條款 章節	依據條文		稽核評分 A B C D E	稽核發現與說明
2.4.3	系統時鐘應予同步	應定期校正系統作業時間，維持系統稽核紀錄的正確性及可信度，作為事後法律上或是紀律處理上的重要依據。	□ □ □ □ □	
2.5	使用者註冊			
2.5.1	使用者註冊之管理	學校應制定電腦系統使用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： 使用唯一的使用者識別碼（ID）。 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。 保存一份包含所有識別碼註冊的記錄。 使用者調職或離職後，應移除其識別碼的存取權限。	□ □ □ □ □	
2.5.2	定期清查帳號	定期（每學期至少一次）檢查並取消多餘的使用者識別碼和帳號。 定期（建議至少一次）檢查新增之帳號，若有莫名帳號產生，應關閉帳號權限。	□ □ □ □ □	
2.6	特權管理			
2.6.1	文件化存取特權人員	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，應予以文件化記錄備查。	□ □ □ □ □	
2.7	通行碼之使用			
2.7.1	使用者通行碼管理	資訊系統與服務應避免使用共同帳號及通行碼。	□ □ □ □ □	

條款 章節	依據條文		稽核評分 A B C D E	稽核發現與說明
2.7.2	通行碼之設定	由學校發佈通行碼（Password）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，內容應包含以下各項： 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，避免使用易於猜測之數字或文字，以及過多的重複字元等。 3.因特殊需要擁有多個帳號時，可考慮使用一組複雜但相同的通行碼。	□ □ □ □ □	
2.8	原始程式庫之存取控制			
2.8.1	原始程式庫之委外管理	學校與系統廠商間的合約應加註對原始程式庫安全之要求，防範資料庫隱碼(SQL-injection)問題，針對存取資料庫程式碼之輸入欄位進行字元合理性檢查	□ □ □ □ □	
2.9	通報安全事件與處理			
2.9.1	資訊安全事件通報	學校應建立資訊安全事件通報程序以及安全事件通報單； 資安適件應即刻進行通報，通報程序應包括學校內部通報，以及學校與所屬縣市教育網路中心的通報。	□ □ □ □ □	
2.9.2	通報程序之公告	訂出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，提供使用者瞭解。	□ □ □ □ □	

條款 章節	依據條文		稽核評分 A B C D E	稽核發現與說明
3	實體安全			
3.1	設備安置及保護			
3.1.1	實體環境安全	學校重要的資訊設備（如主機機房）應置於設有空調空間或通風良好之空間。 學校資訊設備主機機房、電腦教室區域，應設置滅火設備，並禁止擺放易燃物、或飲食。 學校資訊設備主機機房、電腦教室區域內的電源線插頭應有接地的連結、或有避雷針等裝置，避免如雷擊事件所造成損害情況。	□ □ □ □ □	
3.1.2	設備安置地點之保護措施	學校資訊設備主機機房、電腦教室區域，應採取適當控制措施與指引，確保只有授權人員可以進出安全區域。	□ □ □ □ □	
3.2	電源供應			
3.2.1	電源供應	學校重要的資訊設備應有適當的電力設施與電源保護措施，以免斷電或過負載而造成損失。	□ □ □ □ □	
3.3	纜線安全			
3.3.1	佈纜的安全	學校資訊設備主機機房、電腦教室區域內地板上應避免佈明線。	□ □ □ □ □	
3.4	設備與儲存媒體之安全報廢或再使用			
3.4.1	設備報廢與再使用	資訊處理設備在報廢前，應避免內存資料外洩，先進行必要的清除動作，確保已無任何敏感資料和授權軟體。	□ □ □ □ □	

條款 章節	依據條文		稽核評分 A B C D E	稽核發現與說明
3.5	設備維護			
3.5.1	設備之維護	資訊處理設備應予以適當的維護，確保其持續運作。 若委外服務應與設備廠商建立維護合約。維護廠商進入安全區域需簽訂安全保密切結書。	□ □ □ □ □	
3.6	財產攜出			
3.6.1	預防未經授權之移動	未經授權不應將學校的資訊設備、資訊或軟體攜出所在地。 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。	□ □ □ □ □	
3.7	桌面淨空與螢幕淨空政策			
3.7.1	桌面淨空安全管理	應考量採用辦公桌面的淨空政策，以減少具有機密或敏感特性的資料及儲存媒體等在正常的辦公時間之外遭未被授權的人員取用、遺失、竄改或是被破壞的機會。	□ □ □ □ □	
3.7.2	電腦保護裝置	學校提供教職員工或學生使用的個人電腦應設定保護裝置，如個人鑰匙、個人密碼以及螢幕保護。	□ □ □ □ □	
4	人員安全			
4.1	資訊安全職責			
4.1.1	將安全列入工作執掌中	於學校重要會議上宣導相關資安知識，以強化工作上之資訊安全意識。	□ □ □ □ □	

條款 章節	依據條文		稽核評分 A B C D E	稽核發現與說明
4.2	資訊安全教育與訓練			
4.2.1	管理人員資安教育訓練	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，應接受適當之資安訓練與有關資安政策、程序之宣導課程。	□ □ □ □ □	
4.2.2	其他人員資安教育訓練	學校鼓勵或安排老師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。	□ □ □ □ □	
5	相關法規與施行單位政策之符合性			
5.1	法規之遵守			
5.1.1	適用法規之遵循	需制定適當的流程與管制，保護重要紀錄，並確保遵守智慧財產權、個人資料保護及隱私等條文規範，防止資訊處理設施遭不當之使用。	□ □ □ □ □	
5.1.2	適用法規之宣導	蒐集相關法律條文（智慧財產權、資料隱私保護及其他相關法規）、了解與資訊處理設施、軟體系統的關係，並予以書面或公開場合做宣導。	□ □ □ □ □	

稽核員：　　**稽核日期**：