附件 3

D 級教育機構－資訊安全管理稽核表					
文件編號		機密等級		版本	1.0

填表日期：103 年 9 月 20 日

單位：	海口國小
地點：	苗栗縣竹南鎮海口里 7 鄰保福路 20 號
參考條款：	教育體系資通安全管理規範（中華民國 96 年 5 月 30 日版）
日期：	民國　103 年 9 月 20 日
範圍：	校園網路與機房

適用對象：

本稽核表之設計主要參照「教育體系資通安全管理規範（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。本表適用對象為歸類於 D 級之教育機構(屬於規範定義之第二群)，包含高中職學校。

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
A5	資訊安全政策訂定與評估			
A.5.1	資訊安全政策訂定與評估			
A.5.1.1	資訊安全政策制定	資訊安全政策應參考資安相關法令及施行單位業務上的需求，並經由管理階層核准，以適當方式向所有員工公佈與宣導，在必要時告知相關單位及合作廠商，以利共同遵守。	■ □ □ □ □	資訊安全政策在全校性會議，向全校教職員、教師、學生宣導，若有系統外包則同時告知合作廠商。(相關照片、文件留存備查)
A.5.1.2	資訊安全政策評估	面對資安事件的發生、資安相關法令與其他影響因素的改變時，資訊安全政策應進行即時的評估，並定期審查政策的可行性與有效性。	■ □ □ □ □	
A6	資訊安全組織			
A.6.1	資訊安全組織推動與權責			
A.6.1.1	資訊安全組織推動以及權責之分配	由管理階層舉辦定期之資訊安全會報，召集相關單位代表進行工作與責任的分屬，確保資安相關計畫的進行，並展現管理階層的支持。	■ □ □ □ □	
A.6.1.2	資訊設施使用之授權	資訊處理設備的移轉（包含新設備），應由權責主管人員進行授權、移交的程序，確保該設備後續的順利運作及責任所屬。	■ □ □ □ □	

條款章節	依據條文		稽核評分					稽核發現與說明
			A	B	C	D	E	
A.6.1.3	保密條款之簽訂	施行單位之員工（包含正職員工、臨時雇員）應簽署獨立或包含保密條款之合約，確保其了解應有之資安責任與相關限制。	☐	■	☐	☐	☐	簽訂保密切結書或其他相關文件
A.6.1.4	跨單位合作及協調	為確保資訊安全作業的順利運行，需與執法機關、主管機構、資訊服務廠商及電信公司建立適當的溝通管道。	■	☐	☐	☐	☐	
A.6.1.5	資訊安全諮詢與顧問	在必要時，須向單位內部專業人員或外部專業諮詢人員徵詢、協調資訊安全建議。	■	☐	☐	☐	☐	
A.6.1.6	資訊安全政策的獨立檢視	機關制訂之資訊安全政策，應進行獨立及客觀的評估。	■	☐	☐	☐	☐	
A.6.2	施行單位外部人員存取安全管理							
A.6.2.1	施行單位外部人員存取之安全掌控	面對外部人員存取施行單位資訊處理設施的可能風險，應視狀況採取適當的安全控制措施，並條列安全規定於正式合約中。	☐	■	☐	☐	☐	簽訂保密切結書
A.7	資訊資產分類與管制							
A.7.1	資訊資產分類與責任分屬							
A.7.1.1	資訊資產目錄建立	應製作所有資訊資產之清冊，並定期維護、更新。	■	☐	☐	☐	☐	
A.7.1.2	資訊安全等級分類	資訊資產應進行分級與標示，並考量重要資產的需求，於必要時制定保護措施及處理流程。	☐	■	☐	☐	☐	資產進行標示

條款 章節	依據條文		稽核評分					稽核發現與說明
			A	B	C	D	E	
A.8	人員安全管理與教育訓練							
A.8.1	聘任前之處理							
A.8.1.1	所屬角色與責任	施行單位之員工、廠商及第三方使用者的資訊安全角色及責任應視需求以書面或其他方式清楚定義，並與資訊安全政策一致。	■	□	□	□	□	
A.8.2	聘用中之處理							
A.8.2.1	資訊安全教育訓練	施行單位內所有員工、合作廠商與第三方使用者應接受適當之資安訓練與有關資安政策、程序之宣導課程。	■	□	□	□	□	
A.8.2.2	違反規定之處理	依據既定之條款或合約，違反施行單位之資訊安全政策與程序之人員，應予以適當之懲處。	■	□	□	□	□	
A.8.3	結束聘任或改變職務							
A.8.3.1	結束聘用之處理	負責執行結束聘用或改變職務之權責，其職掌應清楚定義並指派。	■	□	□	□	□	
A.8.3.2	資產繳回	離職時，應有正式的資產繳回程序，顯示其已繳回單位資產。	■	□	□	□	□	
A.8.3.3	存取權移除	所有員工、合約商及第三方使用者的存取權限應根據既有的規範或協定進行移除或改變。	■	□	□	□	□	
A.9	實體與環境安全							
A.9.1	區域之安全							

條款章節	依據條文		稽核評分					稽核發現與說明
			A	B	C	D	E	
A.9.1.1	實體環境安全	施行單位應採用適當防護措施保障資訊處理設施所在區域(機房設備、人員辦公區域)的安全。	■	□	□	□	□	
A.9.1.2	人員進出控制	施行單位應實施控制措施，確保只有授權人員可以進出安全區域。	■	□	□	□	□	機房門禁控管，只有授權的人員可進出
A.9.1.3	資訊處理設施安全	在資訊處理設施所在區域工作，應採取適當的控制措施與指引，確保該區域的安全性。	■	□	□	□	□	機房門禁控管，只有授權的人員可進出
A.9.2	設備之安全							
A.9.2.1	設備安置地點之保護措施	施行單位應安置或保護設備，降低環境之威脅、災害，以及未授權存取所造成的可能損失。	■	□	□	□	□	
A.9.2.2	電源供應	施行單位應保護資訊處理設備，降低電力故障或異常的影響。	■	□	□	□	□	電源供應有 UPS 不斷電系統保護
A.9.2.4	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。	■	□	□	□	□	
A.9.2.5	設備報廢與再使用	資訊處理設備在報廢或再使用的過程中，應避免內存資料的外洩，進行必要之清除動作。	■	□	□	□	□	資訊設備報廢前將資料清除
A.9.2.6	預防未經授權之移動	施行單位所屬之設備、資訊或軟體未經授權禁止移動。	■	□	□	□	□	
A.10	通訊與作業安全管理							
A.10.1	作業程序與責任							

條款章節	依據條文		稽核評分					稽核發現與說明
			A	B	C	D	E	
A.10.1.1	作業程序文件化	安全政策所規定之作業程序，應文件化並定期維護。	■	□	□	□	□	
A.10.1.2	作業變更之管理	資訊處理設施、系統之變更，應進行管制。	■	□	□	□	□	
A.10.2	資訊作業委外服務之安全管理							
A.10.2.1	資訊作業服務之管控	施行單位執行資訊業務委外時，應與廠商簽訂適當的資訊安全協定及課予相關的安全管理責任，納入契約條款。	■	□	□	□	□	
A.10.2.2	服務之監控與審查	施行單位應監視和審查廠商提供的服務，確保服務標準達到協議的要求。	■	□	□	□	□	
A.10.3	系統規劃與驗收							
A.10.3.2	新系統上線作業之安全評估	新資訊系統、系統升級與新版本正式上線前應予以適當的測試，建立固定的驗收程序。	■	□	□	□	□	新系統驗收時留存相關文件
A.10.4	電腦病毒、惡意軟體							
A.10.4.1	電腦病毒及惡意軟體之控制	施行單位應進行防備電腦病毒與惡意軟體之偵測及預防的控制措施，以及使用者認知程序。	■	□	□	□	□	宣導資訊安全防護措施，安裝防毒軟體
A.10.5	備份作業之管控							
A.10.5.1	資料備份	重要資訊與軟體應進行定期的備份。	■	□	□	□	□	學校自行建置之系統定期備份

條款 章節	依據條文		稽核評分 A B C D E	稽核發現與說明
A.10.6	網路安全管理 —較適用於學術網路系統			
A.10.6.1	網路安全規劃與管理	應實施網路控制措施，維護網路安全。	□ ■ □ □ □	架設防火牆
A.10.6.2	網路服務之安全控制	使用公用或私用網路，應評估網路服務提供者之安全措施是否足夠，並提供明確的安全措施說明，另應考量使用該項網路對維持機關資料傳輸機密性、資料完整性及可用性等各種安全影響。	■ □ □ □ □	
A.10.7	儲存媒體的處理與安全			
A.10.7.1	電腦媒體之安全管理	電腦儲存媒體、可攜式媒體或印出報表，應制定控管措施。	□ ■ □ □ □	
A.10.7.2	電腦媒體處理之安全	應訂定電腦媒體的處理作業程序，以降低可能的安全風險。	□ ■ □ □ □	
A.10.7.3	資料檔案之保護	重要資料檔案應進行控管，並安全的保存。	□ ■ □ □ □	
A.10.7.4	系統文件之安全	重要系統文件應受到保護，避免未授權之存取。	□ ■ □ □ □	
A.10.8	資訊與軟體交換			

條款 章節	依據條文		稽核評分					稽核發現與說明
			A	B	C	D	E	
A.10.8.1	資訊與軟體交換安全政策與協定	單位間交換資訊與軟體的行為（具機密性或敏感性內容）應有安全保護措施及協議規範，必要時制定正式合約。	☐	■	☐	☐	☐	
A.10.8.2	電子郵件安全管理	應制定電子郵件使用政策，並實施控制措施降低安全風險。	☐	■	☐	☐	☐	依循縣網中心電子郵件使用規則
A.10.8.3	電子辦公系統安全	視需求應制定並實施控制措施，以管制和電子辦公系統有關之單位及安全風險。	☐	■	☐	☐	☐	教職員辦公電腦依循資訊安全政策來管理
A.10.8.4	對外公告資訊之管理	對外公告資訊前應有正式授權程序，並避免未授權之竄改。	☐	■	☐	☐	☐	對外公告前需有主管授權
A.10.9	系統存取及應用之監督							
A.10.9.1	事件記錄	建立及製作例外事件及資訊安全事項的稽核軌跡，並保存一段的時間，以作為日後調查及監督之用。	☐	■	☐	☐	☐	資訊安全事件單及系統 Log 文件保存 1 年以上
A.10.9.2	系統使用之監控	為確保使用者只能執行授權範圍內的事項，應建立系統使用監督程序。	☐	■	☐	☐	☐	重要系統特定人員才能存取
A.10.9.3	紀錄的保護	單位應保護未授權的變更及防止記錄設備操作發生問題。	☐	■	☐	☐	☐	
A.10.9.4	系統管理者與作業人員之紀錄	應忠實記錄系統管理者與作業人員之相關操作紀錄。	☐	■	☐	☐	☐	

條款 章節	依據條文		稽核評分					稽核發現與說明
			A	B	C	D	E	
A.10.9.5	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。	☐	■	☐	☐	☐	
A.10.9.6	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。	☐	■	☐	☐	☐	
A.11	存取控制安全							
A.11.1	使用者存取控制							
A.11.1.1	使用者註冊管理	應制定正式使用者註冊、註銷流程和條款，以供存取資訊系統及服務。	☐	■	☐	☐	☐	
A.11.1.3	一般通行碼之控管	應建立使用者通行碼之管理制度。	■	☐	☐	☐	☐	依循「國中、小學資通安全管理系統實施原則」處理
A.11.2	使用者責任							
A.11.2.1	桌面淨空安全管理	應考量採用辦公桌面的淨空政策，以減少文件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。	☐	■	☐	☐	☐	
A.11.3	網路存取控制措施							
A.11.3.1	網路服務之限制	施行單位須清楚限定使用者只能直接存取准許使用之服務。	☐	■	☐	☐	☐	
A.11.4	作業系統存取控制							

條款 章節	依據條文		稽核評分					稽核發現與說明
			A	B	C	D	E	
A.11.4.1	系統登入程序	使用者存取電腦系統應經由安全的系統登入程序。	☐	■	☐	☐	☐	
A.11.4.2	使用者通行碼管理	應以安全有效的使用者通行碼管理系統鑑別使用者身份。	☐	■	☐	☐	☐	
A.11.5	應用系統的存取控制 —較適用於行政資訊系統							
A.11.5.1	資訊存取限制	依資訊存取規定，配予應用系統的使用者與業務需求相稱的資料存取及應用系統的使用權限。	☐	■	☐	☐	☐	
A.12	系統開發與維護之安全							
A.12.2	應用系統安全 —較適用於行政資訊系統							
A.12.2.1	資料輸入之驗證	輸入應用系統之資料須確認其正確性與適當性。	☐	☐	☐	☐	■	
A.12.2.2	系統內部作業處理之驗證	系統需建立確認檢查機制，以偵知所處理資料的塗改。	☐	☐	☐	☐	■	
A.12.2.4	資料輸出控管	應用系統的資料輸出需經過確認，確保處理程序的正確性與適當性。	☐	☐	☐	☐	■	
A.12.4	系統檔案安全							
A.12.4.1	作業軟體控制	需建立作業系統各個軟體實施的管制程序，避免軟體影響作業系統之完整。	☐	☐	☐	☐	■	
A.13	資訊安全事件之反應及處理							
A.13.1	資訊安全事件與弱點之通報							

條款章節	依據條文		稽核評分					稽核發現與說明
			A	B	C	D	E	
A.13.1.1	資訊安全事件與弱點通報	資安事件需即刻進行通報。	■	□	□	□	□	資訊安全事件於 1 小時內處理並至「教育機構資安通報平台」通報
A.13.2	資訊安全事件之管理							
A.13.2.1	資安事件處理責任與程序建立	應建立處理資訊安全事件之作業程序，並課予相關人員必要的責任，以便迅速有效處理機關資訊安全事件。	■	□	□	□	□	依循「國中、小學資通安全管理系統實施原則」處理
A.13.2.2	從資安事件中學習	監控並紀錄事件的過程與結果，必要時進行檢討會議，討論改善之事宜。	□	■	□	□	□	
A.13.2.3	資安事件證據之收集	電腦稽核軌跡及相關的證據，應以適當的方法保護。	□	■	□	□	□	
A.15	相關法規與施行單位政策之符合性							
A.15.1	法規之遵守							
A.15.1.1	適用法規之鑑別	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）、管理規定及合約要求，了解與資訊處理設施、軟體系統的關係，並予以書面或其他方式留存。	□	■	□	□	□	
A.15.1.2	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。	□	■	□	□	□	

條款 章節	依據條文		稽核評分					稽核發現與說明
			A	B	C	D	E	
A.15.2	安全政策與技術符合性之檢驗							
A.15.2.1	確保遵守安全政策與規範	確保單位內所有區域或作業流程皆定期審查及確保遵守安全政策及規範。	■	□	□	□	□	
A.15.2.2	資訊系統符合性審查	為確保資訊系統之運行符合既定之安全實施標準，應進行定期的審查，並予以書面或其他方式留存。	■	□	□	□	□	每學期至「網站應用程是弱點監測平台」檢測
A.15.3	系統稽核的考量							
A.15.3.1	系統稽核控制	為避免作業系統稽核造成系統中斷的危險，應進行審慎、一致的規劃；必要時可向外部專家顧問尋求協助。	■	□	□	□	□	
A.15.3.2	系統稽核工具之保護	系統稽核之相關工具需建立適當的保護措施，並視需求設立備援及緊急應變方案。	■	□	□	□	□	

稽核員：資訊組長 劉志祥　　稽核日期：103.9.20