南投縣國民中、小學資訊安全與個資管理內部稽核表					
文件編號		機密等級	敏感	版本	1.2

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）、教育機構個人資料保護工作事項（教育部 100年度提升校園資訊安全服務計畫）
稽核日期：	
稽核範圍：	校內電腦、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」及「教育機構個人資料保護工作事項」（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。本表適用對象爲南投縣國民中、小學。

評分標準說明：

A：相關資訊安全與個資管理制度規範已建立，且落實執行

B：相關資訊安全與個資管理制度規範未建立，但已實施替代性資安控管措施

C：相關資訊安全與個資管理制度規範已建立，但未落實執行

D：相關資訊安全與個資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

稽核項目一控制目標與控制項目

條款章節	依據條文		自評	稽核評分	稽核發現與說明
			A B C D E	A B C D E	
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，應經由學術網路之管控，以符合一致性與單一性之安全要求。若有其他連外線路，必須經過學校資安設備（例如防火牆）控管。	☐ ☐ ☐ ☐ ☐	☐ ☐ ☐ ☐ ☐	
1.1.2	學校內特殊系統連線	架設於校內主機之行政系統（例如健康系統、差假系統、圖書系統、國中學籍、國中成績系統等）之資料，當有必要透過網路進行傳輸時，須經由虛擬私有網路（Virtual Private Network, VPN）或同等連線方式（例如加密）進行；若無須透過網路進行傳輸需求時，則建議區隔於網際網路之外。	☐ ☐ ☐ ☐ ☐	☐ ☐ ☐ ☐ ☐	
1.1.3	禁止電話線連結	禁止以電話線（撥接數據機）連結主機電腦或網路設備。	■ ☐ ☐ ☐ ☐	■ ☐ ☐ ☐ ☐	

條款章節	依據條文		自評	稽核評分	稽核發現與說明
			A B C D E	A B C D E	
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[參考文件編號A-01]。	☐ ☐ ☐ ☐ ☐	☐ ☐ ☐ ☐ ☐	
1.2.2	委外合約之簽訂	個人資料檔案若委外建檔，應於委外合約中載明所處理之個人資料保密義務、資訊安全相關責任及違反之罰則。	☐ ☐ ☐ ☐ ☐	☐ ☐ ☐ ☐ ☐	
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（例如財產、人事、公文系統等），系由縣府各主管單位統籌管理。	■ ☐ ☐ ☐ ☐	■ ☐ ☐ ☐ ☐	

條款章節	依據條文		自評					稽核評分					稽核發現與說明
			A	B	C	D	E	A	B	C	D	E	
2.1.3	資訊系統開發之安全需求	自行開發或委外處理個人資料檔案之資訊系統，應在系統開發生命週期之初始階段，將個人資料檔案的安全需求納入考量（如：邏輯測試）；系統之維護、更新、上線、及版本異動等作業，應予安全管制，避免危害個人資料安全。	□	□	□	□	□	□	□	□	□	□	
2.1.4	遠端登入之控管	宜避免允許維護人員或系統服務廠商以遠端登入方式進行牽涉個人資料的資訊系統維護或其他有關之運作；若需使用遠端登入方式進行維護，則應透過加密通道進行（如：HTTPS、SSH等）。	□	□	□	□	□	□	□	□	□	□	
2.1.5	含個資系統之保護與控管	自行開發或委外處理個人資料檔案之資訊系統，應將個人資料(包含測試用個人資料)施予妥善之保護與控管。	□	□	□	□	□	□	□	□	□	□	

條款章節	依據條文		自評					稽核評分					稽核發現與說明
			A	B	C	D	E	A	B	C	D	E	
2.1.6	個資監測平台	各相關網站每年至少至教育機構防洩漏個資掃描平台進行一次掃描，避免洩漏個人資料。	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	
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	學校內的個人電腦應：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，並應每週執行排程掃瞄；定期（至少每個月）進行系統程式更新作業，以防範作業系統及應用程式之漏洞。	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	
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。	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	

條款章節	依據條文		自評					稽核評分					稽核發現與說明
			A	B	C	D	E	A	B	C	D	E	
2.2.4	弱點掃描	各相關網站每年至少進行一次網站弱點監測平台掃描，並完成弱點修補。	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	
2.3	備份作業之控管												
2.3.1	系統備份	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；週期為每月進行一次。	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	
2.3.2	異機備份	資料檔如有異動，至少每月異機備份。	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	
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。	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	

條款章節	依據條文		自評					稽核評分					稽核發現與說明
			A	B	C	D	E	A	B	C	D	E	
2.4.2	記錄日誌內容	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、系統錯誤內容和採取的改正措施。[參考文件編號A-02] 紀錄日誌項目人員姓名與簽名欄	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	
2.4.3	系統時鐘同步	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	個人資料存取限制												
2.5.1	安全保護	個人資料檔案應以安全的方式保護，例如：加密。	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	
2.5.2	傳輸	交換個人資料檔案時，應對資料檔案加密，亦或是透過加密通道傳送。	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	
2.5.3	存放	個人資料禁止存放於網路芳鄰分享目錄，並停用 Guest 帳號。	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	

條款章節	依據條文		自評					稽核評分					稽核發現與說明
			A	B	C	D	E	A	B	C	D	E	
2.5.4	設備隔絕	存放個人資料之資訊設備應與外部網路隔絕或以資安設備保護。	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	
2.6	使用者註冊												
2.6.1	使用者註冊之管理	學校應制定行政系統（如公文管理系統、勞健保）使用的使用者註冊及註銷程序[參考文件編號A-03、A-04]，透過該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。	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	

條款章節	依據條文		自評					稽核評分					稽核發現與說明
			A	B	C	D	E	A	B	C	D	E	
2.6.2	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（建議每學期至少一次）檢查新增之帳號，若有莫名帳號產生，應關閉帳號權限。	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	
2.6.3	人員異動	處理個人資料檔案之人員，其職務如有異動，應將所保管之儲存媒體及有關資料列冊移交 [參考文件編號A-05] ，接辦人員除應於相關系統重置通行碼外，應視需要更換使用者識別帳號。	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	
2.6.4	離職註銷	處理個人資料檔案之人員，應簽訂保密切結書[參考文件編號A-06]，並確認於離職時或合約終止時取消或停用其使用者識別帳號，且收繳其通行證及相關證件。	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	

條款章節	依據條文		自評					稽核評分					稽核發現與說明
			A	B	C	D	E	A	B	C	D	E	
2.7	特權管理												
2.7.1	文件化存取特權人員	學校的電腦與網路系統資訊具存取特權人員（系統管理人員）清單、及其所持有的權限說明，應予文件化記錄備查。	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	
2.7.2	權限區隔	採取權限區隔，非專責處理特定個人資料者不得具有存取或查閱個人資料之權限。	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	
2.8	通行碼之使用												
2.8.1	避免共用帳號	資訊系統與服務應避免使用共同帳號及通行碼。	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	
2.8.2	通行碼之設定原則	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[參考文件編號A-07]，應包含以下各項：1.使用者應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，及過多的重複字元等。	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	

條款章節	依據條文		自評					稽核評分					稽核發現與說明
			A	B	C	D	E	A	B	C	D	E	
2.8.3	多帳號通行碼	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。	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	
2.8.4	通行碼設置	處理個人資料檔案之資訊設備，需設置使用者代碼及通行碼。	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	
2.8.5	通行碼變更	通行碼至少每六個月更換一次，通行碼長度應至少8碼，且包含英文數字。	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	
2.9	原始程式庫之存取控制												
2.9.1	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。	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	

條款章節	依據條文		自評	稽核評分	稽核發現與說明
			A B C D E	A B C D E	
2.10	通報安全事件與處理				
2.10.1	內外之通報	學校應建立資訊安全事件通報程序[參考文件編號A-08]以及安全事件通報單；資安事件應即刻進行通報，通報程序應包括學校內部通報，以及通報本縣教育網路中心(資安通報應變平台)。	☐ ☐ ☐ ☐ ☐	☐ ☐ ☐ ☐ ☐	
2.10.2	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。	☐ ☐ ☐ ☐ ☐	☐ ☐ ☐ ☐ ☐	
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。	☐ ☐ ☐ ☐ ☐	☐ ☐ ☐ ☐ ☐	

條款章節	依據條文		自評					稽核評分					稽核發現與說明
			A	B	C	D	E	A	B	C	D	E	
3.1.2	區域出入管控	學校資訊設備主機機房、電腦教室區域，應至少於入出口處加裝門鎖或其他同等裝置。	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	
3.1.3	設備安置地點之保護措施	學校資訊設備主機機房、電腦教室區域內的電源線插頭應有接地的連結、或有避雷針、穩壓器、不斷電等裝置，避免如雷擊事件所造成之損害情況。	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	
3.1.4	設備管控	儲存個人資料之資訊設備應置放於實體安全區域（如：門禁控管之辦公區域、機房），避免有心人士或非授權人員存取。	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	

條款章節	依據條文		自評					稽核評分					稽核發現與說明
			A	B	C	D	E	A	B	C	D	E	
3.1.5	儲存媒體管控	儲存個人資料檔案之相關儲存媒體，應指定專人管理，並置於實體保護之環境（如：上鎖之防潮箱、書櫃），必要時應建立備援機制，以防止資料損壞、遺失或遭竊取。相關儲存媒體非經權責單位同意並留存紀錄[參考文件編號A-09]，不得任意攜出或拷貝複製。	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	
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盡可能避免佈明線。	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	

條款章節	依據條文		自評					稽核評分					稽核發現與說明
			A	B	C	D	E	A	B	C	D	E	
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與再使用前，應避免內存資料外洩，先進行必要的清除動作，確保已無任何個人資料、敏感資料和授權軟體。	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	
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。	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	
3.5.2	保密切結	廠商進入安全區域需簽訂安全保密切結書。	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	
3.5.3	專人陪同	外部團體或個人更新或維修電腦設備時，應指派專人在場，確保個人資料之安全及防止個人資料外洩。	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	

條款章節	依據條文		自評	稽核評分	稽核發現與說明
			A B C D E	A B C D E	
3.6	財產攜出				
3.6.1	攜出授權與登記	當有必要將設備或授權軟體攜出，應檢視相關授權，並實施登記與歸還記錄[參考文件編號A-10]。	☐ ☐ ☐ ☐ ☐	☐ ☐ ☐ ☐ ☐	
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，並將螢幕保護啟動時間設定為 15 分鐘以內。	☐ ☐ ☐ ☐ ☐	☐ ☐ ☐ ☐ ☐	

條款章節	依據條文		自評	稽核評分	稽核發現與說明
			A B C D E	A B C D E	
4	人員安全				
4.1	資訊安全職責				
4.1.1	加強宣導	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。	☐ ☐ ☐ ☐ ☐	☐ ☐ ☐ ☐ ☐	
4.1.2	禁用即時通訊軟體傳輸個人資料檔案	禁止人員使用 MSN或其他即時通訊軟體傳輸個人資料檔案。	☐ ☐ ☐ ☐ ☐	☐ ☐ ☐ ☐ ☐	
4.1.3	加密傳輸個人資料檔案	使用外部網頁式電子郵件(Webmail)傳輸個人資料檔案須加密	☐ ☐ ☐ ☐ ☐	☐ ☐ ☐ ☐ ☐	
4.1.4	禁止使用 P2P軟體	禁止人員使用點對點(P2P)軟體或相關工具下載或提供檔案分享。	☐ ☐ ☐ ☐ ☐	☐ ☐ ☐ ☐ ☐	

條款章節	依據條文		自評					稽核評分					稽核發現與說明
			A	B	C	D	E	A	B	C	D	E	
4.1.5	禁止利用網際網路公開個人資料	禁止人員在社群網站、部落格、公開論壇或其他利用網際網路形式公開業務所知悉之個人資料。	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	
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與個人資料教育訓練或宣導活動，以提昇資訊安全認知。	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	

條款章節	依據條文		自評	稽核評分	稽核發現與說明
			A B C D E	A B C D E	
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	適用法規之宣導	蒐集相關法律條文（智慧財產權、個人資料保護法、個人資料保護法施行細則、資料隱私保護及其他相關法規)[參考文件編號A-11]、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。	□ □ □ □ □	□ □ □ □ □	

自評簽名：　　自評日期：

稽核員：　　稽核日期：