105 年度教育部全國國民中、小學資安評量項目及準備參考表

說明：

1.本次資安稽核是屬於輔導性質，目的是協助學校能做到較完善的資安管理機制，以符合教育部規定，並因應個資法實施的要求。

2.以下請就文件規範或記錄收集相關資料(如為設定可以擷取畫面)，若是沒有相關客觀證據，訪視團隊將提出改善建議。

3.以下所提出之資料或客觀證據僅作為參考，若有其他相關資訊可以盡量收集，由線上審查或訪視人員判斷是否足夠。

4.每一項目準備資料或客觀證據需先轉成 PDF 格式，單檔大小限制為「3Mb」，如資料為照片請先貼至 word 中加上說明後再轉成 PDF 檔案。

5.每個檢查項目之子項目限上傳 1 個 PDF 檔供審查時使用。

6.填報網站為「教育部全國國中小學資訊安全管理系統」網址 http://isas.moe.edu.tw (測試平台 http://isas.test.ntpc.edu.tw)，請以各縣市 OpenID 帳號、密碼登入。

題號	評量項目	佔分	自評項	準備資料或客觀證據
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	3 分	符合 不符合	學校資通安全管理規範 校長核可簽核記錄 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。	2 分	符合 不符合 不適用	邏輯網路架構圖，及業務與網段對應資料
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。	2 分	符合 不符合	校園網路使用管理規範及其公告畫面

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。	1 分	符合 不符合 不適用	遠端連線作業設定畫面
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。	1 分	符合 不符合 不適用	加密金鑰設定畫面
06	(2)於教學區域、會議室等場所佈建之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。	1 分	符合 不符合 不適用	帳號通行碼登入畫面
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。	1 分	符合 不符合 不適用	教學使用之無線網路管理規定
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。	1 分	符合 不符合 不適用	邏輯網路架構圖，及業務與網段對應資料
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。	1 分	符合 不符合 不適用	設備或機櫃有標示該專屬電腦名稱的照片
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。	2 分	符合 部分符合 不符合	至少 2 位行政人員的個人電腦設定畫面

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。	2 分	符合 不符合	軟體授權證明
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。	1 分	符合 不符合 不適用	簽核後的【文件編號 A-1】啟用與報廢紀錄單
13	【桌面淨空與螢幕淨空政策】 個人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、學籍資料等）妥善存放。	2 分	符合 不符合	至少 2 位行政人員辦公桌面照片
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。	2 分	符合 不符合	管控措施畫面（如：鍵盤鎖、螢幕保護畫面等）
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。	1 分	符合 不符合 不適用	備份工作相關記錄
16	【資料備份】 每年應定期檢查備份資料之可用性與完整性。	1 分	符合 不符合 不適用	檢查備份資料之可用性與完整性的畫面
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。	1 分	符合 不符合 不適用	簽核後的【文件編號 A-2】資訊工作日誌
18	【資訊工作日誌】 系統管理人員應至少每季執行一次校時。	1 分	符合 不符合	系統校時畫面

			不適用	
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）。	2 分	符合 不符合	「安全管控機制」的設定畫面
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，以確保帳號的有效性。	2 分	符合 不符合	簽核後的【文件編號 A-3】帳號申請單
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。	2 分	符合 不符合	簽核後的【文件編號 A-4】系統特權帳號清單，或校務行政系統模組權限設定畫面
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。	2 分	符合 不符合	更改預設通行碼的畫面
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。	2 分	符合 不符合	資訊系統與服務帳號設定畫面
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：	2 分	符合 部分符合 不符合	使用者通行碼的設定畫面

	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，應該包含英文字及數字，長度為 8 碼（含）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。	2 分	符合 不符合	填寫後的【文件編號 A-6】資安事件通報程序
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。	2 分	符合 不符合	資安事件通報規定宣導或公告
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。	2 分	符合 部分符合 不符合	資訊機房偵煙、偵熱與滅火設備照片，及電腦教室使用規定
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。	2 分	符合 不符合	資訊機房空間電源箱接地、設置避雷針或凸波電源保護裝置照片
29	【設備安置及保護】 主機機房及電腦教室應實施門禁管制。	2 分	符合 不符合	資訊設備主機機房及電腦教室區域門禁照片
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。	2 分	符合 不符合 不適用	機房內溫濕度顯示裝置照片
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	2 分	符合 部分符合	電力保護設施照片

	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。		不符合 不適用	
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)。	2 分	符合 部分符合 不符合	線路保護設施照片(如線槽、高架地板、套管等)
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。	2 分	符合 不符合	簽核後的【文件編號 A-1】啟用與報廢紀錄單
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」。	2 分	符合 不符合	簽核後的【文件編號 A-7】設備進出紀錄表
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。	2 分	符合 不符合	登記歸還記錄
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。 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。	2 分	符合 不符合	各類可攜式電腦設備(如平板、筆電、手機等)設定畫面
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。	2 分	符合 不符合	可攜式儲存媒體(如 USB、光碟、外接式硬碟等)安全控管措施照片(如上鎖儲櫃照片、檔案解密畫面等)
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、	1 分	符合 部分符合	簽核後的【文件編號 A-8】保密切結書

	個人權益及學校機敏資料者須填寫保密切結書。		不符合 不適用	
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。	2 分	符合 不符合	資安業務承辦人受訓證明或報名資料
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。	2 分	符合 不符合	學校宣導活動照片，或上課講義及簽到表
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。	1 分	符合 不符合 不適用	擷取資訊業務委外合約有資安規定部分，若無資訊業務委外合約，則第 41、42、43、44 題填選「不適用」
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。	1 分	符合 不符合 不適用	簽核後的【文件編號 A-9】服務委外單位服務暨保密切結書
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。	1 分	符合 不符合 不適用	簽核後的【文件編號 A-10】委外廠商人員保密切結書
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。	1 分	符合 不符合 不適用	簽核後的【文件編號 A-3】帳號申請單
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。	2 分	符合 不符合	學校宣導活動照片，或上課講義及簽到表
九、個人資料保護法				
46	【規劃】 建立個人資料保護管理政策。	2 分	符合 不符合	個人資料保護管理政策及校長核可簽核記錄
47	【界定個人資料之範圍】	2 分	符合	「個人資料檔案大綱」網站公布畫面

	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。		不符合	
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。	2 分	符合 不符合	個人資料提供同意書清冊照片
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。	2 分	符合 不符合	「個資保護聯絡窗口」置於單位網站畫面
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。	2 分	符合 不符合	個資調閱申請表或申請紀錄