108 年度資通安全維護計畫實施情形參考表

說明：

1.本次目的是協助學校完成資訊安全管理機制，以符合資通安全維護計畫之相關要求。

2.請就文件規範記錄或收集相關資料(可以擷取畫面)，若沒有相關客觀證據，請提出改善建議。

3.每題所提出之資料或相關證據僅作參考，若有其他相關資訊可以盡量收集，由線上審查人員或縣市承辦人員判斷是否足夠。

4.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「教育部全國中小學資訊安全管理系統」網址 http://isas.moe.edu.tw，請以各縣市 Open ID 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、核心業務及其重要性				
01	依據資通安全維護計畫，學校應檢視校內資通業務及重要性盤點。	2 分	符合 不符合	資通業務盤點清單或學校資通安全維護計畫中核心與非核心業務部分
二、資通安全政策及目標				
02	訂定學校資通安全政策及目標，並經校長簽核及公告。	2 分	符合 不符合	1.資通安全維護計畫 2.校長核可簽核記錄 3.公告記錄
03	定期召開資通安全管理審查會議，並檢視資安維護計畫實施情形及檢討資通安全政策。	2 分	符合 不符合	相關會議記錄或會議照片
三、設置資通安全推動組織				
04	學校應設置資通安全管理長及資安推動小組，負責推動及執行資通安全相關業務。	2 分	符合 不符合	資通安全維護計畫中設有資通安全長及推動小組，含組織、分工名單
四、人力及經費之配置				
05	依據資通安全維護計畫，學校需設置資通安全人員，並鼓勵相關人員取得資安證照或參加相關教育訓練課程；並考量業務之需求分配資安或資訊相關經費。	2 分	符合 不符合 不適用	資通安全維護計畫中敘明配置資通安全人員及資安或資訊相關經經費情形 (D、E 級可選不適用)
五、資訊及資通系統之盤點及核心資通系統、相關資產之標示				
06	依據資通安全維護計畫，學校應盤點資通訊系統，並完成安全	2 分	符合	盤點資通訊系統清冊 (D、E 級可選

	等級分級防護基準評估。		不符合 不適用	不適用)
六、資通安全風險評估				
07	依據資通安全維護計畫，學校應完成資訊及資產相關之風險分析評估及處理；並將評估結果擬定因應控制措施。	2 分	符合 不符合	相關文件或風險評估表
七、資通安全防護及控制措施				
08	學校應檢視資通安全防護及控制措施，並完成「資通安全責任等級與分級辦法」要求之安全性檢測、資通安全健診及資通安全防護措施。	2 分	符合 不符合 不適用	1.核心資通系統網站弱點掃描報告 2.核心資通系統滲透測試報告 3.資通安全健診報告 4.邏輯網路架構圖(D、E 級可選不適用)
09	【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
10	【網路控制措施】 應禁止以私人架設網路（如：行動網路、電話線等）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或學校資通安全管理規範(或資通安全維護計畫)，並公告畫面
11	【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。	2 分	符合 不符合 不適用	遠端連線作業設定畫面
12	【無線網路存取】	2 分	符合	1.加密金鑰設定畫面

	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，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。 (2)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。		不符合 不適用	2.帳號通行碼登入畫面
13	(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。	2 分	符合 不符合 不適用	教學使用之無線網路管理規定
14	(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。	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
15	【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說明畫面」，並加以描述
16	【存取權限之移除或調整】 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	帳號申請單及帳號清查表

17	【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	系統特權帳號清單，或校務行政系統模組權限設定畫面
18	【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。	2 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
19	【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 不符合	至少 2 位行政人員的個人電腦設定畫面
20	【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
21	【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。	2 分	符合 不符合 不適用	啟用與報廢紀錄單
22	【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）應定期(建議每週至少進行一次)備份工作；建議使用設備執行異地備份或使用外接式硬碟、隨身碟、光碟等執行或異地存放，並定期檢查備份資料之可用性與完整性。	2 分	符合 不符合 不適用	備份工作相關記錄
23	【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。	2 分	符合 不符合 不適用	資訊工作日誌

24	【資訊工作日誌】 系統管理人員應至少每季執行一次校時。	2 分	符合 不符合 不適用	系統校時畫面
25	【桌面淨空與螢幕淨空政策】 (1)個人辦公桌面應避免存放機敏性文件，結束工作時應妥善存放具有機密或敏感特性的資料（如公文、學籍資料等）。 (2)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	至少 2 位行政人員辦公桌面照片(含管控措施畫面如鍵盤鎖、螢幕保護畫面等）
26	【通行碼之使用】 (1)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)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	更改預設通行碼的畫面、資訊系統與服務帳號設定畫面
27	【通行碼之使用】 由學校發佈通行碼制定與使用規則給使用者，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，應該包含英文字及數字，長度為 8 碼（含）以上。	2 分	符合 不符合	使用者通行碼的設定畫面
28	【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 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
29	【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（如接地線、避雷針等）裝置，避免雷擊事件所造成設備損害情況。	2 分	符合 不符合	資訊機房空間電源箱接地線、避雷針或凸波電源保護裝置照片
30	【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
31	【溫濕度控制】	2 分	符合	機房內溫濕度顯示裝置照片

	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。		不符合 不適用	
32	【電源供應保護】 重要的資訊設備（如主機機房）應有適當電力保護設施，如設置 UPS、電源保護措施(如穩壓器、接地線等)，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。	2 分	符合 不符合 不適用	電力保護設施照片(UPS、穩壓器、接地線等)、緊急照明設備照片
33	【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 不符合	線路保護設施照片(如線槽、高架地板、套管等)
34	【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	啟用與報廢紀錄單
35	【財產攜出】 (1)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)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	設備進出紀錄表及登記歸還記錄
36	【設備安全管理】 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；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	【設備安全管理】 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	2 分	符合 不符合	可攜式儲存媒體(如隨身碟、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)

	體存放於上鎖儲櫃或安全處所。			
38	【人員安全責任管理】 非正式人員、臨時人員，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。	2 分	符合 不符合 不適用	學校內可能存取個資資料之臨時人員或義工簽署保密切結書
八、資通安全事件通報、應變及演練相關機制				
39	依據資通安全維護計畫應建置資通安全事件通報、應變及演練等相關機制。學校已建立資訊安全事件（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	資安事件通報程序
九、資通安全情資之評估及因應機制				
40	學校應檢視資通安全情資之評估及因應機制。	2 分	符合 不符合	資安維護計畫中資通安全情資部分、近期收到教育局資安通告處理情況的文件(如:公文)
十、資通系統或服務委外辦理之管理				
41	1.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，應要求委外廠商簽訂安全保密切結書。 2.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。 3.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 4.依據資通安全維護計畫，學校如有資通系統或服務委外辦理之管理，應檢視委外廠商資通安全維護情形。	2 分	符合 不符合 不適用	1.擷取資訊業務委外合約有資安規定部分或服務委外單位服務暨保密切結書 2.委外廠商人員保密切結書 3.帳號申請單 4.廠商資通安全維護文件或計畫 (無資訊委外廠商可選不適用)
十一、資通安全教育訓練				
42	依據資通安全維護計畫，學校應辦理資訊安全教育訓練或宣導活動，提昇校園資訊安全認知能力。	2 分	符合 不符合	學校宣導照片，或講義及簽到表
十二、公務機關所屬人員辦理業務涉及資通安全事項之考核機制				

43	依據資通安全維護計畫，相關人員辦理業務涉及資通安全應建立或列入考核機制。	2 分	符合 不符合	相關考核機制文件或已有規定進行平時及年終考核之文件
十三、資通安全維護計畫及實施情形之持續精進及績效管理機制				
44	依據資通安全維護計畫，提出資通安全維護計畫實施情形，對於不符合事項進行改善。	2 分	符合 不符合	不符合事項改善報告之文件