新北市市立明德高中(D級)

資訊安全線上評量報告書

製作日期：110 年 3 月 17 日

一、依據

資通安全管理法辦理。

二、目的

因應「資通安全管理法」、「資通安全管理法施行細則」、「資通安全責任等級分級辦法」、「資通安全維護計畫」等相關規定，為了解各校資訊安全管理工作執行情形，特安排資訊安全線上評量(稽核)及實地輔導訪視作業，以協助各校建置資訊安全環境，落實資訊安全管理。

三、評量項目

包含以下十三大項，詳見「資通安全維護計畫實施情形參考表」。

(一)核心業務及其重要性網路安全

(二)資通安全政策及目標

(三)設置資通安全推動組織

(四)人力及經費之配置

(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

(六)資通安全風險評估

(七)資通安全防護及控制措施(資安控制項題目)

(八)資通安全事件通報、應變及演練相關機制

(九)資通安全情資之評估及因應機制

(十)資通系統或服務委外辦理之管理

(十一)資通安全教育訓練

(十二)公務機關(構)所屬人員辦理業務涉及資通安全事項之考核機制

(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

四、評量(稽核)方式

第一階段：採學校自行內部自評(稽核)，相關資料請線上填報辦理情形

由參與學校先依「資通安全維護計畫實施情形參考表」自評，於109年6月1日~109年8月31日期間，登入「高中職暨國中小學資訊安全管理系統平台（https://isas.moe.edu.tw）」填報，並上傳相關佐證資料，供本局(處)作線上審查。

第二階段：審查人員線上審查作業

由各縣市相關承辦人員及教育部教育體系稽核人員、資安輔導顧問進行線上審查。

第三階段：實地輔導訪視

線上審查完畢後，安排到校資安訪視輔導(日期另行通知)，由各縣市教育局(處)及資安顧問組成資安訪視輔導團，自受稽學校中抽出部分學校進行到校輔導訪查，確認線上審查項目落實程度。

五、審查(稽核)人員:

本局(處)聘請教育部教育體系稽核人員或資安業務承辦人員、資安輔導團。

六、評定標準

評定以參考「行政院國家資通安全會報資通安全作業管考系統」檢核結果:

「辦理中，未逾限」、「辦理中，已逾限」、「已完成，未逾限」、「已完成，已逾限」、「不適用」作為評比標準。

以下為評定標準定義：

(一)辦理中，未逾限:該題項目正在辦理中，未超過法規期限。

(二)辦理中，已逾限:該題項目正在辦理中，已超過法規期限。

(三)已完成，未逾限:已經完成該題項目，未超過法規期限。

(四)已完成，已逾限:已經完成該題項目，已超過法規期限。

(五)不適用:該題選項不適用。

七、審查結果優點與建議：

(一)建議：

18項：建議使用氣體式滅火器。

八、學校背景資料

序	項目內容	填答
01	學校班級數	62
02	學校處理資訊業務、資訊安全人力概況	設置資訊組，資訊組長一人。
03	學校行政電腦數量	60
04	學校班級電腦數量	62
05	學校電腦教室或專任教室電腦數量	240
06	學校可攜式設備(公發手機、平板電腦、筆記型電腦)數量	117

九、線上評量檢查表

受評量單位：明德高中　評量人員：蔣慧珍　評量日期：109年10月14日
自評結果：50分　　審查結果：48分

評量項目	自評	辦理情形	審查結果	執行現況或改善建議
一、核心業務及其重要性				
01.依據資通安全維護計畫，學校應	已完成，未	依資安法施行細	已完成，未	

檢視校內資通業務及重要性盤點。	逾限	則第七條規定，本校已將落實核心業務及核心資通系統之界定，盤點核心業務及重要性，108年核心業務計4項，並已將敘明於109年維護計畫中。	逾限	
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。	已完成，未逾限	本校資通安全政策已由本校校長核定及公告進行宣導。	已完成，未逾限	
03.定期召開資通安全管理審查會議，並檢視資通安全維護計畫實施情形及檢討資通安全政策。	已完成，未逾限	本校定期檢討資通安全政策及目標， 108學年計檢視 1次。	已完成，未逾限	
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。	已完成，未逾限	本校已指定校長為資通安全長，其職掌已訂於本校資通安全維護計畫內，並已設置資通安全推動小組，負責推動及執行資通安全相關業務。	已完成，未逾限	
四、人力及經費之配置				
05.依據資通安全維護計畫，學校得配置一名資通安全專責人員，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。	不適用	本校屬D級。	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，學校應盤點資通系統及資產。	已完成，未逾限	本校已於109 年07 月24日完成	已完成，未逾限	

		資通訊系統及資產盤點，並建立本校資通系統資產清冊，相關資料如附件，本校並無大陸品牌資訊產設備。		
07.依據資通安全維護計畫，針對自行或委外開發之資通系統，學校應完成資通系統分級及防護基準。(無自行開發、維運等資通訊系統或資安等級D級可選不適用)	不適用	本校依資通安全責任等級分級辦法，被核定為資通安全責任等級D級，已完成資通系統分級及防護準評估。	不適用	
六、資通安全風險評估				
08.依據資通安全維護計畫，學校應完成資通訊(產)相關之風險分析評估及處理；並評估結果擬定因應控制措施。	已完成，未逾限	本校已於109年07月24日完成資訊風險分析評估，其評估方式及評估結果已於風險評估表文件內。本校針對風險評估結果已擬定對應之資通安全防護及控制措施，並敘明於資通安全維護計畫文件內，完成防護及控制措施	已完成，未逾限	
七、資通安全防護及控制措施				
09.學校如有自行開發、維運等資通訊系統，每二年辦理一次資通安全健診、網站弱點掃描、滲透測試。(無自行開發、維運等資通訊系統或資安等級D級可選不適用)	不適用	本校依資通安全責任等級分級辦法，被核定為資通安全責任等級D級，已完成資通系統分級及防護準評估。	不適用	
10.結合學校內部管理機制，每年辦理一次資通安全自我檢查作業。	已完成，未逾限	本校依資安法及校內資通安全維護計畫，已於109 年07月24日	已完成，未逾限	

		完成校內資通安全自我檢查作業。		
11.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，依業務性質之不同，區分不同內部網路網段(如：教學、行政、宿網等)，以降低未經授權存取之風險。	已完成，未逾限	本校依資通安全維護計畫，已於109年07 月24日更新及檢視校內網路架構圖及網段對應資料。	已完成，未逾限	
12.專供行政使用之無線網路熱點建議設定加密金鑰防護，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。	已完成，未逾限	本校依資通安全維護計畫，已於109年07月24日更新及檢視校內無線網路管控措施。	已完成，未逾限	
13.依據資通安全責任等級應辦事項，學校應完成資通安全防護，建置網路防火牆，並持續使用及適時進行軟、硬體之必要更新或升級。	已完成，未逾限	本校依資安法及校內資通安全維護計畫，已於109年07月24日確認並持續完成軟、硬體必要更新或升級。	已完成，未逾限	
14.依據資通安全責任等級應辦事項，學校應完成資通安全防護，電腦應建置防毒軟體，並定期更新軟體病毒碼。	已完成，未逾限	本校依資安法及校內資通安全維護計畫，已於109年07月24日確認並持續完成防毒軟體建置及更新病毒碼。	已完成，未逾限	
15.依據資通安全責任等級應辦事項，學校應完成資通安全防護，學校具有郵件伺服器者，應備電子郵件過濾機制，並持續使用及適時進行軟、硬體之必要更新或升級。	已完成，未逾限	由G suite的Gmail過濾機制管理。	已完成，未逾限	
16.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），個人電腦不使用時，應使用鍵盤鎖或其他控管措施保護個人電腦安全，個人電腦應設定螢幕保護機制。	已完成，未逾限	本校依校內資通安全維護計畫，已提醒學校同仁避免在辦公桌面存放機敏性資料並設置螢幕保護機制。	已完成，未逾限	

17.由學校公告通行碼使用規則，使用者應該對持有通行碼盡保密責任，通行碼設定應包含英文字及數字，長度為8碼（含）以上。	已完成，未逾限	本校依校內資通安全維護計畫，已提醒學校同仁對通行碼盡保密責任並符合相關規定。	已完成，未逾限	
18.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。	已完成，未逾限	本校依校內資通安全維護計畫，已完成電腦教室設置偵煙、偵熱及滅火設備。	辦理中，已逾限	建議使用氣體式滅火器。
19.電腦教室應實施門禁管制。	已完成，未逾限	本校依校內資通安全維護計畫，已完成電腦教室實施門禁管制。	已完成，未逾限	
20.電腦教室等重要資訊設備應有適當電力保護設施，如設置UPS、電源保護措施(如：穩壓器等)，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。	已完成，未逾限	本校依校內資通安全維護計畫，已完成電腦教室設置電力保護(如 :UPS 、穩壓器等)，還有設置緊急照明設備。	已完成，未逾限	
21.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。	已完成，未逾限	本校公務用可攜式電腦設備已設定保護機制，如設定通行碼、圖形辨識、臉孔辨識或指紋辨識等；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。	已完成，未逾限	
22.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。	已完成，未逾限	本校依校內資通安全維護計畫，已完成保密切結書，給非正式人員、臨時人員	已完成，未逾限	

		等因業務需要須接觸機密文件時可以填寫。		
23.依據資通安全責任等級應辦事項，學校除因業務需求且無其他替代方案外，不得採購及使用危害國家資通安全產品。	已完成，未逾限	本校無使用危害國家資通安全產品。	已完成，未逾限	
八、資通安全事件通報、應變及演練相關機制				
24.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。學校應建立資訊安全事件（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。	已完成，未逾限	本校資通安全事件通報、應變及演練相關機制已訂定於資安事件通報程序文件內，並已納入資通安全責任等級分級辦法相關規定，定期檢核其執行情形。 1.資安事件通報：本校108 年通報事件0件。 2.通報應變演練：108年09月辦理1 次，計0次逾限通報。	已完成，未逾限	
九、資通安全情資之評估及因應機制				
25.學校應檢視資通安全情資之評估及因應機制。	已完成，未逾限	本校情資來源計有行政院資安處、教育部、本市教育局、本市資訊中心等4個管道。 資安維護計畫中擬定並檢視資通安全情資之評估及因應機制。 近期並無收到教育局資安通告處理情況的文件。	已完成，未逾限	
十、資通業務或服務委外辦理之管理				

26.採購資訊系統或服務委外廠商，應注意招標文件須包含ISMS導入、安全性檢測、稽核及執行等，學校如有資訊系統或服務委外廠商契約，須納入學校資通安全維護計畫相關規定，並透過會議、稽核等方式檢核執行情形。(無資訊服務委外廠商可選不適用)	不適用	本校無資訊系統或服務委外廠商。	不適用	
十一、資通安全教育訓練				
27.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。	已完成，未逾限	本校資通安全教育訓練要求已辦理本校資訊安全教育訓練或宣導活動。	已完成，未逾限	
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				
28.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。	已完成，未逾限	本校依據建立資通安全維護計畫及本市教育局相關計畫獎懲規定。	已完成，未逾限	
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				
29.依據資通安全維護計畫，對受審查(稽核)後的發現事項，提出改善措施，並進行審核。	已完成，未逾限	本校已透過資安推動小組審查資通安全維護計畫並討論改善。	已完成，未逾限	