臺中市政府教育局所屬學校

資通安全防護計畫

中華民國 109 年 11 月 18 日

臺中市政府教育局所屬學校資通安全防護計畫

目　　錄

內容

壹、依據及目的：

一、依據：本計畫依據教育部 109 年 4 月 20 日臺教資(四)字第 1090054520 號函辦理。

二、目的：

(一)配合教育部資訊資源向上集中計畫，推動本局所屬學校核心資通系統向上集中，並依資通安全責任等級分級辦法第十條第四款，調整本局所屬學校資通安全責任等級為 D 級。

(二)藉以建構校園資通安全環境，保護學校教職員生權益，並降低教師行政負擔。

貳、辦理所屬學校向上集中之主責機關及單位：

一、主責機關：臺中市政府教育局。

二、主責單位：本局課程教學科。

參、所屬學校清單:

本局所屬學校其中高級中等學校計 27 校、國民中學計 71 校(含 3 所國中小)、國民小學計 229 校，合計 327 校，詳如附表 1。

肆、所屬學校核心資通系統向上集中規劃：

一、核心資通系統清單及維運單位：

NO	核心資通系統名稱	維運單位	補充說明
1	各校官方網站(WWW)	本局資訊教育暨網路中心	自建集中式系統平臺
2	網域名稱服務(DNS)-雲端 DNS 管理系統	本局資訊教育暨網路中心	自建集中式系統平臺
3	電子郵件伺服器(MAIL)-教育部雲端電子郵件	教育部	本局無自建郵件伺服器，本局各校教職員工使用縣市帳號登入使用教育部雲端電子郵件帳號做為公務信箱。
4	學習歷程檔案系統	國教署	1. 國中小各校無此系統。 2. 高中職各校使用國教署建置之集中式平臺模組。

5	校務行政 5-1 國中小雲端校務系統	本局資訊教育暨網路中心	1. 國中小各校使用本局自建集中式平臺。 2. 高中職各校使用本局規畫建置之集中式平臺。
	校務行政 5-2 高中職校務行政系統	本局委託北科大管理	

伍、各機關應辦事項及作業時程：

一、學校應配合辦理事項及作業時程：

NO	學校應辦事項	目標	期程
1	資訊及資產盤點作業	盤點各校核心資通系統及非核心資通系統清單。	109 年 4 月 20 日～ 109 年 5 月 7 日。
2	核心資通系統向上集中	各校核心資通系統均於 109 年 12 月 31 日之前申請向上集中。	109 年 4 月 20 日～ 109 年 12 月 31 日。
3	資安防護作業事項 (附表 2)	各校尚維運之非核心系統均依附表 2 應辦事項於期限內完成相關資安防護作業。	109 年 4 月 20 日～ 109 年 12 月 31 日止。

二、向上集中主責單位應配合辦理事項及作業時程：

NO	向上集中主責單位應辦事項	目標	期程
1	檢視其所屬學校資訊資產盤點結果	學校能確實盤點資訊資產，核心資通系統能全部向上集中，非核心資通系統能列冊並進行相關防護作為。	109 年 4 月 20 日～ 109 年 5 月 8 日。
2	核心資通系統向上集中作業事項及期程	各校官方網站(WWW) 向上集中至本局	已辦理培訓，109 年 12 月 31 日前完成所屬學校官網向上集中作業。
		網域名稱服務(DNS) 向上集中至本局	已於 108 年建置完成單一集中平臺。

		Mail 伺服器 向上集中至教育部	已於108年建置完成所屬學校教職員工之openid帳號。
		國(中)小校務行政系統 向上集中至本局	已於108年建置完成單一集中平臺，本市國中小已上線使用。
		高中職校務行政系統 向上集中至本局	109年4月20日～ 109年12月31日止。
		學習歷程檔案系統 向上集中至國教署	109年4月20日～ 109年12月31日止。
3	資安防護作業事項 (如附表3)	依資通安全責任等級分級辦法之附表3資通安全責任等級 B 級之公務機關應辦事項辦理資安防護。	109年4月20日～ 109年12月31日止。

陸、所屬學校之非核心資通系統清單及防護作為：

本局所屬學校之非核心資通系統清單，如附表1（略)；其採行相關之防護及控制措施如下:

一、資訊及資通系統之管理

（一） 資訊及資通系統之保管

1. 資訊及資通系統管理人應確保資訊及資通系統已盤點造冊並適切分級，並持續更新以確保其正確性。
2. 資訊及資通系統管理人應確保資訊及資通系統被妥善的保存或備份。
3. 資訊及資通系統管理人應確保重要之資訊及資通系統已採取適當之存取控制政策。

(二)資訊及資通系統之使用

1. 本局所屬學校同仁使用資訊及資通系統前應經其管理人授權。
2. 本局所屬學校同仁使用資訊及資通系統時，應留意其資通安全要求事項，並負對應之責任。

3. 本局所屬學校同仁使用資訊及資通系統後，應依規定之程序歸還。資訊類資訊之歸還應確保相關資訊已正確移轉，並安全地自原設備上抹除。
4. 非學校人員使用本局所屬學校之資訊及資通系統，應確實遵守各校之相關資通安全要求，且未經授權不得任意複製資訊。
5. 對於資訊及資通系統，宜識別並以文件記錄及實作可被接受使用之規則。

(三)資訊及資通系統之刪除或汰除

1. 資訊及資通系統之刪除或汰除前應評估學校是否已無需使用該等資訊及資通系統，或該等資訊及資通系統是否已妥善移轉或備份。
2. 資訊及資通系統之刪除或汰除時宜加以清查，以確保所有機敏性資訊及具使用授權軟體已被移除或安全覆寫。
3. 具機敏性之資訊或具授權軟體之資通系統，宜採取實體銷毀，或以毀損、刪除或覆寫之技術，使原始資訊無法被讀取，並避免僅使用標準刪除或格式化功能。

二、存取控制與加密機制管理

(一)網路安全控管

1. 應定期檢視防火牆政策是否適當，並適時進行防火牆軟、硬體之必要更新或升級。
2. 對於通過防火牆之來源端主機 IP 位址、目的端主機 IP 位址、來源通訊埠編號、目的地通訊埠編號、通訊協定、登入登出時間、存取時間以及採取的行動，均應予確實記錄。
3. 本機關內部網路之區域應做合理之區隔，使用者應經授權後在授權之範圍內存取網路資源。
4. 使用者應依規定之方式存取網路服務，不得於辦公室內私裝電腦及網路通訊等相關設備。
5. 遵循資通安全管理法暨臺灣學術網路管理規範。

6.無線網路防護

(1)機密資料原則不得透過無線網路及設備存取、處理或傳送。

(2)行動通訊或紅外線傳輸等無線設備原則不得攜入涉及或處理機密資料之區域。

(3)用以儲存或傳輸資料且具無線傳輸功能之個人電子設備與工作站，應安裝防毒軟體，並定期更新病毒碼。

7.網域名稱系統(DNS)防護:

(1)一般伺服器應關閉 DNS 服務，防火牆政策亦應針對 DNS 進行控管，關閉不需要的 DNS 服務存取。

(2)DNS 伺服器應經常性進行弱點漏洞管理與修補、落實存取管控機制。

(3)DNS 伺服器應設定指向 EDU Cache DNS。

(4)內部主機位置查詢應指向機關內部 DNS 伺服器。

(二)資通系統權限管理

1.本局所屬學校之資通系統應設置通行碼管理，通行碼之要求需滿足：

(1)通行碼長度 8 碼以上。

(2)通行碼複雜度應包含英文大寫小寫、特殊符號或數字三種以上。

(3)使用者每 90 天應更換一次通行碼。

2.使用者使用資通系統前應經授權，並使用唯一之使用者 ID，除有特殊營運或作業必要經核准並紀錄外，不得共用 ID。

3.使用者無繼續使用資通系統時，應立即停用或移除使用者 ID，資通系統管理者應定期清查使用者之權限。

(三)特權帳號之存取管理

1.資通系統之特權帳號請應經正式申請授權方能使用，特權帳號授權前應妥善審查其必要性，其授權及審查記錄應留存。

2.資通系統之特權帳號不得共用。

3.對於特權帳號，宜指派與該使用者日常公務使用之不同使用者 ID。

4.資通系統之特權帳號應妥善管理，並應留存特殊權限帳號之使用軌跡。

5.資通系統之管理者每季應清查系統特權帳號並劃定特權帳號逾期之處理方式。

(四)加密管理

1.本局所屬學校之機密資訊於儲存或傳輸時應進行加密。

2.本局所屬學校之加密保護措施應遵守下列規定：

(1)應落實使用者更新加密裝置並備份金鑰。

(2)應避免留存解密資訊。

(3)一旦加密資訊具遭破解跡象，應立即更改之。

三、作業與通訊安全管理

(一)防範惡意軟體之控制措施

1.本局所屬學校之主機及個人電腦應安裝防毒軟體，並時進行軟、硬體之必要更新或升級。

(1)經任何形式之儲存媒體所取得之檔案，於使用前應先掃描有無惡意軟體。

(2)電子郵件附件及下載檔案於使用前，宜於他處先掃描有無惡意軟體。

(3)確實執行網頁惡意軟體掃描。

2.使用者未經同意不得私自安裝應用軟體，管理者並應每半年定期針對管理之設備進行軟體清查。

3.使用者不得私自使用已知或有嫌疑惡意之網站。

4.設備管理者應定期進行作業系統及軟體更新，以避免惡意軟體利用系統或軟體漏洞進行攻擊。

(二)遠距工作之安全措施

1.本局所屬學校資通系統之操作及維護以現場操作為原則，避免使用遠距工作，如有緊急需求時，應申請並經資通安全推動小組同意後始可開通。

2. 資通安全推動小組應定期審查已授權之遠距工作需求是否適當。

3. 針對遠距工作之連線應採適當之防護措施(並包含伺服器端之集中過濾機制檢查使用者之授權)，並且記錄其登入情形。

(1) 提供適當通訊設備，並指定遠端存取之方式。

(2) 提供虛擬桌面存取，以防止於私有設備上處理及儲存資訊。

(3) 進行遠距工作時之安全監視。

(4) 遠距工作終止時之存取權限撤銷，並應返還相關設備。

(三)電子郵件安全管理：

1. 本局所屬學校配合向上集中計畫，本局及所屬學校無建置電子郵件伺服器，本局所屬學校教職員工均申請教育部雲端電子郵件為公務信箱。

2. 遵循資通安全管理法及教育體系電子郵件服務與安全管理指引之相關規範。

(四)確保實體與環境安全措施

1. 資料中心及電腦機房之門禁管理

(1)資料中心及電腦機房應進行實體隔離。

(2)學校人員或來訪人員應申請及授權後方可進入資料中心及電腦機房 ，資料中心及電腦機房管理者並應定期檢視授權人員之名單。

(3)人員進入管制區應配載身分識別之標示，並隨時注意身分不明或可疑人員。

(4)僅於必要時，得准許外部支援人員進入資料中心及電腦機房。

(5)人員及設備進出資料中心及電腦機房應留存記錄。

2. 資料中心及電腦機房之環境控制

(1)資料中心及電腦機房之空調、電力應建立備援措施。

(2) 資料中心及電腦機房之溫濕度管控範圍為：

(3) 各項安全設備應定期執行檢查、維修，並應定時針對設備之管理者進行適當之安全設備使用訓練。

3.辦公室區域之實體與環境安全措施

(1) 應考量採用辦公桌面的淨空政策，以減少文件及可移除式媒體等在辦公時間之外遭未被授權的人員取用、遺失或是被破壞的機會。

(2) 文件及可移除式媒體在不使用或不上班時，應存放在櫃子內。

(3) 機密性及敏感性資訊，不使用或下班時應該上鎖。

(4) 機密資訊或處理機密資訊之資通系統應避免存放或設置於公眾可接觸之場域。

(5) 顯示存放機密資訊或具處理機密資訊之資通系統地點之通訊錄及內部人員電話簿，不宜讓未經授權者輕易取得。

(6) 資訊或資通系統相關設備，未經管理人授權，不得被帶離辦公室。

(五)資料備份

1. 重要資料及核心資通系統應進行資料備份，其備份之頻率應滿足復原時間點目標之要求，並執行異地存放。

2. 本局所屬學校應每季確認非核心資通系統資料備份之有效性。且測試該等資料備份時，宜於專屬之測試系統上執行，而非直接於覆寫回原資通系統。

3. 敏感或機密性資訊之備份應加密保護。

(六)媒體防護措施

1. 使用隨身碟或磁片等存放資料時，具機密性、敏感性之資料應與一般資料分開儲存，不得混用並妥善保管。

2. 資訊如以實體儲存媒體方式傳送，應留意實體儲存媒體之包裝，選擇適當人員進行傳送，並應保留傳送及簽收之記錄。
3. 為降低媒體劣化之風險，宜於所儲存資訊因相關原因而無法讀取前，將其傳送至其他媒體。
4. 對機密與敏感性資料之儲存媒體實施防護措施，包含機密與敏感之紙本或備份磁帶，應保存於上鎖之櫃子，且需由專人管理鑰匙。

(七)電腦使用之安全管理

1. 電腦、業務系統或自然人憑證，若超過十分鐘不使用時，應立即登出或啟動螢幕保護功能並取出自然人憑證。
2. 禁止私自安裝點對點檔案分享軟體及未經合法授權軟體。
3. 連網電腦應隨時配合更新作業系統、應用程式漏洞修補程式及防毒病毒碼等。
4. 筆記型電腦及實體隔離電腦應定期以人工方式更新作業系統、應用程式漏洞修補程式及防毒病毒碼等。
5. 下班時應關閉電腦及螢幕電源。
6. 如發現資安問題，應主動循機關之通報程序通報。
7. 支援資訊作業的相關設施如影印機、傳真機等，應安置在適當地點，以降低未經授權之人員進入管制區的風險，及減少敏感性資訊遭破解或洩漏之機會。

(八)行動設備之安全管理

1. 機密資料不得由未經許可之行動設備存取、處理或傳送。
2. 機敏會議或場所不得攜帶未經許可之行動設備進入。

四、獲取、開發及維護

本局所屬學校之資通系統應依「資通安全責任等級分級辦法」附表九之規定完成系統防護需求分級，依分級之結果，完成附表十之資通系統防護基準，並注意下列事項：

(一)開發過程請依安全系統發展生命週期(Secure Software Development Life Cycle, SSDLC)納入資安要求，並參考行政院國家資通安全會報頒布之最新「安全軟體發展流程指引」、「安全軟體設計指引」及「安全軟體測試指引」。

(二)於資通系統開發前，設計安全性要求，包含機敏資料存取、用戶登入資訊檢核及用戶輸入輸出之檢查過濾，並檢討執行情形。

(三)於上線前執行安全性要求測試，包含機敏資料存取、用戶登入資訊檢核及用戶輸入輸出之檢查過濾測試，並檢討執行情形。

(四)執行資通系統源碼安全措施，包含源碼存取控制與版本控管，並檢討執行情形。

五、業務持續運作演練及安全性檢測

（一）本局所屬學校全部核心資通系統已向上集中至本局或教育部等政府機關，並應配合教育局規定參與持續運作演練計畫。

（二）本局所屬學校全部核心資通系統已向上集中至本局或教育部等政府機關，將配合教育局網站安全弱點檢測及系統滲透測試結果，修補漏洞及更新相關修正程式。

六、執行資通安全健診

本局所屬學校仍維運之非核心資通系統配合教育部規定每二年(109 年)應辦理資通安全健診 1 次，其至少應包含下列項目，並檢討執行情形：

(一)網路架構檢視。

(二)網路惡意活動檢視。

(三)使用者端電腦惡意活動檢視。

(四)具有伺服器主機者，應進行伺服器惡意活動檢視。

(五)具有目錄伺服器者，應檢視目錄伺服器設定。

(六)具有防火牆者，應檢視防火牆連線設定。

七、資通安全防護設備

(一)本局所屬學校應建置防毒軟體、網路防火牆、電子郵件過濾裝置，持續使用並適時進行軟、硬體之必要更新或升級。

(二)資安設備應定期備份日誌紀錄，定期檢視並由主管複核執行成果，並檢討執行情形。

由資通安全推動小組彙整情資後進行風險評估，並依據資通安全維護計畫之控制措施採行相應之風險預防機制。

八、資通系統或服務委外辦理之管理

本局所屬學校委外辦理資通系統之建置、維運或資通服務之提供時，應考量受託者之專業能力與經驗、委外項目之性質及資通安全需求，選任適當之受託者，並監督其資通安全維護情形。

(一)、選任受託者應注意事項

1. 受託者辦理受託業務之相關程序及環境，應具備完善之資通安全管理措施或通過第三方驗證。
2. 受託者應配置充足且經適當之資格訓練、擁有資通安全專業證照或具有類似業務經驗之資通安全專業人員。
3. 受託者辦理受託業務得否複委託、得複委託之範圍與對象，及複委託之受託者應具備之資通安全維護措施。

(二)、監督受託者資通安全維護情形應注意事項

1. 受託業務包括客製化資通系統開發者，受託者應提供該資通系統之第三方安全性檢測證明；涉及利用非自行開發之系統或資源者，並應標示非自行開發之內容與其來源及提供授權證明。

2. 受託者執行受託業務，違反資通安全相關法令或知悉資通安全事件時，應立即通知委託機關及採行之補救措施。
3. 委託關係終止或解除時，應確認受託者返還、移交、刪除或銷毀履行委託契約而持有之資料。
4. 受託者應採取之其他資通安全相關維護措施。
5. 本機關應定期或於知悉受託者發生可能影響受託業務之資通安全事件時，以稽核或其他適當方式確認受託業務之執行情形。

柒、資通安全事件通報、應變及演練相關機制

為即時掌控資通安全事件，並有效降低其所造成之損害，本局所屬學校依「臺灣學術網路各級學校資通安全通報應變作業程序」辦理資通安全事件通報、應變及演練。

捌、資通安全教育訓練

一、資通安全教育訓練要求

(一)本局所屬學校依資通安全責任等級分級屬調降為D級，資安及資訊人員每年至少1名人員接受12小時以上之資安專業課程訓練或資安職能訓練。

(二)本機關之一般使用者與主管，每人每年接受3小時以上之一般資通安全教育訓練。

二、資通安全教育訓練辦理方式

(一)每年參加教育部、各大專院校、臺中市政府、教育局辦理之資通安全教育訓練或利用數位學習以建立員工資通安全認知，提升機關資通安全水準，並應保存相關之資通安全認知宣導及教育訓練紀錄。

(二)員工報到時，應使其充分瞭解學校資通安全相關作業規範及其重要性。

(三)資通安全教育及訓練之政策，除適用所屬員工外，對學校外部的使用者，亦應一體適用。

(四)承辦單位應於每年年初，考量管理、業務及資訊等不同工作類別之需求，擬定資通安全認知宣導及教育訓練計畫，以建立員工資通安全認知，提升學校資通安全水準，並應保存相關之資通安全認知宣導及教育訓練紀錄。

(五)本局所屬學校辦理校內資通安全認知宣導及教育訓練內容得包含：

1. 資通安全政策(含資通安全維護計畫之內容、管理程序、流程、要求事項及人員責任、資通安全事件通報程序等)。
2. 資通安全法令規定。
3. 資通安全作業內容。
4. 資通安全技術訓練。

(六)員工報到時，應使其充分瞭解學校資通安全相關作業規範及其重要性。

(七)資通安全教育及訓練之政策，除適用所屬員工外，對學校外部的使用者，亦應一體適用。

玖、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

本局所屬學校所屬人員之平時考核或聘用，依據公務機關所屬人員資通安全事項獎懲辦法、臺中市政府及所屬各機關學校公務人員平時獎懲案件處理要點，及本機關各相關規定辦理之。

拾、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

一、本局所屬學校資通安全維護計畫之實施

為落實本安全維護計畫，使本局所屬學校之資通安全管理有效運作，相關單位於訂定各階文件、流程、程序或控制措施時，應與本局之資通安全政策、目標及本安全維護計畫之內容相符，並應保存相關之執行成果記錄。

二、所屬學校資通安全維護計畫實施情形之稽核機制

(一)稽核機制之實施

1. 資通安全推動小組應於 12 月前(至少每年一次)或於系統重大變更或組織改造後執行 1 次內部稽核作業(自我檢查

作業)，以確認人員是否遵循本規範與機關之管理程序要求，並有效實作及維持管理制度。

2. 辦理稽核前資通安全推動小組應擬定資通安全稽核計畫並安排稽核成員，稽核計畫應包括稽核之依據與目的、期間、重點領域、稽核小組組成方式、保密義務、稽核方式、基準與項目及受稽單位協助事項，並應將前次稽核之結果納入稽核範圍。

3. 辦理稽核時，資通安全推動小組應於執行稽核前 15 日，通知受稽核單位，並將稽核期程、稽核項目紀錄表及稽核流程等相關資訊提供受稽單位。

4. 本局所屬學校之稽核人員應受適當培訓並具備稽核能力，且不得稽核自身經辦業務，以確保稽核過程之客觀性及公平性；另，於執行稽核時，應填具稽核項目紀錄表，待稽核結束後，應將稽核項目紀錄表內容彙整至稽核結果及改善報告中，並提供給受稽單位填寫辦理情形。

5. 稽核結果應對相關管理階層(含資安長)報告，並留存稽核過程之相關紀錄以作為資通安全稽核計畫及稽核事件之證據。

6. 稽核人員於執行稽核時，應至少執行一項特定之稽核項目（如是否瞭解資通安全政策及應負之資安責任、是否訂定人員之資通安全作業程序與權責、是否定期更改密碼)。

7. 本局所屬學校稽核作業得併同政風單位電腦稽核或主計單位內控稽核辦理，惟稽核項目應參照本機關資通安全維護計畫，檢視機關實施情形及績效。

8. 本局所屬學校應配合上級或監督機關之規定辦理查核作業，以確認人員是否遵循本計畫與機關之管理程序要求，並有效實作及維持管理制度。

(二)稽核改善報告

1. 受稽單位於稽核實施後發現有缺失或待改善項目者，應對缺失或待改善之項目研議改善措施、改善進度規劃，並落實執行。

2. 受稽單位於稽核實施後發現有缺失或待改善者，應判定其發生之原因，並評估是否有其類似之缺失或待改善之項目存在。
3. 受稽單位於判定缺失或待改善之原因後，應據此提出並執行相關之改善措施及改善進度規劃，必要時得考量對現行資通安全管理制度或相關文件進行變更。
4. 本局所屬學校應定期審查受稽單位缺失或待改善項目所採取之改善措施、改善進度規劃及佐證資料之有效性。
5. 受稽單位於執行改善措施時，應留存相關之執行紀錄，並填寫稽核結果及改善報告。

三、資通安全維護計畫之持續精進及績效管理

(一)本局所屬學校之資通安全推動小組應於 12 月前(每年至少一次)召開資通安全管理審查會議，確認資通安全維護計畫之實施情形，確保其持續適切性、合宜性及有效性。

(二)管理審查議題應包含下列討論事項：

1.過往管理審查議案之處理狀態。

2.與資通安全管理系統有關之內部及外部議題的變更，如法令變更、上級機關要求、資通安全推動小組決議事項等。

3.資通安全維護計畫內容之適切性。

4.資通安全績效之回饋，包括：

(1) 過往管理審查議案之處理狀態。

(2) 與資通安全管理系統有關之內部及外部議題的變更，如法令變更、上級機關要求、資通安全推動小組決議事項等。

(3) 資通安全維護計畫內容之適切性。

(4) 資通安全績效之回饋，包括：

A. 資通安全政策及目標之實施情形。

B. 資通安全人力及資源之配置之實施情形。

C. 資通安全防護及控制措施之實施情形。

D. 內外部稽核結果。

E. 不符合項目及矯正措施。

(5) 風險評鑑結果及風險處理計畫執行進度。

(6) 重大資通安全事件之處理及改善情形。

(7) 利害關係人之回饋。

(8) 持續改善之機會。

(三)持續改善機制之管理審查應做成改善績效追蹤報告，相關紀錄並應予保存，以作為管理審查執行之證據。

壹拾壹、資通安全防護計畫實施情形之提出

本局所屬學校依據資通安全管理法第 12 條之規定，依主管機關(行政院)規定期限向上級或監督機關，提出資通安全維護計畫實施情形，使其得瞭解本局所屬學校之年度資通安全計畫實施情形。

壹拾貳、附表及附件

附表 2 仍維運資通系統學校應辦事項及執行期程表

制度面向	辦理項目	辦理項目細項	辦理內容
管理面	資通系統分級及防護基準		初次受核定或等級變更後之二年內(預計於 109 年 5 月 5 日前)，針對自行或委外開發之資通系統，依資通安全責任等級分級辦法附表九完成資通系統分級，其後應每年至少檢視一次(預計於 109 年 5 月 5 日前檢視完成)資通系統分級妥適性。
	內部資通安全稽核		結合學校內部管理機制，每年辦理一次(預計 109 年 12 月 31 日前完成)資通安全自我檢查作業。
	資通安全專責人員		初次受核定或等級變更後之一年內，(預計於 109 年 5 月 5 日前完成)配置一人。
技術面	資通安全健診	網路架構檢視	每二年辦理一次。(預計於 109 年 12 月 31 日前依左列項目內容或採取經教育部認可之措施完成 6 項檢視及缺失改善)。
		網路惡意活動檢視	
		使用者端電腦惡意活動檢視	
		具有伺服器主機者，應檢視伺服器主機惡意活動	
		具有目錄伺服器者，應檢視目錄伺服器設定	
		具有防火牆者，應檢視防火牆連線設定	
	資通安全防護	防毒軟體	初次受核定或等級變更後之一年內，完成各項資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級。 (應於 109 年 5 月 5 日前完成所有電腦及資通系統防毒軟體、網路防火牆更新或升級)
		網路防火牆	
		具有郵件伺服器者，應備電子郵件過濾機制	
認知與訓練	資通安全教育訓練	資通安全人員	每年至少一名資通安全人員（預計於 109 年 12 月 31 日前完成）接受十二小時以上之資通安全專業課程訓練或資通安全職能訓練。
		一般使用者及主管	每人每年（預計於 109 年 12 月 31 日前完成）接受三小時以上之一般資通安全教育訓練。

備註：各學校辦理本表「資通安全健診」時，除依本表所定項目、內容及時限執行外，亦得採取經本部認可之其他具有同等或以上效用之措施。