**資訊安全教育推廣及環境整備各校配合事項**

附件1

1. 資安認知推廣活動

（一）依據：本局以102年8月15日北市教資字第10238266900號函轉知教育部「102年度國中小學資安認知及資安推廣活動種子教師巡迴教育訓練」簡章。

（二）請學校配合事項

1.旨揭教育訓練結合教育部「102年度資安防護學園－網路小鐵人錦標賽」資安認知推廣活動，培訓各國中小學之資訊安全種子教師，並於結訓後協助前揭活動之推廣宣導。

2.請各校種子教師，協助其他資訊教師熟習前揭活動之線上操作，俾便指導全校學生皆於電腦課時參與旨揭資安認知推廣活動。

1. 資安通報聯絡人更新

（一）依據：教育機構資安通報應變手冊。

（二）請學校配合事項

1.填寫聯絡人資料：請各校現任資安聯絡人至教育機構資安通報平臺（網址https://info.cert.tanet.edu.tw）檢視並更新聯絡人之最新資料，並將完成更新後之螢幕畫面擷取成圖檔，並於**102年9月13日（星期五）**前逕寄至本局資訊教育科資安業務承辦人許世杰先生之公務信箱（jbrother@mail.taipei.gov.tw），俾利本局彙整。

2.請各校資安聯絡人手機保持開機，並隨時注意手機與信箱之告知通報，當學校收到EWA資安預警事件通知時，請盡速上資安通報平臺完成回復。

3.倘發生資安事件時，請於1小時內上資安通報平臺完成第一階段通報作業，若是由市網中心偵測到校園資安事件，應變處理完成時間如下：

 （1）2級資安事件：71小時內。

 （2）3、4級資安事件：35小時內。

三、完成教育部「國中、小學資通安全管理實施原則」自我檢測

（一）依據：教育部「國中、小學資通安全管理實施原則」（附件1-1）。

（二）請學校配合事項

1.請各校依教育部「國中、小學資通安全管理實施原則」落實執行。

2.請各校於**102年9月13日（星期五）**前完成填寫前揭自我檢測表（附件1-2），經完成校內核章流程後，將自我檢測表正本擲回本局資訊教育科許世杰先生，並請將自我檢測表掃瞄檔逕寄至jbrother@mail.taipei.gov.tw，本局將於檢視各校自我檢測表後，抽訪本局所屬學校百分之二十以上之校數。

四、線上申請弱點掃瞄服務

（一）依據：102年度教育部對各地方政府統合視導評分指標。

（二）請學校配合事項

1.請各校資訊安全業務承辦人至臺北市政府員工愛上網（網址為http://isw.taipei.gov.tw/）「資訊服務」項下之「設備與網路管理」頁面，於「資安管理」服務項下點選「掃瞄申請」，以線上申請弱點掃瞄服務。

2.請各校於**102年9月24日(星期二)**前將弱點掃瞄結果逕寄至本局資訊教育科資安業務承辦人許世杰先生之公務信箱(jbrother@mail.taipei.gov.tw）。

五、線上填報「教育部國民中小學資訊教學設備與使用狀況」系統

（一）依據：102年度教育部對各地方政府統合視導評分指標。

（二）請學校配合事項

1.本系統填報作業預計於11月份進行，本局資訊教育科將於收到教育部通知後正式函請各校上網填報。

2.請務必於各頁籤填完後都要按「填完送出」，方為完成該頁籤填報，並確認完成數為百分之百。

附件1-1

**國中、小學資通安全管理系統實施原則**

# 文件目標

本文件提供國中、小學資通安全系統管理實施原則建議。

# 適用範圍

國中、小學內電腦、資訊與網路服務相關的系統、設備、程序、及人員。

# 實施原則

1. **網路安全**
	1. 網路控制措施
* 學校與外界連線，應僅限於經由縣網中心之管控，以符合一致性與單一性之安全要求。
* 學校內特殊系統（例如會計系統、學生學籍、成績原始資料系統等）之資料，當有必要透過網路進行傳輸時，建議透過虛擬私有網路（Virtual Private Network, VPN）或同等連線方式進行；若無透過網路進行傳輸需求，則建議區隔於網路之外。
* 應禁止以電話線連結主機電腦或網路設備。
	1. 網路安全管理服務委外廠商合約之安全要求
* 委外開發或維護廠商必須簽訂安全保密切結書（參考切結書範本，文件編號A-1）。
1. **系統安全**
	1. 職責區隔
* 學校主機電腦可依個別應用系統之需要，設置專屬電腦，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）。
* 學校的行政系統主機（例如財務、人事、公文系統等）電腦，建議由各個縣（市）教育網路中心或教育局等單位統籌管理。
	1. 對抗惡意軟體、隱密通道及特洛依木馬程式
* 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
			* 定期（至少每個月）進行如「Windows Update」之程式更新作業，以防範作業系統之漏洞
* 學校內個人電腦所使用的軟體應有授權。
* 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。
	1. 資料備份
* 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；建議週期為每週進行一次。
	1. 操作員日誌
* 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。
* 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。[*參考日誌範本，文件編號A-2*]
			* 紀錄日誌項目人員姓名與簽名欄
	1. 資訊存取限制
* 學校內所共用的個人電腦應以特定功能為目的，並設定特定安全管控機制（例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）。
	1. 使用者註冊
* 學校應制定電腦系統使用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：
	+ - * 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。
			* 定期（建議每學期）檢查並取消多餘的使用者識別碼和帳號。
			* 定期（建議每學期）檢查新增之帳號，若有莫名帳號產生，應關閉帳號權限，並依通報程序請求處理（參照本文件2.10段落）。
	1. 特權管理
* 學校的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，應予以文件化記錄備查。
	1. 通行碼之使用
* 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。
* 資訊系統與服務應避免使用共同帳號及通行碼。
* 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，文件編號A-3*]，內容應包含以下各項：
	+ - * 使用者應該對其個人所持有通行碼盡保密責任
			* 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，例如生日、名字、鍵盤上聯繫的字母與數字（如12345678 或 asdfghjk），以及過多的重複字元等。或建議通行碼應該包含英文字大小寫、數字、特殊符號等四種設定中的三種。
* 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。
	1. 原始程式庫之存取控制
* 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，並防範資料庫隱碼(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。
	1. 通報安全事件與處理
* 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。
* 學校應建立資訊安全事件通報程序[*參照安全事件通報程序，編號A-4*]以及安全事件通報單[*參考安全事件通報單範本，文件編號A-5*]；通報程序應包括學校內部通報，以及學校與所屬縣市教育網路中心的通報。
* 當學校內部無法處理之資通安全事件，應通報其所屬縣市網路中心。
* 所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。
1. **實體安全**
	1. 設備安置及保護
* 學校重要的資訊設備（如主機機房）應置於設有空調空間。
* 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。
* 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、或有避雷針等裝置，避免如雷擊事件所造成損害情況。
* 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。
	1. 電源供應
* 學校重要的資訊設備（如主機機房）應有適當的電力設施，例如設置UPS、電源保護措施，以免斷電或過負載而造成損失。
	1. 纜線安全
* 學校資訊設備主機機房、電腦教室區域內應避免明佈線。
	1. 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，應先確保已將任何敏感資料和授權軟體刪除或覆寫。
	1. 設備維護
* 應與設備廠商建立維護合約。
* 廠商進入安全區域需簽訂安全保密切結書。
	1. 財產攜出
* 未經授權不應將學校的資訊設備、資訊或軟體攜出所在地。
* 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。
* 相關財產之攜出應依教育部或學校既有之相關規定處理。
	1. 桌面淨空與螢幕淨空政策
* 結束工作時，所有學校教職員工應將其所經辦或使用具有機密或敏感特性的資料（例如公文、學籍資料等）及資料的儲存媒體（如USB隨身碟、磁碟片、光碟等），妥善存放。
* 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。
1. **人員安全**
	1. 將安全列入工作執掌中
* 應將資訊安全納入教職員手冊說明中，以強化工作上之資訊安全意識。
	1. 資訊安全教育與訓練 
* 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。
* 學校鼓勵或安排資訊組長/老師/系統管理人員、以及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。
1. **應對以下各項相關法令有基礎之認知**
	1. 智慧財產權
* 經濟部智慧財產局 <http://www.tipo.gov.tw/>
* 著作權法 <http://www.tipo.gov.tw/copyright/copyright_law/copyright_law_92.asp>
	1. 個人資訊的資料保護及隱私
* 電腦處理個人資料保護法[www.fpppc.gov.tw/bulletin/menu4-7/93year/pcinfo.doc](http://www.fpppc.gov.tw/bulletin/menu4-7/93year/pcinfo.doc)
	1. 電子簽章法
* 電子簽章法
<http://www.moea.gov.tw/~meco/doc/ndoc/s5_p05.htm>
* 電子簽章法施行細則[http://www.moea.gov.tw/~meco/doc/ndoc/s5\_p05\_p01.htm](http://www.moea.gov.tw/~meco/doc/ndoc/s5_p05_p01.htm%22%20%5Ct%20%22_blank)
* 核可憑證機構名單
<http://www.moea.gov.tw/~meco/doc/ndoc/s5_p07_p03.htm>

文件編號：A-1

**資訊服務委外單位****服務暨保密切結書範本**

　　　　　　　　　公司(以下簡稱為本公司)為配合 學校（以下簡稱為貴校）之資訊應用業務需求，進行相關資訊系統或軟體開發、測試、建置及維護等工作。本公司提供資訊服務項目如下：

 一、

 二、

 三、

**(註：列出貴公司將會在健保資訊網上提供予醫事服務機構之服務項目)**

本公司願意在對貴校提供上述服務項目範圍內之服務時，保證因提供業務服務需存取貴校資訊系統中所存放，凡屬與公文機密、個人及事業單位權益相關之資料，無論其內容之一部或全部，均負保密之責；相關資料均以留在貴校內部範疇內處理，倘須由本公司攜至校外處理，應簽奉貴校核可。

本公司亦不私自蒐集貴校所擁有之任何資訊。若所提供之資訊業務服務，不符合上述之規定或經營之服務項目超出上述範圍，或違犯法令，本公司同意無異議接受接受法律制裁與及其訴訟費用，並負責所引發之各項損失賠償。此致

**XXX 學校**

申請單位及負責人蓋章：

日期：　　年　　月　　日

**本服務暨保密切結書一式兩份，分別由　　　　　　　公司以及 學校保存**

**操作員日誌範本**

文件編號：A-2

|  |  |
| --- | --- |
| 填寫日期： | 民國 年 月 日 |
| 系統操作起始時間： | 上（下）午 時 分 |
| 系統操作結束時間： | 上（下）午 時 分 |

|  |  |
| --- | --- |
| 操作事項 | * + - * + 系統例行檢查
				+ 系統維護
				+ 系統更新操作
 |
| 系統錯誤說明 |  |
| 採取改正措施說明 |  |

|  |  |
| --- | --- |
| 操作人員：  | 簽名欄  |
| 日誌填寫人員：  | 簽名欄  |

**優質通行碼設定原則與使用原則**

文件編號：A-3

1. **良好的通行碼設定原則**
2. 混合大寫與小寫字母、數字，特殊符號。
3. 通行碼越長越好，最短也應該在8個字以上。
4. 至少每三個月改一次密碼。
5. 使用技巧記住通行碼
	* + 使用字首字尾記憶法：
			1. My favorite student is named Sophie Chen，取字頭成為mFSinsC
			2. There are 26 lovely kids in my English class，取字尾成為Ee6ysnMEc
		+ 中文輸入按鍵記憶法：
			1. 例如「通行碼」的注音輸入為「wj/ vu/6a83」
6. **應該避免的作法**
	1. 嚴禁不設通行碼
	2. 通行碼嚴禁與帳號相同
	3. 通行碼嚴禁與主機名稱相同
	4. 不要使用與自己有關的資訊，例如學校或家裡電話、親朋好友姓名、身份證號碼、生日等。
	5. 不重覆電腦鍵盤上的字母，例如6666rrrr或qwertyui或zxcvbnm。
	6. 不使用連續或簡單的組合的字母或數字，例如abcdefgh或12345678或24681024
	7. 避免全部使用數字，例如52526565
	8. 不使用難記以至必須寫下來的通行碼。
	9. 避免使用字典找得到的英文單字或詞語，如TomCruz 、superman
	10. 不要使用電腦的登入畫面上任何出現的字。
	11. 不分享通行碼內容給任何人，包括男女朋友、職務代理人、上司等。

**延伸參考：**

“Password Management Guideline”, by department of defense computer security center, 12 April 1985 <http://www.radium.ncsc.mil/tpep/library/rainbow/CSC-STD-002-85.pdf>

**安全事件通報程序範本**

文件編號：A-4

  **學校資通安全事件通報單**

文件編號：A-5

編號：

填報時間： 年 月 日 時 分

洽詢電話： 傳真：

E-mail：

或逕送：

**一、發生資通安全之機關(機構)聯絡資料：**

機關(機構)名稱： 聯絡人：

E-mail：

電話： 傳真：

**二、資通安全事件通報事項：**

1.事件發生時間： 年 月 日 時 分

2.主機(伺服器)資料：

* IP位址(IP Address)：
* 網域名稱(Domain name)：
* 主機(伺服器)廠牌、機型：
* 作業系統名稱、版本、序號：
* 網際網路資訊位址(Web URL)：
* 已裝置之安全機制：

3.資通安全事件資料：

◎影響等級：□『A』級：影響公共安全、社會秩序、人民生命財產。

□『B』級：系統停頓，業務無法運作。

□『C』級：業務中斷，影響系統效率。

□『D』級：業務短暫停頓，可立即修復。

* 事件說明：
* 應變措施：

三、期望支援項目：

四、解決辦法：

五、已解決時間： 年 月 日 時 分

**校長： 資訊安全長： 承辦人員：**

  **學校資通安全事件解除單**

編號：

填報時間： 年 月 日 時 分

洽詢電話： 傳真：

E-mail：

或逕送：

一、發生資通安全之機關(機構)聯絡資料：

機關(機構)名稱： 聯絡人：

E-mail：

電話： 傳真：

二、資通安全事件通報事項：

1.事件發生時間： 年 月 日 時 分

2.主機(伺服器)資料：

* IP位址(IP Address)：
* 網域名稱(Domain name)：
* 主機(伺服器)廠牌、機型：
* 作業系統名稱、版本、序號：
* 網際網路資訊位址(Web URL)：
* 已裝置之安全機制：

3.資通安全事件資料：

◎影響等級： □『A』級：影響公共安全、社會秩序、人民生命財產。

□『B』級：系統停頓，業務無法運作。

□『C』級：業務中斷，影響系統效率。

 □『D』級：業務短暫停頓，可立即修復。

* 事件說明：
* 應變措施：

三、已解決時間： 年 月 日 時 分

填寫人：

**國中、小學資安管理系統實施原則自我檢測表**

附件1-2

本查檢表以教育部「國中、小學資安管理系統實施原則」所擬定，作為國中小學就其資通安全實施現況進行自我評量之用途。

學校名稱:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

填寫單位:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

填 寫 者:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

填寫日期:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |  |
| --- | --- | --- | --- |
| **編號** | **檢測項目** | **符合與否** | **補充說明** |
| **網路安全** |
| **1.** | 本校對外網際網路連線只透過縣網中心進行。 | □ 是 □ 否 |  |
| **2.** | 學校自行管理的資訊應用系統包括? | □ 會計系統□ 人事系統□ 學籍系統□ 網站服務□ 電子郵件□ 教學系統□ 視訊系統 |  |
| **3.** | 所勾選之系統所儲存的資訊當有必要和縣(市)網路中心進行網路傳輸時，傳輸連線是否透過專屬線路(如VPN)完成? | □ 是 □ 否 |  |
| **4.** | 學校是否與其資訊系統或設備維護及委外廠商，簽訂適當的資訊安全協定或切結書? | □ 是 □ 否 |  |
| **系統安全** |
| **5.** | 請列舉學校內所使用的電腦設備場所或類別。 | □ 行政辦公室電腦□ 教師辦公室公用電腦□ 電腦教室□ 實驗室教學電腦□ 一般教室之電腦□ 伺服器等重要資訊服務 提供之電腦設備□ 其他\_\_\_\_\_\_\_\_ |  |
| **6.** | 學校所有電腦均安裝防毒軟體? | □ 是 □ 否 |  |
| **7.** | 是否針對防毒軟體進行自動更新病毒碼之設定? | □ 是 □ 否 |  |
| **8.** | 是否定期針對學校所有電腦系統進行全面病毒掃描? | □ 是 □ 否 |  |
| **編號** | 檢測項目 | 符合與否 | **補充說明** |
| **9.** | 電子郵件是否執行過濾(防範)處理? | * 是 □ 否 □ 不適用
 |  |
| **10.** | 學校是否訂定教職員電子郵件使用安全政策 | * 是 □ 否 □ 不適用
 |  |
| **11.** | 是否瞭解使用未取得授權或盜版軟體的資訊安全風險? | □ 是 □ 否 |  |
| **12.** | 請列舉學校內部須保存且重要性高之資料。 | □ 學籍資料□ 教學資料□ 其他□□ |  |
| **13.** | 上提所列出的重要資料是否定期進行備份? | * 是 □ 否 □ 不適用

備份頻率：每  |  |
| **14.** | 備份資料是否存放於機房外之安全區域場所? | * 是 □ 否 □ 不適用
 |  |
| **15.** | 是否備有系統維護日誌? | * 是 □ 否 □ 不適用
 |  |
| **16.** | 學校的資訊系統之使用是否訂定使用者帳號註冊及註銷政策? | * 是 □ 否 □ 不適用
 |  |
| **17.** | 使用者帳號註冊及註銷政策內，是否包含右列各項目? | □ 規定使用唯一的使用者 識別碼□ 檢查使用者是否經過系 統所有人之授權□ 初次登入系統之預設通 行碼更改□ 人員調、離職或退休之帳 號註銷流程□ 保存包含所有識別碼註 冊的記錄 |  |
| **18.** | 基於作業需要，需提供特定人員設定系統存取特權時，是否記綠具有存取特權者身分以及其特權之權限? | * 是 □ 否 □ 不適用
 |  |
| **19.** | 上提存取特權紀錄文件是否妥善保存? | * 是 □ 否 □ 不適用
 |  |
| **20.** | 系統或設備委外廠商因需要必須具備存取權限時，是否另行開設臨時帳號(臨時識別碼與通行碼)，並於委外人員結束服務後，取消該臨時帳號? | * 是 □ 否 □ 不適用
 |  |
| **21.** | 是否每一個獨立的系統均設定獨立的帳號? | * 是 □ 否 □ 不適用
 |  |
| **22.** | 是否要求使用者對其個人通行碼應盡保密責任? | * 是 □ 否 □ 不適用
 |  |
| **編號** | 檢測項目 | 符合與否 | **補充說明** |
| **23.** | 是否要求使用者初次登入系統後必須立即更改預設之通行碼? | * 是 □ 否 □ 不適用
 |  |
| **24.** | 系統安裝後是否管制原始程式? | * 是 □ 否 □ 不適用
 |  |
| **25.** | 學校是否定有資訊安全事件通程序? | * 是 □ 否 □ 不適用
 |  |
| **26.** | 學校相關人員是否知悉安全事件之通報程序? | * 是 □ 否 □ 不適用
 |  |
| **27.** | 宣導學校人員知悉安全事件之通報程序的方式。 | □ 公告□ 通報程序張貼於電腦使 用場所□ 其他\_\_\_\_\_\_\_\_ |  |
| **實體安全** |
| **28.** | 學校電腦機房區域是否獨立或隔離? | * 是 □ 否 □ 不適用
 |  |
| **29.** | 學校電腦機房區域進出口是否加強門鎖或其他防範侵入之裝置? | * 是 □ 否 □ 不適用
 |  |
| **30.** | 學校電腦機房區域之人員進出是否予以管制? | * 是 □ 否 □ 不適用
 |  |
| **31.** | 請說明學校機房區域之人員進出管制方法或限制條件。 | □ 只有授權進入機房之人 員擁有機房門禁鑰匙□ 門口設立禁止進入標示□ 保持門禁的封鎖狀態□ 其他 |  |
| **32.** | 電腦機房內是否嚴禁存放易燃物及未經核准之電器或其他物品? | * 是 □ 否 □ 不適用
 |  |
| **33.** | 電腦作業區(含機房)是否執行禁止抽菸及飲用食物? | * 是 □ 否 □ 不適用
 |  |
| **34.** | 電腦機房內系統是否使用不斷電系統? | * 是 □ 否 □ 不適用
 |  |
| **35.** | 電腦機房內系統的不斷電系統使用年限為? | * 是 □ 否 □ 不適用
 |  |
| **36.** | 電腦機房內連線纜線是否整理分類清楚? | * 是 □ 否 □ 不適用
 |  |
| **37.** | 學校電腦教室內連接纜線是否整理分類清楚? | * 是 □ 否 □ 不適用
 |  |
| **38.** | 電腦機房內的設備纜線插頭是否均接地處理? | * 是 □ 否 □ 不適用
 |  |
| **39.** | 學校電腦教室內的設備連接纜線是否均有接地處理? | * 是 □ 否 □ 不適用
 |  |
| **40.** | 學校報廢電腦及其他儲存媒體之程序中，是否有針對所儲存資料進行刪除或格式化處理之項目? | * 是 □ 否 □ 不適用
 |  |
| **41.** | 學校電腦機房或其他重要資訊設備區域，須有第三方支援人員進入進行維護、維修、或測試等工作時，是否簽署資訊安全切結書? | * 是 □ 否 □ 不適用
 |  |
| **編號** | 檢測項目 | 符合與否 | **補充說明** |
| **42.** | 學校的資訊設備是否列於學校資產清單中? | * 是 □ 否 □ 不適用
 |  |
| **43.** | 學校的資訊設備是否涵蓋於學校資產攜出管理規範中? | * 是 □ 否 □ 不適用
 |  |
| **44.** | 學校重要的資訊設備、個人電腦是否均設定具有通行碼管制之銀幕保護程式? | * 是 □ 否 □ 不適用
 |  |
| **45.** | 學校的重要公文、儲存媒體長時間不使用或不使用時，是否存放於加裝鎖保護的場所或保存櫃當中? | * 是 □ 否 □ 不適用
 |  |
| **人員安全** |
| **46.** | 學校教職員的工作說明書或職員手冊中是否加註對資訊安全保護之要求? | * 是 □ 否 □ 不適用
 |  |
| **47.** | 學校之資訊安全政策是否公佈? | * 是 □ 否 □ 不適用
 |  |
| **48.** | 是否針對學校教職員進行資訊安全認知之教育? | □ 是 □ 否 |  |
| **49.** | 學校的網路管理人員是否接受資訊安全教育訓練? | □ 是 □ 否 |  |

資訊管理人員：

總務主任：

教務(導)主任：

校長：