嘉義縣國中小資通安全管理實施原則(草案)

一、文件目標

依據教育部訂頒之「國中、小學資通安全管理系統實施原則」，參酌各校實際狀況與管理需求，提供建立與實施校園資通安全管理制度之參考。

二、適用範圍

各國中、小連接校園網路之電腦、資訊與網路服務相關的系統、設備、程序、及人員。

三、實施原則

1. 網路安全

1.1 網路控制措施

1.1.1 校園網路對外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。

1.1.2 校內可經由網路存取之重要校務系統(例如會計系統、學生學籍、成績原始資料系統等)應限制僅能由校內特定範圍連線，若有必要由外部網路進行存取或傳輸，建議透過虛擬私有網路（Virtual Private Network, VPN）或同等連線方式進行；無透過網路進行傳輸之必要者，不應置於網路伺服器上。

1.1.3 應禁止使用者私自以未經管控之公眾網路電路(電話撥接或行動上網等)連結至重要伺服器、行政電腦或校園網路設備。

1.2 網路資訊安全

1.2.1 具敏感性資訊之重要網路資訊系統軟硬體委託廠商執行開發、維護或操作時，應簽訂安全保密切結書[參考切結書範本，文件編號 A-1]。

1.2.2 應定期(建議每年一次)針對學校對外開放之網路資訊系統頁面執行網站應用程式弱點掃描，確實檢視並修正可能的弱點。

1.3.3 具定期(建議每年一次)針對學校對外開放之網路資訊系統頁面執行防洩漏個資掃描，確實檢視並移除可能洩漏個人資料之內容。

1.3 無線網路存取

1.3.1 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加密金鑰以防未經許可之盜用。

1.3.2 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：

- 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。
- 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。
- 開放校外人士出入之公共空間可視需要提供民眾無線上服務，其流量應與校園網路隔離，或委由網路服務業者提供。

2. 系統安全

2.1 職責區隔管理

2.1.1 重要行政業務應依權責配置專用電腦設備，並設定存取帳號密碼等管制措施，不得私自將之移(兼)作其他用途。

2.1.2 網站及應用系統伺服器不得兼供一般文書處理、網頁瀏覽及電子郵件收發等個人用途，且應禁止未經授權人員私自操作。

2.2 惡意程式防護

2.2.1 學校內的個人電腦應：

- 安裝防毒軟體，並定期更新病毒碼
- 定期（至少每個月）進行作業系統(如「Windows Update」)之程式更新作業，以防範作業系統之漏洞
- 設有開機自動還原機制之個人電腦應定期(至少每三個月)執行病毒碼與作業系統更新後重建還原映象檔

2.2.2 學校內個人電腦所使用的軟體應有授權。

2.2.3 新系統啟用前，應經過掃毒程序並更換系統預設密碼，以防範可能隱藏的病毒、後門程式、惡意入侵或不當使用。

2.3 重要資料備份

2.3.1 權責管理人員需針對學校重要伺服器(包含系統檔案、應用系統、資料庫等)及行政電腦重要資料定期進行備份工作，或採用自動備份機制；建議週期為每週進行一次。

2.4 建立操作日誌

2.4.1 系統管理及維護人員對校園網路主要設備及包含重要資料的電腦系統進行檢查、維護、更新與設定異動等動作時，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。

2.4.1 日誌內容可包含以下各項：[參考日誌範本，文件編號 A-2]

- 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。
- 紀錄日誌項目人員姓名與簽名欄

2.5 資訊存取限制

2.5.1 校園網路中開放使用的個人電腦不得用於存取及處理重要及敏感性資料，並建議僅提供必要之功能(如採 Windows 系統可設定為標準使用者帳戶，或僅安裝專供上網使用之作業系統環境)。

2.6 使用者帳號管理

2.6.1 學校發給校內使用者之各項應用服務帳號(如學校／班級網站、個人電子郵件、雲端儲存空間等)，應制定註冊審核及註銷作業程序，以管控使用者資訊服務的存取，該作業應包括以下內容：

- 每位使用者應選用唯一的使用者識別碼(ID)，不得與他人共用。
- 檢核使用者在各該資訊服務系統之權限是否適當。
- 保存一份包含所有已核發識別碼的記錄。
- 使用者身分異動(職務調整、離職、重新編班、轉學、畢業)後，應依程序移轉至新單位(班級、學校)管理，或移除其識別碼的存取權限。
- 定期(建議每學期)檢查網站或應用系統新增之帳號，若有莫名帳號產生，應關閉帳號權限，並依資安事件處理程序辦理。
- 定期(建議每學年)清查全校各項使用者帳號核發及使用情形，並註消或移轉不符合權限的使用者識別碼和帳號。

2.7 特殊權限管理

2.7.1 應建立學校重要伺服器、電腦、網路設備及資訊系統(包含以學校名義取得之外部資訊服務)主要管理或操作帳號持有者名單，職務異動時應隨即更新。

2.8 通行碼(Password)之使用

2.8.1 資訊系統與服務應避免使用共同帳號及通行碼；若因業務需要必須由多人共用相同帳號時，應建立持有者名單，職務異動時應立即更新通行碼。

2.8.2 定期向使用者宣導通行碼(Password)選定與使用規則，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
- 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。若系統功能允許，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。
- 因教學或測試用途，或其他特殊需要同時持有多個帳號時，可考慮使用一組複雜但相同的通行碼。

2.8.3 由系統管理者統一建立後發給使用者的預設通行碼，應要求使用者於第一次登入系統時立即自行更改；若純作教學與練習用途而臨時發給通行碼，應於使用完畢後註銷其權限。

2.9 原始程式庫之存取控制

2.9.1 學校網站應用程式應採取以下控制措施，以維護原始程式碼之安全性：

- 自行開發之網站應用程式應加強資料輸入格式及輸出結果之檢查，避免執行過程中遭到置入惡意內容，並應隨時注意開發工具與執行平台之安全性漏洞警訊且隨時執行安全性更新。
- 委外開發之網站應用程式應於合約加註系統廠商對原始程式庫安全性維護之規範，並將系統安全性漏洞通報與修補列入保固服務事項。
- 採用公開銷售或自行下載之網站應用程式套件時，應選用安全信譽良好、開發團隊持續維護，且願意主動發佈安全性通報與提供修正套件之版本，並隨時注意配合修正。
- 禁止使用開發平台、函式庫、程式碼已被發佈安全性通報且迄未修正，或原開發廠商或團隊已停止維護之應用程式套件架設公開之學校網站或應用系統。

2.10 資安事件通報與處理

2.10.1 學校應設置資訊安全連絡人，並建立校內資訊安全事件通報程序。

2.10.2 學校全體人員發現資安事件，或接獲資安事件告知訊息時，應立即通知資訊安全連絡人。

2.10.3 學校資訊安全連絡人接獲資安事件報告，應依規定於一小時內至教育機構資安通報平台完成通報並採取必要應變措施。

3. 實體安全

3.1 設備安置及保護

3.1.1 學校重要資訊設備(如伺服器、防火牆、連線設備及路由設備)應置於適當空間，保持通風並維持清潔以確保散熱良好。

3.1.2 學校重要資訊設備機房及電腦教室區域，應設置滅火設備，並禁止擺放易燃物、或飲食。

3.1.3 學校重要資訊設備之電力及網路線路應採取適當防護措施以降低異常電流(如雷擊)之傷害，並視需要安裝避雷針、電流保安器等裝置。

3.1.4 學校重要資訊設備機房及電腦教室區域，應至少於入出口處加裝門鎖、保全系統或其他同等裝置。

3.2 電源供應

3.2.1 學校重要資訊設備應保持電力供應之穩定，例如設置不斷電系統、穩壓器等電源保護措施，以免斷電或過負載而造成損失。

3.3 纜線安全

3.3.1 校園網路主要佈線應定期(建議每學期一次)清查整理並加以適當標示；建議繪製校園網

路佈線圖備用。

3.3.2 廢棄網路線應隨時剪除，暫時未用之網路線應將接頭從網路設備上移開，避免使用者誤接。留供移動式裝置(如筆記型電腦)使用之線路建議採用資訊插座佈設，並加以標示。

3.4 設備與儲存媒體之安全報廢或再使用

3.4.1 所有具有儲存媒體的設備，在報廢或改變用途前，應先確保已將任何敏感資料和授權軟體刪除或覆寫。

3.5 設備維護

3.5.1 學校資訊設備委託廠商定期執行維護者，應簽訂維護合約，並規範維護人員應穿著制服或配(攜)帶識別證，執行維護前應取得權責管理人員同意並避免影響學校行政及教學之正常進行，完成維護作業後應向權責管理人員報告，並登錄於操作日誌。

3.5.2 執行重要敏感業務期間需請維護廠商進場作業者，廠商人員進入安全管制區域前需簽訂保密切結書並由權責管理人員會同。

3.6 資產攜出

3.6.1 未經授權不應私自將校內定點配置的資訊設備、儲存媒體或授權軟體任意移動或攜出放置處所。

3.6.2 當有必要攜出重要資訊設備時，應經權責管理人員同意，並實施登記與歸還記錄；更動設備配置地點時，應配合更新相關資產記錄與線路標示。

3.7 桌面淨空

3.7.1 結束工作時，所有學校教職員工應將其所經辦或使用之敏感性資料(例如試題卷、公文、學籍資料等)及資料的儲存媒體(如隨身碟、磁碟、光碟等)，妥善存放。

3.7.2 用於處理敏感性資料之個人電腦應設置保護措施，如保護鎖、開機密碼以及螢幕保護。

4. 人員安全

4.1 將安全列入工作執掌中

4.1.1 應將資訊安全納入教職員工聘約、業務職掌或工作守則等說明文件中，以強化工作上之資訊安全意識。

4.2 資安教育訓練

4.2.1 學校行政主管及資訊網管人員應定期參加資訊安全相關研習課程，充實資安知能，並了解校園資安事件之處理程序。

4.2.2 經常針對校內教職員工、學生及家長舉辦資訊安全教育訓練或宣導活動，以提昇資訊安全認知。

5. 法規遵循

5.1 適用法規之鑑別

5.1.1 學校應指定專人蒐集與資訊安全有關之法律條文、管理規定及行政文件，知會相關人員後以書面或其他方式建檔留存，並於法規修訂時隨時更新。

5.2 適用法規之遵循

5.2.1 學校各項資訊作業流程及相關管理規範，應定期檢視以確保符合相關法令規定，並經由校內正式程序(如校務會議或行政會議)通過後確實執行。

文件編號：A-1

資訊軟硬體服務委外安全保密切結書範本

_____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、

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

公司及負責人蓋章：

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

文件編號：A-2

資訊系統及校園網路設施操作日誌範本

填寫日期：　　民國___年___月___日

系統操作起始時間：　___午___時___分

系統操作結束時間：　___午___時___分

操作事項	☐ 例行檢查 ☐ 障礙維護 ☐ 軟硬體更新操作 ☐ 其他：
問題狀況或錯誤訊息說明	
維護措施說明及異動事項記錄	

操作人員： 單位：_____姓名：_____　(簽名)

日誌填寫人員：_____　(簽名)