新竹縣立石磊國小

資通安全管理系統v1.6

中 華 民 國 106 年 9 月 23日

修　訂　紀　錄				
版次	修訂日期	修訂頁次	修訂者	修訂內容摘要
1.0	101.07.13			初版
1.1	101.10.30	P7		5.1 智慧財產權 5.2 個人資訊的資料保護及隱私 5.3 電子簽章法 之網頁連結。
1.2	102.06.27	P14		移除資通安全事件解除單
1.3	102.08.22	P5，P7		2.7 特權管理：建立帳號清冊，[文件編號 A-10]。 4.3 工作職掌交接：完成工作交接手續，以維護學校資訊網路安全。[文件編號 A-11]。
1.4	102.10.04	P13		修正：文件編號 A-5 資通安全事件通報單主管單位核章位置。
1.5	103.04.29	全部		依據教育部 103 年 3 月 20 日臺教資（四）字第 1030041378 號函辦理。
1.6	105.04.07	全部		(1)重新修改排列表單編號 (2)修改表單 A-2 (3)修正 2.10.12 資通安全事件追蹤單 (4)修改 A-4 資通安全事件通報程序表單 (5)修訂 A-5 資通安全事件追蹤單

石磊國小資通安全管理系統實施原則

一、 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，以增進資訊作業之安全性，確保學校資料之機密性、完整性與可用性。

二、 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。

三、 實施原則

1. 網路安全

1.1 網路控制措施

1.1.1 與外界連線，應僅限於經由教育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。

1.1.2 應禁止以私人架設網路（如：電話線、3G 或4G 網路等）連結機房內之主機電腦或網路設備。

1.1.3 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。

1.1.4 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。

1.2 無線網路存取

1.2.1 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帳號通行碼或加密金鑰以防未經許可之盜用。

1.2.2 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。

- 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。
- 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. 系統安全

2.1 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。

2.2 對抗惡意軟體、隱密通道及特洛依木馬程式

2.2.1 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。
- 作業系統及軟體應定期更新，以防範系統漏洞。

2.2.2 個人電腦所使用的軟體應有授權。

2.2.3 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。（參考啟用與報廢紀錄表格式，文件編號A-1）

2.3 桌面淨空與螢幕淨空政策

2.3.1 個人電腦辦公桌面應避免存放機敏性文件，結束工作時，應將其所經辦或使用具有機密或敏感特性的資料（如公文、學籍資料等）妥善存放。

2.3.2 當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。

2.4 資料備份

2.4.1 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）在可接受的風險範圍內定期進行備份工作或應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光碟、隨身碟或外接式硬碟執行異地存放。

2.4.2 每年應定期檢查備份資料之可用性與完整性。

2.5 資訊工作日誌

2.5.1 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。（參考資訊工作日誌格式，文件編號A-2）

2.5.2 系統管理人員 應至少每季執行一次校時。

2.6 資訊資訊存取限制

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）。

2.7 使用者註冊

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：

- 使用唯一的使用者帳號。
- 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。
- 保存一份包含所有帳號註冊的記錄。
- 使用者調職或離職後，應移除其帳號的存取權限。
- 每學期應檢查使用者帳號，以確保帳號的有效性。（參考帳號申請表格式，文件編號A-3）

2.8 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。（參考系統特權帳號清單格式，文件編號A-4）

2.9 通行碼（Password）之使用

2.9.1 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。

2.9.2 資訊系統與服務應避免使用共用帳號及通行碼。

2.9.3 由學校發佈通行碼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，文件編號：A-5)，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，應該包含英文字及數字，長度為8碼(含)以上。

2.10 通報安全事件

2.10.1 資訊安全事件包括：系統被入侵、對外攻擊、針對性攻擊、散播惡意程式、中繼站、電子郵件社交工程攻擊、垃圾郵件、命令或控制伺服器、殭屍電腦、惡意網頁、惡意留言、網頁置換、釣魚網頁、個資外洩等。

2.10.2 資訊安全事件等級，由輕微至嚴重區分等級如下：

- 符合下列任一情形者，屬 0 級事件：
  (1) 未確定事件或待確認工單:來自不同計畫所使用新型技術(A-SOC，miniSOC,…)所產生之工單，但其正確性有待確認。
  (2) 其他單位所告知教育部所屬單位所發生未確定之資安事件。
  (3) 教育部及區、縣網路中心檢舉信箱通告之資安事件。
- 符合下列任一情形者，屬 1 級事件：
  (1) 非核心業務資料遭洩漏。
  (2) 非核心業務系統或資料遭竄改。
  (3) 非核心業務運作遭影響或短暫停頓。
- 符合下列任一情形者，屬 2 級事件：
  (1) 非屬密級或敏感之核心業務資料遭洩漏。
  (2) 核心業務系統或資料遭輕微竄改。
  (3) 核心業務運作遭影響或系統效率降低，於可容忍中斷時間內回復正常運作。
- 符合下列任一情形者，屬 3 級事件：
  (1) 密級或敏感公務資料遭洩漏。
  (2) 核心業務系統或資料遭嚴重竄改。
  (3) 核心業務運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作。

● 符合下列任一情形者，屬 4 級事件：

(1) 國家機密資料遭洩漏。

(2) 國家重要資訊基礎建設系統或資料遭竄改。

(3) 國家重要資訊基礎建設運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作。

2.10.3 本校任何人於校內發現異常情況或疑似資安事件，應立即向資訊組長(連絡人)通報，並儘速進行處理並研判事件等級。

2.10.4 當發生研判事件等級 3（含）以上之事件，資訊組長(連絡人)應立即通報資訊安全官(教務主任)及校長，並以電話聯絡新竹縣教育研究發展暨網路中心網路管理組，由校長儘快召集會議研商處理的方式。(參考資通安全事件通報程序，文件編號：A-6)

2.10.5 當發生無法處理之資通安全事件，應通報新竹縣教育研究發展暨網路中心網路管理組協助處理。

2.10.6 教育機構資安通報平台（網址：https://info.cert.tanet.edu.tw/），帳號為學校OID：

2.10.7 資安通報依情報來源分為「告知通報」與「自行通報」，若收到「告知通報」事件通知，由資安業務承辦人登入教育機構資安通報平台，完成通報及應變作業。

2.10.8 資安事件若為校內人員自行發現，由資安業務承辦人登入教育機構資安通報平台進行「自行通報」完成通報及應變作業。

2.10.9 資安事件須於發生後 1 小時內進行通報，0、1、2 級事件於事件發生後72 小時內處理完成並結案(包括通報與應變)，3、4 級事件於事件發生後36 小時內完成並結案。

2.10.10 如有收到教育機構資安通報平台「資安預警事件」通知，由資安業務承辦人登入教育機構資安通報平台，進行資安預警事件單處理作業。

2.10.11 相關通報應變流程請依照「教育機構資安通報應變手冊」規定辦理。

2.10.12 學校應建立內部資安通報追蹤機制(參考資通安全事件追蹤單，文件編號：A-7)

3. 實體安全

3.1 設備安置及保護

3.1.1 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。

3.1.2 主機機房及電腦教室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。

3.1.3 主機機房及電腦教室應實施門禁管制。

3.1.4 人員進出安全區域(機房)須安全管制登記(如文件編號A-8)

3.2 溫濕度控制

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。(以上為縣網中心對溫濕度控制之建議)

本校位處山區(採NAS系統)，溫度都能維持在25℃以下，惟濕度部分宜逐年爭取經費，購置相關設備以進行濕度控制。

3.3 電源供應

重要的資訊設備（如：主機機房等）應有適當的電力保護設施，例如設置UPS、電源保護措施(如：穩壓器、接地等)，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。

3.4 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)。

3.5 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。（參考啟用與報廢紀錄表格式，文件編號A-1）

3.6 財產攜出

3.6.1 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」。（如文件編號A-9）

3.6.2 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。

3.7 桌面淨空與螢幕淨空政策

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。

3.7.2 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。

4. 可攜式電腦設備與媒體

4.1 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。

4.2 公務用可攜式電腦設備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。

4.3 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體存放於上鎖儲櫃或安全處所。

5. 人員安全

5.1 人員安全責任

非正式人員、約聘(僱)人員者，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。（參考保密切結書格式，文件編號A-10）。

5.2 資訊安全教育與訓練

5.2.1 鼓勵資安業務承辦人參加資安管理系統相關教育訓練。

5.2.2 鼓勵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。

5.3 資訊業務承辦人員業務異動

完成業務交接手續，以維護學校資訊網路安全。（參考工作交接清冊，文件編號A-11）。

6. 資訊業務委外管理

6.1 服務委外廠商合約之安全要求

6.1.1 在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。

6.1.2 應要求委外廠商簽訂安全保密切結書。(參考切結書格式，文件編號A-12)。

6.1.3 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。(參考切結書格式，文件編號A-13)。

6.2 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。(參考帳號申請單格式，文件編號A-3)

7. 應對以下各項相關法令有基礎之認知，並利用各集會場合對全校師生口頭宣導(至少一學期一次)。

7.1 智慧財產權

著作權法

7.2 個人資訊的資料保護及隱私

個人資料保護法及施行細則

7.3 刑法電腦犯罪專章