新竹縣沙坑國小

國中、小學資通安全管理系統 v1.7

中 華 民 國 106 年 6 月 15 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
1.7	106.06.15	P5		2.5.2 系統管理人員應至少每季執行一次校時。若發現異常，隨時更新。

資聯: 教導主任: 校長:

教師兼資訊組長羅正昌　教導主任林梓鈴　校長余志鴻

新竹縣沙坑國民小學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。

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。若發現異常，隨時更新.

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

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)需有安全管制登記(參考人員進出機房登記表格式，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。

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。

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，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。

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。(參考資訊應用委外廠商服務內容暨保密切結書格式，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。(參考委外廠商人員保密切結書格式，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

文件編號：A-2

資訊工作日誌(範本)

操 作 日 期： 民國 年 月 日上(下)午 時 分

系 統 名 稱：

操作事項	□ 系統例行檢查 □ 系統維護 □ 系統更新操作 □ 其它：
操作說明	
系統錯誤改正措施說明	

資訊組長（連絡人）(簽名)：_____

主管覆核(簽名)：_____

文件編號：A-4

系統特權帳號清單(範本)

填寫日期:　　年　　月　　日

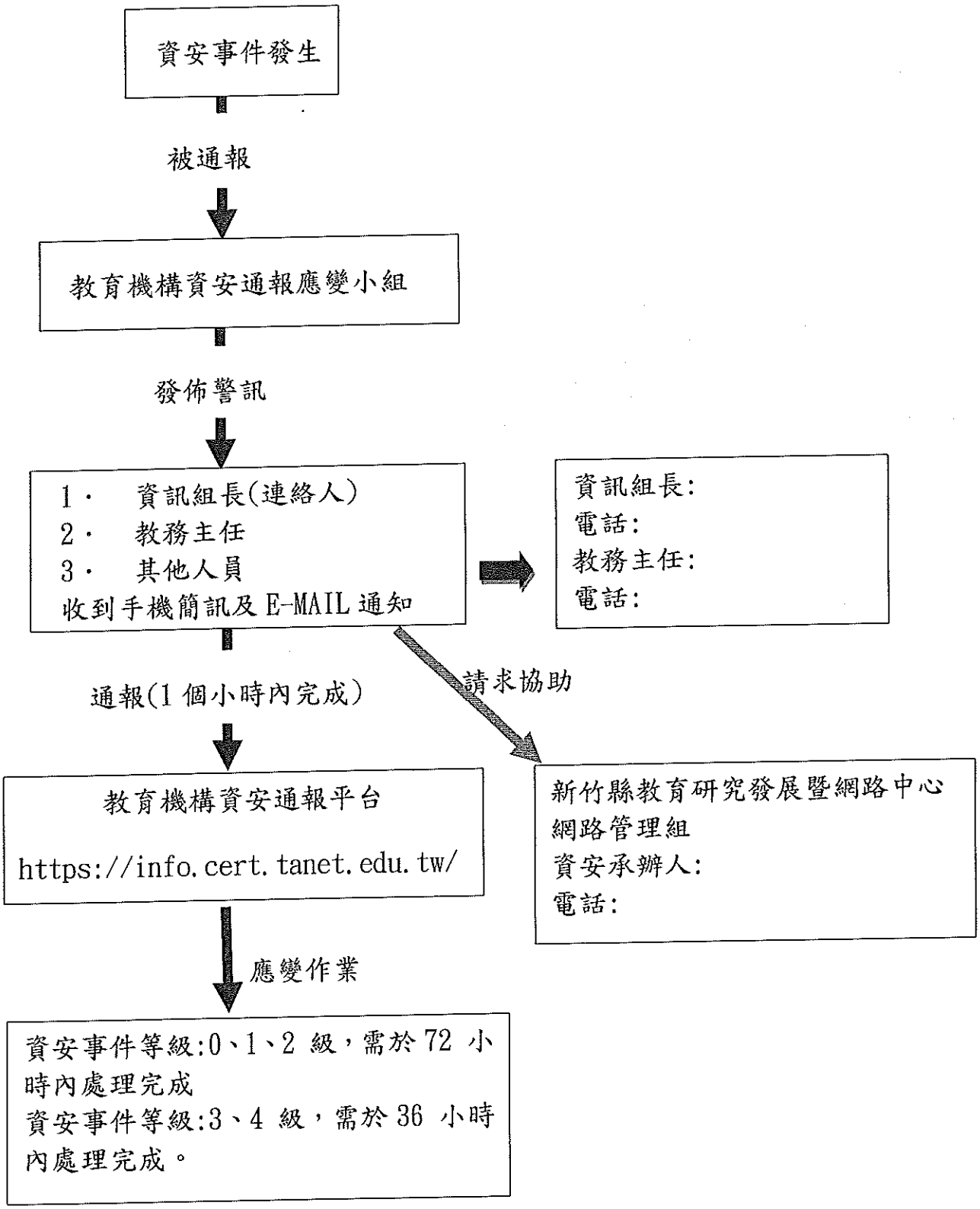
系統名稱	網址	帳號	人員姓名

資訊組長（連絡人）：　　主管覆核：

文件編號：A-6

資通安全事件通報程序

一、教育機構資安通報流程：



文件編號：A-7

_____學校資通安全事件追蹤單

資安事件單之編號：_____ 填報時間：____年____月____日____時____分

資通安全事件應變事項			
單位名稱		通報人	
電　　話		電子郵件	
發生時間	____年____月____日____時____ 分		
設備資料	IP 位址		
	設備種類	□桌機 □筆電 □行動裝置 □監視器 □其他_____	
	設備用途	□行政電腦 □班級電腦 □電腦教室 □公用電腦 □個人資訊設備 □其他_____	
	作業系統名稱、版本		
	防毒軟體(名稱/版本)		
應變流程			
解決辦法	一・電腦重整: □重灌作業系統 □還原作業系統 □更換主機 □無硬碟系統範本更新 □其他_____ 二・系統修補: □安裝最新的修補程式(含作業系統更新) □病毒掃描軟體進行掃描，掃到病毒並刪除 三・宣導措施: □進行師生宣導 □其他:_____ 四・其他處理方法: _____		
解決時間	____年____月____日____時____分		

資安業務承辦人	會辦單位	資安業務主管

文件編號：A-9

設備進出紀錄表

紀錄編號：　　填報日期：　年　月　日

□攜進 □攜出	日期 時間	年　月　日 時　分	攜進/出人員 單　位	
設備名稱			設備序號	
設備 品牌/規格				
攜進/出方式	□自行攜進/出 □貨運代送(公司名稱/電話：＿＿＿＿＿＿＿＿＿＿ 貨運編號：＿＿＿＿＿＿＿＿＿＿) □其他(請說明：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿)			
攜進/出	□備份媒體異地儲存 □異地儲存之備份媒體送回 □新增設備 □設備送修(預計修復完成日期：　/　/　) □調 / □借 / □還 單位：＿＿＿＿＿＿＿＿ 聯 絡 人：＿＿＿＿＿ 聯絡電話：＿＿＿＿＿＿＿＿ (預計歸還日期：　/　/　) □其他(請說明：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿)			
核准單位				
資訊組長(連絡人)		資安業務主管		

文件編號：A-11

工作交接清冊

網路設備、伺服主機	IP	帳號、密碼（還原）	交接人員核章	監交人員核章

系統平台	網址	1. 帳號、密碼(還原) 2. 建立新帳號/密碼 3. 權限轉移	交接人員核章	監交人員核章

◎**繳交物品：**

□ 1. 辦公室及活動櫃鑰匙

□ 2. 繳回個人保管財產

□ 3. 個人電腦之帳號：_____

□ 4. 其它 _____

申請人員:_____ 資安業務主管: _____

日期: 年 月 日

文件編號：A-13

委外廠商人員保密切結書(範本)

_____ (以下簡稱為本人)任職於_____

(委外公司名稱)，因執行_____工作，於 貴校執行服務期間，願遵守 貴校資訊安全相關規範，並對所知悉 貴校機密或任何不公開之文書、電子資料、圖畫、消息、物品或其他資訊，將恪遵保密規定，未經 貴校書面授權，不得以任何形式利用或洩漏、告知、交付、移轉予任何第三人，如有違誤願負法律上之責任。此致

○○學校

切結人：

任職公司：

公司統一編號：

日期：　　年　　月　　日

本保密切結書一式兩份，分別由切結人以及_____學校保存