

新竹縣竹北市博愛國民小學

資通安全管理系統 v1.1

中華民國 105 年 5 月 5 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	102.10.25			初版
1.1	105.5.5	全部		

# 新竹縣竹北市博愛國民小學資通安全管理系統實施原則

## 一、 文件目標

本文件訂定本校資通安全管理系統實施原則建議。文件中所有實作項目應經確認合理風險評鑑及法令法規之後認定可被接受。

## 二、 適用範圍

本校校內電腦、資訊與網路服務相關的系統、設備、程序、及人員(包括教、職員工、學生及於本校進行教學、研習、公務等活動之所有相關人員)。

## 三、 實施原則

### 1. 網路安全

#### 1.1 網路控制措施

- 1.1.1 學校與外界連線，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 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。

#### 1.2 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(文件編號 A-1)。

#### 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帳號通行碼或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。

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。

## 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、隱密通道及特洛伊木馬程式

#### 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-2)

### 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，行政及公務用電腦應設定螢幕保護機制。

### 2.4 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)每學期至少乙次進行備份工作，或採用自動備份機制。

### 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-3)

2.5.2 系統管理人員應至少每季執行一次校時。

### 2.6 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）。

## 2.7 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。
  - 每學年定期檢查並取消多餘的使用者識別碼和帳號。
  - 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-4）

## 2.8 特權管理

- 學校的伺服器重要系統資訊具有存取特權人員清單、及其所持有的權限說明，應每學年建立清冊，並予以文件化記錄備查。（參考系統特權帳號清單格式，文件編號 A-5）

## 2.9 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-6]，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 通報安全事件與處理

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-7)

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-8)

### 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-9）

#### 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°C~25°C，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

- 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，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-2)

#### 3.6 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、移入，應檢視相關授權，並實施登記與歸還記錄。
- 機房財產攜出、入須有管制及登記 [文件編號 A-10]。

## 4 人員安全

### 4.1 人員安全責任

- 教職員工均須簽訂保密切結書 [文件編號 A-1]。
  - 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亦須填寫保密切結書。

### 4.2 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。

4.3 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)。

## 5. 資訊業務委外管理

### 5.1 服務委外廠商合約之安全要求

- 5.1.1 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。
- 5.1.2 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)
- 5.1.3 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)

5.2 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-4)

## 6 應對以下各項相關法令有基礎之認知

### 6.1 智慧財產權

著作權法

### 6.2 個人資訊的資料保護及隱私

個人資料保護法及施行細則

### 6.3 刑法電腦犯罪專章



文件編號：A-1

## 保密切結書

紀錄編號：

日期： 年 月 日

本人 \_\_\_\_\_ 將嚴守工作保密規定與國家相關法令對業務機密負完全保密之責任並已瞭解個人資料保護法之精神及新竹縣竹北市博愛國民小學之資訊安全政策且尊重智慧財產權，絕不擅自洩漏、傳播職務上任何業務相關資料及任職期間經辦、保管或接觸之所有須保密訊息資料且絕不擅自複製、傳播任何侵害智慧財產權之任何程式、軟體，違者願負法律責任。

此致

新竹縣竹北市博愛國民小學

立同意書人：\_\_\_\_\_

中 華 民 國 年 月 日

文件編號：A-2

### 新竹縣竹北市博愛國民小學資訊設備啟用與報廢記錄表

啟用      報廢

執行人		執行日期	
設備用途		設備型號	
啟用 檢查 項目	<input type="checkbox"/> 掃毒 <input type="checkbox"/> 變更預設通行碼 <input type="checkbox"/> 系統更新 <input type="checkbox"/> 其它：_____		
	執行人：		
報廢 檢查 項目	<input type="checkbox"/> 刪除硬碟資料(確認資料無法再還原) <input type="checkbox"/> 實體破壞。 <input type="checkbox"/> 其它：_____		
	執行人：		

執行人主管覆核：

文件編號：A-3

## 新竹縣竹北市博愛國民小學資訊工作日誌

填寫日期： 民國\_\_年\_\_月\_\_日

系統操作起始時間： 上(下)午\_\_時\_\_分

操作事項	<input type="checkbox"/> 系統例行檢查 <input type="checkbox"/> 系統維護 <input type="checkbox"/> 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 \_\_\_\_\_

資訊安全官： \_\_\_\_\_ 簽名欄 \_\_\_\_\_

文件編號：A-4

## 新竹縣竹北市博愛國民小學帳號申請表

申請人：		申請日期：			
所屬單位：		分機：			
系統名稱	帳號	申請項目			說明
<input type="checkbox"/> 1.		<input type="checkbox"/> 新增 <input type="checkbox"/> 停用	<input type="checkbox"/> 刪除 <input type="checkbox"/> 異動	<input type="checkbox"/> 重新啟用 <input type="checkbox"/> 重設通行	
<input type="checkbox"/> 2.		<input type="checkbox"/> 新增 <input type="checkbox"/> 停用	<input type="checkbox"/> 刪除 <input type="checkbox"/> 異動	<input type="checkbox"/> 重新啟用 <input type="checkbox"/> 重設通行	
<input type="checkbox"/> 3.		<input type="checkbox"/> 新增 <input type="checkbox"/> 停用	<input type="checkbox"/> 刪除 <input type="checkbox"/> 異動	<input type="checkbox"/> 重新啟用 <input type="checkbox"/> 重設通行	
<input type="checkbox"/> 4.		<input type="checkbox"/> 新增 <input type="checkbox"/> 停用	<input type="checkbox"/> 刪除 <input type="checkbox"/> 異動	<input type="checkbox"/> 重新啟用 <input type="checkbox"/> 重設通行	
<input type="checkbox"/> 5.		<input type="checkbox"/> 新增 <input type="checkbox"/> 停用	<input type="checkbox"/> 刪除 <input type="checkbox"/> 異動	<input type="checkbox"/> 重新啟用 <input type="checkbox"/> 重設通行	
備註					
執行紀錄					
資訊組長（連絡人）：			資安業務主管覆核：		

### 帳號使用注意事項

1. 使用者須妥善保管帳號通行碼，不可告知他人或書寫於他人可取得之處，如便條紙、螢幕或主機外殼等，亦應避免放置於其他易遭他人窺視之場所。
2. 使用者通行碼的長度最少應由 8 個字元組成，並且英文與數字混和。
3. 使用者通行碼應避免包含使用者相關之個人資訊，如電話號碼、生日或姓名。
4. 使用者通行碼宜定期變更，並避免重複使用或循環使用舊通行碼。
5. 使用者離職須移除其系統帳號始完成離職手續。

文件編號：A-5

新竹縣竹北市博愛國民小學資訊系統特權帳號清單

填寫日期： 年 月 日

系統名稱	網址	帳號	人員姓名

資訊組長：

主管覆核：

## 優質通行碼設定原則與使用原則

### 一、良好的通行碼設定原則

1. 混合大寫與小寫字母、數字，特殊符號。
2. 通行碼越長越好，最短也應該在 8 個字以上。
3. 至少每三個月改一次密碼。
4. 使用技巧記住通行碼
  - 使用字首字尾記憶法：
    - a. My favorite student is named Sophie Chen，取字頭成為 mFSinsC
    - b. There are 26 lovely kids in my English class，取字尾成為 Ee6ysnMEc
  - 中文輸入按鍵記憶法：
    - a. 例如「通行碼」的注音輸入為「wj/ vu/6a83」

### 二、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 6666rrrrr 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。

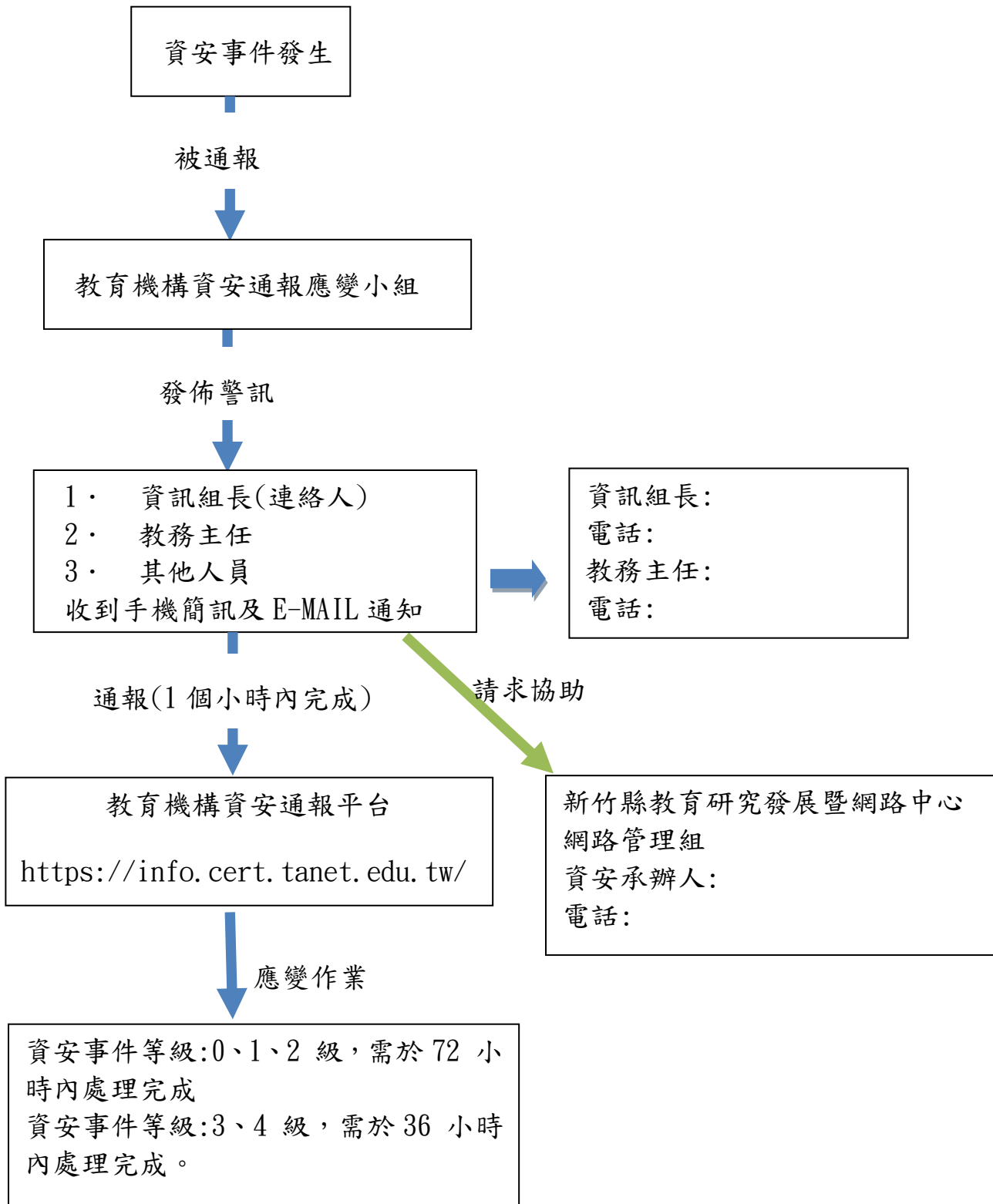
### 延伸參考：

“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>

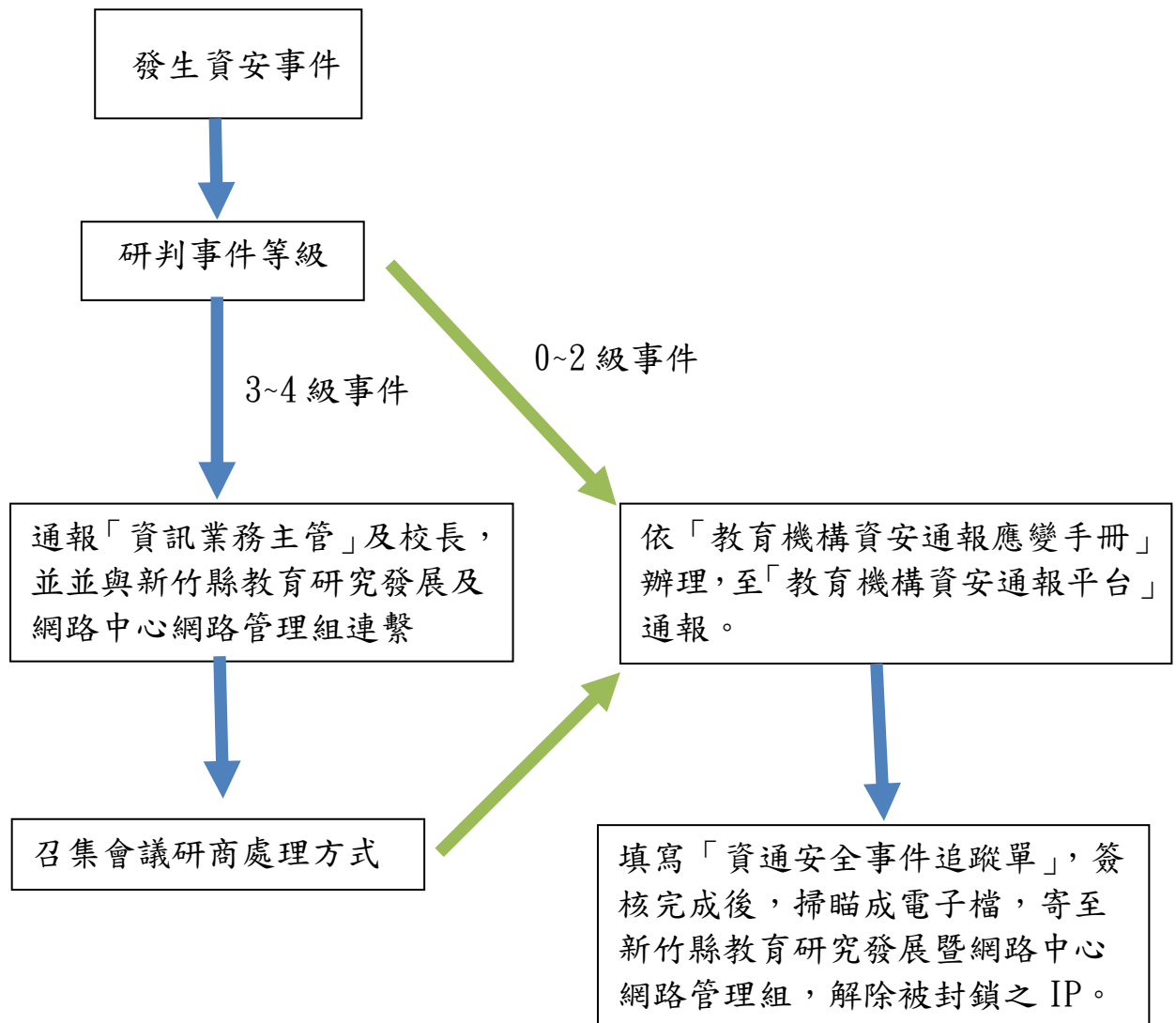
文件編號：A-7

## 新竹縣竹北市博愛國民小學資通安全事件通報程序

### 一．教育機構資安通報流程：



## 二．校內通報流程：





文件編號：A-8

## 新竹縣竹北市博愛國民小學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	<input type="checkbox"/> 桌機 <input type="checkbox"/> 筆電 <input type="checkbox"/> 行動裝置 <input type="checkbox"/> 監視器 <input type="checkbox"/> 其他_____	
	設備用途	<input type="checkbox"/> 行政電腦 <input type="checkbox"/> 班級電腦 <input type="checkbox"/> 電腦教室 <input type="checkbox"/> 公用電腦 <input type="checkbox"/> 個人資訊設備 <input type="checkbox"/> 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： <input type="checkbox"/> 重灌作業系統 <input type="checkbox"/> 還原作業系統 <input type="checkbox"/> 更換主機 <input type="checkbox"/> 無硬碟系統範本更新 <input type="checkbox"/> 其他_____           二·系統修補： <input type="checkbox"/> 安裝最新的修補程式(含作業系統更新) <input type="checkbox"/> 病毒掃描軟體進行掃描，掃到病毒並刪除 三·宣導措施： <input type="checkbox"/> 進行師生宣導 <input type="checkbox"/> 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

新竹縣竹北市博愛國民小學人員進出機房登記表

申請進入機房時間	事 由	進入機房人員 簽 名	陪同人員 簽 名	備註
日 期： 進入時間： 離開時間：		單位：  姓名：		
日 期： 進入時間： 離開時間：		單位：  姓名：		
日 期： 進入時間： 離開時間：		單位：  姓名：		
日 期： 進入時間： 離開時間：		單位：  姓名：		
日 期： 進入時間： 離開時間：		單位：  姓名：		
日 期： 進入時間： 離開時間：		單位：  姓名：		

文件編號：A-10

新竹縣竹北市博愛國民小學設備進出紀錄表

紀錄編號：

填報日期： 年 月 日

<input type="checkbox"/> 攜進 <input type="checkbox"/> 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	<input type="checkbox"/> 自行攜進/出 <input type="checkbox"/> 貨運代送(公司名稱/電話：_____ ) 貨運編號：_____ ) <input type="checkbox"/> 其他(請說明：_____ )			
攜進/出	<input type="checkbox"/> 備份媒體異地儲存 <input type="checkbox"/> 異地儲存之備份媒體送回 <input type="checkbox"/> 新增設備 <input type="checkbox"/> 設備送修(預計修復完成日期：_____ / _____ / _____ ) <input type="checkbox"/> 調 / <input type="checkbox"/> 借 / <input type="checkbox"/> 還 單位： 聯絡人： 聯絡電話： (預計歸還日期：_____ / _____ / _____ )			
核准單位				
資訊組長(連絡人)			資安業務主管	

文件編號：A-11

## 新竹縣竹北市博愛國民小學資訊業務工作交接清冊

網路設備、 伺服器主機	IP 位址	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-12

## 新竹縣竹北市博愛國民小學資訊服務委外單位服務暨保密切結書

\_\_\_\_\_公司(以下簡稱為本公司)為配合新竹縣竹北市博愛國民小學  
(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其訴訟費用，並負責所引發之各項損失賠償。此致

新竹縣竹北市博愛國民小學

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\_\_\_\_\_公司以及新竹縣竹北市博愛國民小學保存

文件編號：A-13

## 新竹縣竹北市博愛國民小學委外廠商人員保密切結書

(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

### 新竹縣竹北市博愛國民小學

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，分別由切結人以及新竹縣竹北市博愛國民小學保存