花蓮縣壽豐國小
資通安全及個資保護管理規範

花蓮縣花蓮縣壽豐國小資通安全及個資保護管理規範

一、 目標

本規範為規定壽豐國小(以下簡稱本校)資通安全管理作業實施方法，以增進資訊作業之安全性，確保學校各項資料之機密性、完整性與可用性。

二、 適用範圍

本校電腦、資訊與網路服務相關的系統、設備、程序、及人員。

三、 實施規定

1. 網路安全

1.1 網路控制措施

- 學校與外界連線，應僅限於經由教網中心之管控，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。

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。

2. 系統安全

2.1 職責區隔

- 本校伺服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)。
- 本校的行政系統主機（例如財務、人事、公文系統等）電腦，由縣教育網路中心或教育處等單位統籌管理。

2.2 對抗惡意軟體、隱密通道及特洛依木馬程式

- 本校的個人電腦應：
  - 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
  - 設定並進行「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。

2.3 資料備份

- 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；週期為每週進行一次。

2.4 操作員日誌

- 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。

2.5 資訊存取限制

- 本校校內之所有電腦設備應以教育及行政辦理功能為目的，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、禁止下載或操作線上遊戲、禁止瀏覽違法、暴力、色情網站或處理及存取相關資料等）。

2.6 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。
  - 每學期檢查並取消多餘的使用者識別碼和帳號。
  - 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。

2.7 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。

2.8 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，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。

2.9 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。

2.10 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。
- 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通報，資訊組儘速進行處理並研判事件等級
- 事件影響等級說明：
  資訊安全事件依影響等級區分為 4 個級別，由重至輕分別為「4 級」、「3 級」、「2 級」及「1 級」。
  ◆4 級事件，符合下列任一情形者：
  - 機密資料遭洩漏。
  - 關鍵業務系統或資料遭嚴重竄改。
  - 關鍵業務系統運作停頓，無法於可容忍中斷時間內回復正常運作。

  ◆3 級事件，符合下列任一情形者：
  - 敏感資料遭洩漏。
  - 關鍵業務系統或資料遭竄改。
  - 關鍵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。

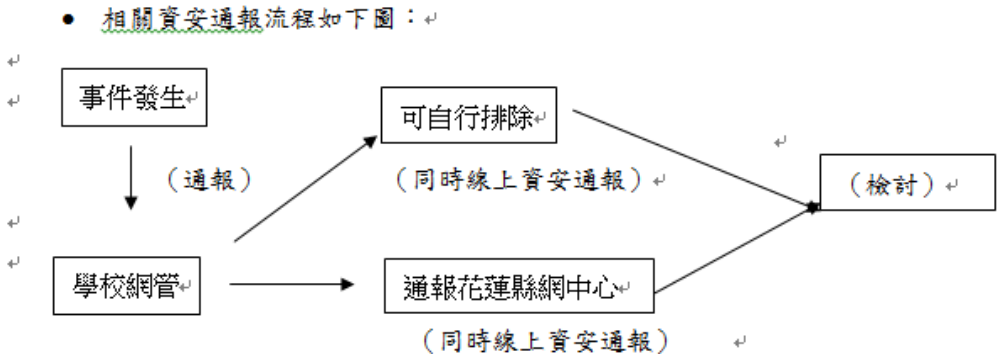
◆2 級事件，符合下列任一情形者：

- 限閱等級資料之關鍵業務系統或資料遭洩漏。
- 關鍵業務系統或資料遭輕微竄改。
- 關鍵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。

◆1 級事件，符合下列任一情形者：

- 非關鍵業務系統或資料遭洩漏。
- 非關鍵業務系統或資料遭竄改。
- 非關鍵業務運作遭影響或短暫停頓可立即修復。

- 資訊組當發生研判事件等級 3(含)以上之事件，應立即通報資訊業務主管及本校校長，並以電話聯絡花蓮縣花蓮縣教育網路中心資安業務承辦人，儘快研商處理方式
- 當學校內部無法處理之資通安全事件，應通報花蓮縣花蓮縣教育網路中心協助處理。
- 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。
- 資安事件如需對外通報，由資訊組登入教育機構資安通報平台進行通報(網址：https://info.cert.tanet.edu.tw)
- 相關資安通報流程如下圖：



3. 實體安全

3.1 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。

3.2 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。

3.3 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。

3.4 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。

3.5 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。

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，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。

3.7 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。

4. 人員安全

4.1 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。
- 因業務需要將機敏資料交付委外廠商時(如辦理保險、校外教學業務等)，廠商必須簽訂安全保密切結書。

4.2 資訊安全教育與訓練

- 本校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。
- 本校鼓勵並安排資訊組長/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。

5. 相關法令網路資源

5.1 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

5.2 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

5.3 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
- 核可憑證機構名單
  http://www.moea.gov.tw/~meco/doc/ndoc/s5_p07_p03.htm

四、 本規範經校長核可後公布實施，修正時亦同

承辦人： 處室主任： 校長：

總務主任林仁傑 總務主任林仁傑 花蓮縣壽豐國小校長張有用