桃園市巴崚國小
資通安全及個資保護管理規範

中 華 民 國 109 年 07 月

- 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

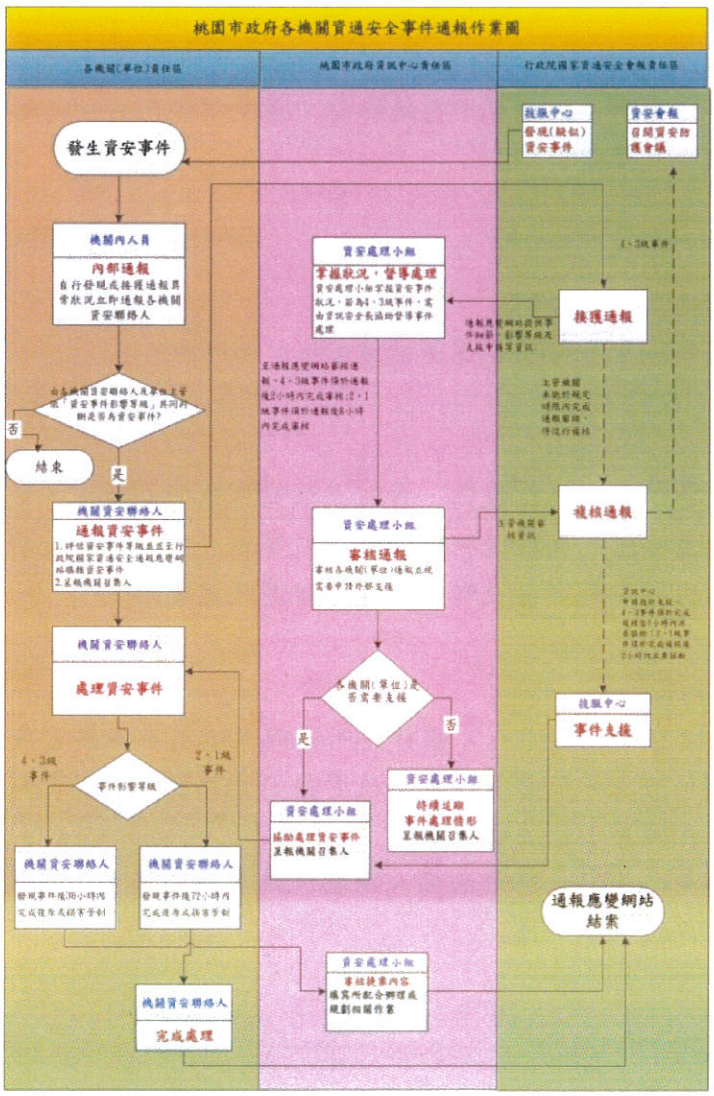
- 學校的電腦與網路系統資訊具有存取特權人員清單、及其所持有的權限說明，應予以文件化記錄備查。

- 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，並以電話聯絡嘉義市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，應通報嘉義市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：



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：

訓導組長陳子安 代理輔導主任李宏謙 巴陵國民小學 校長高理忠(甲)