仁和國小資通安全管理規範

一、目標

本規範為規定重慶國小（以下簡稱本校）資通安全管理作業實施方式，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

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

- 本校與外界連線，應僅限於經由教育局網路管理單位之管控，以符合一致性與單一性之安全要求。
- 應禁止以電話線連結主機電腦或網路設備。

1.2 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（切結書格式參見文件編號 A-1）。

2.系統安全

2.1 職責區隔

- 本校伺服器主機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，由教育局或市政府等單位統籌管理。

2.2 對抗惡意軟體、隱密通道及特洛依木馬程式

- 本校內的個人電腦應：
  - -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「Windows Update」之程式更新作業，以防範作業系統之漏洞。
- 本校內個人電腦所使用的軟體應有授權。
- 新伺服器系統啟用前，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。(伺服主機啟用與報廢申請單格式參見文件編號 A-2)

2.3 資料備份

- 本校系統管理人員需針對學校重要系統(例如系統檔案、網站、資料庫等)定期進行備份工作或採用自動備份機制，週期為每週至少進行一次；並應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 操作員日誌

- 本校系統管理人員需針對重要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。（機房操作日誌文件參見文件編號 A-3）

2.5 資訊存取限制

・本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）。

2.6 使用者註冊

・人員報到或離退職應會辦資訊組長（教師），資訊組長（教師）應執行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。（帳號申請單格式參見文件編號 A-4）

2.7 特權管理

・本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。(特權帳號清單格式參考文件編號 A-5)

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到保密責任。

-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。

・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 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。

・本校資訊安全事件等級，由輕微至嚴重區分等級如下：

- 0 級：教育部及新北市政府教育局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：

□ 非核心業務資料遭洩漏。

□ 非核心業務系統或資料遭竄改。

□ 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：

□ 非屬密級或敏感之核心業務資料遭洩漏。

□ 核心業務系統或資料遭輕微竄改。

□ 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：

□ 密級或敏感公務資料遭洩漏。

□ 核心業務系統或資料遭嚴重竄改。

□ 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：

□ 國家機密資料遭洩漏。

□ 國家重要資訊基礎建設系統或資料遭竄改。

□ 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。

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

・資訊組長（教師）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校長，並以電話聯絡新北市政府教育局資訊安全管理單位資安承辦人，由校長儘快召集會議研商處理的方式。

・當本校發生無法處理之資通安全事件，應通報新北市教育局資訊安全管理單位協助處理。

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

・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，由資訊組長（教師）登入教育機構資安通報平台，完成通報及應變作業。

・資安事件若為校內人員自行發現，由資訊組長（教師）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。

・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。

・如有收到教育機構資安通報平台「資安預警情報」事件通知，由資訊組長(教師)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。

・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。

3. 實體安全

3.1 設備安置及保護

・本校重要的資訊設備（如主機機房）應置於設有空調空間。

・本校資訊設備主機機房及電腦教室區域，應設置偵煙、偵熱與滅火設備(氣體式滅火器），並禁止擺放易燃物或飲食。

・本校資訊設備主機機房及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。

・本校資訊設備主機機房及電腦教室區域，應於入出口處設置門禁的機制。

3.2 溫濕度控制

- 本校重要的資訊設備（如主機機房）應有溫濕度控制措施，以防止資訊設備意外損壞，溫度最好控制在 20℃~25℃，濕度最好控制在相對濕度 50 度~70 度。機房內應懸掛溫濕度計，以觀察實際之溫濕度情況。

3.3 電源供應

- 本校重要的資訊設備(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

- 本校資訊設備主機機房及電腦教室區域內網路線應建佈於高架地板或需設置保護設施。

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，在報廢前應先確保已將任何敏感資料和授權軟體刪除或覆寫。

3.6 設備維護

- 若有需要，宜與設備廠商建立維護合約。
- 廠商進入機房前需先確認已簽訂安全保密切結書。

3.7 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。

3.8 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（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。
- 本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 人員安全責任

- 利用各種場合宣導各層級人員應負之資訊安全責任，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、校外教學等），廠商必須簽訂安全保密切結書。
- 本校臨時人員及志工因業務需要，而接觸公務機密、個人及事業單位權益相關之資料者須填寫校內人員保密切結書。（切結書格式參見文件編號 A-6）

4.2 資訊安全教育與訓練

- 本校系統管理人員應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.應對以下各項相關法令有基礎之認知

5.1 智慧財產權

・著作權法

5.2 個人資訊的資料保護及隱私

・個人資料保護法

・個人資料保護法施行細則

5.3 電子簽章法

・電子簽章法

・電子簽章法施行細則

・核可憑證機構名單