# 國中、小學資通安全管理系統實施原則範例說明—

中小學資訊安全管理系統建置研習

日期:101.11.12

講師:楊淑華

# 一、文件目標

**一．文件目標-**

本文件提供**國民中、小學資通安全系統管理實施原則建議。

◎請依據內容修改符合貴校之資通安全實施原則。

# 文件目標【範例】

1．本文件提供本校資通安全系統管理實施原則建議。

2．為避免校園內部使用相關資訊設備時，因個人操作及其他因素導致重要資料外洩及設備毀損，特訂立此實施辦法。

# 二、適用範圍

- **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。(設定此份文件所適用的範圍與名詞定義。)

# 適用範圍【範例1】

- 校園內電腦、資訊與網路服務相關的系統、設備及人員。
- 茲定義以下名詞：

1.一般區：係指班級教室、電腦教室、專科教室及大辦公室共用電腦區域。

2.敏感區：係指各行政辦公室內行政人員使用電腦所放置區域。

3.機密區：係指學校各項網路及資訊服務主機所放置區域(機房)。

# 適用範圍【範例2】

- 學校內電腦、資訊與網路服務相關的系統、設備、程序、及人員。
- 學生用電腦：電腦教室及各專科教室內提供學生操作使用的電腦設備。
- 教師用電腦：教職員工個人專用的教學或行政用電腦設備。
- 教師公用電腦：辦公室中供所有教師共同使用的電腦設備。

# 適用範圍【範例3】

- 本校電腦、資訊與網路服務相關的系統、設備、程序、及人員。
- 本校電腦依區域劃分可區分成「行政辦公室電腦、班級電腦、電腦教室電腦、專科教室電腦、伺服器」。
- 其中電腦（個人電腦、筆記型電腦）並分成作業系統該分割區有啟動還原及無啟動還原兩類。

# 適用範圍【範例4】

- 本校電腦、資訊與網路服務相關的系統、設備、程序、及人員。
- 特殊系統：公文、會計、人事及學籍等系統。
- 安全區域：機櫃。

# 三、實施原則

1．網路安全

1.1 網路控制措施-

三項內容請調整為符合學校之需求。

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

學校主機電腦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）。

- 學校的行政系統主機（例如財務、人事、公文系統等）電腦，由教育網路中心或上級單位統籌管理。

◎請適學校需要修正「職責區隔」範圍。

# 系統安全【範例】

- 學校主機電腦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、檔案伺服器、虛擬光碟主機）。

# 2.2對抗惡意軟體、隱密通道及特洛依木馬程式【範例1】

- 學生用電腦：
  - 使用還原卡，每次開機都會自動還原系統。
  - 裝置防毒軟體，將軟體設定為自動定期更新病毒碼。
  - 每年一次進行所有程式之更新作業，以防範所有系統之漏洞。
- 教師用電腦、教師公用電腦及伺服器
  - 裝置防毒軟體，將軟體設定為自動定期更新病毒碼。
  - 系統設定自動進行如「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合法授權，並於校務會議中宣導。
- 新系統啟用前，須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。

# 2.2對抗惡意軟體、隱密通道及特洛依木馬程式【範例2】

- 學校內的個人電腦：
  - 裝置防毒軟體，將軟體設定為自動定期更新病毒碼。
  - 定期安裝作業系統漏洞修補程式，以防範作業系統之漏洞：
    - 電腦教室及其他裝有還原系統之主機：每學期更新
    - 其他主機：每日更新
- 學校內個人電腦所使用的軟體有合法授權。
- 新系統啟用前，須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

- 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）定期進行備份工作，或採用自動備份機制；建議週期為每週進行一次。

# 2.3資料備份【範例】

(一）學校系統管理人員針對學校重要系統（如系統檔案、應用系統、資料庫等）每月進行備份工作，或採用自動備份機制。

**（二）本校資訊業務負責人需針對學校網頁伺服器定期（每月）進行資料庫備份工作。本校資訊業務負責人應設定學校檔案伺服器以Raid5進行檔案之備份保存。**

# 2.4 操作員日誌

- 學校(或委託)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，針對這些活動填寫日誌予以紀錄，作為未來需要時之檢查。
- 日誌內容包含以下各項：
  - 系統例行檢查、維護、更新活動的起始時間
  - 系統錯誤內容和採取的改正措施。[*參考日誌範本，文件編號A-2*]
  - 紀錄日誌項目人員姓名與簽名欄與資訊安全官確認欄

# 2.4 操作員日誌【範例】

- 學校資訊業務負責人需每月針對學校網頁伺服器進行檢查、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。
- 日誌內容可包含以下各項：
  - 系統例行檢查、維護、更新活動的起始時間
  - 系統錯誤內容和採取的改正措施。（文件編號A-2）
  - 紀錄日誌項目人員姓名與簽名欄與資訊安全官確認欄

# 2.5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）。

# 2.5資訊存取限制【範例】

- 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）。
  - 安裝還原系統，並設定系統碟為開機還原。
  - 如需使用公用電腦，需向管理單位申請帳號密碼，權限為限制安裝軟體權限（如WindowsXP系統的Users群組）。
  - 禁止安裝P2P軟體。

# 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。
  - 定期（建議每學期）檢查並取消多餘的使用者識別碼和帳號。
  - 定期（建議每學期）檢查新增之帳號，若有莫名帳號產生，應關閉帳號權限，並依通報程序請求處理（參照本文件2.10段落）。

# 2.6 使用者註冊【範例】

- 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。
  - 每學年檢查並取消多餘的使用者識別碼和帳號。
  - 每學年檢查新增之帳號，若有莫名帳號產生，應關閉帳號權限，並依通報程序請求處理（參照2.10）。

# 2.7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，文件應有管理階層確認。

- 範例-

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，每學年建立清冊記錄備查。

# 2.10 通報安全事件與處理

- 學校應建立資訊安全事件通報程序[編號A-4]以及安全事件通報單[編號A-5]；通報程序應包括學校內部通報，以及學校與所屬縣市教育網路中心的通報。

# 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(機房)需簽訂安全保密切結書[文件編號*A-1*]
- 人員進出安全區域(機房)需有安全管制登記[文件編號*A-7*]。

# 資訊服務委外單位服務暨保密切結書範本

- 請填上貴單位名稱。