國中、小學資通安全管理系統實施原則說明

許雅雯 經理
NII 產業發展協進會

簡報大綱

- 背景說明
- 國中、小學資通安全管理系統實施原則
  - 文件目標
  - 適用範圍
  - 實施原則
    1. 網路安全
    2. 系統安全
    3. 實體安全
    4. 人員安全
    5. 法令遵循
- 結語

簡報大綱

- 背景說明
- 國中、小學資通安全管理系統實施原則
  - 文件目標
  - 適用範圍
  - 實施原則
    1. 網路安全
    2. 系統安全
    3. 實體安全
    4. 人員安全
    5. 法令遵循
- 結語

背景說明

- 政府為了滿足各行政單位之需求，民國88年制定了「行政院及所屬各機關資訊安全管理規範」。
- 行政院於民國90年成立「國家資通安全會報」，以協助建立政府機關及重要民間業者建立安全之資通訊及網路系統。

背景說明(續)

行政院國家資通安全會報資通安全責任分級

作業名稱 / 等級	防護縱深	ISMS推動作業(註一)	稽核方式	資安教育訓練(一般主管、資訊人員、資安人員、一般使用者(註二))	專業證照(註四)	檢測機關網站安全弱點
A級	NSOC直接防護/SOC自建或委外、IDS、防火牆、防毒、郵件過濾裝置	通過第三者驗証	每年至少2次內稽	1. 每年至少(3、6、18、3小時) 2. 資訊人員、資安人員需通過資安職能鑑定(註三)	維持至少2張資安專業證照	每年2次
B級	SOC(選項)、IDS、防火牆、防毒、郵件過濾裝置	通過第三者驗証	每年至少1次內稽	1. 每年至少(3、6、16、3小時) 2. 資訊人員、資安人員需通過資安職能鑑定(註三)	維持至少1張資安專業證照	每年1次
C級	防火牆、防毒、郵件過濾裝置	自行成立推動小組規劃作業	自我檢視	每年至少(2、6、12、3小時)	資安專業訓練	每年1次
D級	防火牆、防毒、郵件過濾裝置	推動ISMS觀念宣導	自我檢視	每年至少(1、4、8、2小時)	資安專業訓練	每年1次

背景說明(續)

- 由於學術單位與政府機關的屬性不同，雖然行政院已有頒布可依循之規範，但無法適用於教育體系，因此有必要研擬一套專屬的資通安全管理規範。
- 教育部於 96 年 6 月 11 日發函各機關學校公布推動「教育體系資通安全管理規範」與「國中小學資通安全管理系統實施原則」為教育體系 ISMS 建置參考。

背景說明(續)

- 教育部針對資訊安全責任分級，規劃教育體系機關學校共分為 A、B、C、D 四級。

學研機關（構）資安等級區分表

類別	內　　容
A 級 重要核心	● 教育政策主管機關（教育部） ● 教學醫院（台大醫院、成大醫院）
B 級 核心	● 6 所入學考試常設機構 ● 117 所大學 ● 13 個 TANet 區網中心 ● 22 個縣(市)教育網路中心 ● 陽明大學附設醫院 【承辦全國性入學考試業務學校、機關(構)比照B級單位】
C 級 重要	● 30 所技術學院及 14 所專科學校 ● 14 個部屬館所
D 級 一般	● 491 所公私立高中、職學校 ● 3,398 所國中小學

教育部推動現況

- 推動機制
  - 成立並營運教育體系資安推動組織。
  - 建立教育體系「第三者驗證」機制，大多數區、縣(市)網中心、大專院校皆已通過教育體系資通安全管理規範之驗證。
  - 已成立教育體系資安通報處理程序與通報應變網站。

教育部推動現況(續)

- ISMS推動
  - TANet 區/縣市網中心ISMS建置，已得教育體系第三者驗證。
  - 公私立大學（B級）導入資安管理制度，原則由各校自行推動導入。
  - 依教育體系資通安全管理規範進行ISMS 導入及驗證，並輔導C、D級單位。

教育部推動現況(續)

- 教育訓練
  - 規劃辦理教育體系人員資安證照訓練課程。
  - 針對教育體系主管、資訊技術人員的認知與教育訓練。
  - 國中小學生的資安認知推廣活動。（資安防護學園 102/10/1~11/15）
    http://cissnet.edu.tw/safely/

簡報大綱

- 背景說明
- 國中、小學資通安全管理系統實施原則
  - 文件目標
  - 適用範圍
  - 實施原則
    1. 網路安全
    2. 系統安全
    3. 實體安全
    4. 人員安全
    5. 法令遵循
- 結語

簡報大綱

- 背景說明
- 國中、小學資通安全管理系統實施原則
  - 文件目標
  - 適用範圍
  - 實施原則
    1. 網路安全
    2. 系統安全
    3. 實體安全
    4. 人員安全
    5. 法令遵循
- 結語

文件目標與適用範圍

文件目標

- 提供國中、小學資通安全管理系統實施原則指引。

適用範圍

- 國中、小學資訊系統及其相關處理設施之管理。

簡報大綱

- 背景說明
- 國中、小學資通安全管理系統實施原則
  - 文件目標
  - 適用範圍
  - 實施原則
    1. 網路安全
    2. 系統安全
    3. 實體安全
    4. 人員安全
    5. 法令遵循
- 結語

實施原則 – 1. 網路安全

1.1 網路控制措施

- 學校與外界連線，宜僅經由縣網中心，以符合一致性與單一性之安全控管要求。
- 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）宜區隔於網路之外；當有必要透過網路傳輸資料時，應有安全的控管機制如（加密、VPN、SSL等）。
- 禁止以電話線連結至電腦主機或網路設備。

實施原則 – 1. 網路安全(續)

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。

簡報大綱

- 背景說明
- 國中、小學資通安全管理系統實施原則
  - 文件目標
  - 適用範圍
  - 實施原則
    1. 網路安全
    2. 系統安全
    3. 實體安全
    4. 人員安全
    5. 法令遵循
- 結語

實施原則- 2. 系統安全

2.1 職責區隔

- 學校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）。
- 學校的行政系統主機（例如財務、人事、公文系統等）電腦，建議由各個縣（市）教育網路中心或教育局等單位**統籌管理**。

實施原則- 2. 系統安全(續)

2.2 對抗惡意軟體、隱密通道及特洛依木馬程式

- 學校內的個人電腦應：
  - 安裝防毒軟體，並定期更新病毒碼。
  - 定期（至少每個月）進行如「Windows Update」之程式更新作業，以防範作業系統之漏洞。
- 不得使用非法軟體。
- 新系統啟用前，應經過掃毒與更新系統密碼，以防範可能隱藏的病毒或後門程式。

實施原則- 2. 系統安全(續)

2.3 資料備份

- 學校重要系統（例如系統檔案、應用系統、資料庫等）應定期進行資料備份或自動備份；建議週期為每週進行一次。

實施原則- 2. 系統安全(續)

2.4 操作員日誌

- 敏感度高、或包含特殊資訊的電腦系統應進行檢查、維護、更新等活動，並將這些活動填寫日誌予以記錄，以供查考。
- 日誌內容應包含以下各項：
  - 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。
  - 操作人員簽名。

實施原則- 2. 系統安全(續)

2.5 資訊存取限制

- 學校內之多人共用的電腦應以特定功能為目的，並設定安全管控機制（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）。

實施原則- 2. 系統安全(續)

2.6 使用者註冊

- 學校應制定電腦系統使用者註冊及註銷程序，並透過該註冊及註銷程序來管理使用者存取權限，該作業應包括以下內容：
  - 每位使用者皆有各自（唯一）的識別碼（ID）。
  - 保存一份包含所有識別碼註冊的紀錄。
  - 使用者調職或離職（留職停薪、退休）後，應調整或移除其存取權限。
  - 定期（建議每學期 1 次）檢查使用者之帳號及權限，若有未經授權的帳號產生或不適當之權限設定，應立即調整或取消帳號權限。帳號檢查活動應留存紀錄。
  - 若上述帳號異常狀況研判為駭客入侵應依通報程序處理（參照本文件2.10 段落）。

實施原則- 2. 系統安全(續)

2.7 特權管理

- 學校的電腦與網路系統具有最高權限之帳號應建立使用人員清單。
- 應開啟電腦系統稽核紀錄功能，留存最高權限的使用活動電腦稽核紀錄(log)。

實施原則- 2. 系統安全(續)

2.8 通行碼（密碼）之使用

- 管制使用者第一次登入系統時，必須立即更改預設密碼。
- 資訊系統與服務應避免多人使用共同帳號及密碼。
- 學校應制定及發布密碼 (Password)使用規則[參考優質密碼設定原則與使用原則，附件A-3]，內容應包含以下各項：
  - 使用者應該對其個人所持有密碼盡保密責任
  - 要求使用者的密碼設定，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。或建議密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。

實施原則- 2. 系統安全(續)

2.9 原始程式庫之存取控制

- 應用程式之原始碼存取行為應加以控管。
- 學校對外提供之網頁服務應防範資料庫隱碼(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。

實施原則- 2. 系統安全(續)

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、資料或網頁遭竄改，以及通訊中斷等。
- 學校應建立資訊安全事件通報程序，其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。
- 當遭遇重大或學校內部無法處理之資通安全事件，應通報其所屬縣市教育網路中心。
- 所訂出之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。

簡報大綱

- 背景說明
- 國中、小學資通安全管理系統實施原則
  - 文件目標
  - 適用範圍
  - 實施原則
    1. 網路安全
    2. 系統安全
    3. 實體安全
    4. 人員安全
    5. 法令遵循
- 結語

實施原則- 3. 實體安全

3.1 設備安置及保護

- 學校重要的資訊設備應置於安全地點（如主機機房）並設有空調設施。
- 學校設置大量資訊設備之地點，如：主機機房、電腦教室區域，應設置滅火設備，並避免堆積易燃物或在區域內飲食。
- 學校設置大量資訊設備之地點，如：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，避免如雷擊事件造成損害情況。
- 學校設置大量資訊設備之地點，如：主機機房、電腦教室區域，應於入出口處加裝門鎖或其他安全措施。

實施原則- 3. 實體安全(續)

3.2 電源供應

- 學校重要的資訊設備（如主機機房）應有適當的電力支援設施，例如UPS、電源保護措施，以免斷電或超過負載而造成損失。

3.3 纜線安全

- 學校主機機房、電腦教室區域內應使用符合安全要求之纜線並綑綁整齊，必要時以管線包覆。

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，在報廢或再使用前應先確保已將任何敏感資料和授權軟體刪除或覆寫。

實施原則- 3. 實體安全(續)

3.5 設備維護

- 設備委託廠商維護時應與廠商建立維護合約，並將安全條款納於合約中。
- 廠商受託維護設備或執行任務而接觸學校重要或敏感資訊時，須先請其簽訂安全保密切結書。

3.6 財產攜出

- 財產之攜出應依教育部或學校既有之相關規定處理。包含：
  - 未經授權不得將學校的資訊設備、資訊/資料或軟體攜出校園以外。
  - 財產攜出應予登記並追蹤歸還情形。

實施原則- 3. 實體安全(續)

3.7 桌面淨空與螢幕淨空政策

- 學校教職員工於結束工作時，應將其所經辦或使用具有機密或敏感特性的資料（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電腦應採取適當的安全措施，如鎖匙、登入密碼驗證，以及設定螢幕保護程式。

簡報大綱

- 背景說明
- 國中、小學資通安全管理系統實施原則
  - 文件目標
  - 適用範圍
  - 實施原則
    1. 網路安全
    2. 系統安全
    3. 實體安全
    4. 人員安全
    5. 法令遵循
- 結語

實施原則- 4. 人員安全

4.1 將安全列入工作執掌中

- 應將資訊安全要求納入教職員手冊說明中，以強化工作上之資訊安全意識。

4.2 資訊安全教育與訓練

- 學校資訊系統管理人員應定期參與資訊安全專業訓練，確保有足夠能力執行任務。
- 學校應安排全體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。

簡報大綱

- 背景說明
- 國中、小學資通安全管理系統實施原則
  - 文件目標
  - 適用範圍
  - 實施原則
    1. 網路安全
    2. 系統安全
    3. 實體安全
    4. 人員安全
    5. 法令遵循
- 結語

實施原則- 5. 法令遵循

5.1 智慧財產權

– 應實作適當程序，以確保所使用的資料可能涉及智慧財產權與所使用的專屬軟體產品，可遵循法律、法規及契約的要求。

5.2 個人資訊的資料保護及隱私

– 應如同相關法令，法規及若適用的契約條文所要求的，確保資料保護與隱私。

5.3 電子簽章

資訊服務委外單位服務暨保密切結書範本

文件編號：A-1

資訊服務委外單位服務暨保密切結書範本

_____公司(以下簡稱為本公司)為配合_____學校（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及其訴訟費用，並負責所引發之各項損失賠償。此致

XXX 學校

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_____學校保存

操作員日誌範本

文件編號：A-2

操作員日誌範本

填寫日期：　民國___年___月___日
系統操作起始時間：　上（下）午___時___分
系統操作結束時間：　上（下）午___時___分

操作事項	☐ 系統例行檢查 ☐ 系統維護 ☐ 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_____

優質通行碼設定原則與使用原則

文件編號：A-3

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 6666rrrr 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

簡報大綱

- 背景說明
- 國中、小學資通安全管理系統實施原則
  - 文件目標
  - 適用範圍
  - 實施原則
    1. 網路安全
    2. 系統安全
    3. 實體安全
    4. 人員安全
    5. 法令遵循
- 結語

結論

- 資訊安全是不間斷的工作，應落實執行。
- 時時提高警覺，有效降低資安事件發生。
- 每位同仁皆應遵守組織資訊安全規定。

資訊安全

人人有責

簡報完畢
敬請指教