資訊安全管理系統(ISMS)講習

《ISMS 推動與導入流程說明》

臺南區域網路中心

100 年 11 月 18 日

台南區網中心(成功大學)
ISMS推動及導入流程說明

NII 產業發展協進會
吳昭儀 經理
✉ joycewu@nii.org.tw ☎ (02) 2508-2353

大綱

- ISMS 執行重點
  - ISMS 基本觀念
  - 日常維運、內部稽核、矯正預防、管理審查執行重點
- ISMS程序書架構與重點
  - ISMS管理文件架構說明
  - 政策與各程序書重點說明

ISMS 執行重點 – 基本觀念

- 資訊安全
- 資訊安全管理制度
- 資訊安全管理重點
- 職權分工

何謂資訊安全?

- 資訊的價值
  - 直接可衡量
  - 間接可衡量
- 為了發揮資訊的最大價值，就必須有效的防止資訊遭竊取、竄改、毀損、滅失或遺漏，簡言之，就是確保資訊的：
  - 機密性
  - 完整性
  - 可用性

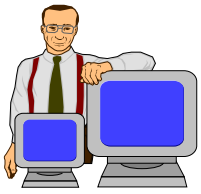
資訊安全三要素

- 機密性，Confidentiality
  - 保護資訊不被非法存取或揭露
- 完整性，Integrity
  - 確保資訊在任何階段沒有不適當的修改或損毀
- 可用性，Availability
  - 經授權的使用者能適時的存取所需資訊

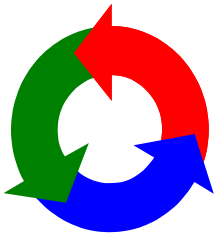
何謂資訊安全管理制度 (ISMS)？

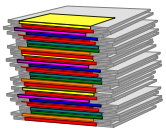
ISMS目的在於保護資訊資產的機密性、完整性與可用性。

資訊安全管理重點



People



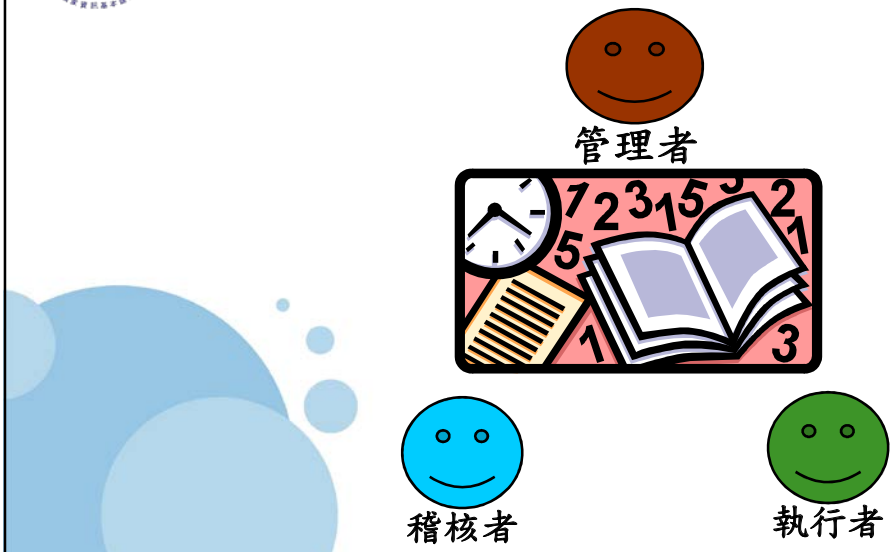


Process

Technology

資訊安全管理重點

ISMS 職權分工



人員定位

ISMS 執行重點 – 維護重點

- 教版規範之 ISMS 建置步驟
- 日常維運
- 內部稽核
- 矯正預防
- 管理審查

教版規範之 ISMS 建置步驟

- ISMS之建立 (Plan)
  - 依據該單位之類型、規模、資源、業務性質等特性，定義ISMS之範圍；考慮相關法律、法規以及合約之要求，於適度評估風險及應對措施後，訂出經由管理階層核准之ISMS政策，並擬定一份適用性聲明書文件。
- ISMS之實施與操作 (Do)
  - 施行單位應確實實施控制措施，以符合控管的目標，並執行訓練與認知計畫，確保偵測安全事件的能力，以及迅速回應和應對處理的時效。

教版規範之 ISMS 建置步驟

- ISMS之監控及審查
  - 施行單位應針對ISMS進行監控程序與其他控制措施，即時鑑別資安事件的發生、處理順序與解決方法；定期審查ISMS之有效性（建議一學年至少一次），並將相關有顯著影響之活動與事件記錄下來。
- ISMS之維持及改進
  - 施行單位應定期實行改進活動，採取適當的矯正與預防措施，並得到管理階層之同意，確保各項措施達到預期目標。

日常維運
內部稽核
矯正預防
管理審查

依PDCA循環執行

- P
  - ISMS時程及工作規劃
- D
  - Asset盤點及評價
  - 執行 RA評鑑
  - BCP演練及風險再評鑑
  - ISMS SOP落實
  - 權限及授權軟體清查

日常維運
內部稽核
矯正預防
管理審查

依PDCA循環執行

- C
  - 內部稽核
  - 管理審查
- A
  - 持續改善（矯正及預防）

日常維運
內部稽核
矯正預防
管理審查

資訊安全稽核

- 資訊安全稽核的目標
  - 確保單位遵循資訊安全政策及標準程序、衡量資訊安全管理制度之有效性
    - 控管程序是否落實
    - 檢查與評估資安控制措施之缺失
    - 評估管理成效
  - 內部稽核為ISMS維護的必要工作之一

內部稽核與外部稽核

- 內部稽核
  - 組織內部預先進行的稽核作業，自行找出組織作業流程的缺失，提出建議改進
- 外部稽核
  - 上級機關對組織進行的稽核
  - 申請驗證所接受的稽核

稽核範圍、作業與抽樣期間

- 稽核範圍
  - 例如計算機及資訊網路中心
- 稽核作業方式
  - 訪談
  - 書面審查
  - 實地審查
- 稽核（抽樣）期間
  - 文件發行日期～迄止日期
  - 上次稽核日期～本次稽核日期

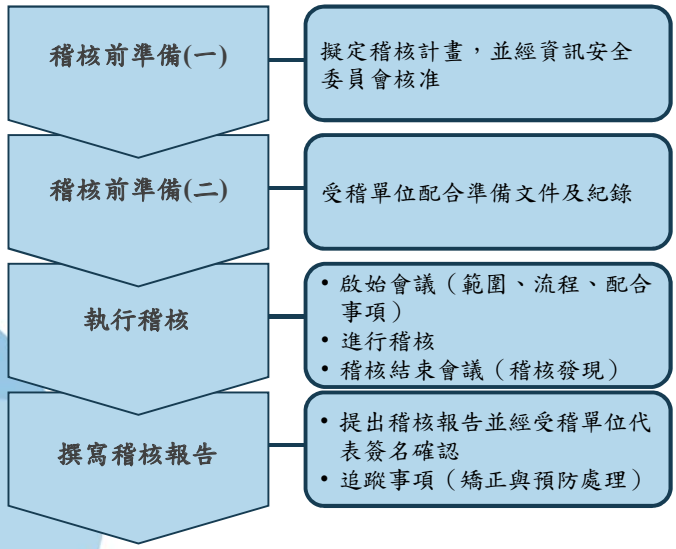
稽核團隊

- 稽核團隊
  - 組長：主導稽核
  - 組員：配合組長指示執行稽核作業
- 團隊成員資格
  - 具有基本與正確的稽核認知
    - 取得ISO 27001 LA證照
    - 上過稽核相關教育訓練課程
    - 具有實際稽核之經驗

相關人員參與的稽核工作/責任

- 資訊安全委員會
  - 指派資訊安全稽核小組
  - 督導作業
- 資訊安全稽核小組（稽核團隊）
  - 稽核作業事宜
  - 追蹤改善情形
- 受稽單位
  - 相關業務人員接受稽核
  - 提供文件與紀錄
  - 針對稽核發現提出矯正及預防措施

稽核進行流程



稽核執行方式－書面審查

- 文件稽核：依稽核依據檢視文件是否已具相關控制項
- 文件稽核範例

  10.5.1 資訊備份

  宜依據所議定的備份政策，定期進行資訊與軟體的備份與測試
  - 各項系統設定檔、網頁資料、伺服器檔案及資料庫資料均應由各系統負責人員訂定備份週期，並依據週期執行系統排程或手動備份，備份狀況應記錄於「備份狀況紀錄表」
  - 應定期於測試主機上測試備份復原是否正確

稽核執行方式－實地審查

- 實地查核：檢視相關之人、事、物是否依文件中所訂之規範落實執行
  - 現場：環境、電腦之系統設定等
  - 紀錄：是否依文件中所訂之規範落實紀錄
- 實地查核範例
  - 禁止使用或下載未經授權或與業務無關之軟體

    →檢查使用者電腦是否安裝非授權軟體
  - 系統管理者密碼設置，至少 7 碼

    →檢查管理者密碼長度是否為7碼

抽查方法

- 抽查一個樣本不符合：疏失
  →建議或缺失
- 抽查兩個樣本皆不符合：系統性缺失
  →缺失

稽核範例－資訊安全政策

- 管理階層是否瞭解資訊安全目的並給予支持？
- 資訊安全政策文件是否由管理階層核准，並正式發布予員工？
- 資訊安全政策是否定期評估，並作必要調整？

稽核範例－安全組織

- 是否具管理階層或成立跨部門單位負責推動、協調及監督資訊安全管理事項？
- 是否指派專人或專責單位負責規劃、執行資訊安全控管工作？
- 是否規範員工的資訊安全作業程序與權責？
- 是否訂定資訊設備的安全作業程序？

稽核範例－資產管理

- 是否建立資產清冊並適時更新？
- 重要資產是否均指定專人負責管理？
- 資訊是否分級？是否建立資訊安全等級之分類標準？
- 對於機密等級的資訊是否標示清楚？

稽核範例－人員安全管理

- 對於具有存取較機密性資訊權限之員工，是否進行分工以分散權責？
- 人員之調動、離職，是否立即取消其各項識別碼與通行碼？
- 是否依員工職務層級進行適當的資訊安全講習？
- 員工是否瞭解組織的資訊安全政策？

稽核範例－實體與環境安全

- 資訊設備設置地點是否已作安全考量？
- 是否檢查及評估水、火、灰塵、電力供應等對於資訊設備之危害？
- 電源供應及備援電源是否作安全考量？
- 設備報廢前是否將機密性資料及版權軟體移除？

稽核範例－通訊與作業管理

- 是否建立系統變更程序？
- 是否全面使用防毒軟體並更新病毒碼？
- 對重要資料及軟體是否定期作備份？
- 儲存媒體是否依保存要求存放在安全的環境？

稽核範例－存取控制

- 多人使用之資訊系統，是否建立使用者註冊管理程序？
- 是否定期檢查並刪除重覆或閒置的使用者帳號？
- 應用系統是否具作業結束或一定期間未操作即自動登出之保護機制？
- 是否管制使用者的連線功能？

稽核範例－資訊系統獲取、開發及維護

- 應用系統在規劃分析時是否將安全需求納入考量？
- 機密性資料在傳輸或儲存過程是否使用加密技術？
- 如須用真實資料進行測試，是否於事前將足以辨識個人身分之資料隱蔽？

稽核範例－資訊安全事故管理

- 是否建立資訊安全事件通報與處理程序？
- 是否建立資訊安全事故管理責任與應變程序？
- 資訊安全事件中相關證據資料是否有適當保存措施？

稽核範例－業務持續管理

- 是否擬訂關鍵性業務及其風險評估、衝擊影響？
- 是否訂有緊急應變計畫？
- 緊急應變計畫是否定期演練與修正？

稽核範例－遵循性

- 是否使用合法軟體？
- 是否依「個人資料保護法」規定辦理？
- 是否定期稽核資訊安全事項辦理情形？

矯正預防

日常維運
內部稽核
矯正預防
管理審查

- 執行時機
  - 內部及外部稽核發現缺失時，缺失權責單位需提出矯正措施，並填寫於「矯正與預防處理單」。
  - 發生資訊安全事件（含重大異常事件）或自行發現缺失時，應執行矯正或預防措施，並填寫於「矯正與預防處理單」。
- 原因分析
  - 防制缺失權責單位應分析問題發生之原因及影響程度，決定優先順序與處理時限。
- 矯正與預防措施評估
  - 缺失權責單位提出矯正與預防措施時，得區分為暫時性對策及永久性對策，防止類似事件發生。
  - 評估措施時須考慮成本效益及可行性。

日常維運
內部稽核
矯正預防
管理審查

矯正預防

- 追蹤執行狀況
  - 矯正與預防措施之執行狀況，應由缺失權責單位依據「矯正與預防處理單」確實執行。
  - 有關執行狀況之追蹤，由稽核組員、組長或相關權責人員負責。
  - 追蹤人最遲應於收到「矯正與預防處理單」後7個工作天內進行首次追蹤，並應於「矯正與預防處理單」上留存追蹤軌跡。
- 管理審查
  - 缺失權責單位應彙整相關矯正及預防措施之執行狀況，於管理審查會議提出報告。

日常維運
內部稽核
矯正預防
管理審查

管理審查會議實施相關規範

- 依據資訊安全組織程序書「5.2管理審查會議」之相關規範召開管理審查會議
- 會議召開頻率：每年至少一次
- 會議參與人員：同資訊安全委員會成員
- 管理審查會議討論項目計有：
  - 審查內容（九大輸入項目）
  - 審查結論（五大輸出項目）
- 管理審查會議為ISMS重要活動，會議過程應完整記錄，並依ISMS文件管理程序保存
- 中心應依會議紀錄落實執行ISMS持續改善作為

審查內容（九大輸入項目）

一、資訊安全稽核結果及建議改善事項
二、員工、上級指導單位及第三方單位等利害相關團體的建議
三、新資訊安全產品或技術導入之審查
四、矯正及預防措施檢討
五、風險評鑑適切性審查
六、前次管理審查會議決議執行狀況
七、影響資訊安全制度之任何變更事項
八、資訊安全組織成員所提出之改善建議
九、資訊安全目標執行狀況報告

****每一項都要有相關的證據當附件**

一、資訊安全稽核結果及建議改善事項

稽核項目	稽核發現	建議事項	附註
其他建議事項			

附件：
1.內、外稽報告。
2.矯正與預防處理單（有幾項缺失，就必須填幾張單子）。
3.建議事項請一併提出改善方案。

二、員工、上級指導單位及第三方單位等利害相關團體的建議

單位	回饋與建議
上級機關	教育部：
各連線單位	XXX區網： XXX大學：
單位內人員	網路組： 系統組：
輔導單位(NII)	● 擬定教育訓練與宣導計畫來持續強化本中心同仁對於資通安全之完整認知 ● 排定年度教育訓練計畫（包含委外人員）以符合行政院對於B級單位人員教育訓練時數要求 ● 透過電子報或內部網站來宣導人員應遵守之資通安全相關規定 ● 選擇適當之評量方式檢視教育訓練及宣導之成效與人員是否擁有足夠之相關知識，並從中找出持續改善之道
其它單位	

為便於日後追蹤與填寫，若無內容則填「無」，不建議刪除

附件：
1. 相關單位（教育部、資安會報、輔導單位等）有關資訊安全的公文、公告、計畫內容等。
2. 單位同仁日常透過E-mail發布有關資訊安全的建議內容。

三、新資訊安全產品或技術導入之審查

例如單位預計導入新的資安設備可列入討論

- 98年第四季導入IDS設備
  - 預計效益
  - 使用預算
  - 對現有網路架構之影響
- 建立資安區域聯防機制
  - 預計完成時程
  - 預計投入人力
  - 預計成本
  - 預期效益

附件：
1. 採購計畫（例如：備份或備援機制、網路安全設備採購…等）。
   年度內有無需要申請添購的資訊安全相關新產品或新技術，若沒有也可以填「無」。

四、矯正及預防措施檢討

〈透過內稽所發現之問題缺失之矯正預防措施可併於第一大項討論，本項可彙整非內稽發現之問題缺失的矯正預防措施〉

項次	問題或缺失說明	原因分析	矯正與預防措施評估	預計完成日期
1	「適用法規之鑑別」，發現參考文件為「資訊安全稽核作業程序書」，惟該程序書尚未對相關權責予以文件化。	未明確鑑別本中心適用之法令法規	於「資訊安全組織程序書」中規範資訊安全小組鑑別適用法規，並將適用法規記錄於「外來文件一覽表」	100/09/30
2	電腦機房內存放易燃物。	因為廠商與中心人員於電腦機房內裝機，未將包裝之紙箱攜出	將電腦機房內之紙箱（易燃物）移除。 進行宣導，請廠商與中心同仁不要將紙箱等易燃物放置於機房內。	100/09/30
3	檢視XXX-ISMS-B-007「通信與作業管理程序書」5.8.7要求『系統負責人應於每日開始上班時依「系統檢查紀錄表」所列項目檢查各主機狀況。』惟經詢問得知，目前單位尚未填寫該表單。	因本中心已有XXX控制機制（軟體），可監測網路與系統使用狀況，故目前未依規範將相關資訊填入「系統檢查紀錄表」	向各系統負責人宣導「通信與作業管理程序書」之內容，要求落實填寫「系統檢查紀錄表」，並應每個月由權責主管進行查核。	100/09/30

附件：

1. 矯正與預防處理單。
   處理單的內容填寫來源 (1)異常事件紀錄表(2)單位內部發生的重大資安事件

五、風險評鑑適切性審查

- 風險值的計算
  - 評估事件發生機率及影響程度後，計算出風險值。
  - 風險值等於
    資產價值×威脅等級×弱點等級
- 威脅的等級對應表

評估標準	等級	評估值
威脅發生之可能性為低	低	1
威脅發生之可能性為中	中	2
威脅發生之可能性為高	高	3

- 弱點的等級對應表

評估標準	等級	評估值
該弱點不容易被威脅利用	低	1
該弱點容易被威脅利用	中	2
該弱點非常容易被威脅利用	高	3

- 本中心接受風險值
  - 可接受風險值原則
  - 高風險資產項目

附件：

1. 風險評鑑報告
2. 威脅弱點評估表（空白表格即可）
3. 風險評鑑彙整表（不可空白）
4. 風險改善計畫表（不可空白）
5. 適用性聲明書

六、前次管理審查會議決議執行狀況

- 前次管理審查會議或資訊安全會議決議事項執行狀況說明

七、影響資訊安全制度之任何變更事項

- <請參酌中心實際狀況填寫，例如資安組織調整、組織重大業務服務變動>

附件：

1.相關變更事項說明。
如：業務變動、人員調動、組織變動、資訊系統變動、重大設施變動、實體環境變動（如機房整建）、法令法規變動、其他不可抗力事件等。

八、資訊安全組織成員所提出之改善建議

資訊安全委員會
●<請參考中心之實際狀況來提供，如委員會並無改善建議，請將本欄刪除>
資訊安全官
●建議擴大資安管理委員會之參與人員，以廣納多方意見
資訊安全小組
●為提升緊急應變能力，建議增加異地備援機制 ●為提升設備維運品質，建議與維護廠商就服務水準簽訂合約
資訊安全稽核小組
●為增加稽核能量，建議增加稽核人員 ●為落實ISMS執行成效，建議邀請他校具ISMS稽核經驗之人員協同執行內部稽核

附件：

1. 先前資訊安全會議的會議決議或建議參考。
2. 如：資訊安全組織成員日常E-mail發布有關資訊安全的建議內容。
   （本項內容可與二、利害相關團體的回饋與建議的單位內人員意見合併）

九、資訊安全目標執行狀況報告(1/4)

量測期間：自文件發行(99年09月**日)至100年09月**日止。(文件發行日至管審會前)

項次	量測項目		目標水準	量測方式	量測結果	差異說明
A.5	資訊安全政策訂定與評估	(1)資訊安全政策審查次數	≧1次/年	管理審查會議紀錄	□符　合 □不符合	
		(2)資訊安全政策宣導次數	≧1次/年	資安會議、教育訓練	□符　合 □不符合	
A.6	資訊安全組織	(1)有否確實簽署保密協議	不符≦2件	稽核結果	□符　合 □不符合	
		(2)管理審查會議召開次數	≧1次/年	管理審查會議紀錄	□符　合 □不符合	
A.7	資訊資產分類與管制	(1)資訊資產清單是否定期更新	≧1次/年	資訊資產清單	□符　合 □不符合	
		(2)資訊資產清單符合分級與標示規定	不符≦2件	稽核結果	□符　合 □不符合	
		(3)是否定期執行風險評鑑	≧1次/年	資訊資產清單、威脅及弱點評估表	□符　合 □不符合	
A.8	人員安全管理與教育訓練	(1)檢查資通安全受訓時數	一般主管≧3小時 資訊人員≧6小時 資安人員≧16小時 一般使用者≧3小時	教育訓練紀錄	□符　合 □不符合	相關研習配合ISMS導入陸續辦理。
		(2)離退人員帳號確實刪除	不符≦2件	清查紀錄、稽核結果	□符　合 □不符合	

九、資訊安全目標執行狀況報告(2/4)

項次	量測項目		目標水準	量測方式	量測結果	差異說明
A.9	實體與環境安全	(1)檢查有否遵守機房門禁規定	不符≦2件	稽核結果	□符　合 □不符合	
		(2)檢查消防器材與UPS有否定期保養	不符≦1件	保養紀錄、稽核結果	□符　合 □不符合	
A.10	通訊與作業安全管理	(1)定期監控重要伺服器執行作業之系統容量（例如CPU、RAM、硬碟）	不符≦2件	檢查紀錄表稽核結果	□符　合 □不符合	
		(2)定期監控網路資源使用率（例如連外頻寬）	不符≦2件	檢查紀錄表稽核結果	□符　合 □不符合	
		(3)病毒爆發次數（年）	≦3次/年	事件紀錄	□符　合 □不符合	
		(4)連外網路斷線次數（年）	≦3次/年	事件紀錄	□符　合 □不符合	
		(5)檢查病毒碼是否即時更新	不符≦2件	稽核結果	□符　合 □不符合	
		(6)檢查重要系統時間是否同步	不符≦2件	稽核結果	□符　合 □不符合	
		(7)檢查防火牆設定是否與防火牆進出規則申請表資料相符	不符≦2件	稽核結果	□符　合 □不符合	
		(8)弱點掃瞄次數	≧2次/年	掃瞄報告	□符　合 □不符合	

九、資訊安全目標執行狀況報告(3/4)

項次	量測項目		目標水準	量測方式	量測結果	差異說明
A.11	存取控制安全	(1)定期審查重要系統存取權限（帳號清查）	≧2次/年	清查紀錄	□符　合 □不符合	
		(2)管理者、使用者密碼長度及複雜度應符合規範	不符≦0件	稽核結果	□符　合 □不符合	
		(3)帳號申請是否依規定填寫表單	不符≦1件	稽核結果	□符　合 □不符合	
		(4)系統稽核日誌是否已開啟	不符≦1件	稽核結果	□符　合 □不符合	
A.12	系統開發與維護之安全	(1)重要系統更新/上線前經測試	不符≦0件	稽核結果	□符　合 □不符合	
		(2)重要系統開發或變更時應更新系統文件	不符≦2件	稽核結果	□符　合 □不符合	
		(3)重要系統上線具有緊急復原機制	不符≦0件	稽核結果	□符　合 □不符合	
A.13	資訊安全事件之反應及處理	(1)發生資安事件未依規定通報之件數	不符≦1件	稽核結果	□符　合 □不符合	
		(2)檢查資通安全事件通報單，是否重複發生相同資安事件件數	重複≦1件	事件通報單	□符　合 □不符合	

九、資訊安全目標執行狀況報告(4/4)

項次	量測項目		目標水準	量測方式	量測結果	差異說明
A.14	業務永續運作管理	(1)檢討業務永續運作計畫演練執行情形	≧1次/年	演練紀錄	□符　合 □不符合	
		(2)執行風險評鑑與營運衝擊分析(BIA)	≧1次/年	BIA紀錄	□符　合 □不符合	
		(3)定期備份重要系統資料	不符≦2件	稽核結果	□符　合 □不符合	
A.15	相關法規與施行單位政策之符合性	(1)合法軟體之安裝	不符≦0件	清查紀錄、稽核結果	□符　合 □不符合	
		(2)是否定期執行資安稽核	≧1次/年	稽核報告	□符　合 □不符合	
		(3)矯正預防措施於規定時間內改善完成	逾期≦2件	稽核結果	□符　合 □不符合	

審查內容（五大輸出項目）

一、資訊安全制度執行之各項改進措施

二、更新風險評鑑與風險改善計畫

三、針對可能影響資訊安全制度之內外部事件，修正資訊安全管理流程與控制措施

四、資訊安全制度所需資源協調

五、控制措施有效性評量方式的改善

一、資訊安全制度執行之各項改進措施

<請參酌中心實際狀況填寫，例如可將「改善建議」或「利害相關團體之回饋」在此一項目中做成決議並列出更具體之相關行動方案>

- 建立本中心年度教育訓練計畫
- 與XX大學互為異地備份，並簽訂 MOU
- 邀請本校資安課程任課老師加入稽核團隊
- 內稽邀請其他學校協同執行稽核
- 與XX廠商簽訂SLA
- 邀請校內相關專家出席參加管理審查會議，並請他們針對組織資安管理制度提供意見

二、更新風險評鑑與風險改善計畫(1/2)

項次	資產編號	資產類別	資產名稱	資產說明	權責單位	資產價值	風險事件		風險值	風險再評估			
							威脅	弱點		資產價值	威脅等級	弱點等級	風險值
1		CM	Core Router & Switch			4	重要人員離職	操作文件不足	24	4	2	2	16
2		CM	網路安全設備			3	重要人員離職	操作文件不足	18	3	2	2	12
3		PE	管理階層人員			3	重要人員離職	人員缺乏（代理人制度缺乏）	18	3	2	2	12
4		PE	網路維護人員			4	重要人員離職	人員缺乏（代理人制度缺乏）	16	4	2	1	8
5		PE	系統維護人員			4	重要人員離職	人員缺乏（代理人制度缺乏）	16	4	2	1	8
6		SW	作業系統（個人電腦用）			4	惡意軟體攻擊	軟體漏洞	16	4	3	1	12
7		SW	套裝軟體（授權軟體）			4	惡意軟體攻擊	軟體漏洞	16	4	3	1	12

1. 請再重新檢視風險評鑑內容（風險再評鑑）

二、更新風險評鑑與風險改善計畫(2/2)

教育體系資通安全管理規範（控制目標）	教育體系資通安全管理規範（控制措施）	現況說明	風險改善建議措施	建議權責單位	預計改善時間與處理方式	與高風險資產之風險評估彙整表對照
A.14.1.1 業務永續運作之規劃程序 A14.1.2 永續運作計畫之測試及更新	A14.1.1施行單位應建立業務永續運作之程序及架構，鑑定測試以及維護之優先順序，訂定與維護永續運作之計畫 A14.1.2永續運作計畫應進行測試與維護，確保該計畫的有效性	Core Router & Switch6509、4506與網路安全設備，因重要操作文件不夠完整，造成重要人員離職無法即時運作與處理	1. 建立Core Router& Switch6509、4506與網路安全設備操作文件 2. 將系統操作手冊電子檔放在系統中供使用者隨時查閱，並於系統明顯處標示服務專線提供使用者以電話方式詢問	網路組	預計改善時間：100/09/15 處理方式：同風險改善建議	1、2

三、可能影響資訊安全制度之內外部事件

變更項目	變更內容	因應作為
營運需求變更	與XX合併，組織變更	相關ISMS組織、文件修訂，營運需求項目整併
安全需求變更	已併於「資訊安全制度執行之各項改進措施」之議題進行討論與決議	
業務程序變更	與XX大學合併，業務服務項目及流程變更	逐步將資訊系統合併
管理或法規需求變更	目前無相關議題	
契約要求變更	ISP服務廠商變更	因應服務廠商轉換擬訂可能發生之突發事件的應變計畫。確保備援線路或替代線路可及時切換應變
可接受風險等級或標準變更	目前無相關議題	

四、資訊安全制度所需資源協調

<建議可將推動ISMS所需之人員、設備與預算列在此項目進行討論，如果目前資源已相當充裕，也可運用本項目來檢視確認， 如果資源不夠也可運用本項目之討論來讓管理階層了解現況並尋求支援>

建議在第三方驗證之前，各中心資安官必須對單位內有關資訊安全預算的分配或運用比例，有一定程度的瞭解，以期能夠充分運用單位的資安資源。
（外部稽核時可能被問及之問題）

五、控制措施有效性評量方式的改善(1/2)

項次	量測項目（修訂前）	目標水準（修訂前）	測量項目（修訂後）	量測水準（修訂後）	修訂理由
	請填入欲修訂項目				

五、控制措施有效性評量方式的改善(2/2)

項次	量測項目（修訂前）	目標水準（修訂前）	測量項目（修訂後）	量測水準（修訂後）	修訂理由
A.6	有否確實簽署保密協議	不符≦2件	有否確實簽署保密條約	不符≦1件	
A.6	目前並無此項量測項目	無	即時公告資訊安全相關訊息	不符合<2次/年	
A.10	目前並無此項量測項目	無	及時通知遭病毒/垃圾郵件攻擊之連線學校	不符合<3次/年	
A.10	弱點掃描次數	≧2次/年	弱點掃描次數	≧4次/年	
A.14	檢討營運持續計畫演練執行情形	≧1次/年	檢討營運持續計畫演練執行情形	≧2次/年	

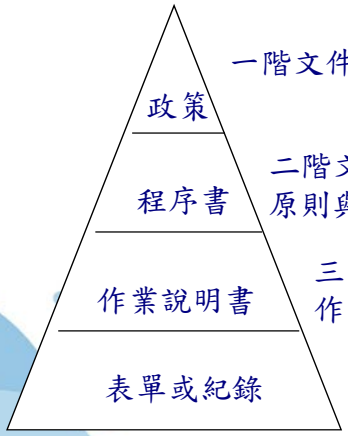
ISMS程序書架構與重點

ISMS程序書架構與重點

- 文件架構
- 資安政策
- 程序書

文件架構

文件架構
資安政策
程序書



一階文件：資訊安全最高指導原則

二階文件：各項作業之管理原則與程序

三階文件：各項作業之標準作業程序(SOP)

四階文件：資訊安全管理系統執行紀錄

ISMS 文件一覽表

文件架構
資安政策
程序書

1. 資訊安全政策
2. 資訊安全組織管理程序書
3. 文件管理程序書
4. 資訊資產管理程序書
5. 風險評鑑與管理程序書
6. 人員安全管理程序書
7. 實體安全管理程序書
8. 通信與作業管理程序書
9. 存取控制程序書
10. 系統開發與維護程序書
11. 委外管理程序書
12. 矯正預防措施管理程序書
13. 資訊安全稽核作業程序書
14. 安全事件管理程序書
15. 業務永續運作管理程序書

1. 資訊安全政策 (1/3)

文件架構
資安政策
程序書

資訊安全政策					
文件編號	NC-00-A-001	機密等級		版本	0.1

目錄

1. 資訊安全政策 (2/3)

- **目的**
  - 確保XXX教育網路中心（以下簡稱本中心）所屬之資訊資產機密性、完整性及可用性，並符合相關法規之要求，使其免於遭受內、外部的蓄意或意外之威脅。
- **適用範圍**
  - 資訊安全管理涵蓋11項管理事項，避免因人為疏失、蓄意或天然災害等因素，導致資料不當使用、洩漏、竄改、破壞等情事發生，對本中心帶來各種可能之風險及危害。
- **政策**
  - 「維護本中心資訊機密性、完整性與可用性，保障使用者資料隱私」
  - 保護本中心學術網路資訊，避免未經授權的存取與修改。
  - 本中心業務執行須符合相關法令或法規之要求。
  - 建立資訊業務永續運作計畫，確保本中心業務永續運作。

1. 資訊安全政策 (3/3)

- **責任**
  - 本中心的管理階層建立及審查此政策。
  - 資訊安全管理者透過適當的標準和程序以實施此政策。
  - 所有人員和合約供應商均須依照程序以維護資訊安全政策。
  - 所有人員有責任報告資訊安全事件，和任何已鑑別出的弱點。
  - 任何蓄意去危及資訊安全的行為將受到相關懲罰或法律行動。
- **審查**
  - 本政策應至少每年評估一次，以反映政府法令、技術及業務等最新發展現況，以確保它對於維持永續運作和提供學術網路相關服務的能力。
- **實施**
  - 資訊安全政策配合管理審查會議進行資訊安全政策審核。
  - 本政策經「資訊安全委員會」核定後實施，修訂時亦同

程序書架構

文件架構
資安政策
程序書

1. 目的
2. 適用範圍
3. 權責
4. 名詞定義
5. 作業說明
6. 相關文件

2. 資訊安全組織管理程序書

1. 目的

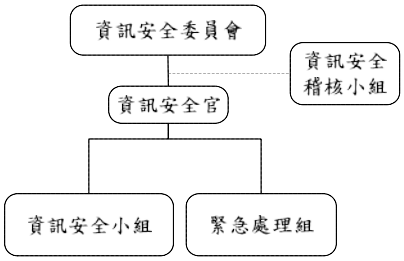
1.1促進教育網路中心資訊安全管理制度執行之有效性，期使本制度達成既定之目標，以增進業務運作之安全。

5. 作業說明

5.1資訊安全組織架構與工作執掌

5.1.1 資訊安全組織架構如下圖所示。

參照程序書範本



3. 文件管理程序書

1. 目的：建立教育網路中心資訊安全管理制度（以下簡稱ISMS）文件管理規範，期使ISMS文件能獲得適切控管，以確保文件之機密性、完整性及可用性。

5.1.1.1 須指派專人擔任「文管人員」，負責ISMS相關文件之發行與管制。

5.1.1.2 ISMS文件須列表控管，非教育網路中心同仁借閱「限閱」等級以上之文件時需填寫「文件調閱申請單」申請使用。

5.1.2.1.1須建立資訊安全管理系統執行之紀錄，以提供資訊安全管理系統有效運作之證據。

5.2.3 各文件之制定程序如下表所示：

作業 / 類別	擬案	會簽	核准	管制
政策	資訊安全小組	N/A	資訊安全委員會	文管人員
程序書	資訊安全小組	N/A	教育網路中心權責主管	
作業說明書	業務承辦人	相關單位	單位主管	
表單或紀錄	業務承辦人	相關單位	單位主管	
外來文件	N/A	N/A	N/A	承辦單位

詳見程序書範本

5.4.1 文件核准後應於一週內，透過內部網站或其它方式向同仁公告，並將該文件列入控管。

5.4.2 文件公告時，應依據「資訊資產管理程序書」之規定設定相關存取權限。

5.5.1 文件由文管人員予以保管、維護、建檔，並建立「文件一覽表」列管。

4. 資訊資產管理程序書

1. **目的**：建立教育網路中心 ISMS 資產管理規範，訂定資訊資產分類、分級、價值評估、標示及處理之遵循原則，並據以辦理各項資訊資產管理及作業方法。用以保護各類資訊資產，避免因人為疏失、蓄意或自然災害等風險所造成之傷害。

4.1.1 資訊資產權責單位：
對該項資訊資產具有判斷資產價值、決定存取權限或新增、刪除、修改權限之單位。

4.1.2 資訊資產保管單位：
依據權責單位之需求標準，執行資訊資產日常保護、異動與維護之執行單位。

4.1.3 資訊資產使用單位：
因業務需求，會直接或間接使用到該資訊資產之單位。

5.2.1 資訊資產依其性質不同，分為7類：人員、文件、軟體、通訊、硬體、資料、環境。

5.2.1.1人員(People；PE)：包含全體同仁以及往來廠商。

5.2.1.2文件(Document；DC)：以紙本形式存在之文書資料、報表等相關資訊，包含公文、列印之報表、表單、計畫、文件等紙本資料。

5.2.1.3軟體(Software；SW)：作業系統、應用系統、套裝軟體等，包含原始程式碼、應用程式執行碼、資料庫等。

5.2.1.4通訊(Communication；CM)：提供資訊傳輸、交換之網路設備或服務。

5.2.1.5硬體(Hardware；HW)：主機設備等相關硬體設施。

5.2.1.6資料(Data；DA)：儲存於硬碟、磁帶、光碟等儲存媒介之數位資訊。

5.2.1.7環境(Environment；EV)：基本設施及服務，包含辦公室實體、實體機房、電力、消防設施等。

詳見程序書範本

簡報完畢，敬請指教。