國際標準-27001號

ISO-27001

CNS-27001：中華民國國家標準27001號

資訊技術-安全技術-資訊安全管理系統-要求事項

章節

- 0.1 概述
  - 本標準之制定係為提供用以建立、實作、運作、監視、審查、維持及改進資訊安全管理系統之模型。
- 0.2 過程導向
  - 本標準採用PDCA過程模型。
- 0.3 與其他管理系統之相容性
  - 本標準與ISO-9001:2008(品質管理系統)及ISO-14001(環境管理系統)相調和。
- 1. 適用範圍
  - 1.1. 概述
  - 1.2. 應用
- 2. 引用標準
  - BS-7799

章節

- 3. 用語釋義
  - 資產 (asset)
    - 對組織有價值的任何事物。
  - 機密性 (confidentiality)
    - 使資訊不可用或不揭露給未經授權之個人、個體或過程的性質。
  - 完整性 (integrity)
    - 保護資產的準確度(accuracy)和完全性(completeness)的性質。
  - 可用性 (availability)
    - 經授權個體因應需求之可存取及可使用的性質。
  - 資訊安全 (information security)
    - 保存資訊的機密性、完整性及可用性；此外，亦能涉及如鑑別性、可歸責性、不可否認性及可靠度等性質。
  - 資訊安全管理系統 (Information Security Management System, ISMS)
    - 整體管理系統的一部份，以營運風險導向(作法)為基礎，用以建立、實作、運作、監視、審查、維持及改進資訊安全。

章節

- 3. 用語釋義
  - 資訊安全事件 (information security event)
    - 系統、服務或網路發生一個已識別的狀態，其指示可能的資訊安全政策違例或保護措施失效，或是可能與安全相關而先前未知的狀況等。
  - 資訊安全事故 (information security incident)
    - 單一或一連串有顯著機率可能危害營運作業與威脅資訊安全之非所欲或非預期的資訊安全事件。
  - 適用性聲明 (statement of applicability)
    - 描述與組織之ISMS相關且對其適用之各項控制目標與控制措施的已文件化聲明。
    - 備考：控制目標與控制措施係以風險評鑑與風險處理之各項過程的結果與結論、法律或法規要求、契約義務，以及組織對資訊安全的營運要求為基礎。

章節

- 3. 用語釋義
  - 風險分析 (risk analysis)
    - 系統性的使用資訊，以識別緣由與估計風險。
  - 風險評估 (risk evaluation)
    - 把預估的風險和已知的風險準則進行比較的過程，以決定風險的顯著性。
  - 風險評鑑 (risk assessment)
    - 風險分析與風險評估的整個過程。
  - 風險接受 (risk acceptance)
    - 決定接受某風險
  - 風險處理 (risk treatment)
    - 選擇與實作措施的過程藉以修正風險。
  - 剩餘風險 (residual risk)
    - 風險處理後所剩餘的風險
  - 風險管理 (risk management)
    - 藉由協調各項活動以指導與控管組織之有關風險。

章節

- 4. 資訊安全管理系統
  - 4.1. 一般要求
  - 4.2. 建立與管理ISMS
    - 4.2.1. 建立ISMS
    - 4.2.2. 實作與運作ISMS
    - 4.2.3. 監視與審查ISMS
    - 4.2.4. 維持與改進ISMS
  - 4.3. 文件化要求
    - 4.3.1. 概述
    - 4.3.2. 文件管制
    - 4.3.3. 紀錄管制

章節

- 5. 管理階層責任
  - 5.1. 管理階層承諾
  - 5.2. 資源管理
    - 5.2.1. 資源提供
    - 5.2.2. 訓練、認知及能力
- 6. ISMS內部稽核
- 7. ISMS之管理階層審查
  - 7.1. 概述
  - 7.2. 審查輸入
  - 7.3. 審查輸出
- 8. ISMS之改進
  - 8.1. 持續改進
  - 8.2. 矯正措施
  - 8.3. 預防措施

附錄A：控制目標與控制措施

- 本附錄所列之各項控制目標與控制措施，乃直接取自BS-7799第5至15節，並能與之校準。此等表格內所列項目並未盡列，個組織可考量必要的各項額外控制目標與控制措施。應選擇此等表格中之控制目標與控制措施，作為本標準第4.2.1節所規定之ISMS過程的部分。
- A.5 安全政策
  - A.5.1 資訊安全政策
    - A.5.1.1 資訊安全政策文件
    - A.5.1.2 資訊安全政策之審查
- A.6 資訊安全的組織
  - A.6.1 內部組織
    - A.6.1.1 管理階層對資訊安全的承諾
    - A.6.1.2 資訊安全協調工作
    - A.6.1.3 資訊安全責任的配置
    - A.6.1.4 資訊處理設施的授權過程
    - A.6.1.5 機密性協議
    - A.6.1.6 與權責機關的聯繫
    - A.6.1.7 與特殊利害相關團體的聯繫
    - A.6.1.8 資訊安全的獨立審查
  - A.6.2 外部團體
    - A.6.2.1 與外部團體相關的風險之識別
    - A.6.2.2 處理客戶事務的安全說明
    - A.6.2.3 第三方協議中之安全說明

附錄A：控制目標與控制措施

- A.7 資產管理
  - A.7.1 資產責任
    - A.7.1.1 資產清冊
    - A.7.1.2 資產的擁有權
    - A.7.1.3 資產之可被接受的使用
  - A.7.2 資訊分類
    - A.7.2.1 分類指導綱要
    - A.7.2.2 資訊標示與處置

附錄A：控制目標與控制措施

- A.8 人力資源安全
  - A.8.1 聘僱之前
    - A.8.1.1 角色與責任
    - A.8.1.2 篩選
    - A.8.1.3 聘僱條款與條件
  - A.8.2 聘僱期間
    - A.8.2.1 管理階層責任
    - A.8.2.2 資訊安全認知、教育及訓練
    - A.8.2.3 懲處過程
  - A.8.3 聘僱的終止或變更
    - A.8.3.1 終止責任
    - A.8.3.2 資產的歸還
    - A.8.3.3 存取權限的移除

附錄A：控制目標與控制措施

- A.9 實體與環境安全
  - A.9.1 安全區域
    - A.9.1.1 實體安全周界
    - A.9.1.2 實體進入控制措施
    - A.9.1.3 保全辦公室、房間及設施
    - A.9.1.4 對外部與環境威脅的保護
    - A.9.1.5 在安全區域內工作
    - A.9.1.6 公共進出、收發及裝卸區
  - A.9.2 設備安全
    - A.9.2.1 設備安置與保護
    - A.9.2.2 支援的公用設施
    - A.9.2.3 佈纜的安全
    - A.9.2.4 設備維護
    - A.9.2.5 場所外設備的安全
    - A.9.2.6 設備的安全汰除或再使用
    - A.9.2.7 財產的攜出

附錄A：控制目標與控制措施

- A.10 通訊與作業管理
  - A.10.1 作業之程序與責任
    - A.10.1.1 文件化作業程序
    - A.10.1.2 變更管理
    - A.10.1.3 職務的區隔
    - A.10.1.4 開發、測試及運作設施的分隔
  - A.10.2 第三方服務交付管理
    - A.10.2.1 服務交付
    - A.10.2.2 第三方服務的監視與審查
    - A.10.2.3 第三方服務變更的管理
  - A.10.3 系統規劃與驗收
    - A.10.3.1 容量管理
    - A.10.3.2 系統驗收
  - A.10.4 防範惡意碼與行動碼
    - A.10.4.1 對抗惡意碼的控制措施
    - A.10.4.2 對抗行動碼的控制措施
  - A.10.5 備份
    - A.10.5.1 資訊備份
  - A.10.6 網路安全管理
    - A.10.6.1 網路控制措施
    - A.10.6.2 網路服務的安全

附錄A：控制目標與控制措施

- A.10 通訊與作業管理
  - A.10.7 媒體的處置
    - A.10.7.1 可移除式媒體的管理
    - A.10.7.2 媒體的汰除
    - A.10.7.3 資訊處置程序
    - A.10.7.4 系統文件的安全
  - A.10.8 資訊交換
    - A.10.8.1 資訊交換政策與程序
    - A.10.8.2 交換協議
    - A.10.8.3 輸送中的實體媒體
    - A.10.8.4 電子傳訊
    - A.10.8.5 營運資訊系統
  - A.10.9 電子商務服務
    - A.10.9.1 電子商務
    - A.10.9.2 線上交易
    - A.10.9.3 公眾可用的資訊

附錄A：控制目標與控制措施

- A.10 通訊與作業管理
  - A.10.10 監視
    - A.10.10.1 稽核存錄
    - A.10.10.2 監控系統的使用
    - A.10.10.3 日誌資訊的保護
    - A.10.10.4 管理者與操作者日誌
    - A.10.10.5 失誤存錄
    - A.10.10.6 鐘訊同步

附錄A：控制目標與控制措施

- A.11 存取控制
  - A.11.1 存取控制的營運要求
    - A.11.1.1 存取控制政策
  - A.11.2 使用者存取管理
    - A.11.2.1 使用者註冊
    - A.11.2.2 特權管理
    - A.11.2.3 使用者通行碼管理
    - A.11.2.4 使用者存取權限的審查
  - A.11.3 使用者責任
    - A.11.3.1 通行碼的使用
    - A.11.3.2 無人看管的使用者設備
    - A.11.3.3 桌面淨空與螢幕淨空政策

附錄A：控制目標與控制措施

- A.11 存取控制
  - A.11.4 網路存取控制
    - A.11.4.1 網路服務的使用政策
    - A.11.4.2 外部連線的使用者鑑別
    - A.11.4.3 網路設備識別
    - A.11.4.4 遠端診斷與組態埠保護
    - A.11.4.5 網路區隔
    - A.11.4.6 網路連線控制
    - A.11.4.7 網路選路控制
  - A.11.5 作業系統存取控制
    - A.11.5.1 保全登入程序
    - A.11.5.2 使用者識別與鑑別
    - A.11.5.3 通行碼管理系統
    - A.11.5.4 系統公用程式的使用
    - A.11.5.5 會談期逾時
    - A.11.5.6 連線時間的限制

附錄A：控制目標與控制措施

- A.11 存取控制
  - A.11.6 應用系統與資訊存取控制
    - A.11.6.1 資訊存取控制
    - A.11.6.2 敏感性系統的隔離
  - A.11.7 行動計算與遠距工作
    - A.11.7.1 行動計算與通信
    - A.11.7.2 遠距工作

附錄A：控制目標與控制措施

- A.12 資訊系統獲取、開發及維護
  - A.12.1 資訊系統的安全要求
    - A.12.1.1 安全要求分析與規格
  - A.12.2 應用系統的正確處理
    - A.12.2.1 輸入資料確認
    - A.12.2.2 內部處理的控制措施
    - A.12.2.3 訊息完整性
    - A.12.2.4 輸出資料確認
  - A.12.3 密碼控制措施
    - A.12.3.1 使用密碼控制措施的政策
    - A.12.3.2 金鑰管理
  - A.12.4 系統檔案的安全
    - A.12.4.1 作業軟體的控制
    - A.12.4.2 系統測試資料的保護
    - A.12.4.3 程式源碼的存取控制

附錄A：控制目標與控制措施

- A.12 資訊系統獲取、開發及維護
  - A.12.5 開發與支援過程的安全
    - A.12.5.1 變更控制程序
    - A.12.5.2 作業系統變更後的應用系統技術審查
    - A.12.5.3 套裝軟體變更的限制
    - A.12.5.4 資料洩漏
    - A.12.5.5 委外的軟體開發
  - A.12.6 技術脆弱性管理
    - A.12.6.1 技術脆弱性控制

附錄A：控制目標與控制措施

- A.13 資訊安全事故管理
  - A.13.1 通報資訊安全事件與弱點
    - A.13.1.1 通報資訊安全事件
    - A.13.1.2 通報安全弱點
  - A.13.2 資訊安全事故與改進的管理
    - A.13.2.1 責任與程序
    - A.13.2.2 從資訊安全事故中學習
    - A.13.2.3 證據的收集

附錄A：控制目標與控制措施

- A.14 營運持續管理
  - A.14.1 營運持續管理的資訊安全層面
    - A.14.1.1 資訊安全納入營運持續管理過程
    - A.14.1.2 營運持續與風險評鑑
    - A.14.1.3 發展與實作包括資訊安全的持續計畫
    - A.14.1.4 營運持續計畫框架
    - A.14.1.5 營運持續計畫的測試、維護及重新評鑑

附錄A：控制目標與控制措施

- A.15 遵循性
  - A.15.1 遵循適法性要求
    - A.15.1.1 識別適用之法條
    - A.15.1.2 智慧財產權
    - A.15.1.3 組織紀錄的保護
    - A.15.1.4 個人資訊的資料保護與隱私
    - A.15.1.5 防止資訊處理設施的誤用
    - A.15.1.6 密碼控制措施的規定
  - A.15.2 安全政策與標準的遵循性以及技術遵循性
    - A.15.2.1 安全政策與標準的遵循性
    - A.15.2.2 技術遵循性查核
  - A.15.3 資訊系統稽核考量
    - A.15.3.1 資訊系統稽核控制
    - A.15.3.2 資訊系統稽核工具的保護