國立成功大學
人工智能數位轉型研究中心

資訊安全管理手冊

文件編號： AI4DT-ISMS-L1-01

機密等級： 一般

版　　本： V1.0

發行日期： 109 年 08 月 10 日

修訂紀錄

版次	修訂 日期	修訂 頁次	修訂者	修訂內容摘要
V1.0	109.06.23	全部	AI4DT	依據 ISO/IEC 27001:2013 之要求，建立本手冊。

目錄

1. 目的

本文件之製定，在於律定國立成功大學人工智能數位轉型研究中心(以下簡稱「本中心」或「中心」)資訊安全管理制度導入之範圍、管理政策、流程、規範、辦法、要求及角色與權責，做為本中心資訊安全管理制度活動之作業準則，以確保資訊安全管理制度之實施，能符合中心之需要與相關國際標準之要求。

2. 範圍

2.1 管理制度

本文件係根據本中心管理之需要，並參考 ISO/IEC 27001:2013 國際標準要求之規定製定，以滿足 ISO/IEC 27001:2013 國際標準認證之要求。

2.2 組織範圍

本文件適用於本中心各單位。

3. 名詞定義

本手冊中所使用名詞，請參考「AI4DT-ISMS-L3-01 名詞解釋」之說明。

4. 政策與目標

4.1 資訊安全政策要求

本中心主任應指派資訊安全長(以下簡稱 資安長)成立資訊安全委員會，負責擬定中心之資訊安全政策。中心之資訊安全政策於中心主任審查核可後，發佈實施。中心之資訊安全政策，包含資訊安全管理政策和資訊安全防護措施政策二個部分，應每年定期進行審查與維護，說明如下：

4.1.1 資訊安全管理政策

4.1.1.1 資安長應確保建立資訊安全政策和目標，且與本中心之營運策略方向相容。

4.1.1.2 本中心之資訊安全管理政策為「提供安全與持續運作之資訊系統設計、開發、測試與維運環境，確保資訊系統及資訊之安全，達成中心資訊安全管理目標。」

4.1.2 資訊安全防護措施政策

4.1.2.1 移動裝置管理政策

所有介接到本中心網路與作業環境之移動裝置，應經中心網路管理員與權責主管審查核准，包括手機、筆記型電腦、平板電腦、或其他具有儲存和連線功能之移動式裝置，始可使用。

4.1.2.2 遠距工作管理政策

經由外部網路連接本中心網路與作業環境之遠距工作，應經中心網路管理員與權責主管審查核准，且作業之資訊設備應具備中心同意之保護機制。

4.1.2.3 存取管制政策

本中心資訊系統與資訊之存取管制，包含實體與邏輯二部分。介接中心之資訊資產設備，不得設於中心外部無人看管或未具有保護機制之位置。具有存取中心資訊系統或網路設施之資訊設備，必須要具有唯一識別機制，且使用者僅能存取和其工作相關之資訊系統與資訊，對於使用者之存取應能記錄存取軌跡。擁有特別存取權限之使用者，應限制存取權限之配置與使用。

4.1.2.4 加密管理政策

機密等級為「機密」之資訊，於進行傳輸或儲存時，皆應加密保護。

4.1.2.5 金鑰管理政策

本中心使用之金鑰，每年應定期審查金鑰的有效性，金鑰生命週期之管理，應由專人管理。

4.1.2.6 螢幕保護與桌面淨空政策

4.1.2.6.1 本中心同仁及合約約聘人員使用之資訊設備，包括伺服器、個人電腦、筆

記型電腦和具有操作畫面之移動裝置，應設定電腦螢幕保護時間，電腦在無人操作情況下，最長不得超過 5 分鐘，系統畫面應自動進入密碼保護狀態。

4.1.2.6.2 本中心同仁及合約約聘人員桌面，不應存放機密等級為「機密」之資訊。人員離開座位時，應將桌面整理淨空，機密等級為「機密」之資訊，應採取保護措施。

4.1.2.7 備份政策

本中心之資訊系統與資訊，應依其可用性要求，擬定備份計畫，並依據計畫進行備份作業、保存及還原測試。

4.1.2.8 資訊移轉管理政策

在本中心內部移轉之資訊，若機密等級為「機密」應設定保護機制。中心與外部團體間之資訊移轉，應事前申請並經資訊保有之權責單位主管核准後，方能移轉。中心與外部團體間如為移轉機密等級為「機密」之資訊，移轉過程應有安全之保護機制。

4.1.2.9 安全開發政策

本中心應參考行政院軟體發展流程指引建立資訊系統安全設計、開發、測試、發行與維護之作業準則，並依據作業準則，進行資訊系統之安全設計、開發、測試、發行與維護作業。

4.1.2.10 委外廠商資訊安全管理政策

本中心應與委外廠商建立專案之資訊安全管理需求，並在委外本廠商履行合約義務過程中，實施必要之管理與稽核活動，確保委外本廠商提供之服務與產品，符合專案之資訊安全管理需求。

4.2 資訊安全管理目標

4.2.1 本中心之資訊安全管理目標為「在合於法令、法規與合約要求條件下，確保資訊資產的機密性、完整性與可用性，提供持續可用之資訊服務。」

4.2.2 為達成本中心資訊安全管理目標，中心參考 ISO/IEC 27001 國際標準要求，建立資訊安全管理制度，對資訊安全管理制度實施範圍內之資訊資產採取適當保護措施，以維持資

訊資產之機密性、完整性與可用性，提供客戶安全之資訊服務並滿足其需求。

4.2.3 為確保本中心資訊安全管理制度之實施，能夠達成中心營運之需要，各項作業流程應根據中心之資訊安全管理目標，訂定作業流程目標。

4.2.4 資訊安全管理目標之評估與檢視

資訊安全工作小組應每年檢視與評估本中心之資訊安全管理目標，提出修訂建議，提請資訊安全委員會審查核准。

5. 資訊安全管理制度制訂與實施

資訊安全工作小組應每年進行組織全景分析作業，分析結果應記錄「AI4DT-ISMS-L4-02 組織全景分析表」中。並依據全景分析結果與本中心資訊安全管理政策與目標之要求，制訂與維護資訊安全管理制度、推動與管理資訊安全管理制度之實施、監控與評估資訊安全管理制度實施績效、持續改善資訊安全管理制度。

本中心資訊安全管理制度要求，係以滿足中心組織全景分析與資訊安全風險評鑑之結果所訂定，資訊安全工作小組應遵循相關政策及作業規定，督導中心同仁依規定實施各項作業流程要求。

6. 審查與修訂「適用性聲明書」

資訊安全工作小組應根據本中心營運與 ISO/IEC 27001 要求，每年審查與修訂資訊安全控制措施之「AI4DT-ISMS-L1-02 適用性聲明書」，並提請資訊安全委員會審查核准。