

國家科學及技術委員會中部科學園區管理局

人工智慧應用內控管理要點總說明

為確保國家科學及技術委員會中部科學園區管理局（以下簡稱本局）於運用人工智慧執行業務或提供服務時，能有效管理潛在風險並保障人民基本權利，落實人工智慧基本法第十九條規定，特訂定「國家科學及技術委員會中部科學園區管理局人工智慧應用內控管理要點」（以下簡稱本要點），其要點如下：

- 一、訂定目的及法源依據。(第一點)
- 二、適用範圍。(第二點)
- 三、權責分工與備查機制。(第三點)
- 四、應遵循之基本原則。(第四點)
- 五、資通安全與個人資料保護之法律遵循。(第五點)
- 六、風險評估檢核時機及各風險等級應辦理之內部控制措施。(第六點)
- 七、運行中異常情事之暫停、備援與通報應變機制。(第七點)
- 八、同仁教育訓練。(第八點)
- 九、定期檢視與滾動式調整機制。(第九點)

國家科學及技術委員會中部科學園區管理局

人工智慧應用內控管理要點

規 定	說 明
一、為確保國家科學及技術委員會中部科學園區管理局(以下簡稱本局)於運用人工智慧執行業務或提供服務時，能有效管理潛在風險並保障人民基本權利，落實人工智慧基本法第十九條規定，特訂定本要點。	本要點訂定之目的及法源依據。
二、本要點適用於本局自行或委外建置、開發之各類人工智慧系統與服務。	本要點之適用範圍。
三、本局使用人工智慧執行業務或提供服務時，應由業務權責單位負責風險管理及內部控制措施之執行，並副知本局資通與個資安全處理小組備查。	明定人工智慧應用之風險管理由業務權責單位負責執行，並建立副知本局資通與個資安全處理小組備查之機制。
四、本局自行開發、委外建置或採購各類人工智慧系統與服務，應遵循人工智慧基本法第四條所定七項原則。	明定各類人工智慧系統與服務應遵循之基本原則。
五、人工智慧系統與服務之資通安全防護，應依本局資通安全維護計畫與資通安全管理法及其相關法令辦理；涉及個人資料蒐集、處理或利用時，應依本局個人資料保護管理制度與個人資料保護法及其相關法令辦理。	規範資通安全防護與個人資料保護之法律遵循事項，參照本局資通與個資安全規範。
六、各業務權責單位於規劃自行開發、委外建置或採購之人工智慧系統與服務前，或既有人工智慧系統與服務發生重大功能變更時，應填具政府人工智慧應用風險評估檢核表(如附表)，識別潛在風險，依綜合判定結果辦理下列內部控制措施： (一)經綜合判定結果為甲類風險者，應辦理下列措施： 1. 人類監督保留：不得將具法律效果或影響民眾權益之行政處分，完全交由人工智慧自動裁定，應保留	明定風險評估檢核表之填具時機與運作機制，並依風險等級（甲、乙、丙類及無顯著風險）採分級管理，規定各類別應辦理之內部控制措施。

適當之人為介入與最終覆核機制。 2. 透明標示：系統與服務自動生成之圖文內容，或提供對外互動服務（如客服機器人）時，應於顯著處標示「本內容由人工智慧輔助/生成」等提示。 3. 明確警語：應明確標示注意事項或警語。 4. 建立救濟機制：針對受人工智慧輔助決策影響權益之民眾，應提供明確之申訴管道、決策解釋及權益救濟流程。 5. 強化防護：應於採購契約或系統與服務規格中，加重對供應商之資安、資料治理與防範歧視偏見之要求。 (二) 經綜合判定結果為乙類風險者，應辦理前款所列措施，並依本局資源配置情形，優先處理甲類風險部分。 (三) 經綜合判定結果為丙類風險者，應辦理第一款第一目及第二目措施。	
七、人工智慧系統與服務於運行中，若發生前點綜合判定結果為甲類風險、演算法嚴重偏差、生成重大違法內容、資料外洩或對民眾權益產生實質損害等異常情事，業務權責單位應立即暫停系統與服務部分或全部功能，並啟動人工備援作業或其他因應措施以進行異常排除，並於知悉異常情事起，依相關之行政程序通報至本局資安長，並同步通知本局資通與個資安全處理小組；如屬資安事件，業務權責單位應依本局資通安全通報機制於一小時內通報本局資通與個資安全處理小組。	明定運行中發生異常情事時之暫停、備援與通報應變機制，參照本局資通與個資安全規範。
八、本局同仁應定期參與人工智慧素	明定本局同仁應定期參與教育訓練，提

養、資訊倫理及風險管理之教育訓練，以提升對於人工智慧技術局限性與資安風險之認知。	升人工智慧素養與風險管理認知。
九、本要點將定期檢視，並視技術與法規修訂做滾動式調整。	本要點之定期檢視與滾動式調整機制。