

國家科學及技術委員會南部科學園區管理局

人工智慧應用內控管理要點

中華民國 115 年 10 月 1 日國家科學及技術委員會南部科學園區管理局
南企字第 1150036070 號函訂定

- 一、為確保國家科學及技術委員會南部科學園區管理局(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。
- 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。
- 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，並副知本局資訊服務、資訊安全暨個資安全委員會之推動處理小組備查。
- 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。
- 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進行事前評估與控管。
- 六、各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。
- 七、人工智慧系統與服務經依政府人工智慧應用風險評估檢核表(如附表)規定綜合判定結果為甲類者，應辦理下列內控措施：
 - (一) 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，應保留適當之人為介入與最終覆

核機制。

- (二) 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。
- (三) 明確警語：應明確標示注意事項或警語。
- (四) 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。
- (五) 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。

八、人工智慧系統與服務經依政府人工智慧應用風險評估檢核表(如附表)規定綜合判定結果為乙類者，應辦理前點所列各款內控措施，並依本局資源，優先處理甲類風險部分。

九、人工智慧系統與服務經依政府人工智慧應用風險評估檢核表(如附表)規定綜合判定結果為丙類者，應辦理第七點第一款及第二款內控措施。

十、人工智慧系統與服務於運行中，若發生第七點綜合判定結果為甲類、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，業務單位應立即暫停系統與服務部分或全部功能、啟動人工備援作業或其他因應措施，並於知悉異常情事起，依行政程序通報至資安長，並副知本局資訊服務、資訊安全暨個資安全委員會之推動處理小組備查；如屬資安事件，應依本局資通安全通報機制即時進行通報。

十一、本局應定期辦理並鼓勵同仁參與人工智慧素養、資訊倫理及風險管理之教育訓練，以提升人員對人工智慧技術局限性及資安風險之認知。

十二、本管理要點所定內控機制應由本局定期檢視；並適時做滾動式檢討。