南投縣政府人工智慧應用內控管理要點

中華民國115年06月23日府計訊字第1150123351號函頒

一、南投縣政府(以下簡稱本府）為確保本府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、本要點適用於本府及所屬機關（構）自行或委外建置、開發之各類人工智慧系統與服務。

三、本府使用人工智慧執行業務或提供服務時，其風險管理、內控監督與內控措施辦理時間，由本府資通安全管理審查委員會統籌辦理。

四、本府自行開發、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，應依本府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，應依本府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，應填具本府人工智慧應用風險評估檢核表(如附表，以下簡稱AI風險評估表)，識別潛在風險。

七、人工智慧系統與服務於進行AI風險評估表填列時，應依發生機率及嚴重程度進行綜合判定結果，並依風險應對機制類別(甲類、乙類及丙類)所規定之必辦內控措施項目進行後續調整，相關內控措施如下：

(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。

八、人工智慧系統與服務經依AI風險評估表規定綜合判定結果為甲類及乙類者，應辦理前點所列各款內控措施，並依機關資源，優先處理甲類風險部分。

九、人工智慧系統與服務AI風險評估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，業務單位應立即依據本府ISMS相關規範進行通報及應變。

十一、本府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府定期檢視；並適時做滾動式檢討。