

經濟部水利署及所屬機關人工智慧應用內控管理 要點

規定	說明
一、經濟部水利署(以下簡稱本署)為確保本署及所屬機關(以下合稱各機關)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。	本要點訂定目的。
二、本要點適用於各機關自行開發、委外建置或採購之各類人工智慧系統與服務。	定明本要點之適用對象及其範疇。
三、各機關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之推動及時程管理，由各機關之資通安全推動小組辦理之。	定明各機關人工智慧應用內控推動及時程管理之統籌組織。
四、各機關自行開發、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。	定明本署及所屬機關各類人工智慧系統與服務於開發或採購階段，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，應依資通安全管理法與其相關法令及各機關資通安全維護計畫辦理；涉及個人資料蒐集、處理或利用時，應依各機關個人資料保護管理制度進行事前評估與控管。	定明人工智慧系統與服務之資安防護與個資保護法律遵循義務。
六、各機關於規劃自行開發、委外建置或採購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，以下簡稱風險評估檢核表)，識別潛在風險。持續使用中之人工智慧系統與服務，應視其風險程度、應用範圍或實際運作情形，適時重新辦理風險評估。	定明人工智慧應用風險評估之啟動時機及辦理方式，以及既有系統與服務發生重大功能變更時，填具風險評估檢核表，以識別潛在風險，並針對持續使用之系統與服務應定期審視評估風險。
七、人工智慧系統與服務經依風險評估檢核表規定綜合判定結果為甲類者，應	定明經綜合風險評估判定為高風險之甲類人工智慧風險等級時，應執行之內部控

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，加強對供應商之資安、資料治理與防範歧視偏見之要求。	制措施。
八、人工智慧系統與服務經依風險評估檢核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，並依機關資源，優先處理甲類風險部分。	定明經綜合風險評估判定為乙類人工智慧風險等級時，應執行之內控措施，並考量機關資源配置，優先處理涉及甲類風險部分。
九、人工智慧系統與服務經依風險評估檢核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。	定明經綜合風險評估判定為丙類人工智慧風險等級時，至少應辦理人類監督保留及透明標示二項內控措施。
十、人工智慧系統與服務於運行中，若發生輸出結果明顯異常、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、公共安全產生實質損害等異常情事，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。 前項異常情事如屬資通安全事件，應另依經濟部水利署資通安全推	一、第一項明定人工智慧系統與服務於運行中發生輸出結果明顯異常等重大異常情事時，業務單位應立即採取相關必要措施。 二、第二項明定如異常情況符合經濟部水利署資通安全推動小組設置及作業要點第二點所定「資通安全事件」者，則應依該要點第七點附表二本署資通安全事件通報及處理流程規

動小組設置及作業要點第七點流程規定辦理。	定，進行通報。
十一、各機關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。	定明各機關應定期辦理教育訓練，提升同仁對人工智慧技術局限性及資訊安全之認知。
十二、本管理要點所定內控機制應由本署定期檢視；並適時做滾動式檢討。	定明機關對內控機制之定期檢視與滾動式檢討修正機制。