國家科學及技術委員會新竹科學園區管理局
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新竹科學園區管理局(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新竹科學園區管理局人工智慧應用內控管理要點」，其要點如下：

一、 訂定目的。(第一點)

二、 適用範圍為本局自行開發、委外建置或採購之各類人工智慧系統與服務。(第二點)

三、 業務權責單位之風險管理、內部控制措施執行。(第三點)

四、 人工智慧運用應遵循之基本原則。(第四點)

五、 資通安全政策、個人資料管理政策及相關法令之遵循。(第五點)

六、 風險評估檢核時機、風險分級及各風險等級應辦理之內部控制措施。(第六點)

七、 人工智慧系統與服務運行中重大異常情事之暫停、備援及通報機制。(第七點)

八、 同仁應定期參與人工智慧素養、資訊倫理及風險管理等相關教育訓練。(第八點)

九、 使用人工智慧系統與服務執行公務業務之注意事項及禁止事項。(第九點)

十、 配合人工智慧技術發展及法規修訂，適時滾動式調整。(第十點)

國家科學及技術委員會新竹科學園區管理局
人工智慧應用內控管理要點

規　　定	說　　明
一、國家科學及技術委員會新竹科學園區管理局(以下簡稱本局)為確保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。	本要點之訂定目的。
二、本要點適用於本局自行開發、委外建置或採購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，應由人工智慧系統與服務管理之業務權責單位(以下簡稱業務權責單位)依據本局資訊安全處理小組之規劃，負責風險管理及內部控制措施之執行。	定明業務權責單位應依據本局資訊安全處理小組之規劃，負責風險管理及內部控制措施之執行。
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。	定明本局自行開發、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，應依本局資通安全政策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，應依本局個人資料管理政策與個人資料保護法及其相關法令辦理。	定明人工智慧系統與服務之資通安全防護及涉及個人資料蒐集、處理或利用時，應遵循本局資通安全政策、個人資料管理政策及相關法令規定。
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，並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：	一、定明風險評估檢核表之填具時機，並依綜合判定結果區分甲類風險、乙類風險、丙類風險及無顯著風險，採風險分級管理方式辦理內部控制措施。 二、第一款、第二款規定甲類及乙類風險應辦理第一款各目措施；同時辦理多項人工智慧風險內控措施時，應依資源配置情形，優先處理甲類風險之內部控制措施。

規　　定	說　　明
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，加重對供應商之資通安全、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。 (四)經綜合判定結果屬無顯著風險者，無須辦理第一款所列措施；惟仍應依系統與服務之實際功能，遵循適用法令及本局相關管理規定，並於發生重大功能變更時重新進行風險評估。	三、第三款規定丙類風險應辦理人類監督保留及透明標示措施。 四、經綜合判定無顯著風險者，於第四款規定其適用情形；另於第五款規定，第一款各目措施因性質不適用者，其處理方式。

規　　定	說　　明
(五)第一款各目措施如因系統與服務之性質不適用者，得敘明理由後免予辦理。	
七、人工智慧系統與服務於運行中，若發生前點第一款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重大異常情事，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督導副局長，並同步通知本局資訊安全處理小組；如屬資通安全事件，業務權責單位應依本局事件通報與應變管理程序，於一小時內通報本局資訊安全處理小組。	定明人工智慧系統與服務運行中發生重大異常情事時，業務權責單位應暫停相關功能、啟動人工備援作業或其他因應措施，並進行相關通報機制。
八、本局同仁應定期參與人工智慧素養、資訊倫理及風險管理等相關教育訓練，以提升對於人工智慧技術侷限性與資通安全風險之認知。	定明本局同仁應定期參與人工智慧素養、資訊倫理及風險管理等相關教育訓練，以提升人工智慧素養與風險管理認知。
九、本局同仁使用人工智慧系統與服務執行公務業務，原則如下： (一) 使用人工智慧系統與服務之注意事項： 1. 本局同仁使用人工智慧系統與服務前應評估使用風險，包含可能產出涉及歧視、侵權、不實、偏見等之結果。 2. 本局同仁使用人工智慧系統與服務產出內容時，應確保資料之合宜性與正確性，並符合個人資料保護及著作權等相關規定，避免發生侵害相關權益之情形；當內	一、定明本局同仁使用人工智慧系統與服務執行公務業務時之注意事項及禁止事項，包括使用前風險評估、產出內容檢核、操作紀錄留存、禁止輸入機密(敏)、未公開、個人或未經合法授權之資料，以及不得使用大陸地區或其他經數位發展部依危害國家資通安全產品審查辦法認定為危害國家資通安全產品之人工智慧系統與服務，或依本局蒐集之外部情資知悉具有資通安全疑慮之人工智慧系統與服務。 二、有關第二款第一目所定機密(敏)、未經機關公開、涉及個人、未經合法授權之資料，係包括機密等級公

規　　定	說　　明
容涉及決策層面、民眾權益、法律層面者應經人工進行專業判斷、檢核；如使用產出內容致有違規事實，應負相關責任。 3. 本局同仁使用人工智慧系統與服務宜留存操作紀錄，包含提示詞語與產出內容，以利追溯。 （二） 使用非落地人工智慧系統與服務之禁止事項： 1. 不得輸入機密(敏)、未經機關公開、涉及個人、未經合法授權之資料。 2. 不得使用大陸地區或其他經數位發展部依危害國家資通安全產品審查辦法認定為危害國家資通安全產品之人工智慧系統與服務。 3. 不得使用依本局蒐集之外部情資知悉具有資通安全疑慮之人工智慧系統與服務。	文與相關附件、含個人資料檔案等；同款第二目所定大陸地區人工智慧系統與服務，例如 DeepSeek、文心一言、通義千問、ChatGLM、百川 AI 等，併予敘明。
十、本要點將視人工智慧技術發展及法規修訂，適時滾動式調整。	定明本要點應配合人工智慧技術發展及法規修訂，適時滾動式調整。