

新竹市政府及所屬機關人工智慧應用內控管理要點

總說明

- 一、為落實一百十五年一月十四日公布施行之「人工智慧基本法」第十九條第二項規定，政府應依使用人工智慧之業務性質，訂定使用規範或內控管理機制，並因應人工智慧應用可能涉及之資通安全、個人資料保護及人民權益等風險，建立適當之風險評估及管理機制，以兼顧行政創新、資訊安全與公共利益，爰訂定本要點。
- 二、中央機關及其他縣市處理情形：環境部、財政部、內政部消防署、宜蘭縣、南投縣均訂有相關規定。
- 三、本要點共計十二點，其訂定重點說明如下：
 - 第一點：明定訂定目的。
 - 第二點：明定適用對象及範圍。
 - 第三點：明定人工智慧應用內控統籌單位。
 - 第四點：明定使用人工智慧應遵循之原則。
 - 第五點：明定使用人工智慧之資安與個資防護應遵循義務。
 - 第六點：明定風險評估表之填具時機。
 - 第七點：明定人工智慧於導入前或重大變更時，應辦理風險評估檢核。
 - 第八點：明定使用人工智慧之較高風險等級之風險內控措施。
 - 第九點：明定使用人工智慧之較低風險等級之風險內控措施。
 - 第十點：明定使用人工智慧之異常應變與通報。
 - 第十一點：明定應定期推動教育訓練。
 - 第十二點：明定內控機制檢視與滾動式檢討修正機制。

新竹市政府及所屬機關人工智慧應用內控管理要點

規 定	說 明
一、新竹市政府（以下簡稱本府）為確保運用人工智慧執行業務或提供服務時，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。	明定本要點之訂定目的。
二、本要點適用於本府各處及所屬機關（以下簡稱各機關）自行或委外建置、開發之各類人工智慧系統與服務。	明定本要點之適用對象及範圍。
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辦理時程，由新竹市政府資訊安全處理小組或其他適當單位統籌辦理。	明定本府人工智慧應用內控統籌單位。
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。	明定自行開發、委外建置或採購各類人工智慧系統或服務應遵循之原則。
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及其相關法令與本府資通安全維護計畫辦理；涉及個人資料蒐集、處理或利用時，應依個人資料保護法及其相關法令與本府個人資料保護管理制度進行事前評估與控管。	明定人工智慧系統與服務之資安防護與個資保護應遵循義務。
六、各機關於規劃自行開發、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、委外廠商或使用目的變更時，應填具新竹市政府人工智慧應用風險評估檢核表（以下簡稱風險評估表），識別潛在風險。	明定人工智慧系統與服務於導入前或重大變更時，應辦理風險評估檢核。
七、人工智慧系統與服務應依風險評估表規定綜合判定結果，及風險應對機制類別（甲類、乙類及丙類）所	明定經風險評估結果後，相關內部控制措施項目。

規定之下列內控措施項目進行後續調整： (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，應辦理前點各款內控措施，並依機關資源，優先處理甲類風險部分。	明定經風險評估結果屬較高風險等級之人工智慧系統與服務，執行單位應辦理之內部控制措施。
九、人工智慧系統與服務經依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。 依風險評估表規定，就風險類型一至三及其嚴重程度綜合判定人工智慧系統與服務為無顯著風險者，得免辦理第七點所定內控措施。但應依風險評估表填列評估結果，並保留相關紀錄備查。	明定風險評估結果屬較低風險等級之人工智慧系統與服務，執行單位應辦理之內部控制措施。
十、人工智慧系統與服務於運行中，如發生第八點綜合判定結果為甲類、演算法嚴重偏差、生成重大違法內	明定人工智慧系統與服務發生重大異常事件時之應變及通報機制。

容、資料外洩或對民眾權益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，並於知悉異常情事後一小時內，依本府資通安全事件通報機制進行通報。 涉及對外服務者，應視情形提供人工服務、人工轉接、申訴或覆核管道；發現對外提供錯誤資訊時，應即時更正並留存改善紀錄。 採購人工智慧系統或服務時，應於採購契約中明定供應商負有異常通報、配合事故調查及受稽核之義務。	
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。	明定各機關應定期推動教育訓練，提升同仁之人工智慧素養與賦能。
十二、本要點所定內控機制應由本府不定期檢視；並適時做滾動式檢討修正，必要時得徵詢外部專家意見。	明定本府對內控機制之檢視與滾動式檢討修正機制。

檔 號：
保存年限：

新竹市政府 函

地址：300191新竹市中正路120號
承辦人：黃蒨楨
電話：03-5216121#419
電子信箱：010739@ems.hccg.gov.tw

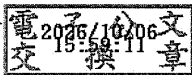
受文者：本府行政處法制科

發文日期：中華民國115年10月6日
發文字號：府數治字第1150174293號
速別：最速件
密等及解密條件或保密期限：
附件：如說明

主旨：訂定「新竹市政府及所屬機關人工智慧應用內控管理要點」，並自中華民國115年10月5日生效，請查照。

說明：檢送「新竹市政府及所屬機關人工智慧應用內控管理要點」1份。

正本：新竹市政府各處暨所屬機關(本府數位發展處除外)
副本：本府行政處法制科、本府數位發展處資通安全科、本府數位發展處綜合規畫科、
本府數位發展處數位治理科



法制科 收文:115/10/07



231150003687 無附件

新竹市政府及所屬機關人工智慧應用內控管理要點

- 一、新竹市政府（以下簡稱本府）為確保運用人工智慧執行業務或提供服務時，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、本要點適用於本府各處及所屬機關（以下簡稱各機關）自行或委外建置、開發之各類人工智慧系統與服務。
- 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辦理時程，由新竹市政府資訊安全處理小組或其他適當單位統籌辦理。
- 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。
- 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及其相關法令與本府資通安全維護計畫辦理；涉及個人資料蒐集、處理或利用時，應依個人資料保護法及其相關法令與本府個人資料保護管理制度進行事前評估與控管。
- 六、各機關於規劃自行開發、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、委外廠商或使用目的變更時，應填具新竹市政府人工智慧應用風險評估檢核表（以下簡稱風險評估表），識別潛在風險。
- 七、人工智慧系統與服務應依風險評估表規定綜合判定結果，及風險應對機制類別（甲類、乙類及丙類）所規定之下列內控措施項目進行後續調整：
 - （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經依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。

依風險評估表規定，就風險類型一至三及其嚴重程度綜合判定人工智慧系統與服務為無顯著風險者，得免辦理第七點所定內控措施。但應依風險評估表填列評估結果，並保留相關紀錄備查。

十、人工智慧系統與服務於運行中，如發生第八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，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，並於知悉異常情事後一小時內，依本府資通安全事件通報機制進行通報。

涉及對外服務者，應視情形提供人工服務、人工轉接、申訴或覆核管道；發現對外提供錯誤資訊時，應即時更正並留存改善紀錄。

採購人工智慧系統或服務時，應於採購契約中明定供應商負有異常通報、配合事故調查及受稽核之義務。

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。

十二、本要點所定內控機制應由本府不定期檢視；並適時做滾動式
檢討修正，必要時得徵詢外部專家意見。