

環境部及所屬機關(構)人工智慧應用內控管理要點

總說明

為落實數位政府轉型，並確保行政創新之安全與倫理，環境部及所屬機關（構）於運用人工智慧技術執行業務或提供公共服務時，需有效識別、評估及管理潛在風險，以保障人民基本權利並維護公共利益。依人工智慧基本法第十九條規定，政府機關應實施人工智慧應用之風險評估，並建立相應之內部控制管理機制。考量人工智慧之應用涉及技術缺陷、人機互動、資通安全、個人資料保護及社會結構衝擊等多維度風險，且相關管理程序與內控措施涵蓋機關內部權責劃分、通報流程及對外權益救濟，以落實人工智慧基本法第十九條規定，爰訂定環境部人工智慧應用內控管理要點（以下簡稱本要點），其要點如下：

一、訂定目的。（第一點）

二、適用對象、範圍及特殊業務適用原則。（第二點）

三、名詞定義。（第三點）

四、統籌管理單位、推動機制與備查作業時程。（第四點）

五、人工智慧應用應遵循之基本原則。（第五點）

六、資通安全與個人資料保護之法律遵循及佐證文件。（第六點）

七、風險評估之啟動時機、重大功能變更定義及定期重新評估頻率。
（第七點）

八、甲類、乙類、丙類及無顯著風險人工智慧風險等級應辦理內控措施。
（第八點至第十點）

九、內控措施落實填列、特殊情境免予辦理之審認及查核程序。（第十一點）

十、運行中異常情事之緊急因應措施與時限通報機制。（第十二點）

十一、辦理人工智慧素養與風險管理之教育訓練。（第十三點）

十二、定期檢視與滾動修正內控管理機制。（第十四點）

環境部及所屬機關（構）人工智慧應用內控管理要點

規定	說明
一、環境部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。	本要點訂定目的。
二、本要點適用於本部與所屬機關（構）（以下合稱本部）自行或委外建置、開發之各類人工智慧系統及服務。所屬機關（構）應依本要點辦理人工智慧應用內控管理工作，如因業務特性或特殊需求，得另訂相關作業程序或補充規定。	明定本要點之適用對象及其範疇，並考量所屬機關（構）之業務特殊性，得另訂高於本要點所定基準之規範，且該規範應依規定提送備查。
三、本要點用詞定義如下： （一）執行單位：指基於業務需求或推動公共服務，而提出規劃、自行開發、委外建置或採購（含雲端軟體服務）之各類人工智慧系統與服務之需求端或執行端之單位。 （二）單位主管：指執行單位二層主管。	定義本要點之用詞定義，以明確釐清內部權責與規範標的。
四、本部使用人工智慧執行業務或提供服務時，其風險管理、內控監督及內控措施之推動與時程管理，由環境部資安及個資保護推動小組（以下簡稱保護推動小組）統籌辦理。	明定本部人工智慧應用內控之統籌權責單位。
五、本部自行開發、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之七項原則。	明定本部各類人工智慧系統與服務於開發或採購階段，應遵循之核心科技倫理與基本原則。
六、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、其相關法令及本部資通安全維護計畫辦理；涉	規範人工智慧系統之資安防護與個資保護法律遵循義務。

及個人資料蒐集、處理或利用時，應依個人資料保護法、其相關法令及本部個人資料保護管理制度辦理事前評估與控管。	
七、執行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，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。 本部應於辦理人工智慧風險評估及內控檢核之日起十五個工作日內完成作業，並經單位主管奉核後提送保護推動小組備查。惟保護推動小組另有規定或公告期限者，從其規定。 持續使用中之人工智慧系統與服務，應每年至少重新辦理一次風險評估。所屬機關（構）得視業務需要增加評估頻率，並更新其評估內容及判定結果。	明定風險評估檢核表之填具時機、操作方法；明確定義重大功能變更之具體指標樣態，並定明持續使用中系統之定期盤點再評估頻率。
八、執行單位依風險評估檢核表規定綜合判定人工智慧系統與服務之結果為甲類者，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。	明定經執行單位判定為高風險甲類人工智慧風險等級時，執行單位應落實執行之六大核心內部控制措施，以杜絕自動化處分及偏見歧視。

(五) 強化防護：應於採購契約或系統與服務規格中，明確要求供應商落實資安及資料治理相關機制。 (六) 防範歧視偏見：應於系統設計、訓練及應用過程中，建立防範歧視偏見之相關措施或機制，包括資料集偏誤檢測、模型公平性評估及相應之修正措施。另得依其模型類型、風險等級、應用範圍或對權益影響程度，進行或要求供應商導入適用之第三方檢測或獨立驗證，以降低演算法對特定族群產生不當差別待遇之風險。	
九、執行單位依風險評估檢核表規定綜合判定人工智慧系統與服務之結果為乙類者，應辦理前點各款內控措施，並得依機關資源及風險程度，調整各項內控措施之執行優先順序。	明定經執行單位判定為乙類人工智慧風險等級應遵行之內控措施，並給予機關考量資源配置時之執行彈性調整權限。
十、執行單位依風險評估檢核表規定，綜合判定人工智慧系統與服務之結果為丙類者，應辦理第八點第一款及第二款內控措施。 執行單位依風險評估檢核表規定，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，執行單位得免辦理第八點所定內控措施，惟仍應依風險評估檢核表填列評估結果，並保留相關紀錄備查。	明定經執行單位判定為丙類風險等級應辦理之最低限度內控項目（人類監督保留及透明標示），以及判定為無顯著風險系統之豁免條件與基本紀錄保留義務。
十一、執行單位應依風險評估檢核表欄位逐項填列內控措施之辦理情形；各項內控措施如因系統與服務性質不適用者，應敘明具體理由，經單位主管審認後，始得免予辦理，並應報送保護推動小組備查；保護推動小組或經環境部授權之查核單位，得依風險程度、業務性質或查核計畫，要求系統與服務管理人及所屬單位提供相關佐證資料，供內部控管或查核作業使	規範內控措施表單應逐項填報，明定因技術特性致不適用時之豁免程序與主管審認機制，並建立後續查核與資料抽查機制。

用。	
十二、人工智慧系統與服務於運行中，若發生輸出結果明顯異常或與業務預期顯著不符、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，執行單位應立即暫停系統與服務之全部或部分功能、啟動人工作業程序，或採取其他必要之因應措施。 執行單位應於知悉異常情事後四小時內，依本部資通安全通報機制或內部既有通報程序辦理通報；並應於七十二小時內提出初步報告，內容至少包括事故標題、情形說明、人工智慧系統與服務及事故間之關聯性、通報者姓名與聯繫方式、事故首次已知發生時間、發生地點、佐證資料或參考來源，以及依據風險評估檢核表 2.4 之嚴重程度分級判定安全事故嚴重程度與損害類型等，若異常情事同時構成資通安全事件者，其通報仍應依資通安全管理法及相關子法辦理。 執行單位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。	建立人工智慧系統運行階段之「異常應變與緊急煞車機制」，規範執行單位應即時處理，並明定「四小時內通報」與「七十二小時內提出初步報告」之時限及報告內容。
十三、本部應定期辦理人工智慧素養、資訊倫理與風險管理之教育訓練，以提升本部人員對人工智慧技術局限性及資安風險之認知。	規定本部應定期推動教育訓練，深化內部人員對於生成式科技風險及技術倫理之素養。
十四、本要點所定內控機制應由環境部定期檢視；並適時做滾動式檢討。	明定機關對內控機制之定期檢視與滾動式檢討修正機制。

第七點 附表

規定	說明
附表：政府人工智慧應用風險評估檢核表 填寫目的：參酌人工智慧基本法規定及人工智慧風險分類框架模式，評估並掌握政府機關人工智慧系統與服務之潛在風險。 填寫範圍：政府機關自行開發、委外建置或採購之各類人工智慧系統與服務，例如生成式人工智慧、決策輔助與預測分析系統、機器學習模型或其他具自動化決策能力之人工智慧應用等。 填寫說明：本表由人工智慧系統與服務管理人或機關（執行單位）指定人員填寫，作為符合人工智慧基本法第十九條進行風險評估與訂定內控管理措施之基礎。 判定說明：人工智慧系統與服務經綜合判定結果應依核心風險識別為之；有一定程度風險情形者，應依風險評估檢核表所列之嚴重程度及發生機率，判定其風險類別。 前項所稱重大功能變更，指對人工智慧系統與服務本身，或其使用條件、情境或範圍所進行之更新，致改變其功能、底層架構或效能，而足以實質影響其應用結果或風險程度，並使先前之評估相關文件可能失其適用性或產生誤導之虞者，包括下列各款情形之一： (1) 模型核心邏輯或演算法架構變更。 (2) 訓練資料來源、範疇或標註方式發生重大異動（如異動比例達百分之五十，或資料性質顯著改變）。 (3) 系統適用對象、利害關係人、使用情境或決策範疇擴大或變更。	一、為評估並掌握政府機關人工智慧系統與服務之潛在風險，政府機關自行開發、委外建置或採購之各類人工智慧系統與服務，由人工智慧系統與服務管理人或機關（執行單位）指定人員填寫本表。 二、本表填寫項目分別為應用情境盤點，其目的係為掌握人工智慧系統與服務之基本資訊，以及核心風險識別與危害評估，本部分參考人工智慧風險分類框架，用以檢視並確認人工智慧系統與服務是否存在風險。

- (4) 輸出結果之後處理邏輯或門檻設定變更，致影響最終決策或裁量結果。
- (5) 其他經評估認定足以影響系統風險等級之變更。

一、 應用情境盤點

本表格目的為掌握人工智慧系統與服務之基本資訊。

檢核項目	填寫內容 / 評估結果	依據來源	備註 / 參考文件
1.1 系統與服務名稱	[請填寫]	人工智慧風險分類框架(附錄 1)	系統清冊
1.2 系統與服務具體用途與服務對象	【具體用途】 [請填寫] 【服務對象】 ☐ 政府(跨機關)內部使用 ☐ 對外公開服務	人工智慧風險分類框架(附錄 1)	系統清冊
1.3 核心人工智慧技術與開發方式			
1.3.1 大型語言模型 (Large Language Model, LLM)	☐ 自行建置 (含委外建置) ☐ 採購	人工智慧風險分類框架(附錄 1)	採購或系統文件

	☐ 未使用			
1.3.2 生成式 AI 使用 （如業務輔助、電腦視覺等）	☐ 自行建置 （含委外建置） ☐ 採購 ☐ 未使用			
1.3.3 其他人工智慧技術 （如：空污與水質趨勢預測、海岸垃圾無人機自動巡航偵測、碳盤查資料分析與預測、清運車輛軌跡異常偵測等屬運用資料分析或機器學習模型進行判斷之應用）	☐ 自行建置 （含委外建置） ☐ 採購 ☐ 未使用			
1.4 辨識利害關係人				
負責開發人工智慧系統與服務	☐ 自行開發 ☐ 委外開發 ☐ 僅進行採購（類 SaaS 服務）	人工智慧風險分類框架(附錄 1)	業務作業說明	

負責部署人工智慧系統與服務	☐ 自行部署 ☐ 委外部署 ☐ 僅進行採購(類SaaS服務)		
可能因人工智慧系統與服務影響之利害關係人 *可複選	☐ 民眾 ☐ 本部公務員 ☐ 跨機關公務員 ☐ 其他： _____		

二、 核心風險識別與危害評估

本部分參考人工智慧風險分類框架，用以檢視並確認人工智慧系統與服務是否存在風險。填寫說明如下：

1. 若 2.0 任一項勾選「是」，該項風險應依本部資通安全或個人資料保護相關機制辦理，其結果不納入後續 2.4 嚴重程度、2.5 風險發生機率判定及風險矩陣計算。
2. 若檢核項目 2.1、2.2、2.3 任一項勾選「是」，請接續填寫 2.4 嚴重程度判定及 2.5 發生機率。
3. 若檢核項目 2.1、2.2、2.3 均勾選「否」，則就風險類型一至三判定為「無顯著風

險」，免進行後續嚴重程度判定、發生機率及風險矩陣分類。

檢核項目	評估結果	情境簡述	依據來源
2.0 風險類型零：資安及個資問題 本人工智慧系統與服務、訓練資料、輸入指令、輸出內容，是否可能因其業務流程、使用情境或設計邏輯，而有違反資通安全或個資保護之疑慮？	資通安全疑慮： ☐ 是 ☐ 否 個資保護疑慮： ☐ 是 ☐ 否	[若評估結果為是，請簡述]	
2.1 風險類型一：人工智慧系統與服務本身之技術設計缺陷 本人工智慧系統與服務，是否可能因其業務流程、使用情境或設計邏輯，而發生演算法偏見、產生錯誤或誤導訊息、缺乏透明度或存在安全漏洞等情況，導致對特定群體不公平或決策錯誤？	☐ 是 ☐ 否	[若評估結果為是，請簡述]	人工智慧風險分類框架 (二、識別風險)
2.2. 風險類型二：部署後操作及人機互動問題			

2.2.1 本人工智慧系統與服務，是否可能因其業務流程、使用情境或設計邏輯，而導致公務員過度依賴而喪失獨立判斷能力？	☐ 是 ☐ 否	[若評估結果為是，請簡述]	人工智慧風險分類框架 (二、識別風險)
2.2.2 本人工智慧系統與服務，是否可能因其業務流程、使用情境或設計邏輯，而導致人工智慧系統與服務遭濫用以生成違法內容、深偽詐欺？	☐ 是 ☐ 否	[若評估結果為是，請簡述]	
2.2.3 本人工智慧系統與服務，是否可能因其業務流程、使用情境或設計邏輯，而導致人工智慧系統與服務遭利用於網路攻擊？	☐ 是 ☐ 否	[若評估結果為是，請簡述]	
2.3 風險類型三：社會結構與環境衝擊			
2.3.1 本人工智慧系統與服務，是否可能因其業務流程、使用情境或設計邏輯之應用，而加劇社會不平等之疑慮或風險？	☐ 是 ☐ 否	[若評估結果為是，請簡述]	人工智慧風險分類框架 (二、識別風險)

2.3.2 本人工智慧系統與服務，是否可能因其業務流程、使用情境或設計邏輯之應用，而耗費能源造成環境傷害？	☐ 是 ☐ 否	[若評估結果為是，請簡述]	
2.3.3 本人工智慧系統與服務，是否可能因其業務流程、使用情境或設計邏輯之應用，而遭利用於認知作戰，影響公眾信任？	☐ 是 ☐ 否	[若評估結果為是，請簡述]	
2.4 嚴重程度判定 若檢核項目2.1、2.2、2.3任一項勾選「是」，請接續進行嚴重程度判定，並採「擇一最高等級」單選勾選（例如：同時符合嚴重與非常嚴重之指標時，請勾選非常嚴重）；若經檢視，本案情境若均未達下方「非常嚴重」、「嚴重」及「一般」之指標門檻者，則下列各項請均勾選「否」。			
嚴重程度(依風險發生時之危害程度判定)	評估結果	依據來源	
2.4.1 【非常嚴重】 符合下列情形之一者屬之： 1. 上開風險發生，可能對機關之營運造成業務中斷運作	☐ 是 ☐ 否	參考人工智慧基本法、「資通安全責任等級分	

達三日（含三日）以上。 2. 上開風險發生，系統可能遭駭客入侵、發生資料外洩，或系統與服務停止運作達三日以上。 3. 上開風險發生，可能致機關財物損失達新臺幣五百萬元以上。 4. 上開風險發生，可能對機關信譽造成重大影響，包括經國際媒體報導負面新聞，或國內四家以上新聞媒體或社群網路平台持續報導負面新聞達三日以上。 5. 上開風險發生，可能引發二十人以上之民眾抗爭或群體性事件。 6. 上開風險發生，可能影響他人合法權益或機關執行業務之公正性及正當性，並使機關所屬人員負刑事責任。 7. 上開風險發生，可能導致特定群體（如特定性別、年齡、身心障礙或弱勢族群）在政府資源分配、資格審查或行政決策上遭嚴重不公平對待。 8. 上開風險發生，可能違反兒少最佳利益原則，或對其身心發展造成嚴重負面影響。 9. 上開風險發生，可能引發社會恐慌，或造成對人類基本權利、生命安全、財產保障、社會秩序或政府公信力之嚴重危害。		級辦法」之「附表九、資通系統防護需求分級原則」、「行政院及所屬各機關風險管理及危機處理作業手冊」	
---	--	---	--

2.4.2 【嚴重】

符合下列情形之一者屬之：

1. 上開風險發生，可能對機關之營運造成影響，包括業務中斷運作逾一日以上，未達三日。
2. 上開風險發生，系統可能遭駭客入侵、發生資料外洩，或系統與服務停止運作達一日以上，未達三日。
3. 上開風險發生，可能致機關財物損失達新臺幣一百萬元以上，未達五百萬元。
4. 上開風險發生，可能對機關信譽造成影響，包括經國際媒體報導負面新聞，或國內二家以上新聞媒體或社群網路平台持續報導負面新聞達一日以上。
5. 上開風險發生，可能引發五人以上，未達二十人之民眾抗爭或群體性事件。
6. 上開風險發生，可能影響他人合法權益或機關執行業務之公正性及正當性，並使機關或其所屬人員受行政罰、懲戒或懲處。
7. 上開風險發生，可能導致特定群體（如特定性別、年齡、身心障礙或弱勢族群）在政府資源分配、資格審查或行政決策上遭不公平對待。
8. 上開風險發生，可能違反兒少最佳利益原則，或對其身心發展造成負面影響。
9. 上開風險發生，可能引發社會恐慌，或造成對人類基

☐是

☐否

參考人工智慧基本法、「資通安全責任等級分級辦法」之「附表九、資通系統防護需求分級原則」、「行政院及所屬各機關風險管理及危機處理作業手冊」

本權利、生命安全、財產保障、社會秩序或政府公信力之危害。			
2.4.3 【一般】 符合下列情形之一者屬之： 1. 上開風險發生，對機關之營運影響有限，包括業務中斷未達一日。 2. 上開風險發生，系統與服務可能停止運作逾一小時，未達一日。 3. 上開風險發生，可能致機關財物損失未達新臺幣一百萬元。 4. 上開風險發生，對機關信譽影響有限，包括國內一家新聞媒體或社群網路平台報導負面新聞不超過一日。 5. 上開風險發生，可能引發四人以下之民眾抗爭或個別陳情事件。 6. 上開風險發生，可能發生違反相關規範之情形。	☐ 是 ☐ 否	參考「資通安全責任等級分級辦法」之「附表九、資通系統防護需求分級原則」、「行政院及所屬各機關風險管理及危機處理作業手冊」	
2.5 風險發生機率 若檢核項目2.1、2.2、2.3任一項勾選「是」，且已判定嚴重程度者，請接續進行風險發生機率判定。			

發生機率為參考區間，機率判定得參考歷史發生紀錄、系統特性、使用情境及其他相關風險評估資料綜合判斷之。

機率判定應以未施加額外控制措施時之固有發生可能性為準，不得以既有防護措施降低機率評等。

發生機率

- ☐高：指發生機率約在百分之六十以上，且於系統與服務運行期間內極可能發生。
- ☐中：指發生機率約在百分之三十以上未達百分之六十，且於系統與服務運行期間內可能發生。
- ☐低：指發生機率未達百分之三十，於系統與服務運行期間內不太可能發生，或僅於特殊或極端情境下始可能發生。

參考澳洲數位轉型署，人工智慧衝擊影響評估工具(AI Impact Assessment Tool)

三、 人工智慧內控管理與應對機制 (Internal Controls & Response)

執行單位請依據前述「核心風險識別與危害評估」之結果（含項目2.0、2.1至2.3核心風險、2.4嚴重程度及2.5發生機率），依下列規定辦理後續內控管理與措施填列：

1. 資安與個資風險處理：若2.0任何一項勾選「是」，該項風險應依本部資通安全維護計畫或個人資料保護管理制度處理，保護推動小組得視內部控管或查核需要，要求執行單位提供相關佐證文件。（例如資通安全維護計畫、風險評鑑報告、風險評鑑彙整表、風險改善計畫、個人資料風險評估紀錄或其他足資證明之文件）。

本案個資與資安風險識別：

☐有資安風險之虞☐有個資風險之虞☐無上述風險

2. 人工智慧風險等級判定

執行單位請依據前述核心風險評估結果，確認風險類別：

(1) 若檢核項目2.1至2.3均為「否」，或2.4嚴重程度均為「否」，則風險類型一至三屬「無顯著風險」，免予對照下方風險矩陣，並逕於下方勾選綜合判定結果。

(2) 若檢核項目2.1至2.3任一項勾選「是」，並已完成2.4嚴重程度及2.5發生機率判定者，請依其判定結果對照下方風險矩陣劃分歸屬類別（甲類、乙類、丙類）：

發生機率 嚴重程度	高	中	低
非常嚴重	甲	甲	乙
嚴重	甲	乙	丙
一般	乙	丙	丙

本案風險綜合判定結果（請擇一勾選）：

☐甲類☐乙類☐丙類☐無顯著風險

3. 內控措施落實填列說明

執行單位請依據前項「本案風險綜合判定結果」，依下列規定填列後續內控措施表：

- (1) 判定為甲類或乙類者：3.1至3.6項為必辦項目，執行單位應逐項採取控制措施並填列辦理情形（乙類之落實優先順序得次於甲類）。
- (2) 判定為丙類者：3.1及3.2項為必辦項目，應採取控制措施並填列辦理情形；其餘3.3至3.6項仍應於表單進行評估填列，惟得免採取該等內控措施。
- (3) 判定為「無顯著風險」者：得免辦理第3.1至第3.6項內控措施，惟仍應依附表填列評估結果，並保留相關紀錄備查。
- (4) 前述各類別之必辦項目，若系統與服務性質確實無涉決策（如3.1）或無涉內容產出（如3.2）等特殊情境者，得免採取措施，惟仍應於表單勾選「不適用」並具體敘明理由。

4. 人工智慧內控措施落實表

檢核項目	落實結果	辦理/不適用說明	參考來源
3.1 人類監督保留： 針對人工智慧提供之決策，作業流程中是否設有適當之人為介入與最終覆核機制，避免完全自動裁決？	☐ 是 ☐ 否 ☐ 不適用	[請填寫]	人工智慧基本法第4條第2款
3.2 透明標示： 系統與服務之產出是否進行適當資訊揭露(如標註「由人工智慧生成」)？	☐ 是 ☐ 否 ☐ 不適用	[請填寫]	人工智慧基本法第5條

3.3 明確警語： 本系統與服務是否依其應用特性與潛在風險，於服務介面或相關文件中明確標示注意事項或使用警語？	☐ 是 ☐ 否 ☐ 不適用	[請填寫]	人工智慧基本法第 5 條
3.4 建立救濟機制： 針對受人工智慧輔助決策影響之民眾，是否提供明確之申訴管道、決策解釋與權益救濟機制？	☐ 是 ☐ 否 ☐ 不適用	[請填寫]	人工智慧基本法第 17 條
3.5 強化防護： 是否於採購契約或系統與服務規格中，明確要求供應商落實資安及資料治理相關機制？	☐ 是 ☐ 否 ☐ 不適用	[請填寫]	人工智慧基本法第 4 條第 3 款、第 4 款
3.6 防範歧視偏見： 是否於系統設計、訓練或應用過程中，建立防範歧視偏見之相關機制（例如資料集偏誤檢測、模型公平性評估及必要之修正措施），或視需要進行或要求供應商導入適用之第三方檢測或獨立驗證？	☐ 是 ☐ 否 ☐ 不適用	[請填寫]	人工智慧基本法第 4 條第 6 款
系統與服務管理人：_____ (簽章)			
單位主管：_____ (簽章)			