

責任人工智慧治理政策聲明

(本聲明經本公司資訊安全推動委員會核准後發布施行)

政策目的與適用範圍

中鼎工程股份有限公司 (下稱「本公司」) 致力於推動人工智慧 (AI) 於工程服務及企業營運領域之負責任應用，以提升工程品質、作業效率、創新能力與整體服務價值。本公司將持續關注國內外 AI 治理趨勢、相關法規及產業實務發展，並於適用範圍內，依循公司治理、法規遵循與風險管理原則，推動 AI 技術之審慎導入與合理應用，以支持數位轉型及企業永續發展。

治理架構與問責制度

本公司將依據既有公司治理、內部控制、資訊安全與風險管理架構，推動 AI 應用之責任分工與管理機制。集團創研中心負責本 AI 政策文件之制訂、維護與定期檢視，並得依 AI 技術發展、法令規範及實務應用情形，適時提出修訂建議。

各相關單位及人員應依其職責範圍，對 AI 工具之導入、使用、管理及輸出結果負相應責任，並確保其應用符合公司政策、法令規範、契約要求及企業倫理。若因 AI 應用導致錯誤、實質損害或衍生法律責任時，應依本公司既有之權責劃分及獎懲辦法進行調查與問責。涉及重大風險、跨單位應用或責任歸屬有疑義之 AI 應用案例，應提報 < 資訊安全推動委員會 >，由其依個案情形進行審議、判定及提出必要之管理要求。

本公司亦將視 AI 技術發展及實務應用情形，持續檢視相關治理措施之適切性。

執行範圍與邊界管理

本公司將依 AI 應用之目的、情境、資料類型及風險程度，審慎界定其使用範圍與執行邊界。相關單位應依業務需求、專案特性及管理要求，明確訂定 AI 應用之授權使用範圍、可執行功能、資料使用限制、輸出結果適用情境及不得使用之情形，並據此建立允許使用規範、防護機制、功能與能力限制，以及需人工介入或升級提報之控制點，以區分 AI 可輔助執行、須經人工確認或不宜使用之情境。

各 AI 應用之使用範圍與執行邊界，應由導入或使用單位依實際需求提出，並依公司權責規範提報相關權責單位審議、確認或備查。AI 應用範圍應隨技術發展、法規要求及公司管理需求適時檢視；如涉及用途擴張、資料範圍變更、功能調整或風險程度提高者，應重新評估並完成必要之審查程序，以確保其使用符合授權範圍、治理原則與合規要求。

合規基準與禁止行為規範

本公司禁止利用 AI 從事違反法令、公司規範、契約義務或倫理原則之行為。AI 技術之導入與應用，應遵循我國《人工智慧基本法》、歐盟《一般資料保護規則》(General Data Protection Regulation, GDPR) 及《人工智慧法》(EU Artificial Intelligence Act, EU AI

Act) 相關法令及公司內部規範。AI 技術不得被用於侵害個人權益、危害資訊安全、規避內部控制、操弄或誤導他人、剝削弱勢族群、進行不當監控、未經授權之生物辨識、社會信用評分，或其他可能損害公共利益、公司信譽或利害關係人權益之用途。相關人員應依公司規範及授權範圍審慎使用 AI 技術，確保其應用符合負責任、合規與可信賴之原則。

隱私保護與資料治理原則

本公司重視個人資料保護、營業秘密、機密資訊及智慧財產權。AI 技術之應用，應依循相關法令、契約義務、公司資安規範及資料治理原則；例如涉及個人資料之蒐集、處理及利用時，應符合我國《個人資料保護法》相關規定。

涉及公司業務、客戶資料、專案資訊、機密資料或智慧財產內容者，應使用符合公司管理要求之授權系統或經核可之工具。相關人員應於 AI 開發、部署、應用及資料處理之生命週期中，包括資料蒐集、輸入、處理、儲存、使用、輸出、分享、保存及刪除等階段，應審慎評估使用情境、資料敏感性、權限控管及資料處理方式，以降低資料外洩、未授權使用、模型不當利用或權利侵害之風險。

資訊安全與系統防護機制

AI 技術之導入與應用，應配合本公司發布之「資訊安全政策聲明」及相關資訊安全管理規範，兼顧系統穩定性、資料安全性與營運可靠性。依該聲明，本公司係依據 ISO 27001 資訊安全管理標準之要求建立資訊安全管理制度，並以確保資訊安全、培育員工資安意識、持續改善資訊安全管理制度，以及遵循相關法規、公司規範與契約要求為必要管理方向。

本公司將依 AI 應用之實際情境、資料敏感程度及風險影響，採取適當之管理、審查及技術防護措施，包括但不限於權限控管、身分驗證、使用紀錄留存、系統監控、資料保護、資料加密、異常事件通報、弱點檢測及必要之滲透測試等，以降低未授權存取、資料外洩、系統濫用、模型誤用或其他潛在資安風險。

AI 系統及相關資訊資產之存取控制，應依工作需要明確訂定，並將存取控制需求告知系統服務提供者，以利執行有效之存取控制機制，配合稽核制度，降低未經授權存取系統之風險。

發生 AI 相關資訊安全事件時，應即時通報，採取必要之應變措施，並建立事件學習機制，以降低事件所造成之損害。

涉及重要營運業務之 AI 系統，應建置及實施適當之備援計畫，於系統中斷或故障時，在可接受時間內恢復營運，確保重要營運業務能及時恢復運作。

透過上述措施，確保 AI 應用符合公司整體安全管理要求。

公平原則與防偏誤管理

本公司支持公平、包容及尊重多元價值之原則。AI 技術之導入與應用，應避免造成不當偏見、差別待遇或歧視性影響，並應於合理可行範圍內，考量其對員工、客戶、合作夥伴及其他利害關係人可能造成之影響。

各單位在進行 AI 模型開發、訓練或微調，以及導入或使用 AI 應用時，應依其用途、影響程度及風險高低，於合理可行範圍內辨識其輸入資料、模型輸出及應用結果，是否可能產生不公平、偏誤或歧視性影響。公司得視 AI 之用途、影響程度、風險高低、實際需求或其他相關因素，辦理必要之稽核措施，稽核重點得包括資料來源及使用情境是否適當、輸出結果是否可能對特定對象或群體造成不合理不利影響，以及應用流程是否保留必要之人工判斷、審查或修正機制。若 AI 應用或相關資料涉及公平、不歧視、包容性或利害關係人權益等疑慮時，必要時得洽請相對應之專責部門協助評估。各單位並得依評估結果及實務需求，採取適當之調整、限制使用、補充人工審查、改善措施，或留存相關紀錄，以減緩不公平與歧視的潛在風險，並維護 AI 應用之公平性與信任基礎。

系統透明度與可解釋性原則

本公司重視 AI 應用之透明性與可理解性。AI 技術之導入與使用，應於合理可行範圍內，使相關人員了解其用途、適用情境、授權使用範圍、主要功能、能力限制及可能風險，避免對 AI 產出或輔助判斷產生不當期待、過度依賴或超出原定目的之使用。

涉及對員工、客戶、合作夥伴或其他利害關係人產生影響之 AI 應用，應視其用途及影響程度，採取適當之透明化措施，例如於適當情況下明確告知使用者其互動對象為 AI 而非真人、標示內容是由 AI 產生或輔助產生，並得視 AI 應用之用途、影響程度及技術可行性，於合理可行範圍內，提供適當且易於理解之說明，說明內容得視實際情況及個案需要，就適當事項予以呈現，例如形成該結果所依據之主要資訊、重要假設、關鍵影響因素、適用條件、結果限制或不確定性、需由人工進一步判斷、確認或補充之事項，以及其他有助於理解該結果之相關資訊。

人類自主與決策監督機制

AI 技術應作為輔助決策、提升效率與支援專業判斷之工具，不應取代相關人員依其職責所應履行之審查、確認、簽核或專業判斷責任。涉及工程設計、專案執行、風險評估、合約義務或其他重要業務決策之 AI 應用，應採行 Human in the Loop (人類參與監督) 機制，依風險程度納入人為干預 (Human-in-the-loop) 、人為監控 (Human-on-the-loop) 或人為控制 (Human-in-command) 等不同層次之作法，以確保納入有效且具文件紀錄之人類監督，並保留專業審查與最終確認程序。相關負責人員應依公司權責規範及實務需求，對 AI 輔助產出進行必要之檢核與判斷，並就最終決策結果負責；必要時，應留存 AI 輔助決策之使用情形、人類監督紀錄、審查過程及確認結果，以確保作業品質、安全性與可靠性。

環境永續與生態足跡管理

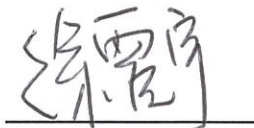
AI 技術之應用應有助於提升工程品質、作業效率、資源運用效益及整體服務價值，以支持企業永續發展。本公司於 AI 技術之開發、導入、採購或使用過程中，將於合理可行範圍內，關注能源使用效率、環境影響及供應商之永續實踐情形。於評估第三方 AI 服務或相關技術方案時，應於合理可行範圍內，將能源效率、運算資源使用、降低生態足跡及供應商永續表現等因素納入綜合考量，以呼應綠色工程與環境永續理念。



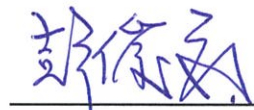
李定壯
總管理處
總經理



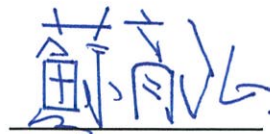
鍾政雄
煉油石化
工程事業部
總經理



徐震宇
基礎及環能
工程事業部
總經理



彭俊賓
高科技設施
工程事業部
總經理



蘇育弘
工程技術部
總經理



李銘賢
總經理(兼任資安長)