廣宇科技股份有限公司
人工智慧（AI）治理政策規範

目的與宗旨

人工智慧（Artificial Intelligence, AI）發展突飛猛進，強烈衝擊現有產業發展，同時也創造出新產業的商機，廣宇科技股份有限公司及其子公司(以下簡稱本集團)為妥善管理人工智慧技術之導入、開發與日常應用，確保本集團在提升營運效率、製造智慧化及研發創新之同時，落實資訊安全、營業秘密保護、個人資料隱私維護及符合法令倫理規範，特訂定本政策，作為開發及使用人工智慧遵循之依據。

適用範圍

本政策適用於廣宇科技集團旗下所有營運據點（包含台灣總部及中國大陸、馬來西亞、美國等全球生產基地與營運子公司），並推廣至全體供應鏈及合作夥伴共同遵守。

核心治理原則

本公司 AI 應用與推動應恪遵以下核心原則：

1. **合法合規與營業秘密保護**：未經本集團授權，不得將核心製程技術、設計圖說、客戶機敏資料、商業報價或未公開財務數據上傳至 AI 平台。
2. **人為監督與當責機制（Human-in-the-Loop）**：AI 產出之數據、代碼、決策建議僅供輔助參考，相關權責人員得視需要修正、否決 AI 產出或停止其應用。各單位最終決策與業務產出仍由業務承辦人員與該權責主管負最終審查責任。
3. **資訊安全與隱私防護**：系統應符合最小授權原則，落實資料存取權限控管、數據去識別化，並抵禦潛在的提示詞注入（Prompt Injection）與模型資料外洩威脅。
4. **透明度與可解釋性**：應用於品管、生產排程或內部重要評核之演算法，應具備合理的可追溯性與校準紀錄，並清楚說明重要產出或決策之依據，以利相關人員審查。
5. **公平無偏見**：AI 於內部人力資源管理或外部採購篩選時，不得包含種族、性別、宗教等不合理之歧視性偏誤。
6. **AI 使用邊界與限制**：明確規範 AI 系統之允許用途、使用權限及禁止事項。人工智慧不得超出核准之業務範圍、存取未授權資料，或在缺乏適當人為監督情況下執行重大或不可逆之決策。亦不得使用涉及操控行為、不當社會評分、剝削個人或特定群體弱點，或未經授權之生物辨識監控的 AI 系統。
7. **違規與問責機制**：利害關係人得就疑似違反本政策之情形提出申訴或檢舉，由指定權責單位進行調查，並將調查結果回覆申訴人。對於申訴人的身分將嚴格保密，禁止任何形式的責難及報復。

智慧財產權與法律責任

1. **內部成果歸屬**：員工於職務範圍內利用公司提供之 AI 工具產出之各項發明、設計、程式碼與研究文件，其智慧財產權依本公司聘僱合約與法規歸本公司所有。
2. **侵權防範**：引進外部模型訓練集或直接採用 AI 生成代碼/圖像時，應確認其授權條款，避免侵害第三方之智慧財產權或違反開源軟體授權協議。

施行與修訂

本政策經永續委員會核定、呈報董事長簽核後實行，後續因應國內外法律變更（如人工智慧基本法規公布）、技術演進及業務需要，由專責小組適時檢討修訂。

董事長：李光明

2026.10.29