東元集團 AI 治理政策

第一條　目的

為促進東元集團 (以下簡稱「本集團」) 各公司安全、負責任且具效益地導入與使用人工智慧 (AI)，提升營運效率、創新能力、服務品質與集團競爭力，並有效控管 AI 可能衍生之資訊安全、資料外洩、個人資料保護、智慧財產權、模型偏誤、錯誤決策、法令遵循風險、供應商依賴及永續風險，特制定本政策。

本政策以「鼓勵創新、風險可控、權責明確、合規可信、持續改善」為核心，使 AI 應用在明確治理原則下穩健落地。

第二條　基本原則

1. 策略一致與價值導向：AI 應用應與本集團營運策略、數位轉型方向及實際業務價值一致，避免重複建置、無效投入或偏離業務需求。
2. 合法合規與誠信使用：AI 之導入、開發、採購、測試、使用及對外發布，應遵循適用法令、客戶契約、公司規章、資訊安全與資料治理要求。
3. 資料保護與必要範圍使用：AI 之資料使用應尊重資料隱私、營業秘密及智慧財產權；使用資料時，應以達成業務目的所需之必要範圍為限 (只使用完成任務所真正需要的資料，不多取、不多傳、不多留)，並確保資料取得經適當授權、使用過程受到合理保護，且可追溯其來源與使用紀錄。
4. 資訊安全與受控環境：涉及公司資料、內部知識、系統串接或自動化流程之 AI 應用，

本文件可能包含本公司相關機密資訊。未經本公司事先書面同意，不得將其中一部分或全部洩漏予與業務無關之人。

應於母公司核可或可控之安全環境中使用。

5. 風險分級與權責核可：AI 應用（包含但不限於 AI Agent、生成式 AI、機器學習、影像辨識及自動化決策輔助）應依風險程度分級管理，並應經權責單位核可後上線或正式使用。

6. 人類自主與責任歸屬：AI 產出原則上為輔助資訊，不得取代權責人員之專業判斷、核准責任及管理責任。涉及重大權益、法律效果、財務承諾、工安品質或對外承諾事項，應保留人工覆核與決策。

7. 透明可解釋與可追溯：AI 對外互動、對外發布或產生可能造成誤認之內容時，應依情境揭露 AI 使用事實，並保留來源、版本、時間與覆核紀錄。

8. 公平性與偏誤管理：AI 應用應避免產生不合理差別待遇、歧視性結果或偏誤擴大，並於必要時進行檢視與改善。

9. 供應商與第三方風險管理：採購、訂閱、試用、串接或導入第三方 AI 工具或服務時，應評估資料使用、資安控制、合規能力、契約權利、模型限制及退場安排。

10. 成本效益與永續責任：AI 導入應兼顧效益、成本、能源使用與永續責任，避免重複投資及無效算力消耗。於評估 AI 模型、運算資源或雲端服務時，應適度考量其能源效率、運算資源消耗、碳排放及永續影響，並優先採用符合節能減碳或具永續承諾之技術與服務。

11. 機密與敏感資料防護：使用外部或未核可 AI 工具時，嚴禁公開、共享或輸入任何機密或敏感資訊。

本文件可能包含本公司相關機密資訊。未經本公司事先書面同意，不得將其中一部分或全部洩漏予與業務無關之人。

12. 機密與敏感資料包括但不限於：員工或客戶之個人識別資訊、特種個資、設計圖、施工計畫、成本估算、投標文件、財務資訊、尚未公開之業務秘密及內部評等為「機密」與「密」之資訊。

第三條　適用範圍

本政策適用於本集團各公司董事、經理人、全體員工、約聘僱人員、實習生、派遣人員、供應商、承包商、委外廠商、顧問及其他經本集團授權使用或接觸 AI 系統之人員。

本政策適用於本集團各公司自行開發、委外開發、採購、訂閱、試用或公開可取得之 AI 模型、AI Agent、生成式 AI、機器學習、電腦視覺、語音辨識、推薦或預測模型、RPA+AI、LLMOps/MLOps 平台及其整合應用。

凡使用本集團資料、設備、網路、雲端、私雲、地端系統、內部知識庫或公司帳號所進行之 AI 使用、測試、訓練、推論、上線與維運，均適用本政策。

第四條　治理權責

本集團各公司應依公司治理與核決架構，建立 AI 治理所需之權責分工、審議機制、風險管理與持續改善機制。

數位發展處為本政策之權責單位，負責 AI 治理制度規劃、企業 AI 平台推動、相關規範維護、教育推廣及治理資訊彙整；資訊安全、法遵/個資、採購及各資料或系統權責單位，依其職掌參與 AI 相關審查與管理。

本文件可能包含本公司相關機密資訊。未經本公司事先書面同意，不得將其中一部分或全部洩漏予與業務無關之人。

各公司單位主管應督導所屬人員依本政策使用 AI，並對所轄業務中採用 AI 產出所形成之決策、文件、服務或作業結果，依權責負管理責任。

第五條　AI 使用與風險管理

本集團鼓勵各公司於文書處理、知識查詢、程式輔助、資料分析、流程改善、客戶服務、品質提升、工安管理、營運決策輔助等場景合理運用 AI，以提升工作效能與創新能力。

AI 應用應依使用情境、資料敏感度、對外影響及可能造成之權益或營運影響，進行必要之風險判斷與權責確認。各公司單位主管應督導所屬人員依風險程度完成相應同意或審查，並保留必要紀錄，以利追蹤、稽核及風險管理。

違法、侵權、詐欺、惡意攻擊、未授權監控、歧視性評估、、操控性行為、社會評分，或其他違反人權、倫理及法令規範之高風險 AI 用途，均不得為之。

第六條　資訊安全治理

涉及敏感資料或高風險之 AI 應用，應依公司資訊安全管理程序辦理，並經相關權責單位審查核准後執行。所稱高敏感資料，包括機密資訊、個人資料、客戶資料、供應商資料、財務資料、投標採購、研發設計、原始碼、帳號密碼、金鑰，或其他依公司資料分級認定為機密之資料。

本文件可能包含本公司相關機密資訊。未經本公司事先書面同意，不得將其中一部分或全部洩漏予與業務無關之人。

所稱高風險情境，係指 AI 應用之輸出、判斷或自動化行為，可能對公司營運、資安、法遵、財務、商譽、客戶 / 員工權益、工安品質或重大決策產生實質影響者。

各公司資訊安全權責單位應依本政策另訂「人工智慧應用資安管理規範」、技術控制要求及 AI 資安事件應變程序，作為本政策之接軌文件；相關細部控制、檢核項目、事件處理流程與技術基準，依該接軌文件及公司既有資安規範辦理。

1. 共同審查情境：涉及機敏資訊(包括但不限於個資、客戶資料、財務資料)、原始碼、內部系統串接、自動化流程、AI Agent、對外服務、工安品質或重大營運流程之 AI 應用，應依風險程度納入相關權責單位共同審查。

2. AI Agent 特別控管：AI Agent 因可能具備任務規劃、工具調用、資料查詢或流程執行能力，應依風險程度建立身分識別、最小權限、工具白名單、人工覆核、稽核紀錄與緊急停用機制。

3. AI 資安事件範圍：AI 資安事件應納入公司事件通報與應變範圍，包括但不限於敏感資料外洩、未授權 AI 工具使用、錯誤對外承諾、Prompt Injection、資料投毒、模型濫用、AI Agent 異常行為、Deepfake 詐欺及 AI 生成內容造成重大誤導等。

4. 事故通報與應變：如發現 AI 工具或 AI 應用疑似造成資料外洩、錯誤對外承諾、重大錯誤判斷、侵權、偏見歧視、客訴、資安事件、異常自動化行為或其他重大風險，應立即停止擴大使用並依公司事件通報與應變機制辦理。

本文件可能包含本公司相關機密資訊。未經本公司事先書面同意，不得將其中一部分或全部洩漏予與業務無關之人。

第七條　資料、內容與對外發布管理

1. 資料保護:使用各類 AI 技術與應用時，不得為提升回答品質而犧牲資料安全。涉及機密、個人資料、客戶資料、供應商資料、財務成本、投標、研發設計、原始碼、帳號密碼、金鑰或其他高敏感資訊者，應遵循以下原則：

   1-1. 工具選用要求：處理敏感資料時，應優先使用經公司核准之企業級 AI 工具。所謂企業級工具，係指透過付費訂閱或企業合約，且服務提供者明確承諾不將使用者資料用於模型訓練、服務改善或與其他使用者共享之工具。

   1-2. 資料處理規範：必要時應進行去識別化或遮罩處理，確保敏感資訊不以明文形式傳輸或儲存於 AI 服務端。

   1-3. 使用紀錄保存：使用過程應保留必要紀錄 (包括使用者、時間、資料類型、工具名稱)，以利後續追蹤、稽核與風險管理。

2. 內容驗證 ：AI 產生之文字、程式碼、圖像、影音、報告、簡報、設計或其他內容，使用前應確認正確性、來源可信度、智慧財產權歸屬、是否違反契約義務及對外承諾風險。

3. 重大文件管控：新聞稿、重大公告、財務/法務/技術承諾、客戶提案、投標文件、合約文字、正式簡報或其他重大對外文件，如使用 AI 輔助產出，應由權責單位主管完整覆核並審核同意後始得發布。

本文件可能包含本公司相關機密資訊。未經本公司事先書面同意，不得將其中一部分或全部洩漏予與業務無關之人。

第八條　第三方 AI 工具與供應商管理

第三方 AI 工具或服務之採購、訂閱、試用、串接或正式導入，應依公司核決與供應商管理規範辦理，並視風險程度評估資料使用、資料主權、跨境傳輸、資安控制、合規證明、模型限制、輸出風險、稽核權與退場安排。

供應商不得將本集團資料用於未經授權之模型訓練、商業利用或其他目的；如涉及公司機密、個資、客戶資料或重大營運流程，應於契約、技術控制及管理程序中明確約束。

第九條　教育訓練、紀錄、稽核與改善

本集團應視業務需要推動 AI 使用教育、風險意識宣導及必要之專業訓練，提升同仁對 AI 能力、限制、風險與責任之理解。

AI 應用應依風險程度保留必要紀錄，並應就使用情形、效益、成本、錯誤、客訴、資安事件及合規狀態定期或必要時進行檢視。對低效益、高風險、違規或不再符合原核准目的之 AI 應用，得要求改善、限制、停用或退場。

第十條　施行與修訂

本政策由財務暨管理中心數位發展處擬訂，依本集團內部授權規範及權責分工完成核准後，公告施行。本政策應至少每年檢視一次；如有修訂必要，應依本集團內部授權規範及權責分工完成修訂、核准及公告。

本政策經董事長核定後發布施行，修正時亦同。

本文件可能包含本公司相關機密資訊。未經本公司事先書面同意，不得將其中一部分或全部洩漏予與業務無關之人。