



2026 年度責任 AI 計畫

一、計畫目的

為落實《華邦電子責任 AI 政策》，本公司建立責任 AI 計畫（Responsible AI Program），透過治理制度、風險管理、教育訓練、技術控制與持續改善機制，確保人工智慧（AI）於導入、開發、採購、使用及退場之全生命週期中，符合安全、透明、公平、可解釋、永續及法規遵循之要求。

本計畫旨在：

- 落實責任 AI 治理原則
- 降低 AI 相關資安、隱私、法遵與營運風險
- 建立可信賴之 AI 應用環境
- 提升員工 AI 倫理與安全意識
- 支持企業 ESG 永續發展目標

二、適用範圍

本計畫適用於華邦電子及全球各子公司所使用、開發、採購或管理之 AI 系統與服務，包括：

- 自行開發之 AI 系統
- 第三方 AI 服務
- 生成式 AI（Generative AI）
- 代理式 AI（Agentic AI）
- Low-Code/No-Code AI 應用

涵蓋：

- 資料蒐集與處理
- 模型開發
- 系統測試
- 上線部署
- 維運管理
- 退場管理

等全生命週期活動。

三、責任 AI 推動計畫

1. 明確標示 AI 生成內容與 AI 決策結果

計畫內容

公司宣導 AI 產出之內容、分析結果或決策建議，應依風險等級採取適當揭露措施。

執行措施

- AI 輸出結果標示 AI 參與資訊
- AI 生成文件標示 AI 協助產出
- AI 分析結果提供適當說明
- 建立 AI 結果覆核流程



- 對重大決策保留人工審核機制

2. 監測與修正 AI 模型漂移 (Drift) 或退化

計畫內容

建立 AI 模型效能監測與持續改善機制。

執行措施

- 建立模型效能基準值
- 定期監測準確率與可靠性
- 定義模型漂移告警門檻
- 建立模型重新訓練程序
- 建立模型版本管理與追蹤機制

3. 定期評估 AI 模型公平性與偏見

計畫內容

降低因訓練資料、演算法或模型設計造成之偏見與不公平風險。

執行措施

- 導入公平性 (Fairness) 評估機制
- 評估資料代表性與偏差風險
- 對高風險 AI 進行偏見測試
- 對傳統機器學習模型建立偏見修正與改善流程
- 對傳統機器學習模型定期檢視模型產出合理性

4. 降低 AI 數據中心與模型生態足跡

計畫內容

於 AI 規劃與導入階段納入永續發展考量。

執行措施

- 評估 AI 模型能源消耗
- 優先採用高效率 AI 模型
- 善用雲端共享服務降低重複建置
- 評估 AI 方案 ESG 表現
- 納入供應商永續管理評估

5. 建立使用者與利害關係人申訴機制

計畫內容

建立透明且可追蹤之 AI 申訴與改善機制。



執行措施

- 納入公司 HelpDesk 服務流程
- 建立調查與回覆程序
- 高風險案件納入跨部門審查
- 建立矯正及預防措施追蹤機制

6. 量化 AI 對永續發展成果之影響

計畫內容

建立 AI 價值衡量機制，評估 AI 對環境、社會與治理之影響。

執行措施

環境（E）

- 能源效率提升
- 碳排放減量
- 資源利用最佳化

社會（S）

- 作業效率提升
- 人工工時節省
- 員工 AI 能力提升

治理（G）

- AI 風險管理成熟度
- AI 專案納管比例
- 責任 AI 符合度

7. AI 倫理與安全教育訓練

計畫內容

建立「AI 倫理與安全教育訓練計畫」，以培養全體員工之責任 AI 意識及 AI 治理能力，並將教育訓練納入公司 AI 治理體系之重要推動措施。透過系統化課程、宣導活動及定期評量機制，強化員工對 AI 倫理、資安、隱私保護、智慧財產權及法規遵循之理解，提升對生成式 AI、代理式 AI、AI 幻覺、Prompt Injection、Shadow AI 及敏感資料保護等新興風險之辨識與應對能力，確保 AI 應用符合公司責任 AI 政策、資訊安全管理要求及國際法規趨勢，進而建立可信賴、安全且可持續發展之 AI 應用環境。

執行措施

- 建立全員責任 AI 意識與能力發展計畫。
- 執行措施
- 教育及宣導內容包含：
- 責任 AI 政策



- AI 倫理
- AI 偏見與公平性
- 個資保護
- 智慧財產權
- 生成式 AI 使用風險
- Agentic AI 風險
- AI 資安風險與防護
- Prompt Injection 與 Prompt 安全
- AI 幻覺（Hallucination）風險
- 敏感資料保護與資料分類要求
- AI 結果人工覆核原則
- 第三方 AI 服務使用規範
- Shadow AI 風險管理
- AI 事件通報與處理程序
- AI 法規與公司治理要求

8. AI 治理驗證與持續改善

計畫內容

公司將持續評估並提升 AI 治理成熟度，以符合國際最佳實務與法規要求。

執行措施

狀態:已完成

- 建立《華邦電子責任 AI 政策》
- 建立集團 Responsible AI Governance Framework
- 建立 AI 治理角色與責任制度
- 建立 AI 使用規範與宣導機制

狀態:建置中

- AI 風險評估與分級制度
- AI 事件管理與追蹤機制
- AI 治理指標管理機制

狀態:持續改善

- 每年檢視政策與法規符合性



- 定期進行教育訓練
- 持續提升 AI 治理成熟度
- 追蹤改善措施執行成效