

# 啓基科技人工智慧安全管理政策

## 1. 公司治理承諾與 AI 發展方針

啓基科技股份有限公司與所屬關係企業（以下簡稱為本公司或啓基科技），承諾在運用人工智慧（AI）技術提升營運效率與創新能力的同時，建立完善的治理架構，確保 AI 的使用符合資訊安全、法律合規、資料隱私保護及環境永續之最高標準。本政策旨在向利害關係人公開說明本公司之 AI 治理原則、核准工具清單、資料保護措施及責任歸屬機制。

### 1.1 治理架構

本公司規劃設立 AI 治理委員會，由資訊長（CIO）擔任召集人，負責審議 AI 發展策略、資源分配、高風險應用之最終核准，以及非標準化工具之導入審查。委員會每年召開定期治理審查會議，並於重大資安事件、法規修訂或技術架構變更時啟動動態風險驅動審查。

### 1.2 我們支持負責任的 AI 使用

本公司支持合理運用 AI 提升工作效率與員工賦能。針對具自主執行能力之代理式 AI（Agentic AI），因其可存取本機資源、執行系統指令並串接第三方擴充元件，本公司已採取更嚴謹之治理原則，確保自動化操作處於安全受控狀態。

## 2. 適用範圍

本政策適用於本公司及所屬關係企業所擁有、管理、開發、採購、部署或使用之 AI 系統、模型、資料、API、應用程式、知識庫、開發工具與相關基礎架構，包含但不限於各種正式、生產、開發、測試或沙盒環境（以下合稱為 AI 工具及平台）。適用主體包含本公司全體同仁、派遣及契約人員、及因業務需要而使用本公司 AI 工具及平台之供應商及客戶（以下合稱為本政策利害關係人）。

## 3. 核准使用之 AI 工具及平台

本政策利害關係人處理業務時，應優先使用由本公司數位資訊管理處（DMIS）為企業導入或建置之 AI 工具及平台，以及經 AI 治理委員會核可之 AI 工具及平台。

### 3.1 本公司已導入之企業內部專屬 AI 工具及平台

本政策利害關係人應優先使用下列本公司已導入或建置之 AI 工具及平台。

#### a. Orion AI

Orion AI 為本公司配置之企業級 AI 整合平台，提供模型串接與開發應用。本政策利害關係人應優先使用此平台進行各類生成式 AI 作業。

**b. Microsoft Copilot (企業版)**

Microsoft Copilot (企業版) 係整合於 Microsoft 365 (M365) 生態系之 AI 助手。其使用必須嚴格遵守 M365 之企業資料保護規範，確保商業數據不會被用於訓練公共模型。本政策利害關係人亦應優先使用此工具。

**c. 其他經核可之工具**

本政策利害關係人亦可使用經數位資訊管理處為企業導入、建置之 AI 系統，以及經 AI 治理委員會核可之工具。

**3.2 工具申請流程**

本政策利害關係人需使用核准之標準工具 (如 Orion AI、Microsoft Copilot) 時，應透過本公司 ITSR 流程申請。

**4. 受限使用之 AI 系統**

為確保資料安全與智慧財產權保護，下列類別之 AI 系統與工具受到限制。本政策利害關係人在使用受限工具前應落實 AI 風險自我安全評估或經由 AI 治理委員會審查，且嚴禁將本公司具機敏性之資料輸入受限使用之 AI 系統與工具。

**a. 嵌入式 AI 工具與套件**

用於研發專案之開源或專有套件、向量資料庫等，須符合公司資安與合規要求。具自主執行能力之代理式 AI (Agentic AI/ AI Agents) — 具備自主檢索、程式碼執行、本機檔案存取、瀏覽器與 SaaS 系統操作、或第三方擴充元件安裝執行能力之代理系統 — 因其具高權限操作特性，列為高度風險類別，須通過 DMIS 與 AI 治理委員會之專案審查後始得使用。

**b. 第三方瀏覽器外掛**

具備網頁讀取、資料抓取或自動翻譯功能之 AI 擴充功能，本政策利害關係人於安裝前應由所屬業務單位落實自我安全評估並留存紀錄，必要時得向資安部諮詢。

**c. 特定開源或高風險協作工具**

具自主執行能力之代理式 AI 工具，例如 OpenClaw (含其前身或衍生名稱 Clawdbot、Moltbot)、Claude Cowork 等其他未通過本公司資安審查之代理式

AI 工具，本公司網路將禁止存取，嚴禁私自安裝或串接。若有特殊業務需求，須經 DMIS 安全評估並由 AI 治理委員會核可後方得使用。

**d. 其他**

其餘種類之 AI 工具，或有針對涉及本公司機敏資料與雲端 AI 平台串接、或其他第三方 AI 服務導入，應由單位主管依業務價值評估後核可，並由資安部協同評估技術可行性與合規方案。

**5. 禁止性 AI 系統**

基於《歐盟人工智慧法案》(EU AI Act) 以及本公司資安合規需求，本公司嚴禁開發、部署、使用或銷售以下類型之 AI 系統，包括但不限於：

**a. 未授權之公開版 AI 工具**

嚴禁將本公司機密、客戶機密、研發及技術資料、個人資料、或專案代碼輸入未經審核之公共 AI 平台（如各類個人免費版、未簽署企業保密協議之服務）。

**b. 操縱行為之 AI**

使用潛意識、刻意操縱或欺騙技術，實質性地扭曲個人行為之 AI 系統。

**c. 利用弱點之 AI**

利用因年齡、身心障礙或特定社會經濟狀況所產生之弱點，進而實質扭曲行為之 AI 系統。

**d. 社會評分系統**

根據個人一段時間內之社會行為或性格特質，對其誠信度進行評估或分類，導致其在無關情境中遭受不利對待之 AI 系統。

**e. 未經授權之生物辨識監控**

即時遠端生物辨識監控 於公共場所或不特定多數人可進出之空間，在當事人未主動參與下，對不特定人員進行即時遠端生物辨識（如即時人臉辨識與追蹤）之 AI 系統。以確認特定人員所宣稱身分為唯一目的之一對一生物特徵驗證（如門禁、裝置解鎖、帳號驗證），不屬本款禁止範圍，應依第 6.2 節以高風險級管理。

**f. 透過生物辨識進行人類監控**

侵害性生物辨識應用 (1) 未經告知且無合法依據，以臉部辨識或其他生物特徵對特定個人或群體進行持續追蹤或行為監控；(2) 利用生物特徵資料推斷個人

之種族、政治傾向、工會成員身分、宗教或哲學信仰、性生活或性傾向；(3) 自網際網路或監視錄影畫面無差別擷取臉部影像，以建立或擴充人臉辨識資料庫之 AI 系統。

## **6. AI 系統風險分級架構**

本公司依據 AI 系統之應用情境、資料敏感度、自動化決策影響程度、自主執行權限及對利害關係人權利之潛在衝擊，建立四級風險分級架構，作為差異化治理與資源分配之基礎。

### **6.1 禁止級 (Prohibited)**

「禁止級 (Prohibited)」係指本公司絕對禁止開發、部署、使用或銷售之 AI 系統。凡屬前述「禁止性 AI 系統」所定義之類型皆歸屬此級，任何單位不得提出豁免申請。

### **6.2 高風險級 (High-Risk)**

「高風險級 (High-Risk)」係指可能對人權、安全、健康或財產造成重大不利影響之 AI 系統，包含但不限於：具自主執行系統指令能力之代理式 AI、處理機敏資料之客戶互動型 AI、人臉辨識與生物辨識系統、影響員工權益之 AI、影響客戶或供應商權益之自動化決策。高風險級 AI 系統於部署前須通過 AI 治理委員會專案審查，執行人權影響評估，建立人機協同機制 (Human-in-the-loop, HITL)，留存完整技術文件與審查紀錄。涉及人臉辨識或生物辨識者，另須完成個人資料保護影響評估、事前告知並提供非生物辨識之替代方式 (適用時)，且生物特徵資料應加密儲存並訂定保存期限。

### **6.3 有限風險級 (Limited-Risk)**

「有限風險級 (Limited-Risk)」係指與人互動且須確保使用者知情之 AI 系統，如對外使用之生成式 AI 內容、客服輔助工具、公開於網站之 AI 功能等。此類系統須於互動前或內容中清楚標示其為 AI 生成或 AI 驅動，並提供使用者選擇權或申訴管道。

### **6.4 最小風險級 (Minimal-Risk)**

「最小風險級 (Minimal-Risk)」係指僅供內部使用、不處理機敏資料、不產生對外影響之 AI 工具，如文書編修輔助、程式碼自動補全、內部資料分析等。此類工具應遵循本公司一般資安與合規規範，無需額外專案審查，但應納入 AI 系統庫存清冊統一管理。

### **6.5 風險分級之動態管理**

風險分級之評定由業務單位提出初評，經資安部與 AI 治理委員會覆核後定案。  
當 AI 系統之應用情境、資料類別或技術架構發生重大變更時，應重新評估其風險等級。

## **7. 資料保護與隱私防護**

本公司將資料安全與個人隱私保護置於 AI 治理的核心。所有 AI 工具及平台之設計、開發與營運全生命週期中，皆須遵循適用之資料保護法規。

### **7.1 資料分級管制**

嚴禁將公司機密、產品設計、核心原始碼、金鑰憑證、未公開財務資料、員工個人資料、供應商報價及受管制技術等機敏資料，輸入任何公開版 AI 或未受控之第三方服務。

### **7.2 去識別化處理**

執行單位應確保輸入資料已移除個人識別資訊 (PII)，並主動評估資訊特徵組合後的「重識別風險」，以保護隱私並符合法規要求。

### **7.3 機密金鑰治理**

所有 AI 服務之 API 金鑰與憑證必須儲存於受控之機密管理系統，嚴禁明文存放。金鑰配發以系統帳號為原則，嚴禁個人私自存放於終端設備。

## **8. 透明度、可解釋性與問責**

本公司致力於確保 AI 工具及平台具備透明度與可解釋性，清楚揭露 AI 工具及平台之用途、能力、限制、資料來源與風險，使利害關係人能充分理解 AI 工具及平台之運作方式。所有 AI 工具及平台產出內容在正式發布或執行前，須經過具專業能力之人員進行實質審查，以確保人員保有最終決策權，並落實法律與行政責任之歸屬。

### **8.1 最終審核責任**

AI 生成之所有內容應視為「初稿」或「參考基準」。使用者負有最終校對責任，應透過專業判斷過濾模型幻覺，確保產出之準確性與專業品質；任何產出之商務後果由該作業執行人負責。代理式 AI 之輸出涉及程式碼變更、系統設定變更、資料處理或對外回應之自動化執行時，不得直接作為最終決策或自動執行依據，須經適當人工審核後始得執行。

### **8.2 利害關係人要求**

使用 AI 輔助之研發成果或正式文件，應預先確認符合客戶或利害關係人之合約要求。

## 9. 倫理、公平與偏見管理

本公司承諾確保 AI 工具及平台不會使現有之不平等現象持續惡化或衍生新形式之歧視。

### 9.1 訓練資料多元性與代表性

用於 AI 模型訓練或微調之資料集，應具備多元性與代表性，涵蓋不同人口統計群體之相關特徵，以避免因資料偏差導致歧視性或不公平之模型輸出。

### 9.2 敏感性 AI 功能存取限制

針對可能引發倫理或隱私疑慮之敏感性 AI 應用（如人臉辨識、生物辨識監控、情緒分析等），實施嚴格之存取控制。

### 9.3 AI 倫理專責窗口

本公司規劃設立 AI 倫理專責窗口，作為所有 AI 倫理相關詢問之第一聯絡窗口。其職責包含提供倫理諮詢與指導、統籌高風險 AI 使用案例之審查、協調定期 AI 模型公平性評估與偏見稽核。

## 10. 環境永續與生態足跡管理

本公司承諾在 AI 工具及平台之開發、部署與使用過程中，遵循公司對環境管理之承諾，於 AI 解決方案之整個生命週期中，考量減碳與效率表現。本公司要求自有或第三方之 AI 資料中心與模型具備低生態足跡，並持續監測與改善其環境影響，其考量因素包含但不限於：綠色設計、基礎架構最佳化、供應鏈要求、硬體生命週期、監測與改善。

### 10.1 生態足跡監測指標

AI 治理委員會定期審查 AI 資料中心與模型之能源使用、水資源消耗及碳排放強度等量化指標與改善進度。

## 11. 風險管理與安全護欄

本公司於 AI 工具及平台之開發與維運過程中，建立多層次的安全防護措施與風險管理機制。

### 11.1 安全護欄機制

AI 開發團隊應於 AI 介面部署動態過濾機制，即時攔截惡意指令，主動防禦系統漏洞。具備外部工具調用能力之代理式 AI 工具應實施最小權限原則，並落實執行控管。未具備上述控管能力之代理式 AI 工具，不得於公司網路或設備中使用。

## 11.2 提示詞工程安全

開發人員應實施防禦性提示詞設計，包含提示詞中禁止包含硬編碼之憑證、金鑰或具高度識別性之系統架構細節，以降低「提示詞洩漏」與「指令注入攻擊」之風險性。針對要求高度準確與一致性之任務，開發者應調校參數（如將 Temperature 趨近於 0），以極大化輸出之確定性。

## 11.3 緊急應變

當公司 AI 工具及平台經辨識發生重大資安漏洞、敏感資料外洩、或產生具法律違規風險之內容時，資安部具有最高決策權啟動「緊急強制停機機制」，要求使用單位執行緊急停機或服務隔離，以即時止損並確保合規。若 RAG 知識庫遭受資料投毒或惡意污染，應立即清空受影響之索引，並在排除污染源後，重新執行資料清洗與匯入作業。

## 12. AI 決策申訴機制

本公司規劃建立 AI 決策申訴機制，適用於使用者或受 AI 驅動決策影響之第三方，對 AI 系統所做出之決策或產出結果存有異議時提出申訴。

### 12.1 申訴處理流程

申訴案件由 AI 倫理專責窗口受理並協調處理。處理程序包括：確認受理並提供案件追蹤機制；評估申訴之合理性、嚴重程度與影響範圍，必要時暫停相關 AI 系統之運作；協同業務單位與資安部調查 AI 決策依據、資料輸入及模型行為；以書面回覆申訴人調查結果與改善措施。若申訴人不服處理結果，得向 AI 治理委員會提起覆審。具體申訴受理條件、處理時程及作業程序，由 AI 治理委員會另定之。

### 12.2 紀錄與報告

所有申訴案件之受理、調查、決議與改善措施應詳實記錄，並定期彙整交由 AI 治理委員會審查。申訴統計數據應作為 AI 治理審查之參考指標。

### 12.3 通報信箱

官方通報信箱：[security.issues@wnc.com.tw](mailto:security.issues@wnc.com.tw)

## 13. 員工教育訓練與安全意識

本公司透過系統化教育訓練與持續性宣導，建立全員負責任使用 AI 之組織文化。新進同仁應於入職培訓期間完成 AI 安全課程，了解公司之 AI 使用規範與安全作業標準，於正式投入業務前具備正確工具使用觀念與風險防範能力；資安部另針對新型態 AI 威

脅每年發布資安宣導，並納入定期教育資源，以持續提升全員對於 AI 風險之防禦韌性。

#### **14. 法規遵循與治理標準**

本公司 AI 治理架構遵循國際與國內之相關法規與標準，確保 AI 應用之合法性、合規性與國際接軌。

#### **15. 政策審查與修訂**

本政策經本公司資訊長（CIO）審查通過，並定期檢視修訂，以確保公司 AI 治理方向符合利害關係人期待及各項標準之要求。AI 治理委員會每年進行定期治理審查，檢視法規環境變化、新興風險議題與執行成效。