大江生醫集團
負責任人工智慧政策
TCI Group — Responsible Artificial Intelligence Policy

一、政策目的

1. Purpose

大江生醫集團（以下簡稱「本公司」）運用人工智慧（AI）技術於研發探勘、功效驗證、專利與法規審查、流程自動化、知識管理及營運決策支援。為兼顧創新、風險治理與利害關係人權益，本公司依負責任人工智慧原則建立人工智慧管理體系（AIMS），並參照 ISO/IEC 42001:2023，對 AI 之開發、採購、導入、使用、監督、重大變更及退役進行治理。

TCI Group (the "Company") applies artificial intelligence (AI) to research discovery, efficacy verification, patent and regulatory review, process automation, knowledge management, and operational decision support. To balance innovation, risk governance, and stakeholder interests, the Company maintains an Artificial Intelligence Management System (AIMS), developed with reference to ISO/IEC 42001:2023, governing the development, procurement, deployment, use, monitoring, material change, and retirement of AI systems.

二、適用範圍

2. Scope

本政策適用於本公司及所有合併報表子公司之全體員工、約聘人員、顧問及代表本公司執行業務之人員，並涵蓋自行開發、委外客製、商用套裝軟體、雲端 AI 服務（SaaS/API）、基礎模型、開源模型、RAG、AI Agent 及其他具人工智慧功能之系統或服務。提供 AI 服務、模型、資料處理或相關技術之供應商與合作夥伴，應依契約及風險程度遵循適用之治理要求。

This Policy applies to personnel across the Company and its consolidated subsidiaries, including employees, contractors, consultants, and persons acting on behalf of the Company. It covers internally developed AI, outsourced solutions, commercial software, cloud AI services (SaaS/API), foundation models, open-source models, retrieval-augmented generation (RAG), AI agents, and other AI-enabled systems or services. Suppliers and partners providing AI services, models, data processing, or related technologies are subject to applicable governance requirements based on contract and risk level.

三、政策承諾

3. Policy Commitments

本公司透過本政策，承諾：

- 遵循並持續滿足適用之法令、法規、契約及利害關係人之相關要求。
- Meeting applicable legal, regulatory, contractual, and stakeholder requirements relevant to AI systems.
- 依負責任人工智慧原則——包括風險管理、資料治理、資安、公平性、人類監督、透明度與問責——發展與使用 AI。
- Developing and using AI in accordance with responsible AI principles, including risk management, data governance, security, fairness, human oversight, transparency, and accountability.
- 持續改善本公司之人工智慧管理體系（AIMS）及其有效性。
- Continually improving the effectiveness of the Company's Artificial Intelligence Management System (AIMS).

- 定期檢視並適時更新本政策，以反映法規、技術與風險情勢之變化。
- Periodically reviewing and updating this Policy to reflect changes in regulation, technology, and the risk landscape.

四、政策原則與核心管控

4. Policy Principles and Core Controls

4.1 AI 風險、機會與治理目標

4.1 AI Risk, Opportunity and Objectives

本公司採風險導向方式管理 AI，依系統用途、資料敏感度、自主程度、業務關鍵性、可能影響之個人與利害關係人、法規要求及合理可預見之誤用情境，進行風險識別、分析、評估與處理。對重大風險應指定責任人、處理措施與核准權責，並記錄剩餘風險之評估與接受。

The Company manages AI using a risk-based approach. Risks are identified, analysed, evaluated, and treated with consideration of system purpose, data sensitivity, autonomy, business criticality, potentially affected individuals and stakeholders, legal requirements, and reasonably foreseeable misuse. Material risks shall have assigned owners, treatment actions, approval authorities, and documented evaluation and acceptance of residual risk.

本公司依適用要求、風險程度與營運需求建立可衡量之 AI 治理目標及績效指標，定期監督其達成情形，並將風險降低、品質提升、創新效益與永續價值納入持續改善。

The Company establishes measurable AI governance objectives and performance indicators based on applicable requirements, risk level, and business needs. Progress is monitored periodically, with risk reduction, quality improvement, innovation benefits, and sustainability value incorporated into continual improvement.

4.2 資料治理、品質與隱私保護

4.2 Data Governance, Quality and Privacy

用於 AI 訓練、微調、測試或 RAG 之資料，應具有合法且可追溯之來源，並依用途實施適當之完整性、準確性、代表性、時效性與資料品質檢核。對資料投毒、未授權資料混入、標註錯誤及其他可能導致模型或決策偏差之風險，應採取相應控制。

Data used for AI training, fine-tuning, testing, or RAG shall have lawful and traceable provenance and be subject to controls appropriate to its purpose, including completeness, accuracy, representativeness, timeliness, and data quality. Controls shall address risks such as data poisoning, unauthorised data inclusion, labelling errors, and other conditions that may distort model or decision outcomes.

AI 系統僅得於核准之流程、目的與授權範圍內存取及處理資料，並遵循最小權限、資料最小化及用途限制原則。涉及人體臨床資料、基因資訊、客戶機密、營業秘密或個人資料之應用，應遵循本公司隱私與資料治理要求及營運所在地之適用法令，並依風險採取去識別化、匿名化、假名化、加密或其他適當保護措施。

AI systems may access and process data only within approved workflows, purposes, and authorisation boundaries, following least privilege, data minimisation, and purpose limitation principles. Applications involving human clinical data, genomic information, customer confidential information, trade secrets, or personal data shall comply with Company privacy and data governance requirements and applicable laws in operating jurisdictions, using de-identification, anonymisation, pseudonymisation, encryption, or other appropriate safeguards according to risk.

4.3 AI 資訊安全、系統韌性與追溯性

4.3 AI Security, System Resilience and Traceability

AI 相關風險應納入本公司資訊安全管理及事件應變機制。針對提示詞注入、敏感資料外洩、越權存取、模型或資料竊取、對抗性攻擊、供應鏈風險及 AI Agent 非預期行動等威脅，應依風險實施適

當之身分鑑別、權限控管、輸入輸出防護、內容與工具存取限制、異常偵測、測試及安全閘道。
AI-related risks are integrated into the Company's information security and incident response processes. Appropriate controls shall be applied according to risk to address threats such as prompt injection, sensitive data leakage, unauthorised access, model or data theft, adversarial attacks, supply-chain risks, and unintended AI-agent actions, including authentication, access control, input/output protection, restrictions on content and tool access, anomaly detection, testing, and security gateways.

本公司依 AI 系統之風險等級、法令、隱私及營運需求建立適當之日誌、追溯性及完整性保護機制。高風險或關鍵 AI 系統應保留足以支持事件調查、責任追溯、合規查核及模型治理之必要紀錄，並依資料最小化及保存期限要求管理。對關鍵 AI 服務應規劃合理之降級、替代或人工接管機制，以維持營運韌性。
The Company maintains logging, traceability, and integrity protections appropriate to AI system risk, legal, privacy, and operational requirements. High-risk or critical AI systems shall retain records sufficient to support incident investigation, accountability, compliance review, and model governance, subject to data minimisation and retention requirements. Critical AI services shall include reasonable degradation, fallback, or human takeover arrangements to support operational resilience.

4.4 公平性、偏誤與品質管理
4.4 Fairness, Bias and Quality Management

本公司對重要 AI 模型、設定、提示工程、知識來源、微調資料集及重大變更維持適當之版本與變更管理，並依系統用途監控輸出品質、資料漂移、概念漂移、異常、不一致或可能造成不公平影響之結果。
The Company maintains appropriate version and change management for material AI models, configurations, prompt engineering, knowledge sources, fine-tuning datasets, and significant changes. Output quality, data drift, concept drift, anomalies, inconsistencies, and potentially unfair impacts are monitored according to system purpose.

經辨識之偏誤或品質問題，應依其嚴重度與影響進行調查及風險處理，可採取資料改善、模型或提示調整、限制使用、增加人工覆核、風險接受或停止使用等措施，並保留必要之評估與驗證紀錄。
Identified bias or quality issues shall be investigated and treated based on severity and impact. Actions may include data improvement, model or prompt adjustment, use restrictions, enhanced human review, risk acceptance, or suspension of use, with appropriate assessment and validation records retained.

4.5 人類監督與介入
4.5 Human Oversight and Intervention

本公司依 AI 系統之風險、用途、自主程度與可能影響配置適當之人類監督。涉及重大權益、法規、安全、研發結論、財務或其他高風險事項者，AI 應作為輔助工具，最終決策、核准或對外承諾須由具權責及適當專業能力之人員執行。低風險且經核准之自動化流程，得於既定控制與監控條件下自動執行。
The Company applies human oversight proportionate to AI system risk, purpose, autonomy, and potential impact. For matters involving significant rights, regulatory obligations, safety, R&D conclusions, finance, or other high-risk contexts, AI shall serve as a support tool and final decisions, approvals, or external commitments must be made by authorised and appropriately competent personnel. Approved low-risk automation may operate automatically within defined controls and monitoring conditions.

授權人員應能於必要時停止、介入、覆寫、修正或退回 AI 建議或行動。AI 介面或相關文件應依技術特性提供適當之限制、不確定性、驗證狀態、資料來源或其他可靠性資訊；於技術上適用且經驗證時，得提供準確率、可信度或其他效能指標。
Authorised personnel shall be able, where necessary, to stop, intervene in, override, amend, or reject AI

recommendations or actions. Interfaces or related documentation shall provide appropriate information on limitations, uncertainty, validation status, data sources, or other reliability indicators based on technical characteristics; where technically applicable and validated, accuracy, confidence, or other performance metrics may be provided.

4.6 透明度、可解釋性與利害關係人溝通
4.6 Transparency, Explainability and Stakeholder Communication

AI 系統應依其風險與使用情境提供適當之透明度資訊，包括系統用途、輸出之主要依據或來源、重要限制、適用範圍、必要之人類監督及使用注意事項，使使用者能合理理解並適當使用 AI 輸出。

AI systems shall provide transparency information appropriate to their risk and context of use, including system purpose, principal basis or sources for outputs, material limitations, intended scope, required human oversight, and usage considerations, enabling users to understand and appropriately use AI outputs.

對外提供、公開發布或直接影響利害關係人之 AI 內容或互動，應依適用法令、客戶契約及避免重大誤解之需要，採取適當之 AI 使用揭露或標示。本公司提供適當之意見反映、申訴或人工複查管道，使受到 AI 實質影響之利害關係人得提出疑義並獲得合理處理。

AI-generated or AI-mediated content and interactions that are externally provided, publicly released, or directly affect stakeholders shall include appropriate AI disclosure or labelling where required by applicable law, customer contract, or necessary to avoid material misunderstanding. The Company provides appropriate feedback, complaint, or human-review channels for stakeholders materially affected by AI to raise concerns and receive reasonable handling.

4.7 AI 系統生命週期與衝擊評估
4.7 AI System Life Cycle and Impact Assessment

本公司對 AI 系統實施生命週期治理，涵蓋需求與用途定義、可行性、設計、資料整備、開發或採購、驗證與確認、試行、部署、監控、重大變更及退役。控制要求應依風險程度與系統角色（如自建、採購、平台、基礎模型或第三方服務）適度調整。

The Company governs AI systems across their life cycle, including requirements and intended use, feasibility, design, data preparation, development or procurement, verification and validation, pilot testing, deployment, monitoring, material change, and retirement. Controls shall be proportionate to risk and adapted to the Company's role in the AI system, such as developer, procurer, platform operator, foundation-model user, or third-party service consumer.

於專案立項、重要採購或部署前，應依風險執行 AI 系統衝擊評估（AI System Impact Assessment, AI SIA），考量對人身安全、權益、隱私、公平性、資訊安全、智慧財產、法令遵循、環境與企業商譽之潛在正負面影響，以及合理可預見之誤用。重大用途變更、模型或資料重大更新、法規變更或重大事件發生時，應重新評估。

Before project approval, material procurement, or deployment, an AI System Impact Assessment (AI SIA) shall be performed according to risk, considering potential positive and negative impacts on safety, rights, privacy, fairness, cybersecurity, intellectual property, legal compliance, the environment, corporate reputation, and reasonably foreseeable misuse. Reassessment shall occur when there are material changes in use, model or data, applicable regulations, or significant incidents.

當 AI 系統無法維持可接受之風險、品質、法規符合性、安全性或服務可持續性時，應依既定程序限制、暫停、替換或退役，並妥善處理資料、帳號、介接、模型與必要紀錄。

When an AI system can no longer maintain acceptable risk, quality, compliance, security, or service continuity, it shall be restricted, suspended, replaced, or retired under defined procedures, with appropriate handling of data, accounts, integrations, models, and required records.

4.8 AI 供應鏈與第三方管理
4.8 AI Supply Chain and Third-Party Management

人員不得使用未經本公司核准之免費版、個人版或其他 AI 工具處理公司機密、研發資料、配方、專利草案、受管制資料或個人資料。經核准之企業 AI 服務，應依資料敏感度與風險，透過契約與技術控制管理資料留存、模型訓練使用、存取權限及其他資料處理條件。

Personnel shall not use unapproved free-tier, personal-tier, or other AI tools to process Company confidential information, R&D data, formulations, patent drafts, regulated data, or personal data. Approved enterprise AI services shall use contractual and technical controls, proportionate to data sensitivity and risk, to govern data retention, use for model training, access rights, and other processing conditions.

採購商業 AI、基礎模型 API、開源模型或其他第三方 AI 能力時，應依風險執行供應商盡職調查，必要時涵蓋資訊安全、隱私、資料所在地、次處理者、模型與服務重大變更、智慧財產、事件通報、服務持續性、法規遵循、資料刪除與退出機制。

When procuring commercial AI, foundation-model APIs, open-source models, or other third-party AI capabilities, supplier due diligence shall be performed according to risk and may cover cybersecurity, privacy, data location, subprocessors, material model and service changes, intellectual property, incident notification, service continuity, legal compliance, data deletion, and exit arrangements.

4.9 應用邊界與禁止用途
4.9 Boundaries of AI Use and Prohibited Uses

AI 不得在缺乏適當人類監督下單獨作成下列重大決定或最終核准：

AI shall not autonomously make the following material decisions or final approvals without appropriate human oversight:

- 人事重大決策，包括聘僱甄選、績效考核、職等晉升、懲戒與解僱之最終判定。
- Final material employment decisions, including hiring selection, performance evaluation, promotion, disciplinary action, and termination.
- 產品安全性、功效宣稱及各國衛生主管機關法規符合性之最終核可。
- Final approval of product safety, efficacy claims, and compliance with health authority requirements.
- 臨床前與人體臨床試驗資料之最終判讀與研究結論。
- Final interpretation and research conclusions concerning preclinical or human clinical trial data.
- 法定財務報表、重大內控判斷及重大資金核決之最終核可。
- Final approval of statutory financial reporting, material internal-control judgments, and material capital commitments.
- 對外具法律拘束力之重大合約、專利申請或公司承諾文件之最終核可。
- Final approval of material legally binding agreements, patent filings, or corporate commitments.

本公司禁止開發、採購、整合或部署違反適用法令或本公司倫理原則之 AI 實踐，包括不當操縱、利用特定弱勢族群之脆弱性、違法社會評分、未經法令授權之生物特徵監控，以及其他於適用法域被明確禁止之 AI 用途。

The Company prohibits developing, procuring, integrating, or deploying AI practices that violate applicable law or Company ethical principles, including improper manipulation, exploitation of the vulnerabilities of specific groups, unlawful social scoring, biometric surveillance without legal authorisation, and other AI uses expressly prohibited in applicable jurisdictions.

4.10 智慧財產權與法律合規
4.10 Intellectual Property and Legal Compliance

AI 之開發、採購與使用應遵循適用之專利、著作權、營業秘密、資料使用權、契約義務及其他法律要求。對涉及研發成果、產品設計、配方、專利申請、重要商業成果或對外發布之 AI 產出，應依風險採取適當之來源、授權、相似度或侵權風險檢查；高風險案件應提交法務、智財或其他權責單位複核。

AI development, procurement, and use shall comply with applicable patent, copyright, trade secret, data-use rights, contractual obligations, and other legal requirements. AI outputs involving R&D results, product design, formulations, patent filings, material commercial work products, or external publication shall undergo source, licensing, similarity, or infringement-risk checks appropriate to risk; high-risk cases shall be escalated to Legal, Intellectual Property, or other responsible functions for review.

對 AI 產出之權利歸屬、可保護性與對外使用條件，應依適用法令、契約及本公司規範確認，並避免將未經授權之第三方機密或受保護內容納入 AI 系統或公開成果。

Ownership, protectability, and conditions for external use of AI outputs shall be determined under applicable law, contract, and Company requirements. Unauthorised third-party confidential or protected content shall not be incorporated into AI systems or public deliverables.

涉及支援 GMP／GxP 相關流程（如研發、品質、法規審查）之 AI 系統，應納入本公司電腦化系統驗證（CSV/CSA）及變更管理程序，確保其可靠性、可追溯性與法規符合性。本公司亦持續關注台灣、美國、中國及東南亞等主要營運地之 AI 專法與監理發展，並適時調整治理作法。

AI systems supporting GMP/GxP-related processes (such as R&D, quality, and regulatory review) shall be subject to the Company's computerised system validation (CSV/CSA) and change management procedures to ensure reliability, traceability, and regulatory compliance. The Company also monitors AI-specific regulatory developments in Taiwan, the United States, China, Southeast Asia, and other key operating jurisdictions, and adjusts its governance practices accordingly.

4.11 綠色 AI 與環境永續

4.11 Green AI and Environmental Sustainability

本公司依重大性原則，在技術可行且可合理取得資料之範圍內，評估 AI 訓練、微調、推論及雲端運算資源之能源使用與環境影響，並逐步納入集團永續及溫室氣體管理機制。

Applying a materiality principle, the Company evaluates energy use and environmental impacts associated with AI training, fine-tuning, inference, and cloud computing where technically feasible and data can reasonably be obtained, progressively integrating relevant impacts into Group sustainability and greenhouse-gas management.

在品質、資安、法規與服務條件可接受之前提下，本公司優先考量具能源效率、碳管理與再生能源措施之雲端或 AI 服務供應商，並持續提升模型、工作負載與資源使用效率。

Subject to acceptable quality, security, regulatory, and service conditions, the Company gives preference to cloud or AI service providers with energy-efficiency, carbon-management, and renewable-energy practices and continually seeks to improve the efficiency of models, workloads, and resource use.

五、治理架構、組織權責與持續改善

5. Governance Structure, Roles and Continual Improvement

5.1 治理架構與責任

5.1 Governance and Accountability

本公司由高階管理階層支持並監督 AI 治理，設置跨職能之 AI 治理委員會（AI Governance Committee），成員涵蓋資訊科技、資訊安全、研發、法務／智財、法規／品質、人力資源及其他必要職能，負責審議 AI 治理方向、重大風險、高風險應用及跨部門議題。

The Company's AI governance is supported and overseen by executive management through a cross-functional AI Governance Committee comprising Information Technology, Information Security, R&D,

Legal/IP, Regulatory/Quality, Human Resources, and other relevant functions. The Committee reviews AI governance direction, material risks, high-risk applications, and cross-functional issues.

導入或使用 AI 之業務／研發單位主管對其業務成果、適法性與風險承擔最終管理責任；資訊科技及相關治理職能負責建立與維護 AI 系統資產清冊（AI Inventory）、技術與治理標準、風險協調及定期檢視。各項角色與責任應於內部程序中明確界定並避免責任真空。

Business or R&D leaders deploying or using AI retain management accountability for business outcomes, lawful use, and risk ownership. Information Technology and relevant governance functions maintain the AI system inventory, technical and governance standards, risk coordination, and periodic review. Roles and responsibilities shall be clearly defined in internal procedures to avoid accountability gaps.

本 AIMS 與本公司既有資訊安全與隱私管理體系（如 ISO 27001、ISO 27701）整合運作，共用治理架構、風險管理程序及稽核機制，以避免重複建置並強化整體治理一致性。

The AIMS operates in an integrated manner with the Company's existing information security and privacy management systems (such as ISO 27001 and ISO 27701), sharing governance structures, risk management processes, and audit mechanisms to avoid duplication and strengthen overall governance consistency.

5.2 能力、意識與溝通

5.2 Competence, Awareness and Communication

本公司依人員在 AI 系統之開發、採購、設定、使用、監督、稽核及核准等角色，提供相應之 AI 治理、資訊安全、隱私、倫理、資料品質與法令遵循教育訓練，確保相關人員具備履行職責所需之能力與風險意識。

The Company provides role-appropriate training on AI governance, cybersecurity, privacy, ethics, data quality, and legal compliance for personnel involved in AI development, procurement, configuration, use, oversight, audit, and approval, ensuring that relevant personnel have the competence and risk awareness required for their responsibilities.

本公司建立適當之內外部 AI 治理溝通機制，對重大政策、風險、事件、系統變更與使用要求，依權責及需要進行通報、協調與溝通。

The Company maintains appropriate internal and external AI governance communication mechanisms. Material policies, risks, incidents, system changes, and usage requirements are communicated and coordinated according to responsibility and need.

5.3 績效評估、內部稽核、管理審查與矯正改善

5.3 Performance Evaluation, Internal Audit, Management Review and Corrective Improvement

本公司定期監督 AIMS 與 AI 控制措施之績效及有效性，至少每年向 AI 治理委員會及高階管理階層（或董事會）提出治理報告，內容得包括 AI Inventory、風險與衝擊評估、治理目標達成情形、重大 AI 事件、資安與個資事件、品質／偏誤議題、供應商風險、例外事項及改善措施。

The Company periodically monitors the performance and effectiveness of the AIMS and AI controls. At least annually, a governance report is provided to the AI Governance Committee and executive management (or the Board of Directors), which may include the AI inventory, risk and impact assessments, progress against governance objectives, material AI incidents, cybersecurity and privacy events, quality/bias issues, supplier risks, exceptions, and improvement actions.

本公司依既定週期執行 AIMS 內部稽核與管理審查，以確認管理體系之適切性、充分性與有效性。對不符合事項、重大 AI 事件或控制失效，應執行原因分析、矯正措施、責任追蹤及有效性驗證，並作為持續改善之依據。

The Company conducts AIMS internal audits and management reviews on a defined cycle to confirm the system's suitability, adequacy, and effectiveness. Nonconformities, material AI incidents, or control failures shall be subject to root-cause analysis, corrective action, accountability tracking, and

effectiveness verification, informing continual improvement.

5.4 政策核准、檢視與維護

5.4 Policy Approval, Review and Maintenance

本政策經董事會核准後生效，重大修訂亦循適當之核准程序。本政策至少每年檢視一次；於重大法規演進、AI 技術或業務模式重大變更、重大安全／倫理事件、風險情勢明顯改變或管理審查認定必要時，應啟動滾動檢視與修訂。

This Policy becomes effective upon Board approval, and material amendments shall follow the appropriate approval process. The Policy is reviewed at least annually and shall be reviewed and updated when required by material regulatory developments, significant changes in AI technology or business models, major safety or ethical incidents, meaningful changes in the risk landscape, or management review.