人工智慧倫理與治理政策

Artificial Intelligence Ethics and Governance Policy

一　政策目的 Policy Purpose

本公司承諾以安全、負責、可信賴且符合法令與倫理之方式導入、開發、採購、使用及管理人工智慧，兼顧創新、個人權利、資訊安全、營業秘密與永續發展。

The Company is committed to introducing, developing, procuring, using, and managing artificial intelligence in a safe, responsible, trustworthy, lawful, and ethical manner, while balancing innovation, individual rights, information security, trade secrets, and sustainable development.

二　適用範圍 Scope of Application

本政策適用於本公司及子公司之全體員工與營運活動，並期望供應商、外包商、承攬商、合作夥伴及其他價值鏈成員共同重視並遵循本政策精神。

This Policy applies to all employees and operating activities of the Company and its subsidiaries. The Company also expects suppliers, outsourced service providers, contractors, business partners, and other members of the value chain to recognize and observe the principles of this Policy.

三　政策承諾 Policy Commitment

明基材料承諾，於使用及管理人工智慧過程中，遵循以下國際規範及原則：

BenQ Materials is committed to observing the following international standards and principles in the use and management of artificial intelligence:

1.　人工智慧治理架構與組織承諾

AI Governance Framework and Organizational Commitment

建立明確之人工智慧治理架構、角色職責與監督機制，依風險基礎管理人工智慧之導入與使用，確保相關決策符合本政策、內部規範及營運需求。

Establish a clear artificial intelligence governance framework, roles and responsibilities, and oversight mechanisms, and manage the introduction and use of artificial intelligence on a risk-based basis to ensure that relevant decisions comply with this Policy, internal requirements, and operational needs.

2. 法令遵循與責任問責

Legal Compliance and Accountability

遵循個人資料保護、資訊安全、智慧財產、營業秘密、消費者與客戶權益保護、人權及人工智慧相關法令；明確界定責任歸屬，落實審查、紀錄與問責。

Comply with laws and regulations relating to personal data protection, information security, intellectual property, trade secrets, protection of consumer and customer rights and interests, human rights, and artificial intelligence; clearly define accountability and implement review, recordkeeping, and accountability mechanisms.

3. 風險為基礎之治理

Risk-Based Governance

依人工智慧用途、資料類型、影響範圍與可能風險進行評估，針對較高風險之應用採取較嚴謹的核准、測試、監控及改善措施。

Assess artificial intelligence based on its intended use, data types, scope of impact, and potential risks, and apply more stringent approval, testing, monitoring, and improvement measures to higher-risk applications.

4. 生命週期控管

Lifecycle Controls

於規劃、開發、採購、測試、上線、使用、監控、變更及退場等階段，建立必要控管，確保人工智慧系統持續符合安全、合規、可靠與可管理之要求。

Establish necessary controls throughout the planning, development, procurement, testing, deployment, use, monitoring, change, and retirement stages to ensure that artificial intelligence systems continuously meet requirements for safety, compliance, reliability, and manageability.

5. 人類自主與適當干預

Human Autonomy and Appropriate Intervention

涉及重大權益、關鍵決策或高風險情境時，應保留人為監督、判斷、覆核與介入機制，避免人工智慧取代必要之專業責任與管理責任。

Where significant rights or interests, critical decisions, or high-risk situations are involved, human oversight, judgment, review, and intervention mechanisms shall be retained to prevent artificial intelligence from replacing necessary professional and managerial responsibilities.

6. 公平性與無歧視

Fairness and Non-Discrimination

降低資料、模型與演算法偏見，避免對特定個人或群體造成不合理差別待遇；必要時持續監測、評估並修正偏差。

Reduce bias in data, models, and algorithms and avoid unreasonable differential treatment of specific individuals or groups; where necessary, continuously monitor, assess, and correct bias.

7. 資料治理、隱私與權益保護

Data Governance, Privacy and Rights Protection

資料之蒐集、處理、利用與保存應具合法性、必要性與最小化原則，妥善保護個人資料、客戶資料、機密資訊、營業秘密及智慧財產，並尊重使用者或客戶之選擇與權益。

The collection, processing, use, and retention of data shall comply with the principles of lawfulness, necessity, and minimization. Personal data, customer data, confidential information, trade secrets, and intellectual property shall be appropriately protected, and the choices and rights and interests of users or customers shall be respected.

8. 資訊安全與系統穩健

Information Security and System Robustness

建立適當之資訊安全、存取控管、資料保護、備援及監控措施，降低未授權存取、資料外洩、提示注入、模型濫用、服務中斷及其他安全威脅。

Establish appropriate information security, access control, data protection, backup, and monitoring measures to reduce unauthorized access, data leakage, prompt injection, model misuse, service disruption, and other security threats.

9. 透明性與可解釋性

Transparency and Explainability

依風險程度與技術可行性，揭露人工智慧之使用情境、限制、可能影響及必要資訊，使相關人員、使用者或利害關係人能合理理解其運作與輸出。

Based on the level of risk and technical feasibility, disclose the use scenarios, limitations, potential impacts, and necessary information relating to artificial intelligence so that relevant personnel, users, or stakeholders can reasonably understand its operation and

outputs.

10. 生成式人工智慧使用管理

Generative AI Use Management

使用生成式人工智慧時，應審慎管理輸入資料與輸出內容；不得輸入未經允許之個人資料、機密、營業秘密或受限制資訊，輸出內容不得未經適當覆核即作為重大決策或對外正式內容。

When using generative artificial intelligence, input data and output content shall be managed with due care. Personal data, confidential information, trade secrets, or restricted information shall not be entered without authorization, and outputs shall not be used for major decisions or as formal external content without appropriate review.

11. 禁止操縱與不當行為

Prohibition of Manipulation and Improper Conduct

不得將人工智慧用於非法、欺騙、操縱、侵犯權利、未經授權監控、社會評分、規避管制或其他違反公司倫理、法令與內部規範之用途。

Artificial intelligence shall not be used for illegal, deceptive, manipulative, rights-infringing, unauthorized surveillance, social scoring, regulatory evasion, or other purposes that violate Company ethics, laws and regulations, or internal requirements.

12. 供應鏈與第三方管理

Supply Chain and Third-Party Management

導入或委託第三方提供人工智慧系統、模型、平台或服務時，應評估其資安、資料保護、法遵、服務穩定、風險管理及責任分工，並透過契約或管理措施加以規範。

When introducing or engaging third parties to provide artificial intelligence systems, models, platforms, or services, their information security, data protection, legal compliance, service

stability, risk management, and allocation of responsibilities shall be assessed and governed through contractual or management measures.

13. 利害關係人參與與溝通

Stakeholder Engagement and Communication

建立適當溝通、回饋、申訴或救濟管道，將客戶、使用者、員工、合作夥伴及其他利害關係人之需求與疑慮納入人工智慧治理考量。

Establish appropriate communication, feedback, grievance, or remedy channels, and incorporate the needs and concerns of customers, users, employees, business partners, and other stakeholders into artificial intelligence governance considerations.

14. 事件處理與持續改善

Incident Handling and Continuous Improvement

若人工智慧系統發生異常、資安事件、錯誤輸出或可能侵害權益之情形，應依事件處理程序進行通報、處置、補救、紀錄與改善。

If an artificial intelligence system experiences an anomaly, information security incident, erroneous output, or a situation that may infringe rights or interests, reporting, response, remediation, recordkeeping, and improvement shall be carried out in accordance with the incident handling procedures.

15. 教育訓練與能力建立

Education, Training and Capability Building

提供必要之教育訓練及宣導，使員工具備人工智慧風險意識、合規要求、安全使用方法及允許與禁止行為之基本認知。

Provide necessary education, training, and awareness activities so that employees have a

basic understanding of artificial intelligence risks, compliance requirements, safe-use practices, and permitted and prohibited conduct.

16. 永續發展與環境責任

Sustainable Development and Environmental Responsibility

人工智慧之導入與應用應兼顧環境、社會與治理面向，促進資源有效使用，降低不必要之環境負荷，並關注對員工工作型態與權益之影響。

The introduction and application of artificial intelligence shall take environmental, social, and governance aspects into consideration, promote the efficient use of resources, reduce unnecessary environmental burdens, and consider impacts on employees' working patterns and rights and interests.

17. 定期檢視與政策維護

Periodic Review and Policy Maintenance

本公司應定期檢視人工智慧應用情形、風險控管與本政策適切性，並因應法令、技術、營運及外部環境變化適時調整。The Company shall periodically review the application of artificial intelligence, risk controls, and the appropriateness of this Policy, and make timely adjustments in response to changes in laws and regulations, technology, operations, and the external environment.

本政策經董事會核定後施行，修正時亦同。This Policy shall take effect upon approval by the Board of Directors. The same shall apply to any amendments.

本政策訂定於中華民國一一五年七月三十日。

This Policy was established on July 30, 2026

董事長兼執行長 Chairman and Chief Executive Officer 陳建志