



CIMB Statement on Responsible Artificial Intelligence (AI)

August 2026

Version 1.0

1. Purpose & Framework Alignment

As a responsible bank, we seek to continuously strengthen our approach to the responsible use of AI. This Statement sets out the principles that guide us today and the practices we seek to progressively embed across the Group.

The application of these principles is intended to be risk-based and proportionate, taking into account the nature, purpose, complexity, materiality and impact of each AI use case, as well as CIMB's existing governance, risk management and control processes

At CIMB, we seek to use Artificial Intelligence (AI) responsibly to support financial services, drive innovation and contribute to sustainable development. We recognise that as AI continues to evolve, its use should be guided by ethical principles, human oversight and appropriate governance controls.

Our Board-approved Group AI Governance Framework aims to guide our AI activities in alignment with our corporate values, regional standards including Malaysia's National Guidelines on AI Governance and Ethics (AIGE), Bank Negara Malaysia (BNM) guidance on AI, the Monetary Authority of Singapore (MAS) Fairness, Ethics, Accountability and Transparency (FEAT) principles and applicable data protection laws.

2. AI Governance and Oversight

AI and data governance are structured under CIMB's Enterprise-Wide Risk Management Framework (EWRMF) across a Three Lines of Defence (3 LOD) model.

i. Board and Senior Management Oversight

The Board provides oversight of AI governance through the approval of the Group AI Governance Framework and by ensuring appropriate accountabilities are in place for AI governance and risk management activities.

Senior Management and the Group Data & AI Governance Committee (GDAIGC) support implementation through the review of AI risk controls, lifecycle decision-making and escalation of material AI-related matters to the relevant committees where appropriate.

ii. AI Risk Integration

AI-related vulnerabilities are mapped into existing risk taxonomies, specifically Model, Technology, Data Management, Reputational, Operational and Shariah Risk, with controls intended to be proportionate to model complexity and business impact.

iii. Model and Application Lifecycle Management

AI models, applications and bots are subject to lifecycle management, progressively incorporating quality assurance activities from ideation through pre-implementation testing to decommissioning.

iv. Training of employees on the ethical use and/or security of AI

Building upon our existing data privacy, ethics and cybersecurity awareness programmes, CIMB continues to enhance relevant employee awareness and capability-building efforts, including areas relating to the ethical use and security of AI.

3. Responsible AI Principles

i. Avoiding potential bias in the use and/or development of AI

We seek to avoid potential bias in the use and/or development of AI. Where applicable and proportionate to the nature and risk of the AI use case, we seek to conduct regular assessments of deployed AI models for fairness/bias, working to identify potential biases in training data, conducting bias testing where appropriate, and promoting the use of representative datasets.

CIMB recognises the importance of providing appropriate channels for users and affected third parties to contest an AI decision or outcome and seek clarification or redress where applicable, using relevant existing feedback, review, escalation or complaint-handling channels, and strengthening such mechanisms where needed.

ii. Not using/deploying AI systems that engage in manipulative behaviour, exploitation of vulnerabilities, social scoring or unauthorised biometric surveillance

CIMB does not support the deployment of AI systems that engage in manipulative behaviour, exploitation of vulnerabilities, social scoring or unauthorised biometric surveillance. This includes working to avoid AI systems that utilise manipulative techniques, exploit vulnerabilities related to age, disabilities or socio-economic circumstances, undertake social scoring based on personal traits or social behaviour, or facilitate unauthorised real-time remote biometric identification.

iii. Establishing clear accountability for outcomes produced by AI models/tools

We believe accountability should remain central to the use of AI. CIMB seeks to maintain clear ownership, defined responsibilities and appropriate oversight of AI-influenced decisions, in support of establishing clear accountability for outcomes produced by AI models/tools.

CIMB aims to prioritise keeping humans “in the loop” for critical decisions and allowing human intervention where appropriate by including human reviews, oversight and escalation mechanisms for high-impact decision-making.

iv. Ensuring transparency of AI systems and explainability of AI generated results/decisions

CIMB recognises the importance of transparency and explainability in the use of AI. Where appropriate and proportionate to the nature, context and impact of the AI use case, CIMB seeks to provide meaningful information regarding AI capabilities, limitations, intended usage and associated risks, in support of ensuring transparency of AI systems and explainability of AI generated results/decisions.

This may include appropriate disclosure, notices or other transparency measures relating to AI-generated content or AI-assisted outcomes where relevant and taking into account the nature of the AI use case. CIMB also seeks to provide understandable explanations of AI-generated outputs where appropriate and maintain records and logs to support traceability.

v. Defining clear boundaries for what the AI can and cannot do

CIMB seeks to define clear boundaries for what the AI can and cannot do through approved use cases, governance requirements, capability restrictions and operational guardrails.

CIMB supports the establishment and ongoing refinement of mechanisms to detect and correct drift or degradation of AI models over time to support ongoing effectiveness, performance and reliability, where such monitoring is relevant to the nature and risk of the AI model or tool.

vi. Respecting data privacy in the use and/or development of AI and Protecting the cybersecurity of systems in the use and/or development of AI

CIMB is committed to respecting data privacy and protecting the cybersecurity of systems in the use and/or development of AI, while continuing to strengthen related controls and practices as technology and risks evolve.

CIMB restricts the processing of personal data to legitimate and authorised purposes and applies appropriate technical and organisational controls, including secure development practices, encryption, testing and incident response measures.

CIMB also focuses on limiting access to sensitive AI capabilities, such as facial recognition and surveillance, to authorised personnel and approved business purposes under defined governance controls.

vii. Requiring own and/ or third-party AI data centres/models to have a low ecological footprint

CIMB recognises the importance of reducing the environmental impact of AI and supports initiatives, that promote the responsible use of own and/or third-party AI data centres/models with a lower ecological footprint.

We support initiatives whether internally or with suppliers, to lower the ecological footprint of AI data centres/models, including promoting energy efficiency, resource optimisation and the responsible use of technology infrastructure.

CIMB continues to assess appropriate approaches to measure and report, where relevant, the impact of AI initiatives/tools on sustainability outcomes through suitable metrics and reporting mechanisms.

4. Responsible Partnerships and Verification

CIMB encourages alignment with responsible AI, governance and sustainability practices when engaging with third-party providers and partners.

Through our Third-Party Risk Management processes, CIMB evaluates relevant vendor commitments and controls during onboarding and ongoing oversight, exploring considerations relating to energy efficiency, climate resilience and sustainability practices where appropriate.

Developed in alignment with recognised international standards and industry practices, CIMB aims to continually benchmark our AI management system, learn from evolving global practices, and consider opportunities for future independent external verification where appropriate, including recognised standards such as ISO 42001.

-END-