

POLICY

RAM

Artificial Intelligence (AI) Governance Policy



Title	Artificial Intelligence (AI) Governance Policy	Version No.	1
Initial Approved Date	24 September 2025 Board Meeting (5/2025)	Last Reviewed Date	24 September 2025 Board Meeting (5/2025)

Table of Contents

1.	INTRODUCTION	3
2.	ROLES AND RESPONSIBILITIES	3
3.	POLICY ON THE USE OF ARTIFICIAL INTELLIGENCE (AI).....	4
3.1	Guidelines on Acceptable Use	4
3.2	Prohibited Uses of AI	6
3.3	Use of Third-Party Services	7
3.4	Reporting Procedures	7
3.5	Accountability	7
4.	REVIEW.....	7
	Definitions	8

Title	Artificial Intelligence (AI) Governance Policy	Version No.	1
Initial Approved Date	24 September 2025 Board Meeting (5/2025)	Last Reviewed Date	24 September 2025 Board Meeting (5/2025)

1. INTRODUCTION

- 1.1 RAM Holdings Berhad (RAM Holdings) and its subsidiaries¹, collectively known as “RAM Group” or “Company” express commitment to managing information security risks effectively and efficiently, in compliance with applicable regulations wherever it conducts business including with the Securities Commission’s Guidelines on Technology Risk Management² (“Guidelines”). For the purpose of this Policy the term RAM shall mean RAM Group.
- 1.2 The purpose of this AI Governance Policy (“AI Policy” or “Policy”) is to guide responsible, ethical, and compliant use of AI tools within the legal and compliance functions; in particular the Use of AI – GenAI and Agentic AI. This AI Policy establishes guidelines for the responsible, ethical, and secure application and the use of Public GenAI and Public Agentic-AI technologies and ensures compliance with regulatory requirements, protects company’s data, and promotes trustworthy AI adoption in line with the national policies, prevailing laws including Personal Data Protection Act 2010. AI also include Machine Learning (ML).
- 1.3 The Policy also describes users’ responsibilities and privileges including but not limited to what is considered as “acceptable to use” access.
- 1.4 This Policy should be read together with the Cyber Security Policy and Procedures, IT Policy, IT Standard Operating Procedures (SOP), Risk Management Policy, Personal Data Protection Policy and the Business Continuity Plan (BCP) as well as other relevant policies.
- 1.5 This Policy applies to:
- (a) All employees, contractors and third-party vendors involved in the AI-related activities or use of public GenAI and Agentic-AI tools when interacting with company data, systems, and processes.
 - (b) All AI systems and tools that are used for decision-making processes, automation, or data processing.
 - (c) All personal data collected, processed, or stored by AI systems.

This covers all use cases, including but not limited to text, image, audio, video, and code generation on RAM’s equipment and systems, on the AI Users’ personal devices.

2. ROLES AND RESPONSIBILITIES

- 2.1 This Policy shall be approved by RAM Holdings’ Board of Directors.
- 2.2 The Chief Digital Officer (CDO) shall be responsible for the following:
- (a) Implement, communicate and enforce this Policy;

¹ All subsidiaries except Bond Pricing Agency Malaysia Sdn Bhd.

² Securities Commission Guidelines on Technology Risk Management supercedes the SC Guidelines on Cyber Risk.

Title	Artificial Intelligence (AI) Governance Policy	Version No.	1
Initial Approved Date	24 September 2025 Board Meeting (5/2025)	Last Reviewed Date	24 September 2025 Board Meeting (5/2025)

- (b) Establish, for the Group CEO’s approval, internal control systems, technical guidelines and procedures to facilitate implementation of this Policy; and
- (c) Conduct regular review on the internal control systems, technical guidelines and procedures at such intervals as may be necessary.

2.3 The CEO Group shall be responsible for the following:

- (a) Ensure that RAM Group’s AI governance and use policy needs are aligned with RAM Group’s corporate objectives.
- (b) Amend, delete, approve internal control systems, technical guidelines and procedures developed by CDO under this Policy; and
- (c) Review and grant request for exception to the Policy.

2.4 The following personnel shall be responsible for the specific responsibilities as follows:

- (a) CDO and Risk Officer: Oversees public GenAI & Agentic-AI use, reviews high-risk use cases, ensures compliance, and updates the policy as required.
- (b) Data Protection Officer: Ensures compliance with data protection laws.
- (c) IT Security & Support Team: Ensure secure deployment, enforce access controls, conduct monitoring, and manage incident response.
- (d) Business Units: Ensure responsible application of public GenAI & Agentic-AI within their operations.
- (e) All Employees/Staff: Use public GenAI and Agentic-AI responsibly, comply with this policy, and report any potential security issue or misuse.

2.5 EXCEPTIONS

No exception will be made to this Policy without the written approval of the CEO Group.

3. POLICY ON THE USE OF ARTIFICIAL INTELLIGENCE (AI)

3.1 Guidelines on Acceptable Use

Public GenAI and Agentic-AI tools shall be used to improve efficiency, innovation, and decision-making processes in performing their job-related tasks. Public GenAI and Agentic-AI output must not replace critical human judgment in areas such as rating decisions, legal interpretation, or advisory services. All proposed use cases must be reviewed and approved by company management. The following principles shall also apply:

- (a) Fairness

There shall be ethical and responsible Use of Public GenAI and Agentic-AI and it must not be used to create discriminatory, offensive or misleading content. Output must be reviewed for factual accuracy, bias, and potential harm before use.

Title	Artificial Intelligence (AI) Governance Policy	Version No.	1
Initial Approved Date	24 September 2025 Board Meeting (5/2025)	Last Reviewed Date	24 September 2025 Board Meeting (5/2025)

(b) Reliability, Safety and Control

Human oversight is mandatory in all decision-making processes that is supported by public GenAI and Agentic-AI applications or platforms that have been evaluated for use and authorized by the Chief Data Officer (CDO) and Risk Officer to ensure compliance with the RAM's security, data protection, and regulatory requirements.

(c) Privacy and Data Security

- Confidential, personal, or regulated data (e.g., customer confidential information, unpublished rating information, confidential business information belonging to RAM, proprietary information, trade secrets, any information classified as confidential) must not be entered or uploaded onto public GenAI tools without prior approval.
- When using AI Tools, AI Users must comply with relevant policies including Treatment of Confidential Information, Personal Data Protection Policy, Record Retention and Disposal Policy, Non-disclosure Agreements and IT Policy.
- Only approved public GenAI and Agentic-AI tools that have been evaluated for use and authorized by the CDO and Risk Officer, may be used for such purposes. Data shared with public GenAI and Agentic-AI must comply with company's data classification and retention policies.

If unsure, to seek advice from Compliance and Legal Officer.

(d) Fairness, Non-Discrimination and Human Benefit

The use of AI systems must be used in ways that are fair, non-discriminatory, and beneficial to people. Human oversight shall be maintained to ensure ethical outcomes and prevent harm.

(e) Transparency, Explainability and Accountability

Public GenAI and Agentic-AI models used by RAM will be monitored for performance and accuracy as AI systems' performance may change over time, for example, when the underlying AI models change or encounter new types of data. Usage and performance to be reviewed periodically to ensure AI systems remain fit for purpose.

(f) Safeguard of Intellectual Property Rights

Employees must not input, disclose, or upload Company intellectual property including proprietary methodologies, source code, models, datasets, copyrighted material, or trade secrets into Public GenAI or Agentic-AI tools unless explicit approval has been granted. All outputs generated using AI tools that relate to Company work remain the intellectual property of RAM unless otherwise governed by law or contractual obligations. The use of AI to generate content that infringes third-party intellectual property rights is strictly prohibited.

Title	Artificial Intelligence (AI) Governance Policy	Version No.	1
Initial Approved Date	24 September 2025 Board Meeting (5/2025)	Last Reviewed Date	24 September 2025 Board Meeting (5/2025)

3.2 Prohibited Uses of AI

The use of AI technologies including Public GenAI or Agentic-AI tools and its systems, or tools within RAM Group or in connection with its operations shall be subject to strict compliance with applicable laws, internal policies, and ethical standards. Subject to the provision herein, the following uses of AI are expressly prohibited:

(a) Unlawful or Unethical Activities

AI shall not be used to:

- Engage in or facilitate any activity that is illegal, fraudulent, deceptive, or unethical.
- Circumvent laws, regulations, or contractual obligations.
- Generate or disseminate false, misleading, or harmful content.

(b) Promote Discrimination and Bias

AI systems must not be used in a manner that:

- Results in discriminatory outcomes based on race, religion or other protected characteristics.
- Reinforces or amplifies existing biases in decision-making processes.

(c) Privacy and Surveillance Violations

AI shall not be used to:

- Collect, process, or analyse personal data without proper authorisation as set out in Para 3.1(c) or legal basis.

(d) Acts that compromise Security and Safety Risks

AI must not be deployed in ways that:

- Compromise the security, integrity, or availability of systems, networks, or data.
- Pose risks to physical safety, public health, or critical infrastructure as set out in the relevant legislations.

(e) Autonomous Decision Making

AI shall not be used to make autonomous decisions in key areas (e.g., rating decisions, legal, compliance, employment, finance) without appropriate human oversight, review, and accountability mechanisms.

(f) Intellectual Property Violations

AI must not be used to:

- Infringe upon the intellectual property rights of third parties.
- Generate or replicate content that violates copyright, trademark, or patent laws.
- Misrepresent facts, plagiarise or infringe on intellectual property, or create outputs that could harm RAM Group, its clients, or its stakeholders.

Title	Artificial Intelligence (AI) Governance Policy	Version No.	1
Initial Approved Date	24 September 2025 Board Meeting (5/2025)	Last Reviewed Date	24 September 2025 Board Meeting (5/2025)

3.3 Use of Third-Party Services

When third-party software, services, or contractors are utilized or employed, any AI usage by software used by these parties or services must be noted and evaluated carefully. Contracted services that utilize AI technology should be considered in the same light as individual AI usage. Consult the CDO or the Compliance and Legal Officer on the inclusion of an AI-specific clause in any vendor or contractor agreements.

3.4 Reporting Procedures

- (a) AI Users shall contact their supervisor/manager/CDO/CEO immediately if they become aware of:
 - (i) an actual or possible violation of this AI Governance Policy;
 - (ii) a breach of data privacy or security;
 - (i) AI system failure; and/or
 - (ii) circumstance where an AI Tool is generating output which is erroneous, misleading, offensive.
- (b) Reports made under this section will be investigated, and AI Users must cooperate with any such investigation.
- (c) RAM may, in its sole discretion, decide to suspend use of the AI Tool during any such investigation.
- (d) To the extent corrective measures are required following the investigation, AI users must cooperate in the implementation of those measures.

The implementation of AI within the Company shall also be reported to the Securities Commission (SC) via the SC Vault system, with the Chief Data Officer (CDO), together with the Compliance and Legal Officer, responsible for ensuring that such reporting is timely, accurate, and in full compliance with regulatory requirements.

3.5 Accountability

A breach of this Section may result in disciplinary action, including but not limited to:

- (a) Formal warning or reprimand;
- (b) Suspension or termination of employment or engagement;
- (c) Revocation of system access or privileges and/or
- (d) Legal action, including civil or criminal proceedings where applicable.

4. REVIEW

This Policy is subject to annual review by the ARMSC. This Policy may be reviewed and amended, at the discretion of the Board of RAM Holdings from time to time as and when necessary for implementation in RAM Group to ensure its relevance and

Title	Artificial Intelligence (AI) Governance Policy	Version No.	1
Initial Approved Date	24 September 2025 Board Meeting (5/2025)	Last Reviewed Date	24 September 2025 Board Meeting (5/2025)

effectiveness in keeping with RAM Group’s changing business environment, administrative or operational needs as well as changes to legislations.

Definitions

The following definitions shall apply in this Policy unless expressly stated otherwise:

“Artificial Intelligence (AI)” related definitions include;

- “Public GenAI” shall mean AI technologies capable of creating new content such as text, images, audio, video, or code based on training data and user prompts. Public GenAI refers to tools and platforms that are openly available for external/public use.
- “Public Agentic-AI” shall mean AI systems capable of autonomously performing tasks, making decisions, or executing multi-step actions on behalf of users, with minimal or no human intervention. Public Agentic-AI refers to tools and platforms that are openly available for external/public use.

“CEO” shall mean Chief Executive Officer

“CDO” shall mean Chief Digital Officer

“Company Data” shall mean any data owned, processed, or controlled by the company, including confidential, restriction, internal, personal, or regulated information.

“DPO” shall mean Data Protection Officer

“IT” shall mean Information Technology

“SC” shall mean Securities Commission Malaysia

“GTRM” shall mean SC’s Guidelines on Technology Risk Management.

“Machine Learning (ML)” is a subject of AI that uses statistical techniques to give computer systems the ability to “learn” from data.

“Use Case” shall mean a defined business scenario or process in which GenAI is applied to support or enhance organizational operations.

Published by RAM Holdings Berhad and its Group of Companies

Reproduction or transmission in any form is prohibited except by permission from RAM Holdings Berhad and its Group of Companies.

© Copyright 2025 by RAM Holdings Berhad and its Group of Companies

RAM Holdings Berhad
Level 8 Mercu 2, KL Eco City
No 3, Jalan Bangsar
59200 Kuala Lumpur

T: (603) 2708 8288

F: (603) 2708 8201

E: complaint@ram.com.my

W: www.ram.com.my