Jardine Matheson

Responsible AI Policy

Jardine Matheson (Jardines) is an investment company dedicated to building a diverse portfolio of high-quality, scaled businesses in Asia Pacific. Jardines and our portfolio companies are committed to the responsible use, development, procurement and oversight of artificial intelligence (AI) systems in a manner that is lawful, secure, ethical and aligned with our values.

AI can deliver significant benefits, but also creates risks relating to privacy, cybersecurity, bias, opacity, misuse, accountability and environmental impact. Responsible governance of AI is therefore essential to maintaining trust with our stakeholders.

This Responsible AI Policy (the Policy) applies to employees, contractors, and other third parties who use, develop, procure, manage or oversee AI for or on behalf of Jardines. This Policy sets out high-level principles for responsible AI and should be read in conjunction with the internal standards and guidelines developed and disseminated by Jardines. Our portfolio companies, associated companies and joint venture partners are encouraged to adopt this Policy or incorporate its principles into their own policies where appropriate, taking into account their industry, operating context and legal requirements.

We are committed to the following principles:

Governance and accountability

- Establish appropriate governance for AI across its lifecycle, including use, development, procurement, deployment, monitoring and review.
- Assign clear accountability for the use of AI systems, the review of their outputs, relevant risk management and compliance decisions and the business outcomes that result from them.
- Ensure that the relevant business owner, process owner or system owner remains responsible for decisions and actions taken with the support of AI.

Lawful and purpose-bound use

- Use AI only for lawful, legitimate and clearly defined business purposes consistent with our values and policies.
- Define appropriate boundaries for what AI systems are intended to do, the context in which they may be used, and the circumstances in which they must not be used.

- Avoid uses of AI that are misleading, deceptive, discriminatory, abusive or otherwise inconsistent with our ethical standards.

Privacy and data protection

- Respect privacy and data protection requirements in the use and development of AI.
- Protect personal data, confidential information and other sensitive information in accordance with applicable data protection law and Jardines policies, using only authorised tools and appropriate safeguards.
- Apply appropriate data governance measures, including data minimisation, protection, and anonymisation or pseudonymisation where relevant.

Cybersecurity and technical safeguards

- Protect the cybersecurity of AI systems and related data through appropriate technical and organisational controls.
- Apply information security measures across the lifecycle of AI systems, including secure design, penetration testing, data encryption, access control, monitoring, incident management and change management.
- Subject AI-related technologies to appropriate information security oversight in line with Jardines' standards.

Fairness and bias mitigation

- Take reasonable steps to identify and mitigate material bias in data training, discriminatory outcomes and other unfair impacts arising from the use or development of AI, including by assessing relevant input data sources and taking proportionate measures to reduce the impact of identified bias.
- Exercise particular care where AI may materially affect individuals, customers, employees or other stakeholders.
- Review and, where necessary, correct, constrain or discontinue AI use cases where bias or unfairness is identified.

Human oversight

- Keep humans appropriately involved in the use of AI, especially where decisions may significantly affect individuals, customers, employees, safety, legal rights, financial outcomes or the reputation of Jardines.
- Ensure that AI supports, and does not replace, appropriate human judgment and intervention in critical decisions.
- Enable users to review, challenge, override or escalate AI outputs where necessary.

Transparency and explainability

- Promote appropriate transparency regarding when and how AI is used, taking into account the audience, context, confidentiality and legal requirements.
- Disclose the use of AI where appropriate, particularly where outputs are provided externally or may reasonably be relied upon by others.
- Seek to ensure that AI-supported outcomes can be explained to a degree appropriate for their purpose and context.

Reliability and monitoring

- Recognise that AI systems may generate inaccurate, incomplete, fabricated, biased or outdated outputs.
- Validate AI outputs to a level appropriate to the use case and degree of risk before reliance is placed on them.
- Monitor material AI systems over time for performance, drift, degradation and continued fitness for purpose, taking into account the maturity of the use case and the practicality of available controls.

Third-party AI and suppliers

- Conduct appropriate due diligence before procuring or adopting third-party AI systems, models, platforms or embedded AI features.
- Consider privacy, security, governance, contractual protections and other relevant risks when assessing third-party AI.
- Retain accountability within Jardines for business use of third-party AI systems and services.

Sustainability and environmental responsibility

- Consider the environmental impact of material AI deployments where reasonably practicable.
- Encourage proportionate steps by Jardines and relevant suppliers to reduce unnecessary compute use, improve energy and water efficiency, and increase the use of zero-carbon energy.
- Apply this principle in a practical and proportionate manner, recognising that methods for measuring and comparing the ecological footprint of AI systems are still evolving.

Prohibited uses

- Prohibit the use, development, procurement or deployment of AI for unlawful purposes or in ways inconsistent with this Policy.

- Avoid AI uses involving unlawful discrimination, manipulative or deceptive practices, exploitation of vulnerabilities, unlawful social scoring, or biometric identification or surveillance that is unauthorised under applicable law or Jardines approval requirements.
- Require enhanced review, additional safeguards or formal approval for certain higher-risk AI use cases.

Reporting and compliance

Suspected or actual breaches of this Policy, harmful AI outcomes, or AI-related incidents must be reported through designated channels, such as the IT Service Desk or the Information Security team.

Non-compliance with this Policy may result in disciplinary action, up to and including termination of employment or contract, and may lead to legal action.

This Policy has been endorsed by Executive Management and will be reviewed periodically and updated as required to reflect changes in law, technology, business use and stakeholder expectations.