TRACE LAW PARTNERS

AI Policies: Managing AI Risk within the Organisation

Introduction

AI is increasingly becoming integral to operations of organisations with use ranging from improving routine processes to supporting core business functions and, in some cases, high-stakes decisions. While AI tools offer significant efficiencies, their use also creates risks, including breaches of confidentiality, data protection concerns, uncertainty around intellectual property ownership and non-compliance with regulatory requirements. An AI policy is therefore an important first step in defining how AI may be used within an organisation and the safeguards that must apply.

At present, India does not have a law governing use of AI. However, in this article we discuss how AI adoption and use within an organisation is already subject to existing laws and regulatory requirements, including those relating to data protection, cybersecurity, intellectual property, advertising, consumer protection and other sector-specific aspects. Further, sectoral regulators have begun actively examining the use of AI within regulated industries and have issued guidance in some or the other form on usage of AI. An AI policy can help organisations translate such guidance into clear internal rules.

In this article, we discuss when businesses should consider adopting an AI policy and what such policies should cover.

When should entities consider having an AI policy?

Organisations should assess whether any of the following apply to them:

- Employees/team members use AI tools (including code assistants) to write or assist with writing proprietary software or create other assets like movie scripts, music, etc.

- Access to generative AI tools (such as ChatGPT) on work devices has not been formally restricted, approved or monitored.

- AI is used to assist with core business functions, such as claims review in insurance, credit appraisal in lending, medical diagnostics, fraud detection or regulatory reporting.

- Proprietary data or customer information is shared with third-party vendors who may use AI, such as marketing agencies.

- AI features such as chatbots are built using third party large language models (LLMs).

Key Legal Considerations

Although India does not yet have a comprehensive AI law, AI-related activities are already subject to existing legal and regulatory frameworks. An AI policy can help ensure that AI tools are used in compliance with laws already applicable to the organisation.

01	02	03	04	05	06
General Laws	Sectoral Laws	Contractual Issues	Vendor Risks	Investor Due Diligence	IP Issues

General Laws

Use of AI for internal purposes is likely to trigger various general laws. Some of the key aspects are discussed below:

- **Processing of personal data:** Under the Digital Personal Data Protection Act, 2023 ("**DPDPA**"), processing of personal data may be on the basis of consent or for one of the specifically listed legitimate purposes.[1] Accordingly, where an organisation inputs customers' personal data into an AI tool, or uses an integrated AI chatbot or other AI-enabled feature that processes such data, it must obtain the customers' consent unless the processing falls within one of the specified legitimate uses. An AI policy should therefore clearly identify when and under what conditions personal data may be used with AI tools.

- **Labelling:** Where organisations are creating AI-generated audio, visual or audio-visual content, which may constitute "synthetically generated information" under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ("**IT Rules**"), they must ensure that such content is appropriately labelled. "Synthetically generated information" means AI-generated or AI-manipulated audio, visual or audio-visual content that appears authentic or is likely to be perceived as depicting a real person or event. The definition excludes ordinary editing, formatting, accessibility enhancements and the creation of documents or educational materials, so

[1] Section 7, DPDPA

long as these do not materially alter the underlying content or create false records.[2] Failure to label content may lead to action against the organisation based on the terms of use of the platform, such as suspension of the account, which may disrupt marketing campaigns.[3]

- **Advertising and Consumer Laws**: The Advertising Standards Council of India (ASCI) has also recently issued Draft Guidelines for Responsible Labelling of Synthetically Generated Content in Advertising that also contemplate disclosures in certain circumstances where AI-generated or AI-altered content is used, making it important for organisations to establish internal controls over AI-generated marketing materials.[4] If AI is being used to generate advertisements, make claims about products/services, compliance with advertising laws must be ensured.

Regulatory concerns for regulated entities

Regulated entities such as banks, NBFCs and insurance companies, etc. must assess if general sectoral compliances apply to their AI usage. For instance, where AI is used to support core business functions such as processing of loan applications or processing of insurance claims, do these activities amount to "outsourcing" under applicable sectoral laws and therefore subject to compliances under the relevant outsourcing guidelines. Where such guidelines apply, the regulated entity may be required to conduct due diligence on the AI service provider, monitor its performance and risks, and include prescribed safeguards in its contract with the provider.

Similarly, organisations must assess whether any applicable data localisation requirements are being complied with. This includes determining where data processed through AI tools is stored and whether any data subject to localisation requirements is being transferred outside India. For instance, RBI requires localisation of all data relating to payment systems.[5] Similarly, the Insurance Regulatory and Development Authority of India (Maintenance of Insurance Records) Regulation, 2015 requires insurers to maintain records relating to insurance policies and claims in India only.[6]

Contractual Risk

The use of AI tools may create contractual risks where customer agreements contain confidentiality, data handling or technology-specific restrictions. For example, an employee may upload customer information to a generative AI tool to summarise a contract or analyse data, without appreciating that doing so could amount to an unauthorised disclosure of confidential

---

[2] Rule 2(wa), IT Rules

[3] For more information, see https://6fbce365-82e9-4a61-8af0c64510aed0d0.usrfiles.com/ugd/6fbce3_375e6cec7345491487689903fb451ee8.pdf

[4] ASCI, Draft Guidelines for Responsible Labelling of Synthetically Generated Content in Advertising (May 8, 2026), https://www.ascionline.in/wp-content/uploads/2026/05/asci-ai-labelling-guidelines.pdf

[5] https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11244&Mode=0

[6] Regulation 3(9), Available at https://financialservices.gov.in/sites/default/files/Act-Policies/2026-01/IRDAI--Maintenance-of-Insurance-Records--Regulations--2015.pdf

information or a breach of contractual obligations. Similarly, some customer agreements prohibit the use of AI tools in the performance of services or require prior written consent before AI tools may be used.

Vendor Risk

Organisations must also consider how vendors use AI while providing services on their behalf. For example, a marketing agency may use AI to create advertisements, social media posts or other promotional content without the organisation's knowledge or approval. A robust AI policy should therefore be complemented by contractual provisions requiring vendors to disclose their use of AI and comply with applicable labeling requirements.

Investor and Due Diligence Risk

Seasoned investors are now assessing how organisations are using AI as part of their diligence on cybersecurity, intellectual property and regulatory compliance. This is especially relevant for entities in regulated sectors like insurance, healthcare, etc. where automated decision making may lead to liability. Typically investors seek information on how AI is used across the business, what safeguards apply to customer data and confidential information, how intellectual property risks are managed, and whether there is adequate oversight of the AI tools being used.

Intellectual Property Ownership

As is now well known, Indian law remains unclear on the ownership of AI-generated and AI-assisted content. One commonly adopted safeguard is to ensure meaningful human involvement throughout the creation process, including through detailed prompts, multiple iterations, negative prompts and substantive human review and refinement. Organisations using AI to develop proprietary technology, content or other assets should therefore ensure that their AI policies require employees to follow and document such processes.

An AI policy will not, by itself, eliminate these risks. It does, however, show that the organisation has identified the legal and commercial implications of AI use and has put in place a framework for managing them.

Existing Regulatory Guidance

RBI	The RBI published its Framework for Responsible and Ethical Enablement of AI in Financial Services (the "**RBI FREE-AI Paper**"),[7] which sets out principles including fairness, accountability, transparency, ethics and robustness for AI systems deployed in banking and financial services. Building on this, the RBI has recently issued draft Guidance on Regulatory

[7]https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/FREEAIR130820250A24FF2D4578453F824C72ED9F5D5851.PDF

	Principles for Model Risk Management, 2026,[8] which proposes a comprehensive governance framework for models, including AI/ML models, used by regulated entities. It requires Board-level oversight, risk-based classification, independent validation, continuous monitoring, human oversight and additional safeguards addressing explainability, bias, hallucinations and cybersecurity risks.
IRDAI	The IRDAI has also constituted a Working Group on Artificial Intelligence in Insurance which will suggest an AI governance framework for the ethical, transparent and explainable adoption of AI tools and models in the insurance sector, including for claims and fraud prevention.[9]
SEBI	SEBI's regulatory approach to algorithmic trading, automated advisory services and the use of data analytics similarly reflects an emphasis on governance, auditability and investor protection where technology is used in regulated functions.[10]

Across these frameworks, common themes emerge:

- Governance and accountability for AI systems at the board and senior management level;
- Risk management and internal controls specific to AI model development and deployment;
- Oversight and ongoing monitoring of AI models and their real-world outcomes;
- Vendor and third-party risk management for AI tools and infrastructure; and
- Ongoing evaluation of AI impacts.

Separately, news reports indicate that the Government may consider a central AI law based on a graded, risk-based approach.[11]

These developments are relevant even for businesses that are not directly regulated by the RBI, IRDAI or SEBI. They indicate the issues that regulators are likely to focus on: accountability, board oversight, human involvement, data governance and vendor controls. Businesses can use these principles when framing their AI policies, while ensuring that the policy separately identifies the requirements that are legally binding on them.

What Should an AI Policy Address?

[8] https://www.rbi.org.in/Scripts/bs_viewcontent.aspx?Id=5089

[9] See https://www.business-standard.com/finance/insurance/irdai-sets-up-working-group-to-guide-ai-adoption-in-insurance-sector-126061801084_1.html

[10] https://www.sebi.gov.in/reports-and-statistics/reports/jun-2025/consultation-paper-on-guidelines-for-responsible-usage-of-ai-ml-in-indian-securities-markets_94687.html

[11] https://www.business-standard.com/finance/insurance/irdai-sets-up-working-group-to-guide-ai-adoption-in-insurance-sector-126061801084_1.html

AI policy terms will depend on factors such as the organisation's business model, the sensitivity of the data involved and the extent to which AI is embedded into products and operations. Broadly, most organisations should consider at least the following questions when designing an AI policy:

- Which AI tools and use cases are permitted, restricted or prohibited within the organisation?

- What due diligence should be undertaken before approving a new AI tool? For example, do the provider's terms and conditions assign all IP rights to the organisation and allow commercial usage of output?

- What categories of information, for example, confidential data, customer data, health data, etc., can and cannot be shared with AI systems?

- How should AI be used in creating intellectual property? Where AI is used to generate content, software code, designs or other intellectual property, what level of human input, review and modification is required?

- For regulated entities, does the adoption of a particular AI tool constitute outsourcing of a material business activity under applicable sectoral guidelines and if so, what additional due diligence, contractual and oversight requirements must be met?

- What disclosures, if any, should be made to customers or counterparties about AI-enabled features or workflows?

- If AI is being used to assist with core business functions, what level of human oversight is to be ensured?

- What is the role of the Board in assessing and approving use of AI?

Conclusion

The absence of a dedicated AI law does not mean that businesses are operating in a legal vacuum. Employees and vendors are already using AI in ways that may engage confidentiality, data protection, intellectual property, advertising and sector-specific obligations. An AI policy is therefore not only about preparing for a future law but ensuring that usage is in line with existing laws that remain applicable to businesses.

For more information, reach out to us at info@tracelawpartners.com. We would like to thank Thanush S from GLC Trivandrum for his contributions to this article.