PINAC
ADVOCATES AND SOLICITORS

Artificial Intelligence (AI) Governance Policy for Indian Workplaces

- *Essential Considerations*

October 31, 2025

In 2023, engineers of a South Korean consumer goods company inadvertently uploaded proprietary source code to a generative AI platform for routine de-bugging, which became permanently embedded in the AI platform's training data. The employer promptly implemented an enterprise level ban for use of unauthorised or external AI tools. This highlights the risk of unauthorised AI usage without a well-thought governance framework.

For instance, a recent report notes that 'Shadow AI', use of AI without employer approval or oversight, adds nearly $670,000 to average breach costs globally.[1] Further, the report indicates that 65% of Shadow AI breaches also compromise customer personally identifiable information, and over 40% involve intellectual property theft.[2] Unlike external cyberattacks, these incidents happen as employees lack clear guidance of what is permitted or employees who have been negligent.

80% of Indian companies have identified AI as a core strategic priority, surpassing the global average of 75%.[3] However, AI adoption is outpacing oversight. It is estimated that nearly 60% of organizations lacked an AI governance policy ("AI Governance Policy") or were still in the process of developing one.[4]

The risk is not academic - the Indian Digital Personal Data Protection Act imposes significant penalties up to INR 250 crores ($30 million). The risk will be particularly heightened for Indian companies handling customer personal data in healthcare and financial services sectors.

Regulatory Framework.

India presently lacks a dedicated AI legislation although a proposed Digital India Act was on the horizon

---

1 Jason M. Loring, *The AI Oversight Gap: IBM's 2025 Data Breach Report Reveals Hidden Costs of Ungoverned AI*, available at The AI Oversight Gap: IBM's 2025 Data Breach Report Reveals Hidden Costs of Ungoverned AI | Jones Walker LLP See also Cost of a data breach 2025. IBM & Ponemon Institute Research Team (n.d.). https://www.ibm.com/reports/data-breach ("**IBM Report**").

2 *Ibid*.

3 *80 pc of Indian companies find AI a core strategic priority: Report*, (Economic Times, 16 Jan 2025) available at 80 pc of Indian companies find AI a core strategic priority: Report, ETCIO. See also IBM Report.

4 Nearly 60% of Indian organisations lack AI governance policy: Report, (The Hindu, 07 August 2025) available at Nearly 60% of Indian organisations lack AI governance policy: Report - The Hindu. See also IBM Report.

(although it is unclear if the Digital India Act is still at play). That said, the sectoral regulators are rapidly releasing frameworks and guidelines for AI usage. For instance, the Reserve Bank of India (India's central bank) and SEBI, India's securities and capital have issued guidelines requiring AI lifecycle management protocols, with a focus on ensuring on risk mitigation. Further, Ministry of Electronics and Information Technology (MeitY) advisory dated 15 March 2024, requires intermediaries and platforms to implement specific compliance measures for AI use, aligned with their due diligence obligations under the Information Technology Act, 2000 (IT Act) and related rules.[5] The IT Act broadly requires intermediaries to exercise due diligence when discharging their duties and ensure prompt censorship of unlawful content upon gaining knowledge of the same.

Business Case for AI Governance Policy.

With India veering towards a light-touch decentralised regulatory regime for AI governance, there is a business case for companies to incorporate their own individual guardrails. Beyond mitigating regulatory risks also, a well thought AI Governance Policy could result in operational efficiencies as well.

(i) *Efficient AI Deployment*: Without defined internal AI frameworks, each enterprise level AI initiative requires case-by-case evaluation which creates bottlenecks and consumes senior management time. Board approved AI Governance Policies enable quicker adoption and vendor onboarding.

(ii) *Investors and Client Onboarding*: Vendor and supply chain compromise is a major attack vector, second only to phishing.[6] Enterprise-level procurement processes now routinely include vendor security assessments through questionnaires and internal policy reviews. Similarly, vendors / *suppliers* or companies, in general, that can demonstrate comprehensive AI internal policies gain competitive advantages in client onboarding. From an investors' due diligence perspective as well, we observe extensive questions around AI adoption and governance framework.

(iii) *Internal Training and Combatting Human Errors*: Early evidence indicates that a substantial part of recorded breaches stemmed from human errors and IT failures, both entirely preventable through proper governance.[7] Shadow AI incidents typically fall into the human error category. Interestingly, analysis of infostealer malware logs reveals 46% of systems that contained corporate login *credentials* were unmanaged devices — highlighting the risks that companies face from compromised personal devices containing company data.[8] When enterprise passwords are available on grey web marketplaces, malicious actors can leverage these

---

5 Ministry of Electronics and Information Technology, Government of India, *Due Diligence by Intermediaries/Platforms under the Information Technology Act, 2000 and Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021* (eNo.2(4)/2023-CyberLaws-3) (2024), https://www.meity.gov.in/static/uploads/2024/02/9f6e99572739a3024c9cdaec53a0a0ef.pdf.

6 Jaroslav Kalfar, *IBM Data Breach Report 2025: The Soaring Costs of Email Attacks*, available at IBM Data Breach Report 2025: The Soaring Cost of Email… | Abnormal AI. See also IBM Report.

7 Matt Kapko, *Research shows data breach costs have reached an all-time high*, (Cyberscoop, 30 July 2025) available at Research shows data breach costs have reached an all-time high | CyberScoop. See also IBM Report.

8 Dwayne Mcdaniel, *The Secrets Sprawl Is Worse Than You Think: Key Takeaways from the 2025 Verizon DBIR*, available at https://blog.gitguardian.com/verizon-dbir-2025/#:~:text=These%20compromises%20often%20occur%20in,Secrets%20Lead%20the%20Breach%20Chain ; Also refer Verizon 2025 Data Breach Investigations Report.

credentials to access corporate AI platforms, resulting in enterprise-level vulnerabilities. Companies implementing clear AI policies, coupled with regular training programs and device management protocols, can significantly reduce their AI-related risk.

Broad Contours of AI Governance Policy.

Scope	a. While employees are the obvious starting point, it should be assessed if policy governance should also extend to key contractors, consultants, third-party service providers, and other parties, with access to company systems or information. b. Modern working arrangements have move beyond the physical confines of a brick-and-mortar office and this necessitates companies to thoughtfully consider how the policy would apply across different contexts.
Device Management Policies	Personal devices are prime access points for loss or inadvertent breach of enterprise data. Companies should have strict device management protocols in place and company data should be strictly restricted to company provided devices.
Authorised and Prohibited Applications	Policies adopted can either provide for: (i) a permissive framework (where all tools are allowed unless specifically prohibited), or (ii) a restrictive framework (where tools are prohibited unless specifically authorized). Where the data handled by the company involves sensitive, confidential or proprietary information (such as, healthcare or financial services), a restrictive approach is generally advisable.
AI vendor onboarding assessment	AI vendor onboarding should involve comprehensive diligence to determine availability of data usage opt-out mechanisms, data hosting servers, data retention policies, AI training, security protocols, etc.
Tiered Access Controls	Access rights to organisation's sensitive data for AI platforms should be monitored, and generally made available only on pre-identified terms, such as role-based access.
Categorize Prohibited Information	AI platforms retain user inputs for various purposes, including model training, service improvement, and abuse prevention, with limited or no ability to retrieve or delete it. Clearly delineate information categories that should not be uploaded to AI platforms, without specific authorization. These typically include confidential information, trade secrets, proprietary data, personal data subject to privacy regulations, and client or customer information.
Creation of	a. Effective AI adoption, particularly for financial and healthcare sector, relies

Hygienic Data Sets for Effective Use	heavily on the quality of data sets. Inaccurate or incomplete data mislead AI models resulting in bias, wrong outputs, etc. For instance, in the manufacturing sector, high-quality data may result in effective predictive maintenance, quality control, and supply chain optimization.[9] Organisations should establish internal standards before data is fed into AI systems. b. Beyond technical data quality, organizations must address certain foundational principles: (A) fairness and bias mitigation to prevent discriminatory outcomes, (B) transparency and explainability to ensure AI decision-making processes remain understandable, and (C) accountability and responsibility to establish clear ownership for AI-driven results. c. Critically, hygienic datasets must be coupled with informed consent, either through contracts or consent forms, to enable legitimate data usage for AI training purposes.
Training and Mandated Human-in-Loop Review	Large language models are known to generate outputs that may be inaccurate, incomplete, or entirely fabricated (hallucinations). Companies must invest in mandatory periodic training and establish clear expectations that AI-generated outputs require human review and verification before being used, relied upon, or disseminated. A professional services firm had to refund service fees as one of its report contained fabricated academic citations, false references and a quote wrongly attributed to a federal court judgment, proving AI usage without strict quality control could be disastrous.
Consequences of breach	The policy should provide for consequences for policy violations, calibrated basis inadvertent minor breaches, negligent conduct, and wilful misconduct. Further, terms of employment should ensure that breach of company's AI Governance Policies could be grounds for disciplinary actions, including termination.

Concluding Thoughts.

Although hushed up, stories are consistently emerging where Indian businesses have been disrupted by improper use of AI applications. Given that early evidence shows a majority of data breaches are attributable to insiders, combined with high penalty costs and reputational costs associated with

[9] McKinsey & Company: "Clearing data-quality roadblocks: Unlocking AI in manufacturing" by Lapo Mori, Bryan Richardson, Tamim Saleh, Richard Sellschop, and Ian Wells, available at: https://www.mckinsey.com/capabilities/tech-and-ai/our-insights/clearing-data-quality-roadblocks-unlocking-ai-in-manufacturing.

breaches, Indian businesses have a compelling reason to adopt and implement robust AI Governance Policies.

However, policy alone is insufficient. Mandatary periodic training for employees is a must to ensure policies translate into practice and the risks associated with unauthorised AI use is well understood across the organisation. AI Governance Policies should also be periodically updated to ensure regulatory compliance, particularly for companies in sensitive sectors such as banking, financial services and life sciences.

Authors: *Raghunath Seshadri*, *Eeshan Mohapatra*