

Draft Guidelines for Consultation



भारतीय दूरसंचार विनियामक प्राधिकरण
Telecom Regulatory Authority of India



Draft Guidelines on Responsible Use of Artificial Intelligence (AI) in Telecommunication Networks and Provision of Telecommunication Services

New Delhi, India

30.10.2026

Tower-F, World Trade Centre, Nauroji Nagar, New Delhi- 110029

Written comments on the draft guidelines are invited from stakeholders by 27.11.2026.

Comments will be posted on TRAI's website www.trai.gov.in. The comments may be sent, preferably in electronic form, to Shri Akhilesh Kumar Trivedi, Advisor (Networks, Spectrum and Licensing), TRAI on the email ID advmn@trai.gov.in.

For any clarification/ information, Shri Akhilesh Kumar Trivedi, Advisor (Networks, Spectrum and Licensing), TRAI, may be contacted at Telephone No. +91-11-23210481.

Draft Guidelines on Responsible Use of Artificial Intelligence (AI) in Telecommunication Networks and Provision of Telecommunication Services

1. Introduction

- 1.1. In February 2026, the Government of India released the 'India AI Governance Guidelines' with the goal to harness the transformative potential of artificial intelligence for inclusive development and global competitiveness, while addressing risks it may pose to individuals and society. The guidelines are anchored in seven guiding sutras or principles — *Trust is the Foundation, People First, Innovation over Restraint, Fairness & Equity, Accountability, Understandable by Design, and Safety, Resilience & Sustainability*. Part 4 of the guidelines provides practical guidance for industry actors and regulators to increase clarity, predictability and accountability in the ecosystem.
- 1.2. The telecommunication sector constitutes a significant part of India's digital infrastructure. Today, the telecommunication sector supports connectivity for the public, delivery of public and essential e-services, conduct of trade and commerce, and secure and resilient functioning of the country's critical information infrastructure. It is critical not only for social, economic and commercial activities but also for national security and emergency response in the country.
- 1.3. At present, AI is increasingly being integrated into telecommunication networks and provision of telecommunication services. While the integration of AI into telecommunications is likely to significantly enhance efficiency, it may also introduce new risks if due diligence is not exercised before deployment of AI systems or if due supervision is not exercised over autonomous learning, and systemic interactions. These risks, including

inadvertent biases which may creep in AI systems during training and usage, unintended model behavior such as model drift, and adversarial attacks, can adversely affect the resilience of telecommunications infrastructure, particularly in its critical components. Such risks can be mitigated if suitable AI governance practices are followed.

- 1.4. The Telecom Regulatory Authority of India (TRAI) has been established under the Telecom Regulatory Authority of India Act, 1997 (24 of 1997) [Hereinafter referred to as "TRAI Act"] to regulate telecommunication services, and to protect the interests of service providers and consumers of the telecom sector, to promote and ensure orderly growth of the telecom sector, and for matters connected therewith or incidental thereto. Further, sub-clause (v) of clause (b) of sub-section (1) of section 11 of the TRAI Act mandates TRAI to lay down the standards of quality of service to be provided by the service providers and ensure the quality of service and conduct the periodical survey of such service provided by the service providers so as to protect interest of consumers of telecommunication service. In consideration of 'India AI Governance Guidelines' issued by the Government of India and the mandate entrusted to TRAI under the TRAI Act, the Authority hereby makes these guidelines on responsible use of AI in telecommunication networks and provision of telecommunication services (hereinafter referred to as "TRAI's guidelines on responsible use of AI in telecom"). These guidelines are issued with a view to ensuring consistent and responsible implementation of the India AI Governance Guidelines in the telecommunication sector, and to increase clarity, predictability and accountability in the ecosystem.

2. Applicability

- 2.1. TRAI's guidelines on responsible use of AI in telecom will be applicable to any entity (hereinafter referred to as "applicable authorised entity" in these guidelines) that holds -

- (a) a license under the Telegraph Act, 1885 or an authorisation under the Telecommunications Act, 2023 - for providing telecommunication services; or
- (b) an authorisation under the Telecommunications Act, 2023 - for establishing, operating, maintaining or expanding telecommunication networks;

and -

is using or intending to use AI system(s) in telecommunication networks, or provision of telecommunication services, or both.

3. TRAI's guidelines on responsible use of AI in telecom

A. Internal AI policy on telecom

- 3.1. The applicable authorised entity shall formulate and implement an 'internal policy for the use of AI in telecommunication networks and/or provision of telecommunication services' (hereinafter also referred to as "Internal AI policy on telecom"). Such policy shall be approved by the board of directors, or an equivalent governing body of the applicable authorised entity.
- 3.2. The Internal AI policy on telecom of any applicable authorised entity shall contain, *inter alia*, the following:
 - (a) Risk classification of AI system: Each AI system used or intended to be used in telecommunication networks and/or provision of telecommunication services by the applicable authorised entity shall be classified as high-risk, medium-risk, and low-risk AI system - based on the materiality of the AI system i.e. significance of the AI system to the telecommunication networks and/or provision of telecommunication services, including its impact on financial and operational outcomes, and its potential implications for consumers - of the applicable authorised entity.

- (b) Use of AI systems: Any AI system shall be used only after approval by an officer of the applicable authorised entity designated for this purpose. The approval to the use of AI systems may be delegated to suitable officers based on the risk classification of AI systems.
- (c) Classification of AI incidents: Each AI incident occurring in telecommunication networks and/ or provision of telecommunication services shall be classified as critical-severity AI incident, high-severity AI incident, moderate-severity AI incident, and low-severity AI incident.
- (d) Mechanism of recording, mitigation, investigation, analysis and reporting of AI incidents: All AI incidents occurring in telecommunication networks and/ or provision of telecommunication services shall be recorded in a central database in a predefined format. The harms arising out of AI incidents shall be mitigated as per a predefined standard operating procedure (SOP) based on the classification of AI incidents. All AI incidents shall be investigated and analyzed as per a predefined mechanism. Critical severity AI incidents and high severity AI incidents shall be informed to TRAI in a prescribed format, manner and timeframe.
- (e) Human oversight: All AI systems shall be subject to an appropriate human oversight for risk mitigation as per a predefined mechanism.
- (f) Data governance: The data used or generated at each stage of the lifecycle of deployed AI systems shall be lawfully and securely collected, used, shared, and disposed of in accordance with the applicable data-protection, privacy protection, confidentiality, cybersecurity requirements and other statutory requirements.
- (g) Consumer protection and grievance redressal mechanism: AI-related harms reported by users shall be resolved within a reasonable timeframe as per a predefined grievance redressal mechanism.

3.3. The applicable authorised entity shall review its internal AI policy on telecom - at least once in a financial year, and additionally whenever such a review is necessary - to ensure its continuing suitability, adequacy and effectiveness.

- 3.4. The internal AI policy on telecom and its subsequent amendment(s), if any, shall be filed with TRAI for record within seven working days from the date of its coming into effect.

B. Implementation of internal AI policy on telecom

- 3.5. The applicable authorised entity shall -
- (a) Maintain a comprehensive, up-to-date inventory of all active, inactive and decommissioned AI systems. The record of each AI system in the inventory shall include the source, purpose and risk classification of the AI system. No AI system shall be used unless it is a part of the inventory.
 - (b) Undertake due diligence prior to acquisition or use of an AI system procured from a third party. The due diligence should, *inter alia*, include credibility of the supplier, soundness of the AI system and its limitations, and the suitability and quality of data used for training.
 - (c) Ensure validation, conformity assessment, and impact assessment before deployment of any new AI system or modification of an existing AI system. The conformity assessment shall cover accuracy, robustness, explainability, fairness, drift resilience and human oversight to mitigate undesirable outcomes. For instance, for the purpose of fairness assessment, the most recent version of Telecommunication Engineering Center (TEC) standard 57050:2023 for Fairness Assessment and Rating of Artificial Intelligence Systems or an applicable international standard may be used, where appropriate.
 - (d) Assess and categorize each AI system as per the risk classification of AI systems defined in the internal AI policy on telecom. Appropriate human oversight shall be provided to the deployed AI system based on the assessment. The categorization of each AI system shall be reviewed at least once in a financial year, or in response to specific AI incidents.
 - (e) Obtain disclosures of AI systems along with necessary details from suppliers/ prospective suppliers at the time of procuring

telecommunication equipment/ system/ solution embedded with AI system(s).

- (f) Incorporate necessary enforceable provisions in supplier agreements relating to regulatory compliance, audit and inspection rights, incident management, risk allocation and accountability in respect of each AI system procured from third parties before their deployment.
- (g) Establish and maintain a central database for recording AI incidents arising from AI systems, including testing events. AI incidents shall be categorized based on severity of the incident as per the classification of AI incidents defined in the internal AI policy on telecom. AI incidents should be recorded using the TEC standard 57090:2025 on Schema and Taxonomy of an AI Incident Database in Telecommunications and Critical Digital Infrastructure, or an equivalent taxonomy.
- (h) Mitigate the disruptions caused by AI incidents as per the predefined standard operating procedure (SOP).
- (i) Investigate and analyze all AI incidents as per the mechanism defined in the internal AI policy on telecom. The analysis of AI incidents shall be shared with all relevant units of the applicable authorised entity.
- (j) Establish and maintain a central database for recording reports of AI-related harm caused to telecommunication users of the applicable authorised entity and resolution thereof.
- (k) Conduct periodic AI-related training for the relevant technical, operational, regulatory, and business personnel involved in human oversight on AI systems.

C. Oversight on the implementation of internal AI policy on telecom

- 3.6. To oversee the implementation of the internal AI policy on telecom, the applicable authorised entity shall establish an *AI Governance and Safety Committee (AGSC)* with the approval of its board of directors, or an equivalent

governing body. The AGSC shall include appropriate representation from various relevant verticals of the organization such as network operation, service delivery, information technology, data management, regulatory, consumer affairs, and other relevant business functions, as necessary. The AGSC shall be headed by an *AI Governance and Safety Officer (AGSO)* who shall be a senior executive.

- 3.7. AGSC shall periodically review - at least once in a financial year, and additionally whenever such a review is necessary - the performance of the deployed AI systems, including AI incident records and other relevant information to identify significant vulnerabilities, oversight weaknesses, fairness concerns, and emerging or systemic risks. Based on such reviews, AGSO shall ensure that appropriate corrective measures, including modification, decommissioning of relevant AI system(s), where necessary, are undertaken.

D. Enforcement and compliances

- 3.8. The applicable authorised entity shall be accountable for the outcome of all AI systems used by it, irrespective of whether the AI systems are developed internally, procured/ outsourced from third party or a combination thereof.
- 3.9. The applicable authorised entity shall report critical-severity AI incidents and high-severity AI incidents, including material malfunctions, recurring failures, and mitigation measures to TRAI in a prescribed form, manner, and timeframe. Such information may be used for sector-wide learning, risk assessment, advisories, preventive measures, and other lawful regulatory purposes.

- 3.10. The applicable authorised entity shall maintain adequate records to demonstrate compliance with these guidelines and furnish relevant records, assessments, reports, or other information to TRAI as and when required.
- 3.11. Nothing contained in these guidelines shall limit, derogate from, or otherwise affect the applicability of any law, rule, regulation, direction, order, authorisation or license condition, or other binding requirements. Any act or omission arising out of or in connection with the development, procurement, integration, testing, deployment, operation, use, modification, or decommissioning of an AI system that constitutes a contravention, violation, or offence under applicable law shall be dealt with in accordance with the relevant provisions thereof.

Definitions Used in these Guidelines

1. **Artificial Intelligence** means the ability of machines to perform tasks that normally require human intelligence. It enables systems to learn from experience, adapt to new situations, and solve complex problems independently.
2. **AI system** means a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate output such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment.
3. **AI Incident** means an event where an AI system malfunctions, produces unintended outcomes, or behaves unpredictably, potentially causing harm or violating legal rights.
4. **Accuracy** means closeness of results of observations, computations, or estimates to the true values or the values accepted as being true.
5. **Accountability** means the obligation of individuals or organizations to account for their actions, accept responsibility, and disclose results transparently through specific means and criteria.
6. **Explainability** means property of an AI system to express important factors influencing the output of the AI system in a way that humans can understand.
7. **Fairness** means ensuring AI decisions are free from harmful bias or discrimination.

8. **Risk** means the composite measure of an event's probability of occurring and the magnitude or degree of the consequences of the corresponding event.
9. **Robustness** means the ability of a system to maintain its level of performance under a variety of circumstances.
10. **Resilient AI system** means an AI system that can withstand unexpected adverse events or unexpected changes in their environment or use – or if they can maintain their functions and structure in the face of internal and external change and degrade safely and gracefully when this is necessary.
11. **Validation** means the confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled.

Stakeholders are requested to provide detailed input with justification on the above draft guidelines.