The Draft Artificial Intelligence (Development & Regulation) Act, 2023

AIACT.IN

ARTIFICIALINTELLIGENCEACT.IN

Version **5.0** | April 3, 2025 | Author: **Abhivardhan**, Indic Pacific Legal Research

Read the Original Version of the Draft Bill here

The Terms of Use of this resource can be read at
indicpacific.com/ai | aiact.in | artificial intelligenceact.in

About AIACT.IN

AIACT.IN is India's first privately proposed artificial intelligence regulation for India, authored and prepared by Abhivardhan, the Managing Partner of Indic Pacific Legal Research, and the Chairperson & Managing Trustee of the Indian Society of Artificial Intelligence and Law. The purpose behind drafting and proposing AIACT.IN is to promote a democratic, practical and inclusive discourse around AI regulation in India. The first version of AIACT.IN was proposed and published by Indic Pacific Legal Research on November 7, 2023. This is the **fourth version** of AIACT.IN released on **November 8, 2024**.

About Abhivardhan

Abhivardhan is honoured to serve as the Chairperson & Managing Trustee of the Indian Society of Artificial Intelligence and Law and as the Managing Partner at Indic Pacific Legal Research. Throughout his journey, he has gained valuable experience in international technology law, corporate innovation, global governance, and cultural intelligence.

With deep respect for the field, Abhivardhan has been fortunate to contribute to esteemed law, technology, and policy magazines and blogs. His book, "Artificial Intelligence Ethics and International Law" (2nd edition, 2024), modestly represents his exploration of the important connection between artificial intelligence and ethical considerations. Emphasizing the significance of an Indic approach to AI Ethics, Abhivardhan aims to bring diverse perspectives to the table.

Abhivardhan remains humbled by the opportunity to share knowledge through various papers on international technology law. Alongside his consulting and policy advocacy, he has been involved in both authoring and editing books, focusing on public international law and its relationship with artificial intelligence.

Some of his notable books, reports and research publications also include:

- 2020 Handbook on AI and International Law [RHB 2020 ISAIL] (2021)
- 2021 Handbook on AI and International Law [RHB 2021 ISAIL] (2022)
- Deciphering Artificial Intelligence Hype and its Legal-Economic Risks, VLiGTA-TR-001 (2022)
- Deciphering Regulative Methods for Generative AI, VLiGTA-TR-002 (2023)
- Reinventing & Regulating Policy Use Cases of Web3 for India, VLiGTA-TR-004 (2023)
- A New Artificial Intelligence Strategy for India and the Artificial Intelligence (Development & Regulation) Bill, 2023 (2023)

Maintaining a down-to-earth approach, Abhivardhan's speaking and research interests revolve around Indo-Pacific affairs, disruptive technology ethics and policies, artificial intelligence governance, Indo-European culture and music, global governance, sustainable development, digital connectivity, and public international law.

Table of Contents

CHAPTER I: PRELIMINARY

Section 1 – Short Title and Commencement

(1) This Act may be called the **Artificial Intelligence (Development & Regulation) Act, 2023**.

(2) It shall come into force on such date as the Central Government may, by notification in the Official Gazette, appoint and different dates may be appointed for different provisions of this Act and any reference in any such provision to the commencement of this Act shall be construed as a reference to the coming into force of that provision.

Section 2 – Definitions

[Please note: we have not provided all definitions, which may be required in this Act. We have only provided those definitions which are more essential, in signifying the legislative intent of the Act.]

In this Act, unless the context otherwise requires —

(a) "Artificial Intelligence", "AI", "AI technology", "artificial intelligence technology", "artificial intelligence application", "artificial intelligence system" and "AI systems" mean an information system that employs computational, statistical, or machine-learning techniques to generate outputs based on given inputs. Such a system constitutes a diverse class of technology that includes various sub-categories of technical, commercial, and sectoral nature, in accordance with the means of classification set forth in Section 3.

(b) "AI-Generated Content" means content, physical or digital that has been created or significantly modified by an artificial intelligence technology, which includes, but is not limited to text, images, audio, and video created through a variety of techniques, subject to the test case or the use case of the artificial intelligence application.

(c) "Algorithmic Bias" includes –

  (i) the inherent technical limitations within an artificial intelligence product, service or system that lead to systematic and repeatable errors in processing, analysis, or output generation, resulting in outcomes that deviate from objective, fair, or intended results; and

  (ii) the technical limitations within artificial intelligence products, services and systems that emerge from the design, development, and operational stages of AI, including but not limited to:

    (a) programming errors;

    (b) flawed algorithmic logic; and

    (c) deficiencies in model training and validation, including but not limited to:

      (1) the incomplete or deficient data used for model training;

(d) "Appellate Tribunal" means the Telecom Disputes Settlement and Appellate Tribunal established under section 14 of the Telecom Regulatory Authority of India Act, 1997;

(e) "Business end-user" means an end-user that is -

(i) engaged in a commercial or professional activity and uses an AI system in the course of such activity; or

(ii) a government agency or public authority that uses an AI system in the performance of its official functions or provision of public services.

(f) "Combinations of intellectual property protections" means the integrated application of various intellectual property rights, such as copyrights, patents, trademarks, trade secrets, and design rights, to safeguard the unique features and components of artificial intelligence systems;

(g) "Content Provenance" means the identification, tracking, and watermarking of AI-generated content using a set of techniques to establish its origin, authenticity, and history, including:

(i) The source data, models, and algorithms used to generate the content;

(ii) The individuals or entities involved in the creation, modification, and distribution of the content;

(iii) The date, time, and location of content creation and any subsequent modifications;

(iv) The intended purpose, context, and target audience of the content;

(v) Any external content, citations, or references used in the creation of the AI-generated content, including the provenance of such external sources; and

(vi) The chain of custody and any transformations or iterations the content undergoes, forming a content and citation/reference loop that enables traceability and accountability.

(h) "Corporate Governance" means the system of rules, practices, and processes by which an organisation is directed and controlled, encompassing the mechanisms through which companies, and organisations, ensure accountability, fairness, and transparency in their relationships with stakeholders including but not limited to employees, shareholders, customers, and the public.

(i) "Data" means a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by human beings or by automated or augmented means;

(j) "Data Fiduciary" means any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data;

(k) "Data portability" means the ability of a data principal to request and receive their personal data processed by a data fiduciary in a structured, commonly used, and machine-readable format, and to transmit that data to another data fiduciary, where:

(i) The personal data has been provided to the data fiduciary by the data principal;

(ii) The processing is based on consent or the performance of a contract; and

(iii) The processing is carried out by automated means.

(l) "Data Principal" means the individual to whom the personal data relates and where such individual is—

(i) a child, includes the parents or lawful guardian of such a child;

(ii) a person with disability, includes her lawful guardian, acting on her behalf;

(m) "Data Protection Officer" means an individual appointed by the Significant Data Fiduciary under clause (a) of sub-section (2) of section 10 of the Digital Personal Data Protection Act, 2023;

(n) "Data Scraping" means the automated collection, extraction, or mining of data from websites, online platforms, or digital sources through technical means including but not limited to automated tools, web crawlers, or software applications that extract information from websites or online platforms;

(o) "Digital Office" means an office that adopts an online mechanism wherein the proceedings, from receipt of intimation or complaint or reference or directions or appeal, as the case may be, to the disposal thereof, are conducted in online or digital mode;

(p) "Digital personal data" means personal data in digital form;

(q) "End-user" means -

(i) an individual who ultimately uses or is intended to ultimately use an AI system, directly or indirectly, for personal, domestic or household purposes; or

(ii) an entity, including a business or organisation, that uses an AI system to provide or offer a product, service, or experience to individuals, whether for a fee or free of charge.

(r) "Knowledge asset" includes, but is not limited to:

(i) Intellectual property rights including but not limited to patents, copyrights, trademarks, and industrial designs;

(ii) Documented knowledge, including but not limited to research reports, technical manuals and industrial practices & standards;

(iii) Tacit knowledge and expertise residing within the organisation's human capital, such as specialized skills, experiences, and know-how;

(iv) Organisational processes, systems, and methodologies that enable the effective capture, organisation, and utilisation of knowledge;

(v) Customer-related knowledge, such as customer data, feedback, and insights into customer needs and preferences;

(vi) Knowledge derived from data analysis, including patterns, trends, and predictive models; and

(vii) Collaborative knowledge generated through cross-functional teams, communities of practice, and knowledge-sharing initiatives.

(s) "Knowledge management" means the systematic processes and methods employed by organisations to capture, organize, share, and utilize knowledge assets related to the development, deployment, and regulation of artificial intelligence systems;

(t) "IAIC" means Indian Artificial Intelligence Council;

(u) "Inherent Purpose", and "Intended Purpose" means the underlying technical objective for which an artificial intelligence technology is designed, developed, and deployed, and that it encompasses the specific tasks, functions, and capabilities that the artificial intelligence technology is intended to perform or achieve;

(v) "Insurance Policy" means measures and requirements concerning insurance for research & development, production, and implementation of artificial intelligence technologies;

(w) "Interoperability considerations" means the technical, legal, and operational factors that enable artificial intelligence systems to work together seamlessly, exchange information, and operate across different platforms and environments, which include:

(i) Ensuring that the combinations of intellectual property protections, including but not limited to copyrights, patents, trademarks, and design rights, do not unduly hinder the interoperability of AI systems and their ability to access and use data and knowledge assets necessary for their operation and improvement;

(ii) Balancing the need for intellectual property protections to incentivize innovation in AI with the need for transparency, explainability, and accountability in AI systems, particularly when they are used in decision-making processes that affect individuals and public good;

(iii) Developing technical standards, application programming interfaces (APIs), and other mechanisms that facilitate the seamless integration and communication between AI systems, while respecting intellectual property rights and maintaining the security and integrity of the systems;

(iv) Promoting the development of open and interoperable AI frameworks, libraries, and tools that enable developers to build upon existing AI technologies and create new applications;

(x) "Open-Source Software" means computer software that is distributed with its source code made available and licensed with the right to study, change, and distribute the software to anyone and for any purpose.

(y) "National Registry of Artificial Intelligence Use Cases" means a national-level digitised registry of use cases of artificial intelligence technologies based on their technical, commercial & risk-based

features, maintained by the Central Government for the purposes of standardisation and certification of use cases of artificial intelligence technologies;

(z) "Person" includes—

(i) an individual;

(ii) a Hindu undivided family;

(iii) a company;

(iv) a firm;

(v) an association of persons or a body of individuals, whether incorporated or not;

(vi) the State; and

(vii) every artificial juristic person, not falling within any of the preceding sub-clauses including otherwise referred to in sub-section (r);

(aa) "Post-Deployment Monitoring" means all activities carried out by Data Fiduciaries or third-party providers of AI systems to collect and review experience gained from the use of the artificial intelligence systems they place on the market or put into service;

(bb) **"Public Interest Use" includes research, education, analysis, journalism, and non-commercial innovation that may qualify under Section 52 of the Copyright Act, 1957 as fair dealing or permitted use.**

(cc) "Quality Assessment" means the evaluation and determination of the quality of AI systems based on their technical, ethical, and commercial aspects;

(dd) "Significant Data Fiduciary" means any Data Fiduciary or class of Data Fiduciaries as may be notified by the Central Government under section 10 of the Digital Personal Data Protection Act, 2023;

(ee) "Sociotechnical" means the recognition that artificial intelligence systems are not merely technical artifacts but are embedded within broader social contexts, organisational structures, and human-technology interactions, necessitating the consideration and harmonisation of both social and technical aspects to ensure responsible and effective AI governance;

(ff) "State" shall be construed as the State defined under Article 12 of the Constitution of India;

(gg) "Strategic sector" shall mean any sector classified as strategic under the Foreign Exchange Management (Overseas Investment) Directions, 2022, and shall further include any sector or sub-sector as may be designated by the Central Government, having regard to considerations of national security, economic sovereignty, critical infrastructure, or technological advancement, in accordance with the principles set forth in Section 21A.

(hh) "techno-solutionism" means the systematic implementation of artificial intelligence systems or computational technologies as primary solutions to public administration challenges while failing to adequately address underlying non-technical factors;

Explanation.—For the purposes of this definition, techno-solutionism includes—

(i) implementing automated decision systems that directly impact legally recognized rights without providing affected persons a clear mechanism to present their case before or after such decisions;

(ii) deploying AI systems that create demonstrable risk of unfairness by prioritizing computational processing over consideration of individual circumstances;

(iii) automating administrative processes in ways that prevent affected persons from obtaining specific explanations for decisions affecting their legal interests;

(iv) replacing necessary human evaluation with automated systems in contexts where established law requires case-specific assessment, proportionality testing, or application of discretion;

(v) justifying technological implementation primarily based on operational metrics (such as cost-reduction or processing speed) without measuring improvement in addressing the underlying public issue; and

(vi) allocating public resources to technological systems for problems that fundamentally result from policy deficiencies, resource limitations, or structural issues that technology alone cannot solve;

(ii) "training data" means data used for training an AI system through fitting its learnable parameters, which includes the weights of a neural network;

(jj) "testing data" means data used for providing an independent evaluation of the artificial intelligence system subject to training and validation to confirm the expected performance of that artificial intelligence technology before its placing on the market or putting into service;

(kk) "use case" means a specific application of an artificial intelligence technology, subject to their inherent purpose, to solve a particular problem or achieve a desired outcome;

CHAPTER II: CATEGORISATION AND PROHIBITION

Section 3 - Classification of Artificial Intelligence

(1) All artificial intelligence technologies are categorised on the basis of the means of classification provided as follows –

(i) **Conceptual methods of classification**: These methods as described in Section 4 categorize artificial intelligence technologies through a conceptual assessment of their utilisation, development, maintenance, and proliferation to examine & recognise their inherent purpose. These methods include:

(a) Issue-to-Issue Concept Classification (IICC)
(b) Ethics-Based Concept Classification (EBCC)
(c) Phenomena-Based Concept Classification (PBCC)
(d) Anthropomorphism-Based Concept Classification (ABCC)

(ii) **Technical methods of classification**: These methods as described in Section 5 classify artificial intelligence technologies subject to their scale, inherent purpose, technical features and technical limitations. These methods include:
   (a) General Purpose Artificial Intelligence Applications with Multiple Stable Use Cases (GPAIS)
   (b) General Purpose Artificial Intelligence Applications with Multiple Short-Run or Unclear Use Cases (GPAIU)
   (c) Specific-Purpose Artificial Intelligence Applications with One or More Associated Standalone Use Cases or Test Cases (SPAI)

(iii) **Commercial methods of classification**: These methods as described in Section 6 involve the categorisation of commercially and industrially produced and disseminated artificial intelligence technologies subject to their inherent purpose.
   (a) Artificial Intelligence as a Product (AI-Pro)
   (b) Artificial Intelligence as a Service (AIaaS)
   (c) Artificial Intelligence as a Component (AI-Com)
   (d) Artificial Intelligence as a System (AI-S)
   (e) Artificial Intelligence-enabled Infrastructure as a Service (AI-IaaS)
   (f) Artificial Intelligence for Preview (AI-Pre)

(iv) **Risk-centric methods of classification**: These methods as described in Section 7 classify artificial intelligence technologies based on their outcome and impact-based risks.
   (a) Narrow Risk AI Systems
   (b) Medium Risk AI Systems
   (c) High Risk AI Systems
   (d) Unintended Risk AI Systems

Section 4 – Conceptual Methods of Classification

(1) These methods as designated in clause (i) of sub-section (1) of Section 3 categorize artificial intelligence technologies through a conceptual assessment of their utilisation, development, maintenance, and proliferation to examine & recognise their inherent purpose. This classification is further categorised as –
   (i) Issue-to-Issue Concept Classification (IICC) as described in sub-section (2)
   (ii) Ethics-Based Concept Classification (EBCC) as described in in sub-section (3)
   (iii) Phenomena-Based Concept Classification (PBCC) as described in in sub-section (4)
   (iv) Anthropomorphism-Based Concept Classification (ABCC) as described in in sub-section (5)

(2) Issue-to-Issue Concept Classification (IICC) involves the method to determine the inherent purpose of artificial intelligence technologies on a case-to-case basis, to examine & recognise their inherent purpose on the basis of these factors of assessment:
   (i) **Utilisation**: Assessing the specific use cases and applications of the AI technology in various domains.
   (ii) **Development**: Evaluating the design, training, and deployment processes of the AI technology.
   (iii) **Maintenance**: Examining the ongoing support, updates, and modifications made to the AI technology.

(iv) **Proliferation**: Analysing the dissemination and adoption of the AI technology across different sectors and user groups.

Illustrations

(1) An AI system designed for medical diagnostics is classified based on its purpose to enhance patient outcomes. For instance, if an AI software assists doctors in diagnosing diseases more accurately, it is classified under medical AI applications.
(2) An AI system for financial trading is classified based on its purpose to optimize investment strategies. For example, if an AI-driven algorithm analyses market data to recommend stock trades, it is classified under financial AI applications.

(3) Ethics-Based Concept Classification (EBCC) involves the method of recognising the ethics-based relationship of artificial intelligence technologies in sector-specific & sector-neutral contexts, to examine & recognise their inherent purpose on the basis of these factors:
(i) **Utilisation**: Evaluating how AI technology impacts ethical principles during its use in specific sectors or across multiple domains.
(ii) **Development**: Assessing whether ethical considerations were integrated during the design, training, and deployment phases of the AI technology.
(iii) **Maintenance**: Examining how ethical responsibilities are upheld during updates and modifications to the AI system.
(iv) **Proliferation**: Analyzing how the widespread adoption of the AI system affects ethical standards across sectors and user groups.

Illustration

An AI for social media content moderation is assessed based on fairness and bias prevention. For example, if an AI filters hate speech and misinformation on social media platforms, it is classified under content moderation AI with an emphasis on ensuring unbiased and fair treatment of all users' content.

(4) Phenomena-Based Concept Classification (PBCC) involves the method of addressing rights-based issues associated with the use and dissemination of artificial intelligence technologies to examine & recognise their inherent purpose on the basis of these factors:
(i) **Utilisation**: Assessing how the AI system affects individual or collective rights during its use in various domains.
(ii) **Development**: Evaluating whether evaluates whether AI systems incorporate protections for rights recognized under Indian law during their design, training, and deployment phases, considering legal constitutional, and commercial rights.
(iii) **Maintenance**: Reviewing how ongoing support and updates to the AI system protect user rights.
(iv) **Proliferation**: Analysing the rights-based implications of AI technology dissemination and adoption across different sectors and user groups.

Illustrations

(1) An AI system that analyses personal data for targeted advertising is classified based on its compliance with data protection rights. For example, an AI that personalizes ads based on user behaviour is classified under advertising AI with data privacy considerations.
(2) An AI used in autonomous vehicles is classified based on its implications for road safety and user rights. For instance, an AI that controls self-driving cars is classified under automotive AI with a focus on safety and user rights.

(5) Anthropomorphism-Based Concept Classification (ABCC) involves the method of evaluating scenarios where AI systems ordinarily simulate, imitate, replicate, or emulate human attributes, which include:

(i) **Autonomy**: The ability to operate and make decisions independently, based on a set of corresponding scenarios including but not limited to:

- **Simulation**: AI systems model autonomous decision-making processes using computational methods;
- **Imitation**: AI systems learn from and reproduce human-like autonomous behaviours;
- **Replication**: AI systems accurately reproduce specific human-like autonomous functions;
- **Emulation**: AI systems replicate and potentially enhance human-like autonomy;

Illustration

An AI-powered drone delivery system that navigates through urban environments, avoiding obstacles and adapting its route based on real-time traffic conditions to efficiently deliver packages without human intervention.

(ii) **Perception**: The ability to interpret and understand sensory information from the environment, based on a set of corresponding scenarios including but not limited to:

- **Simulation**: AI systems model human-like perception using computational methods;
- **Imitation**: AI systems learn from and reproduce specific human-like perceptual processes;
- **Replication**: AI systems accurately reproduce specific human-like perceptual abilities;

Illustration

A service robot in a hotel uses computer vision and natural language processing to recognize and greet guests by name, interpret their facial expressions and tone of voice to gauge emotions, and respond appropriately to verbal requests.

(iii) **Reasoning**: The ability to process information, draw conclusions, and solve problems, based on a set of corresponding scenarios including but not limited to:

- **Simulation**: AI systems model human-like reasoning using computational methods;
- **Imitation**: AI systems learn from and reproduce specific human reasoning patterns;
- **Replication**: AI systems accurately reproduce specific human-like reasoning abilities;
- **Emulation**: AI systems surpass specific human-like reasoning abilities;

Illustration

A medical diagnosis AI system analyses a patient's symptoms, medical history, test results and imaging scans. It uses this information to generate a list of probable diagnoses, suggest additional tests to rule out possibilities, and recommend an optimal treatment plan.

(iv) **Interaction**: The ability to communicate and engage with humans or other AI systems, based on a set of corresponding scenarios including but not limited to:

- **Simulation**: AI systems model human-like interaction using computational methods;
- **Imitation**: AI systems learn from and reproduce specific human interaction patterns;
- **Replication**: AI systems accurately reproduce specific human-like interaction abilities;
- **Emulation**: AI systems enhance human-like interaction;

Illustration

An AI-powered virtual assistant engages in natural conversations with users, understanding context and nuance. It asks clarifying questions when needed, provides relevant information or executes tasks, and even interjects with suggestions or prompts.

(v) **Adaptation**: The ability to learn from experiences and adjust behaviour accordingly, based on a set of corresponding scenarios including but not limited to:

- **Simulation**: AI systems model human-like adaptation using computational methods.
- **Imitation**: AI systems learn from and reproduce human adaptation behaviours.
- **Replication**: AI systems reproduce human-like adaptation abilities, recognizing the inherent complexity.
- **Emulation**: AI systems surpass human-like adaptation as an aspirational goal.

Illustration

An AI system for stock trading continuously analyses market trends, world events, and the performance of its own trades. It identifies patterns and correlations, learning which strategies work best in different scenarios. The AI optimizes its trading algorithms and adapts its approach based on accumulated experience, demonstrating adaptive abilities.

(vi) **Creativity**: The ability to generate novel ideas, solutions, or outputs, based on a set of corresponding scenarios including but not limited to:

- **Simulation**: AI systems model human-like creativity using computational methods;
- **Imitation**: AI systems learn from and reproduce human creative processes;
- **Replication**: AI systems accurately reproduce human-like creative abilities, acknowledging the complexity involved;
- **Emulation**: AI systems enhance human-like creativity as a forward-looking objective;

Illustration

An AI music composition tool creates an original symphony. Given a theme and emotional tone, it generates unique melodies, harmonies and instrumentation. It iterates and refines the composition based on aesthetic evaluation models, ultimately producing a piece that is distinct from existing music in its training data.

Section 5 – Technical Methods of Classification

(1) These methods as designated in clause (ii) of sub-section (1) of Section 3 classify artificial intelligence technologies subject to their scale, inherent purpose, technical features and technical limitations such as –

(i) General Purpose Artificial Intelligence Applications with Multiple Stable Use Cases (GPAIS) as described in sub-section (2);

(ii) General Purpose Artificial Intelligence Applications with Multiple Short-Run or Unclear Use Cases (GPAIU) as described in sub-section (3);

(iii) Specific-Purpose Artificial Intelligence Applications with One or More Associated Standalone Use Cases or Test Cases (SPAI) as described in sub-section (4);

(2) General Purpose Artificial Intelligence Systems with Multiple Stable Use Cases (GPAIS) are classified based on a technical method that evaluates the following factors in accordance with relevant sector-specific and sector-neutral industrial standards:

(i) Scale: The ability to operate effectively and consistently across a wide range of domains, handling large volumes of data and users.

(ii) Inherent Purpose: The capacity to be adapted and applied to multiple well-defined use cases within and across sectors.

(iii) Technical Features: Robust and flexible architectures that enable reliable performance on diverse tasks and requirements.

(iv) Technical Limitations: Potential challenges in maintaining consistent performance and compliance with sector-specific regulations across the full scope of intended use cases.

Illustration

An AI system used in healthcare for diagnostics, treatment recommendations, and patient management. This AI consistently performs well in various healthcare settings, adhering to medical standards and providing reliable outcomes. It is characterized by its large scale in handling diverse medical data and serving multiple institutions, its inherent purpose of assisting healthcare professionals in decision-making and care improvement, robust technical architecture and accuracy while adhering to privacy and security standards, and potential limitations in edge cases or rare conditions.

(3) General Purpose Artificial Intelligence Systems with Multiple Short-Run or Unclear Use Cases (GPAIU) are classified based on a technical method that evaluates the following factors in accordance with relevant sector-specific and sector-neutral industrial standards:

(i) Scale: The ability to address specific short-term needs or exploratory applications within relevant sectors at a medium scale.

(ii) Inherent Purpose: Providing targeted solutions for emerging or temporary use cases, with the potential for future adaptation and expansion.

(iii) Technical Features: Modular and adaptable architectures enabling rapid development and deployment in response to evolving requirements.

(iv) Technical Limitations: Uncertainties regarding long-term viability, scalability, and compliance with changing industry standards and regulations.

Illustration

An AI system used in experimental smart city projects for traffic management, pollution monitoring, and public safety. Deployed at a medium scale in specific locations for limited durations, its inherent purpose is testing and validating AI feasibility and effectiveness in smart city applications. It features a modular, adaptable technical architecture to accommodate changing requirements and infrastructure integration, but faces potential limitations in scalability, interoperability, and long-term performance due to the experimental nature.

(4) Specific-Purpose Artificial Intelligence Systems with One or More Associated Standalone Use Cases or Test Cases (SPAI) are classified based on a technical method that evaluates the following factors:

(i) Scale: The ability to address specific, well-defined problems or serve as proof-of-concept implementations at a small scale.

(ii) Inherent Purpose: Providing specialized solutions for individual use cases or validating AI technique feasibility in controlled environments.

(iii) Technical Features: Focused and optimized architectures tailored to the specific requirements of the standalone use case or test case.

(iv) Technical Limitations: Constraints on generalizability, difficulties scaling beyond the initial use case, and challenges ensuring real-world robustness and reliability.

Illustration

An AI chatbot used by a company for customer service during a product launch. As a small-scale standalone application, its inherent purpose is providing automated support for a specific product or service. It employs a focused, optimized technical architecture for handling product-related queries and interactions, but faces limitations in handling queries outside the predefined scope or adapting to new products without significant modifications.

Section 6 – Commercial Methods of Classification

(1) These methods as designated in clause (iii) of sub-section (1) of Section 3 involve the categorisation of commercially produced and disseminated artificial intelligence technologies based on their inherent purpose and primary intended use, considering factors such as:

(i) The core functionality and technical capabilities of the artificial intelligence technology;

(ii) The main end-users or business end-users for the artificial intelligence technology, and the size of the user base or market share;

(iii) The primary markets, sectors, or domains in which the artificial intelligence technology is intended to be applied, and the market influence or dominance in those sectors;

(iv) The key benefits, outcomes, or results the artificial intelligence technology is designed to deliver, and the potential impact on individuals, businesses, or society;

(v) The annual turnover or revenue generated by the artificial intelligence technology or the company developing and deploying it;

(vi) The amount of data collected, processed, or utilized by the artificial intelligence technology, and the level of data integration across different services or platforms; and

(vii) Any other quantitative or qualitative factors that may be prescribed by the Central Government or the Indian Artificial Intelligence Council (IAIC) to assess the significance and impact of the artificial intelligence technology.

(2) Based on an assessment of the factors outlined in sub-section (1), artificial intelligence technologies are classified into the following categories –

(i) Artificial Intelligence as a Product (AI-Pro), as described in sub-section (3);

(ii) Artificial Intelligence as a Service (AIaaS), as described in sub-section (4);

(iii) Artificial Intelligence as a Component (AI-Com) which includes artificial intelligence technologies directly integrated into existing products, services & system infrastructure, as described in sub-section (5);

(iv) Artificial Intelligence as a System (AI-S), which includes layers or interfaces in AIaaS provided which facilitates the integration of capabilities of artificial intelligence technologies into existing systems in whole or in parts, as described in sub-section (6);

(v) Artificial Intelligence-enabled Infrastructure as a Service (AI-IaaS) which includes artificial intelligence technologies directly integrated into existing components and layers of digital infrastructure, as described in sub-section (7);

(vi) Artificial Intelligence for Preview (AI-Pre), as described in sub-section (8);

(3) Artificial Intelligence as a Product (AI-Pro) refers to standalone AI applications or software that are developed and sold as individual products to end-users. These products are designed to perform specific tasks or provide particular services directly to the user;

Illustrations

(1) An AI-powered home assistant device as a product is marketed and sold as a consumer electronic device that provides functionalities like voice recognition, smart home control, and personal assistance.

(2) A commercial software package for predictive analytics is used by businesses to forecast market trends and consumer behaviour.

(4) Artificial Intelligence as a Service (AIaaS) refers to cloud-based AI solutions that are provided to users on-demand over the internet. Users can access and utilize the capabilities of AI systems without the need to develop or maintain the underlying infrastructure;

Illustrations

(1) A cloud-based machine learning platform offers businesses and developers access to powerful AI tools and frameworks on a subscription basis.

(2) An AI-driven customer service chatbot service that businesses can integrate into their websites to handle customer inquiries and support.

(5) Artificial Intelligence as a Component (AI-Com) refers to AI technologies that are embedded or integrated into existing products, services, or system infrastructures to enhance their capabilities or performance. In this case, the AI component is not a standalone product but rather a part of a larger system;

Illustrations

(1) An AI-based recommendation engine integrated into an e-commerce platform to provide personalized shopping suggestions to users.
(2) AI-enhanced cameras in smartphones that utilize machine learning algorithms to improve photo quality and provide features like facial recognition.

(6) Artificial Intelligence as a System (AI-S) refers to end-to-end AI solutions that combine multiple AI components, models, and interfaces. These systems often involve the integration of AI capabilities into existing workflows or the creation of entirely new AI-driven processes in whole or in parts;

Illustrations

(1) An AI middleware platform that connects various enterprise applications to enhance their functionalities with AI capabilities, such as an AI layer that integrates with CRM systems to provide predictive sales analytics.
(2) An AI system used in smart manufacturing, where AI interfaces integrate with industrial machinery to optimize production processes and maintenance schedules.

(7) Artificial Intelligence-enabled Infrastructure as a Service (AI-IaaS) refers to the integration of AI technologies into the underlying computing, storage, and network infrastructure to optimize resource allocation, improve efficiency, and enable intelligent automation. This category focuses on the use of AI at the infrastructure level rather than at the application or service level.

Illustrations

(1) An AI-enabled traffic management system that integrates with city infrastructure to monitor and manage traffic flow, reduce congestion, and optimize public transportation schedules.
(2) AI-powered utilities management systems that are integrated into the energy grid to predict and manage energy consumption, enhancing efficiency and reducing costs.

(8) Artificial Intelligence for Preview (AI-Pre) refers to AI technologies that are made available by companies for testing, experimentation, or early access prior to wider commercial release. AI-Pre encompasses AI products, services, components, systems, platforms and infrastructure at various stages of development. AI-Pre technologies are typically characterized by one or more of the following features that may include but not limited to:
   (i) The AI technology is made available to a limited set of end users or participants in a preview program;
   (ii) Access to the AI-Pre technology is subject to special agreements that govern usage terms, data handling, intellectual property rights, and confidentiality;
   (iii) The AI technology may not be fully tested, documented, or supported, and the company providing it may offer no warranties or guarantees regarding its performance or fitness for any particular purpose.
   (iv) Users of the AI-Pre technology are often expected to provide feedback, report issues, or share data to help the company refine and improve the technology.
   (v) The AI-Pre technology may be provided free of charge, or under a separate pricing model from the company's standard commercial offerings.

(vi) After the preview period concludes, the company may release a commercial version of the AI technology, incorporating improvements and modifications based on feedback and data gathered during the preview. Alternatively, the company may choose not to proceed with a commercial release.

Illustration

A technology company develops a new general-purpose AI system that can engage in open-ended dialogue, answer questions, and assist with tasks across a wide range of domains. The company makes a preview version of the AI system available to select academic and industry partners with the following characteristics:

(1) The preview is accessible to the partners via an API, subject to a special preview agreement that governs usage terms, data handling, and confidentiality.
(2) The AI system's capabilities are not yet fully tested, documented or supported, and the company provides no warranties or guarantees.
(3) The partners can experiment with the system, provide feedback to the company to help refine the technology, and explore potential applications.
(4) After the preview period, the company may release a commercial version of the AI system as a paid product or service, with expanded capabilities, service level guarantees, and standard commercial terms.

Section 7 – Risk-centric Methods of Classification

(1) These methods as designated in clause (iv) of sub-section (1) of Section 3 classify artificial intelligence technologies based on their outcome and impact-based risks –
(i) Narrow risk AI systems as described in sub-section (2);
(ii) Medium risk AI systems as described in sub-section (3);
(iii) High risk AI systems as described in sub-section (4);
(iv) Unintended risk AI systems as described in sub-section (5);

(2) Narrow Risk AI Systems:

(i) Narrow risk AI systems are classified as those with minimal outcome and impact risks, where:

(a) The system is deployed in a limited scope for non-critical functions, so its outcomes do not significantly affect users or systems.
(b) The system causes minimal harm, with impacts limited to temporary inconvenience.
(c) Users can easily opt out of the system's operations, ensuring they are not forced to accept its outcomes.
(d) The system is fully explainable, allowing users to understand and mitigate any risks from its outcomes.
(e) Errors in the system's outcomes are easily reversible, with no lasting impact.

(ii) Risk recognition is achieved by assessing the system's outcomes, such as errors in non-critical tasks, and their impacts, such as temporary inconvenience, ensuring the category provisions directly identify minimal risks without abstract definitions.

Illustration: A virtual assistant on a smartphone app for task scheduling is a narrow risk system. It operates in a non-critical context, causes only temporary inconvenience if it fails, allows users to disable it, is fully explainable, and errors are easily reversible by resetting the app.

(3) Medium Risk AI Systems:

(i) Medium risk AI systems are classified as those with moderate outcome and impact risks, where:

(a) The system causes moderate harm, with outcomes that may lead to incorrect decisions affecting users' opportunities or resources.
(b) Users have limited ability to opt out or understand the system's operations, increasing the impact of its outcomes.
(c) The system may produce inconsistent outputs due to technical bias, such as overfitting to training data, affecting the reliability of its outcomes.
(d) Correcting errors in the system's outcomes requires active intervention, with impacts that may persist until addressed.

(ii) Risk assessment focuses on the system's technical features, such as model complexity or unverified data, which contribute to its outcome risks.
(iii) Risk recognition is achieved by assessing the system's outcomes, such as incorrect decisions in resource allocation, and their impacts, such as reduced opportunities for users, ensuring the category provisions directly identify moderate risks without abstract definitions.

Illustration: An AI loan approval system used by a regional bank is a medium risk system. It may lead to incorrect loan denials, limits users' ability to opt out, may overfit to biased training data, requires intervention to correct errors, and its risks stem from technical features like model complexity.

(4) High Risk AI Systems:

(i) High risk AI systems are classified as those with severe outcome and impact risks, where:

(a) The system is deployed in critical sectors, with outcomes that can disrupt essential services or infrastructure.
(b) The system causes severe harm, with impacts that may lead to physical harm, economic loss, or societal disruption.
(c) Users cannot opt out or control the system's operations, making its outcomes unavoidable.
(d) The system's lack of transparency increases the risk of undetected errors, amplifying the impact of its outcomes.
(e) Errors in the system's outcomes are irreversible or cause permanent harm, with significant long-term impacts.

(ii) Risk recognition is achieved by assessing the system's outcomes, such as disruptions in critical services, and their impacts, such as economic loss or societal harm, ensuring the category provisions directly identify severe risks without abstract definitions.

Illustration: An AI system controlling a power grid is a high risk system. It operates in a critical sector, can cause outages leading to economic loss, offers no user opt-out, lacks transparency, and failures have irreversible impacts like societal disruption.

(5) Unintended Risk AI Systems:

(i) Unintended risk AI systems are classified as those with emergent and unpredictable outcome and impact risks, where:

(a) The system's behaviour deviates from its intended design, leading to unexpected outcomes.
(b) The system processes data beyond its intended scope, increasing the risk of unintended impacts.
(c) The system evolves after deployment without oversight, causing outcomes that cannot be predicted or controlled.
(d) The system's operations are not explainable, making it impossible to understand or mitigate the risks of its outcomes.

(ii) Risk recognition is achieved by assessing the system's outcomes, such as unexpected behaviours in operation, and their impacts, such as unpredictable harm to users or systems, ensuring the category provisions directly identify emergent risks without abstract definitions.

Illustration: An autonomous vehicle navigation system with emergent behaviour is an unintended risk system. It deviates from its intended design, processes unintended data, evolves without oversight, and its operations are not explainable, leading to unpredictable outcomes like accidents.

Section 8 - Prohibition of Unintended Risk AI Systems

The development, deployment, and use of unintended risk AI systems, as classified under the sub-section (5) of Section 7, is prohibited.

Section 9 - High-Risk AI Systems in Strategic Sectors

(1) The Central Government shall designate strategic sectors where the development, deployment, and use of high-risk AI systems shall be subject to sector-specific standards and regulations, based on the risk classification methods outlined in Chapter II of this Act.
(2) In the event of any conflict between the provisions of this Act and sector-specific regulations concerning high-risk AI systems in strategic sectors, the provisions of this Act shall prevail, unless otherwise specified.

CHAPTER III: INDIAN ARTIFICIAL INTELLIGENCE COUNCIL

Section 10 - Composition and Functions of the Council

(1) With effect from the date notified by the Central Government, there shall be established the Indian Artificial Intelligence Council (IAIC), a statutory body for the purposes of this Act.

(2) The IAIC shall be an autonomous body corporate with perpetual succession, a common seal, and the power to acquire, hold and transfer property, both movable and immovable, and to contract and be contracted, and sue or be sued by its name.

(3) The IAIC shall coordinate and oversee the development, deployment, and governance of artificial intelligence systems across all government bodies, ministries, departments, and regulatory authorities, adopting a whole-of-government approach.

(4) The headquarters of the IAIC shall be located at the place notified by the Central Government.

(5) The IAIC shall consist of a Chairperson and such number of other Members, not exceeding [X], as the Central Government may notify.

(6) The Chairperson and Members shall be appointed by the Central Government through a transparent and merit-based selection process, as may be prescribed.

(7) The Chairperson and Members shall be individuals of eminence, integrity and standing, possessing specialized knowledge or practical experience in fields relevant to the IAIC's functions, including but not limited to:

(i) Data and artificial intelligence governance, policy and regulation;

(ii) Administration or implementation of laws related to consumer protection, digital rights and artificial intelligence and other emerging technologies;

(iii) Dispute resolution, particularly technology and data-related disputes;

(iv) Information and communication technology, digital economy and disruptive technologies;

(v) Law, regulation or techno-regulation focused on artificial intelligence, data protection and related domains;

(vi) Any other relevant field deemed beneficial by the Central Government.

(8) At least three Members shall be experts in law with demonstrated understanding of legal and regulatory frameworks related to artificial intelligence, data protection and emerging technologies.

(9) The IAIC shall have the following functions:

(i) Develop and implement policies, guidelines and standards for responsible development, deployment and governance of AI systems in India;

(ii) Coordinate and collaborate with relevant ministries, regulatory bodies and stakeholders to ensure harmonised AI governance across sectors;

(iii) Establish and maintain the National Registry of AI Use Cases as per Section 12;

(iv) Administer the certification scheme for AI systems as specified in Section 11;

(v) Develop and promote the National AI Ethics Code as outlined in Section 13;

(vi) Facilitate stakeholder consultations, public discourse and awareness on societal implications of AI;

(vii) Promote research, development and innovation in AI with a focus on responsibility and ethics;

(viii) Engage with international AI regulatory bodies, standard-setting organizations, and global AI safety initiatives to promote knowledge exchange and align India's AI governance framework with global best practices. This includes:

(a) Developing bilateral and multilateral agreements to support collaborative research, data sharing, and risk management.
(b) Participating in international AI safety and ethics dialogues to shape global AI norms.
(c) Coordinating on cross-border data flow standards and AI certification criteria to ensure seamless compliance for international AI applications in India.

(ix) Take regulatory actions to ensure compliance with the policies, standards, and guidelines issued by the IAIC under this Act, which may include:
(a) Issuing show-cause notices requiring non-compliant entities to explain the reasons for non-compliance and outline corrective measures within a specified timeline;
(b) Imposing monetary penalties based on the severity of non-compliance, the risk level involved, and the potential impact on individuals, businesses, or society, with penalties being commensurate with the financial capacity of the non-compliant entity;
(c) Suspending or revoking certifications, registrations, or approvals related to non-compliant AI systems, preventing their further development, deployment, or operation until compliance is achieved;
(d) Mandating independent audits of the non-compliant entity's processes at their own cost, with audit reports to be submitted to the IAIC for review and further action;
(e) Issuing directives to non-compliant entities to implement specific remedial measures within a defined timeline, such as enhancing data quality controls, improving governance frameworks, or strengthening decision-making procedures;
(f) In cases of persistent or egregious non-compliance, recommending the temporary or permanent suspension of the non-compliant entity's AI-related operations, subject to due process and the principles of natural justice;
(g) Taking any other regulatory action deemed necessary and proportionate to ensure compliance with the prescribed standards and to safeguard the responsible development, deployment, and use of AI systems.

(x) Advise the Central Government on matters related to AI policy, regulation and governance, and recommend legislative or regulatory changes as necessary;
(xi) Perform any other functions necessary to achieve the objectives of this Act or as assigned by the Central Government.

(10) The IAIC may constitute advisory committees, expert groups or task forces as deemed necessary to assist in its functions.
(11) The IAIC shall endeavour to function as a digital office to the extent practicable, conducting proceedings, filings, hearings and pronouncements through digital means as per applicable laws.

CHAPTER III-A: INDIAN ARTIFICIAL INTELLIGENCE SAFETY INSTITUTE

Section 10-A – Composition and Functions of the Institute

(1) With effect from the date notified by the Central Government, there shall be established the Indian Artificial Intelligence Safety Institute (AISI), a statutory body for the purposes of this Act.
(2) The Indian Artificial Intelligence Safety Institute (AISI) shall be established as an autonomous body corporate with perpetual succession, a common seal, and the power to acquire, hold and

transfer property, both movable and immovable, and to contract and be contracted, and sue or be sued by its name.

(3) The Governing Body of the Indian Artificial Intelligence Safety Institute shall consist of the following members:

(i) A Director General of AI Safety, with at least **15 years of experience** in artificial intelligence research, who shall serve as the Chief Executive Officer of AISI.

(ii) One representative from the Ministry of Electronics and Information Technology (MeitY), not below the rank of Joint Secretary.

(iii) One representative from the Ministry of Science and Technology (DST), not below the rank of Joint Secretary.

(iv) One representative from the Ministry of Defence, not below the rank of Joint Secretary.

(v) One representative from the Ministry of Communications, not below the rank of Joint Secretary.

(vi) One representative from NITI Aayog, not below the rank of Joint Secretary.

(vii) One representative from the Committee for AI Centers of Excellence (CoEs) as an ex-officio member

(viii) One Representative from the Committee for Technical Institutions in Critical AI Research as an ex-officio member

(ix) One Representative from the Committee on AI Ethics and Safety as an ex-officio member

(4) In addition to the Governing Body, AISI shall include the following ex-officio members:

(i) The **Principal Scientific Advisor** to the Government of India, or their nominee.

(ii) One member from the **Prime Minister's Economic Advisory Council**.

(iii) One representative, being a government official or expert appointed by the Central Government, responsible for coordinating with global AI safety institutes to ensure knowledge exchange and collaboration on emerging risks and best practices.

(5) The AISI shall establish specialized committees as deemed necessary for fulfilling its mandate. These committees shall include but are not limited to:

(i) **Committee for AI Centers of Excellence (CoEs)**: This committee shall represent all AI-related Centers of Excellence across India.

(ii) **Committee for Technical Institutions in Critical AI Research**: This committee shall coordinate with technical institutions engaged in critical research on AI systems.

(iii) **Committee on AI Ethics and Safety**: This committee shall guide AISI on ethical principles governing AI systems.

(6) The AISI shall undertake the following functions under this Act:

(i) Develop protocols for risk assessment, monitoring, and mitigation concerning high-risk AI applications, particularly in strategic sectors such as healthcare, defence, finance, and public administration.

(ii) Formulate and establish safety standards for high-risk AI applications for the IAIC. These standards shall be aligned with national security priorities and international norms governing AI safety.

(iii) Conduct annual audits of high-risk AI systems deployed across various sectors. The findings from these audits shall be reported to IAIC for further action or policy formulation.

(iv) Undertake research initiatives focused on identifying emerging risks associated with new developments in artificial intelligence. Such research shall be conducted in partnership with

IAIC, academic institutions, technical bodies and centres of excellence (CoEs), and international organizations dedicated to AI safety.

(v) Submit an annual report to the Central Government and IAIC, detailing safety incidents, audit findings, and research advancements.

(7) AISI may engage in international partnerships and dialogues, contributing to India's leadership in responsible AI governance.

CHAPTER IV: CERTIFICATION AND ETHICS CODE

Section 11 – Registration & Certification of AI Systems

(1) The IAIC shall establish a voluntary certification scheme for AI systems based on their industry use cases and risk levels, on the basis of the means of classification set forth in Chapter II. The certification scheme shall be designed to promote responsible AI development and deployment.

(2) The IAIC shall maintain a National Registry of Artificial Intelligence Use Cases as described in Section 12 to register and track the development and deployment of AI systems across various sectors. The registry shall be used to inform the development and refinement of the certification scheme and to promote transparency and accountability in artificial intelligence governance.

(2) The certification scheme shall be based on a set of clear, objective, and risk-proportionate criteria that assess the inherent purpose, technical characteristics, and potential impacts of AI systems.

(3) **AI systems classified as narrow or medium risk under Section 7 and AI-Pre under sub-section (8) of Section 6 may be exempt from the certification requirement if they meet one or more of the following conditions:**

(i) The AI system is still in the early stages of development or testing and has not yet achieved technical or economic thresholds for effective standardisation;

(ii) The AI system is being developed or deployed in a highly specialized or niche application area where certification may not be feasible or appropriate; or

(iii) **The AI system is being developed or deployed by start-ups, micro, small & medium enterprises, or research institutions.**

(4) AI systems that qualify for exemptions under sub-section (3) must establish and maintain incident reporting and response protocols specified in Section 19. Failure to maintain these protocols may result in the revocation of the exemption.

(5) Applicability of Section 4 Classification Methods:

(i) The conceptual methods of classification outlined in Section 4 are intended for consultative and advisory purposes only. Their application is not mandatory for the National AI Registry of Use Cases under this Section. The IAIC is empowered to:

(a) Issue advisories, clarifications, and guidance documents on the interpretation and application of the classification methods outlined in Section 4.

(b) Provide sector-specific recommendations for the voluntary use of these classification methods by stakeholders, including developers, regulators, and industry professionals.

(c) While these classification methods are not mandatory, stakeholders are encouraged to adopt them on a self-regulatory basis. Voluntary application of these methods can help:
  (i) Enhance transparency in AI development.
  (ii) Promote responsible AI deployment across sectors.
  (iii) Facilitate alignment with ethical standards outlined in the National Artificial Intelligence Ethics Code (NAIEC) under Section 13.

(ii) The IAIC may periodically review and update its advisories, clarifications and guidance documents to reflect advancements in AI technologies and emerging best practices, ensuring that stakeholders have access to the latest guidance for applying these conceptual methods.

(6) Notwithstanding anything contained in sub-section (5), entities registering high-risk AI systems as defined in the sub-section (4) of Section 7 and those associated with strategic sectors as specified in Section 9 must apply the conceptual classification methods outlined in Section 4.

(7) The certification scheme and the methods of classification specified in Chapter II shall undergo periodic review and updating every 12 months to ensure its relevance and effectiveness in response to technological advancements and market developments. The review process shall include meaningful consultation with sector-specific regulators and market stakeholders.

Section 12 – National Registry of Artificial Intelligence Use Cases

(1) The National Registry of Artificial Intelligence Use Cases shall include the metadata for each registered AI system as set forth in sub-sections (1)(i) through (1)(xvi):

(i) Name and version of the AI system (required)
(ii) Owning entity of the AI system (required)
(iii) Date of registration (required)
(iv) Sector associated with the AI system and whether the AI system is associated with a strategic sector (required)
(v) Specific use case(s) of the AI system (required)
(vi) Technical classification of the AI system, as per Section 5 (required)
(vii) Key technical characteristics of the AI system as per Section 5, including:
  (a) Type of AI model(s) used (required)
  (b) Training data sources and characteristics (required)
  (c) Performance metrics on standard benchmarks (where available, optional)
(viii) Commercial classification of the AI system as per Section 6 (required)
(ix) Key commercial features of the AI system as per Section 6, including:
  (a) Number of end-users and business end-users in India (required, where applicable)
  (b) Market share or level of market influence in the intended sector(s) of application (required, where ascertainable)
  (c) Annual turnover or revenue generated by the AI system or the company owning it (required, where applicable)
  (d) Amount & intended purpose of data collected, processed, or utilized by the AI system (required, where measurable)
  (e) Level of data integration across different services or platforms (required, where applicable)

(x) Risk classification of the AI system as per Section 7 (required)
(xi) Conceptual classification of the AI system as per Section 4 (required only for high-risk AI Systems)
(xii) Potential impacts of the AI system as per Section 7, including:
  (a) Inherent Purpose (required)
  (b) Possible risks and harms observed and documented by the owning entity (required)

(xiii) Certification status (required) (registered & certified / registered & not certified)
(xiv) A detailed post-deployment monitoring plan as per Section 17 (required only for high-risk AI Systems), including:
  (a) Performance metrics and key indicators to be tracked (optional)
  (b) Risk mitigation and human oversight protocols (required)
  (c) Data collection, reporting, and audit trail mechanisms (required)
  (d) Feedback and redressal channels for impacted stakeholders (optional)
  (e) Commitments to periodic third-party audits and public disclosure of:
    (i) Monitoring reports and performance indicators (optional)
    (ii) Descriptions of identified risks, incidents or failures as per sub-section (3) of Section 17 (required)
    (iii) Corrective actions and mitigation measures implemented (required)

(xv)Incident reporting and response protocols as per Section 19 (required)
  (a) Description of the incident reporting mechanisms established (e.g. hotline, online portal)
  (b) Timelines committed for incident reporting based on risk classification
  (c) Procedures for assessing and determining incident severity levels
  (d) Information to be provided in incident reports as per guidelines
  (e) Confidentiality and data protection measures for incident data
  (f) Minimum mitigation actions to be taken upon incident occurrence
  (g) Responsible personnel/team for incident response and mitigation
  (h) Commitments on notifying and communicating with impacted parties
  (i) Integration with IAIC's central incident repository and reporting channels
  (j) Review and improvement processes for incident response procedures
  (k) Description of the insurance coverage obtained for the AI system, as per Section 25, including the type of policy, insurer, policy number, and coverage limits;
  (l) Confirmation that the insurance coverage meets the minimum requirements specified in the sub-section (3) of Section 25 based on the AI system's risk classification;
  (m) Details of the risk assessment conducted to determine the appropriate level of insurance coverage, considering factors such as the AI system's conceptual, technical, and commercial classifications as per Sections 4, 5, and 6;
  (n) Information on the claims process and timelines for notifying the insurer and submitting claims in the event of an incident covered under the insurance policy;
  (o) Commitment to maintain the insurance coverage throughout the lifecycle of the AI system and to notify the IAIC of any changes in coverage or insurer.
(xvi) Contact information for the owning entity (required)

Illustration

A technology company develops a new AI system for automated medical diagnosis using computer vision and machine learning techniques. This AI system would be classified as a high-risk system under Section 7(4) due to its potential impact on human health and safety. The company registers this AI system in the National Registry of Artificial Intelligence Use Cases, providing the following metadata:

(i) *Name and version:* **MedVision AI Diagnostic System v1.2**
(ii) *Owning entity:* **ABC Technologies Pvt. Ltd.**
(iii) Date of registration: **01/05/2024**
(iv) Sector: **Healthcare**
(v) Use case: **Automated analysis of medical imaging data (X-rays, CT scans, MRIs) to detect and diagnose diseases**
(vi) *Technical classification:* **Specific Purpose AI (SPAI) under Section 5(4)**
(vii)Key technical characteristics:

- **Convolutional neural networks for image analysis**
- **Trained on de-identified medical imaging datasets from hospitals**
- **Achieved 92% accuracy on standard benchmarks**

(viii) Commercial classification: **AI-Pro under Section 6(3)**
(ix) Key commercial features:

- **Intended for use by healthcare providers across India**
- **Not yet deployed, so no market share data**
- **No revenue generated yet (pre-commercial)**

(x) Risk classification: **High Risk under Section 7(4)**
(xi) Conceptual classification: **Assessed under all four methods in Section 4 due to high-risk**
(xii) Potential impacts:

- **Inherent purpose is to assist medical professionals in diagnosis**
- **Documented risks include misdiagnosis, bias, lack of interpretability**

(xiii) Certification status: **Registered & certified**
(xiv) Post-deployment monitoring plan:

- **Performance metrics like accuracy, false positive/negative rates**
- **Human oversight, periodic audits for bias/errors**
- **Logging all outputs, decisions for audit trail**
- **Channels for user feedback, grievance redressal**
- **Commitments to third-party audits, public incident disclosure**

(xv)Incident reporting protocols:

- **Dedicated online portal for incident reporting**
- **Critical incidents to be reported within 48 hours**
- **High/medium severity incidents within 7 days**

- **Procedures for severity assessment, confidentiality measures**
- **Minimum mitigation actions, impacted party notifications**
- **Integration with IAIC incident repository**
- **Insurance coverage details:**
- **Professional indemnity policy from XYZ Insurance Co., policy #PI12345**
- **Coverage limit of ₹ 50 crores, as required for high-risk AI under Section 25(3)(i)**
- **Risk assessment considered technical complexity, healthcare impact, irreversible consequences**
- **Claims to be notified within 24 hours, supporting documentation within 7 days**
- **Coverage to be maintained throughout AI system lifecycle, IAIC to be notified of changes**

(xvi) *Contact:* **info@abctech.com**

(2) The IAIC may, from time to time, expand or modify the metadata schema for the National Registry as it deems necessary to reflect advancements in AI technology and risk assessment methodologies. The IAIC shall give notice of any such changes at least 60 days prior to the date on which they shall take effect.

(3) The owners of AI systems shall have the duty to provide accurate and current metadata at the time of registration and to notify the IAIC of any material changes to the registered information within:

(i) 15 days of such change occurring for AI systems classified as High Risk under sub-section (4) of Section 7;
(ii) 30 days of such change occurring for AI systems classified as Medium Risk under sub-section (3) of Section 7;
(iii) 60 days of such change occurring for AI systems classified as Narrow Risk under sub-section (2) of Section 7;
(iv) 90 days of such change occurring for AI systems classified as Narrow Risk or Medium Risk under Section 7 that are exempted from certification under sub-section (3) of Section 11.

(4) Notwithstanding anything contained in sub-section (1), the owners of AI systems exempted under sub-section (3) of Section 11 shall only be required to submit the metadata specified in sub-sections (4)(i) through (4)(xi) to register their AI systems:

(i) Name and version of the AI system (required)
(ii) Owning entity of the AI system (required)
(iii) Date of registration (required)
(iv) Sector associated with the AI system (optional)
(v) Specific use case(s) of the AI system (required)
(vi) Technical classification of the AI system, as per Section 5 (optional)
(vii) Commercial classification of the AI system as per Section 6 (required)
(viii) Risk classification of the AI system as per Section 7 (required, narrow risk or medium risk only)
(ix) Certification status (required) (registered & certification is exempted under sub-section (3) of Section 11)

(x) Incident reporting and response protocols as per Section 19 (required)
  (a) Description of the incident reporting mechanisms established (e.g. hotline, online portal)
  (b) Timelines committed for reporting high/critical severity incidents (within 14-30 days)
  (c) Procedures for assessing and determining incident severity levels (only high/critical)
  (d) Information to be provided in incident reports (incident description, system details)
  (e) Confidentiality measures for incident data based on sensitivity (scaled down)
  (f) Minimum mitigation actions to be taken upon high/critical incident occurrence
  (g) Responsible personnel/team for incident response and mitigation
  (h) Commitments on notifying and communicating with impacted parties
  (i) Integration with IAIC's central incident repository and reporting channels
  (j) Description of the insurance coverage obtained for the AI system, as per Section 25, including the type of policy, insurer, policy number, and coverage limits (required for high-risk AI systems only);
(xi) Contact information for the owning entity (required)

Illustration

A small AI startup develops a chatbot for basic customer service queries using natural language processing techniques. As a low-risk AI system still in early development stages, they claim exemption under Section 11(3) and register with the following limited metadata:

(i) Name and version: **ChatAssist v0.5 (beta)**
(ii) Owning entity: **XYZ AI Solutions LLP**
(iii) *Date of registration:* **15/06/2024**
(iv) Sector: **Not provided (optional)**
(v) *Use case:* **Automated response to basic customer queries via text/voice**
(vi) Technical classification: **Specific Purpose AI (SPAI) under Section 5(4) (optional)**
(vii)Commercial classification: **AI-Pre under Section 6(8)**
(viii) Risk classification: **Narrow Risk under Section 7(2)**
(ix) Certification status: **Registered & certification exempted under Section 11(3)**
(x) Incident reporting protocols:

- **Email support@xyzai.com for incident reporting**

Timelines committed for reporting high/critical severity incidents (within 14-30 days)

- **High/critical incidents to be reported within 30 days**

Procedures for assessing and determining incident severity levels (only high/critical)

- **Only incident description and system details required**

Information to be provided in incident reports (incident description, system details)

Confidentiality measures for incident data based on sensitivity (scaled down)

- **Standard data protection measures as per company policy**

Minimum mitigation actions to be taken upon high/critical incident occurrence

- **Mitigation by product team, notifying customers if major**

Responsible personnel/team for incident response and mitigation

Commitments on notifying and communicating with impacted parties

Integration with IAIC's central incident repository and reporting channels

(xi) Contact: **support@xyzai.com**

(5) The IAIC shall put in place mechanisms to validate the metadata provided and to audit registered AI systems for compliance with the reported information. Where the IAIC determines that any developer or owner has provided false or misleading information, it may impose penalties, including fines and revocation of certification, as it deems fit.

(6) The IAIC shall publish aggregate statistics and analytics based on the metadata in the National Registry for the purposes of supporting evidence-based policymaking, research, and public awareness about AI development and deployment trends. Provided that commercially sensitive information and trade secrets shall not be disclosed.

(7) Registration and certification under this Act shall be voluntary, and no penal consequences shall attach to the lack of registration or certification of an AI system, except as otherwise expressly provided in this Act.

(8) The examination process for registration and certification of AI use cases shall be conducted by the IAIC in a transparent and inclusive manner, engaging with relevant stakeholders, including:

(i) Technical experts and researchers in the field of artificial intelligence, who can provide insights into the technical aspects, capabilities, and limitations of the AI systems under examination.

(ii) Representatives of industries developing and deploying AI technologies, who can offer practical perspectives on the commercial viability, use cases, and potential impacts of the AI systems.

(iii) Technology standards & business associations and consumer protection groups, who can represent the interests and concerns of end-users, affected communities, and the general public.

(iv) Representatives from diverse communities and individuals who may be impacted by AI systems, to ensure their rights, needs, experiences and perspectives across different contexts are comprehensively accounted for during the examination process.

(v) Any other relevant stakeholders or subject matter experts that the IAIC deems necessary for a comprehensive and inclusive examination of AI use cases.

(9) The IAIC shall publish the results of its examinations for registration and certification of AI use cases, along with any recommendations for risk mitigation measures, regulatory actions, or guidelines, in an accessible format for public review and feedback. This shall include detailed explanations of the classification criteria applied, the stakeholder inputs considered, and the rationale behind the decisions made.

Section 13 – National Artificial Intelligence Ethics Code

(1) A National Artificial Intelligence Ethics Code (NAIEC) shall be established to provide a set of guiding moral and ethical principles for the responsible development, deployment, and utilisation of artificial intelligence technologies;

(2) The NAIEC shall be based on the following core ethical principles:

(i) AI systems must respect human dignity, well-being, and fundamental rights, including the rights to privacy, non-discrimination and due process.

(ii) AI systems should be designed, developed, and deployed in a fair and non-discriminatory manner, ensuring equal treatment and opportunities for all individuals, regardless of their personal characteristics or protected attributes, **including caste and class**.

(iii) AI systems should be transparent in their operation, enabling users and affected individuals to understand the underlying logic, decision-making processes, and potential implications of the system's outputs. AI systems should be able to provide clear and understandable explanations for their decisions and recommendations, in accordance with the guidance provided in sub-section (4) on intellectual property and ownership considerations related to AI-generated content.

(iv) AI systems should be developed and deployed with clear lines of accountability and responsibility, ensuring that appropriate measures are in place to address potential harms, in alignment with the principles outlined in sub-section (3) on the use of open-source software for promoting transparency and collaboration.

(v) AI systems should be designed and operated with a focus on safety and robustness, minimizing the potential for harm, unintended consequences, or adverse impacts on individuals, society, or the environment. Rigorous testing, validation, and monitoring processes shall be implemented.

(vi) AI systems should foster human agency, oversight, and the ability for humans to make informed decisions, while respecting the principles of human autonomy and self-determination. Appropriate human control measures should be implemented;

(vii) AI systems should be developed and deployed with due consideration for their ethical and socio-economic implications, promoting the common good, public interest, and the well-being of society. Potential impacts on employment, skills, and the future of work should be assessed and addressed.

(viii) AI systems that are developed and deployed using frugal prompt engineering practices should optimize efficiency, cost-effectiveness, and resource utilisation while maintaining high standards of performance, safety, and ethical compliance in alignment with the principles outlined in sub-section (5). These practices should include the use of concise and well-structured prompts, transfer learning, data-efficient techniques, and model compression, among others, to reduce potential risks, unintended consequences, and resource burdens associated with AI development and deployment.

(3) The Ethics Code shall encourage the use of open-source software (OSS) in the development of narrow and medium-risk AI systems to promote transparency, collaboration, and innovation, while ensuring compliance with applicable sector-specific & sector-neutral laws and regulations. To this end:

(i) The use of OSS shall be guided by a clear understanding of the open source development model, its scope, constraints, and the varying implementation approaches across different socio-economic and organisational contexts.
(ii) AI developers shall be encouraged to release non-sensitive components of their AI systems under OSS licenses, fostering transparency and enabling public scrutiny, while also ensuring that sensitive components and intellectual property are adequately protected.
(iii) AI developers using OSS shall ensure that their systems adhere to the same standards of fairness, accountability, and transparency as proprietary systems, and shall implement appropriate governance, quality assurance, and risk management processes.

(4) The Ethics Code shall provide guidance on intellectual property and ownership considerations related to AI-generated content. To this end:

(i) Specific considerations shall include recognizing the role of human involvement in developing and deploying the AI systems, establishing guidelines on copyrightability and patentability of AI-generated works and inventions, addressing scenarios where AI builds upon existing protected works, safeguarding trade secrets and data privacy, balancing incentives for AI innovation with disclosure and access principles, and continuously updating policies as AI capabilities evolve.
(ii) The Ethics Code shall encourage transparency and responsible practices in managing intellectual property aspects of AI-generated content across domains such as text, images, audio, video and others.
(iii) In examining IP and ownership issues related to AI-generated content, the Ethics Code shall be guided by the conceptual classification methods outlined in Section 4, particularly the Anthropomorphism-Based Concept Classification to evaluate scenarios where AI replicates or emulates human creativity and invention.
(iv) The technical classification methods described in Section 5, such as the scale, inherent purpose, technical features, and limitations of the AI system, shall inform the assessment of IP and ownership considerations for AI-generated content.
(v) **The commercial classification factors specified in the sub-section (1) of Section 6, including the user base, market influence, data integration, and revenue generation of the AI system, shall also be taken into account when determining IP and ownership rights over AI-generated content.**

(5) The Ethics Code shall provide guidance on frugal prompt engineering practices for the development of AI systems, ensuring efficiency, accessibility, and the equitable advancement of artificial intelligence, as follows:

(i) Encourage the use of concise and well-structured prompts that specify desired outputs and constraints, minimizing unnecessary complexity in AI interactions;
(ii) Recommend the adoption of transfer learning and pre-trained models to reduce the need for extensive fine-tuning, thereby conserving computational resources;
(iii) Promote the use of data-efficient techniques, such as few-shot learning or active learning, to decrease the volume of training data required for effective model performance;
(iv) Suggest the implementation of early stopping mechanisms to prevent overfitting and enhance model generalisation, ensuring robust performance with minimal training;

(v) Advocate for the use of techniques such as model compression, quantisation, or distillation to reduce computational complexity and resource demands, making AI development more sustainable;

(vi) Require the documentation and maintenance of records on prompt engineering practices, detailing the techniques used, performance metrics achieved, and any trade-offs between efficiency and effectiveness, to ensure transparency and accountability;

(vii) Declare that prompt engineering, as a fundamental practice for optimizing AI systems, constitutes a global commons and a shared resource for the benefit of all humanity, and as such:

(a) Shall not be monetized, commercialized, or subject to proprietary claims, ensuring that the knowledge and techniques of prompt engineering remain freely accessible to all;

(b) Shall be treated as a universal public good, akin to principles established in international agreements governing shared resources, to foster global collaboration and innovation in AI development & education.

(6) The Ethics Code shall provide guidance on ensuring fair access rights for all stakeholders involved in the AI value and supply chain, including:

(i) All stakeholders should have fair and transparent access to datasets necessary for training and developing AI systems. This includes promoting equitable data-sharing practices that ensure smaller entities or research institutions are not unfairly disadvantaged in accessing critical datasets.

(ii) Ethical use of computational resources should be promoted by ensuring that all stakeholders have transparent access to these resources. Special consideration should be given to smaller entities or research institutions that may require preferential access or pricing models to support innovation.

(iii) Ethical guidelines should ensure that ownership rights over trained models, derived outputs, and intellectual property are clearly defined and respected. Stakeholders involved in the development process must have a clear understanding of their rights and obligations regarding the usage and commercialization of AI technologies.

(iv) The benefits derived from AI technologies should be distributed ensuring that smaller players contributing critical resources like proprietary datasets or specialized algorithms are fairly compensated.

(7) Adherence to the NAIEC shall be voluntary for all AI systems, as well as those exempted under the sub-section (3) of Section 11.

(8) Strategic Sector Safeguards: AI systems deployed in strategic sectors, particularly those classified as high-risk under Section 7, shall adhere to heightened ethical standards that prioritize:

(i) Safety Imperative: Developers and operators of AI systems shall design, implement, and maintain robust safety measures that minimize potential harm to individuals, property, society, and the environment throughout the system's lifecycle;

(ii) Security by Design: AI systems shall incorporate security measures from the earliest stages of development to protect against unauthorized access, manipulation, or

misuse, with particular emphasis on safeguarding data integrity and system confidentiality;

(iii) Reliability and Resilience: All AI systems shall demonstrate consistent, accurate, and dependable performance through rigorous testing, validation, and continuous monitoring, with enhanced requirements for systems in critical infrastructure or essential services;

(iv) Transparent Operations: AI systems shall implement mechanisms that enable appropriate stakeholder understanding of underlying algorithms, data sources, and decision-making processes, adhering to disclosure needs in line with intellectual property protections;

(v) Accountable Governance: Clear lines of responsibility shall be established for AI system outcomes, with specified channels for redress and remediation in cases of adverse impacts, particularly for systems affecting fundamental rights or public welfare;

(vi) Legitimate Purpose Alignment: AI systems shall be developed and deployed exclusively for purposes that comply with the legitimate uses framework established under Section 7 of the Digital Personal Data Protection Act, 2023 and shall not be repurposed for unauthorized applications without appropriate review.

CHAPTER V: KNOWLEDGE MANAGEMENT

Section 14 - Model Standards on Knowledge Management

(1) The IAIC shall develop, document and promote comprehensive model standards on knowledge management practices concerning the development, maintenance, and governance of **high-risk AI systems**. These standards shall focus on the effective management of knowledge assets;

(2) The model standards shall encompass the following areas:

(i) Intellectual property management practices to safeguard and leverage AI-related intellectual property rights such as patents, copyrights, trademarks and industrial designs.

(ii) Processes for documenting and organizing technical knowledge assets like research reports, manuals, standards and industrial practices related to AI systems.

(iii) Frameworks for capturing, retaining and transferring the tacit knowledge and expertise of human capital involved in AI development and deployment.

(iv) Organisational systems and methodologies to enable effective knowledge capture, storage, retrieval and utilisation across the AI system lifecycle.

(v) Mechanisms for leveraging customer-related knowledge assets such as data, feedback and insights to enhance AI system development and performance.

(vi) Analytical techniques to derive knowledge from data analysis, including identifying patterns, trends and developing predictive models for AI systems.

(vii) Collaborative practices to foster cross-functional knowledge sharing and generation through teams, communities of practice and other initiatives.

(3) All entities engaged in the development, deployment, or utilisation of high-risk AI systems shall be bound by the model standards on knowledge management and decision-making as provided by this section. The compliance timeline for such high-risk AI systems shall be determined by the

IAIC and may vary based on the technical, commercial and risk-based classification of those systems under Section 12.

(4) For artificial intelligence technologies subject to commercial classification as determined by the factors outlined in sub-section (1) of Section 6, the requirement to comply with these model standards on knowledge management shall be assessed by the IAIC on a case-by-case basis, taking into consideration the specific commercial classification factors applicable to each AI technology.

Illustration

A startup has developed an AI-powered language translation app that allows users to translate text, documents, and speech between multiple Indian languages. Based on an assessment of the factors in Section 6(1), such as the app's user base, market influence, and data integration, the IAIC may determine that this AI technology falls under the AI-Pro or AIaaS category. The IAIC will then evaluate if the startup needs to fully comply with the knowledge management standards or if certain requirements can be relaxed or made optional based on the app's specific use case and commercial profile.

(5) In determining the case-by-case application of these model standards to commercially classified AI technologies under sub-section (1) of Section 6, the IAIC shall take into account any relevant sector-specific standards, codes of practice, or regulatory guidelines pertaining to knowledge management practices in the sector to which the AI technology belongs or is intended to be deployed.

Illustration

An agritech startup has developed an AI system that analyzes satellite imagery and weather data to provide crop yield predictions and advisory services to farmers. As this AI technology falls within the agriculture sector, the IAIC's assessment of its knowledge management requirements will consider any relevant guidelines or standards issued by bodies like the Indian Council of Agricultural Research (ICAR) or the Ministry of Agriculture & Farmers' Welfare. These may include data governance norms for agricultural data, model validation protocols for AI-based advisory services, or best practices for maintaining data trails and audit logs in agritech applications.

(6) Failure to adhere to the prescribed model standards for knowledge management and decision-making processes shall result in regulatory actions by the IAIC, which may include:

(i) Issuance of show-cause notices to the non-compliant entity, requiring them to explain the reasons for non-compliance and outline corrective measures within a specified timeline.

(ii) Imposition of monetary penalties, determined based on the severity of non-compliance, the risk level of the AI system involved, and the potential impact on individuals, businesses, or society. The monetary penalties shall be commensurate with the financial capacity of the non-compliant entity.

(iii) Suspension or revocation of certifications or registrations related to the non-compliant AI system, preventing its further development, deployment, or operation until compliance is achieved.

(iv) Mandating independent audits of the non-compliant entity's knowledge management and decision-making processes at their own cost, with the audit reports to be submitted to the IAIC for review and further action.

(v) Issuing directives to the non-compliant entity to implement specific remedial measures, such as enhancing data quality controls, improving model governance frameworks, or strengthening decision-making procedures, within a defined timeline.

(vi) In cases of persistent or egregious non-compliance, the IAIC may recommend the temporary or permanent suspension of the non-compliant entity's AI-related operations, subject to due process and the principles of natural justice.

(vii) Any other regulatory action deemed necessary and proportionate by the IAIC to ensure compliance with the prescribed model standards and to safeguard the responsible development, deployment, and use of high-risk AI systems.

(7) The IAIC shall encourage the sharing of AI-related knowledge, including datasets, models, and algorithms, through open-source software repositories and platforms, subject to applicable intellectual property rights and the provisions of the Digital Personal Data Protection Act, 2023 and other relevant data protection and governance frameworks as may be prescribed.

CHAPTER VI: GUIDANCE AND MONITORING

Section 15 - Guidance Principles for AI-related Agreements

(1) The following guidance principles shall apply to AI-related agreements to promote transparent, fair, and responsible practices in the development, deployment, and use of AI technologies:

(vii) AI Software License Agreement (ASLA):

(a) The AI Software License Agreement (ASLA) shall be mandatory for AI systems classified as AI-Pro or AI-Com as per Section 6, if they are designated as High Risk AI systems under Section 7.

(b) The ASLA shall clearly define:

(i) The scope of rights granted to the licensee, including limitations on use, modification, and distribution of the AI software;

(ii) Intellectual property rights and ownership provisions;

(iii) Term, termination, warranties, and indemnification clauses.

(viii) AI Service Level Agreement (AI-SLA):

(a) The AI Service Level Agreement (AI-SLA) shall be mandatory for AI systems classified as AIaaS or AI-Com as per Section 6, if they are designated as High Risk or Medium Risk AI systems under Section 7.

(b) The AI-SLA shall establish:

(i) Service levels, performance metrics, availability, and support commitments;

(ii) Monitoring, measurement, change management, and problem resolution mechanisms;

(iii) Data handling, security, and business continuity requirements.

(ix) AI End-User License Agreement (AI-EULA) or AI End-Client License Agreement (AI-ECLA):
  (a) The AI End-User License Agreement (AI-EULA) shall be mandatory for all AI system classifications intended for end-user or client deployment;
  (b) The AI-EULA or AI-ECLA shall specify:
    (i) Permitted uses and user obligations;
    (ii) Data privacy provisions aligned with the Digital Personal Data Protection Act, 2023 and other cyber and data protection frameworks;
    (iii) Intellectual property rights, warranties, and liability limitations.

(x) AI Explainability Agreement (AI-ExA):
  (a) The AI Explainability Agreement (AI-ExA) shall be mandatory for all high-risk AI systems under Section 7;
  (b) The AI-ExA shall specify:
    (i) Clear and understandable explanations for AI system outputs and decisions;
    (ii) Documentation and reporting on the AI system's decision-making processes;
    (iii) Provisions for human review and intervention mechanisms

(2) The following agreements shall be voluntary in nature, but are recommended for adoption by entities engaged in the deployment of AI systems:
  (i) An AI Data Licensing Agreement, which shall govern the terms and conditions for licensing data sets used for training, testing, and validating AI systems;
  (ii) An AI Model Licensing Agreement, which shall cover the licensing of pre-trained AI models or model components for use in developing or deploying AI systems;
  (iii) An AI Collaboration Agreement, which shall facilitate collaboration between multiple parties, such as research institutions, companies, or individuals, in the development or deployment of AI systems;
  (iv) An AI Consulting Agreement, which shall govern the terms and conditions under which an AI expert or consulting firm provides advisory services, technical assistance, or training related to the development, deployment, or use of AI systems;
  (v) An AI Maintenance and Support Agreement, which shall define the terms and conditions for ongoing maintenance, support, and updates for AI systems.

(3) Agreements that are mandatory in nature must include provisions addressing the following:
  (i) Requirements for post-deployment monitoring of AI systems classified as High Risk AI systems;
  (ii) Protocols for incident reporting and response in the event of any issues or incidents related to the AI system;
  (iii) Penalties or consequences for non-compliance with the terms of the agreement or any applicable laws or regulations.

(4) The IAIC shall develop and publish model AI-related agreements incorporating these guidance principles, taking into account the unique characteristics and risks associated with different types of AI systems, such as:
  (i) The inherent purpose of the AI system, as determined by the conceptual classifications outlined in Section 4;

(ii) The technical features and limitations of the AI system, as specified in Section 5;
(iii) The commercial factors associated with the AI system, as outlined in Section 6;
(iv) The risk level of the AI system, as classified under Section 7.

(5) **Consultative Principles on AI Value & Supply Chain**

(i) Entities involved in the development, supply, distribution, and commercialization of AI technologies are encouraged to adopt the following consultative principles when forming agreements. The following principles should guide contractual practices:

(a) **Transparency in Ownership & Intellectual Property**: Agreements should clearly define ownership rights over trained models, derived outputs, and any intellectual property generated during the development process.

Illustration

An AI startup develops a machine learning model for financial trading in collaboration with a large financial institution. The contract specifies that while the startup retains ownership of the trained model, the financial institution has exclusive rights to use the model's outputs for its internal trading operations.

(b) **Liability & Risk Allocation**: Contracts should clearly allocate risks associated with potential failures in AI systems, ensuring that liability is fairly distributed among stakeholders based on their role in the value chain.

Illustration

A manufacturer integrates an AI-powered quality control system into its production line. The contract with the AI provider specifies that if the system fails due to faulty training data provided by a third-party vendor, liability will be shared between the AI provider and the vendor, based on their respective contributions to the failure.

(c) **Data Sharing & Privacy Protections**: Contracts should include provisions for secure data sharing between entities while ensuring compliance with the Digital Personal Data Protection Act, 2023.

Illustration

A healthcare provider contracts with an AI company to develop a diagnostic tool using patient data. The contract includes detailed clauses on anonymizing patient data before sharing it with the AI company, ensuring compliance with the Digital Personal Data Protection Act.

(ii) The Indian Artificial Intelligence Council (IAIC) may issue advisories on best practices for drafting contracts related to different stages of the value & supply chains. These advisories will provide sector-specific guidance on how these principles can be applied effectively without imposing mandatory requirements.
(iii) While these principles are not mandatory under this Act, entities are encouraged to adopt them as part of a self-regulatory framework. Voluntary adherence to these principles can help foster trust among stakeholders and promote responsible commercialization of AI technologies.

(6) Entities engaged in the *development*, *deployment*, or *use* of AI systems may adopt and customize the model templates provided by the IAIC to suit their specific contexts and requirements.
(7) The IAIC may mandate the use of model agreements for certain high-risk sectors, high-risk use cases as per Section 6, or types of entities, where the potential risks associated with the AI system are deemed significant.
(8) The model agreements shall be reviewed and updated periodically to reflect advancements in AI technologies, evolving best practices, and changes in the legal and regulatory landscape.

Section 16 - Guidance Principles for AI-related Corporate Governance

(1) Entities involved in the development, deployment, and use of artificial intelligence (AI) techniques, tools or methods across their governance structures and decision-making processes must adhere to the following guiding principles as per the National Artificial Intelligence Ethics Code under Section 13:
  (i) Accountability and Responsibility:
    (a) Clear accountability for decisions and actions involving the use of AI techniques must be maintained within the organisation by the appropriate leadership or management.
    (b) Robust governance frameworks must be established to assign roles, responsibilities and oversight mechanisms related to the development, deployment and monitoring of AI systems used for corporate governance purposes.

  (ii) Transparency and Explainability:
    (a) AI systems used to aid corporate decision-making must employ transparent models and techniques that enable interpretability of their underlying logic, data inputs and decision rationales
    (b) Comprehensive documentation must be maintained on the AI system's architecture, training data, performance metrics and potential limitations or biases
    (c) Internal policies, directives and guidelines must be made by entities for impacted stakeholders to access explanations of how AI-driven decisions were made and what factors influenced those decisions

  (iii) Human Agency and Oversight:
    (a) The use of AI techniques in corporate governance must be subject to meaningful human control, oversight and the ability to intervene in or override AI system outputs when necessary.
    (b) Appropriate human review mechanisms must be implemented, particularly for high-stakes decisions impacting all relevant stakeholders, including employees, shareholders, customers, and the public interest;
    (c) Company or Organisation policies must clearly define the roles and responsibilities of humans versus AI systems in governance and decision-making processes;

  (iv) Intellectual Property and Ownership Considerations:
    (a) Corporate entities should establish clear policies and processes for determining ownership, attribution, and intellectual property rights over AI-generated content, inventions, and innovations.
    (b) These policies should recognize and protect the contributions of human creators, inventors, and developers involved in the development and deployment of AI systems.

(c) Corporations should balance the need for incentivizing innovation through intellectual property protections with the principles of transparency, accountability, and responsible use of AI technologies.

(v) Encouraging Open-Source Adoption:
(a) Companies and organisations are encouraged to leverage open-source software (OSS) and open standards in the development and deployment of AI systems, where appropriate.
(b) The use of OSS can promote transparency, collaboration, and innovation in the AI ecosystem while ensuring compliance with applicable laws, regulations, and ethical principles outlined in Section 13.
(c) Companies and organisations should contribute to and participate in open-source AI communities, fostering knowledge sharing and collective advancement of AI technologies.

(2) For the purposes of these Guidance Principles, the artificial intelligence (AI) techniques, tools or methods across governance structures and decision-making processes shall refer to:
(i) AI systems that replicate or emulate human decision-making abilities through autonomy, perception, reasoning, interaction, adaptation and creativity, as evaluated under the Anthropomorphism-Based Concept Classification (ABCC) described in sub-section (5) of Section 4;
(ii) AI systems whose development, deployment and utilisation within corporate governance structures necessitates the evaluation and mitigation of potential ethical risks and implications, in accordance with the Ethics-Based Concept Classification (EBCC) under sub-section (3) of Section 4;
(iii) AI systems that may impact individual rights such as privacy, due process, non-discrimination as well as collective rights, requiring a rights-based assessment as per the Phenomena-Based Concept Classification (PBCC) outlined in sub-section (4) of Section 4;
(iv) General Purpose AI Applications with Multiple Stable Use Cases (GPAIS) that can reliably operate across various governance functions as per the technical classification criteria specified in sub-section (2) of Section 5;
(v) Specific Purpose AI Applications (SPAI) designed for specialized governance use cases based on the factors described in sub-section (4) of Section 5;
(vi) AI systems classified as high-risk under the sub-section (4) of Section 7 due to their potential for widespread impact, lack of opt-out feasibility, vulnerability factors or irreversible consequences related to corporate governance processes;
(vii) AI systems classified as medium-risk under the sub-section (3) of Section 7 that require robust governance frameworks focused on transparency, explainability and accountability aspects;
(viii) AI systems classified as narrow-risk under the sub-section (2) of Section 7 where governance approaches should account for their technical limitations and vulnerabilities.

(3) For AI systems exempted from certification under Section 11(3), companies and organisations may adopt a lean governance approach, focusing on:
(i) Establishing basic incident reporting and response protocols as per Section 19, without the stringent requirements applicable to high-risk AI systems.
(ii) Maintaining documentation and ensuring interpretability of the AI systems to the extent feasible, given their limited risk profile.

(iii) Conducting periodic risk assessments and implementing corrective measures as necessary, commensurate with the AI system's potential impact.

(4) The IAIC may mandate the application of the guidance principles outlined in this section for certain high-risk sectors, high-risk use cases as per Section 6, or types of entities, where the potential risks associated with the AI system are deemed significant.
(5) The guidance principles shall be reviewed and updated periodically to reflect advancements in AI technologies, evolving best practices, and changes in the legal and regulatory landscape.

Section 17 - Post-Deployment Monitoring of High-Risk AI Systems

(1) High-risk AI systems as classified in the sub-section (4) of Section 7 shall be subject to ongoing monitoring and evaluation throughout their lifecycle to ensure their safety, security, reliability, transparency and accountability.
(2) The post-deployment monitoring shall be conducted by the providers, deployers, or users of the high-risk AI systems, as appropriate, in accordance with the guidelines established by the IAIC.
(3) The IAIC shall develop and establish comprehensive guidelines for the post-deployment monitoring of high-risk AI systems, which may include, but not be limited to, the following:
(i) Identification and assessment of potential risks, which includes:
(a) performance deviations,
(b) malfunctions,
(c) unintended consequences,
(d) security vulnerabilities, and
(e) data breaches;

(ii) Evaluation of the effectiveness of risk mitigation measures and implementation of necessary updates, corrections, or remedial actions;
(iii) Continuous improvement of the AI system's performance, reliability, and trustworthiness based on real-world feedback and evolving best practices; and
(iv) Regular reporting to the IAIC on the findings and actions taken as a result of the post-deployment monitoring, including any incidents, malfunctions, or adverse impacts identified, and the measures implemented to address them.

(4) The post-deployment monitoring facilitated by the IAIC shall involve collaboration and coordination among providers, deployers, users, and sector-specific regulatory authorities, to ensure a comprehensive and inclusive approach to AI system oversight.

CHAPTER VII: REPORTING AND SHARING

Section 18 - Third-Party Vulnerability Reporting

[***][1]

Section 19 - Incident Reporting and Mitigation Protocols

(1) All developers, operators, and users of AI systems shall establish mechanisms for reporting incidents related to such AI systems.

[1] Omitted in Version 5.

(2) Incident reporting mechanisms must be easily accessible, user-friendly, and secure, such as a dedicated hotline, online portal, or email address.
(3) Incidents involving high-risk AI systems shall be treated as a priority and reported immediately, but not later than 48 hours from becoming aware of the incident.
(4) For other AI systems, incidents must be reported within 7 days of becoming aware of such incidents.
(5) All incident reports shall be submitted to a central repository established and maintained by the IAIC.
(6) The IAIC shall collect, analyse, and share incident data from this repository to identify trends, potential risks, and develop mitigation strategies.
(7) The IAIC shall publish guidelines on incident reporting requirements, including:
  (i) Criteria for determining incident severity:
    (a) Critical: Incidents involving high-risk AI systems posing an imminent threat to human life, safety, or fundamental rights;
    (b) High: Incidents causing significant harm, disruption, or financial loss;
    (c) Medium: Incidents with moderate impact or potential for risk escalation;
    (d) Low: Incidents with minimal impact.
  (ii) Information to Provide in Incident Reports:
    (a) Detailed description of the incident and its impact;
    (b) Details of the AI system (type, use case, risk level, deployment stage);
    (c) For high-risk AI systems: Root cause analysis, mitigation actions, and supporting data.
  (iii) Timelines and Procedure for Reporting:
    (a) Critical incidents with high-risk AI systems must be reported within 48 hours;
    (b) High or medium severity incidents must be reported within 7 days if involving high-risk AI systems, and within 14 days for all other systems;
    (c) Low severity incidents must be reported monthly.
  (iv) Confidentiality measures for incident data:
    (a) All AI systems must ensure to have:
    (b) Data encryption at rest and in transit;
    (c) Role-based access controls for incident data;
    (d) Maintaining audit logs of all data access;
    (e) Secure communication channels for data transmission;
    (f) Retaining data as per requirements under cyber and data protection frameworks;
    (g) Regular risk assessments on data confidentiality;
    (h) Employee training on data protection and handling.
  (v) All high-risk AI systems must ensure to have:
    (a) Proper encryption key management practices;
    (b) Encryption for removable media with incident data;
    (c) Multi-factor authentication for data access;
    (d) Physical security controls for data storage;
    (e) Redacting/anonymizing personal information;
    (f) Secure data disposal mechanisms;
    (g) Periodic external audits on confidentiality;
    (h) Disciplinary actions for violations.
  (vi) The following measures are optional for low-risk AI systems:
    (a) Key management practices (recommended);
    (b) Removable media encryption (as needed);
    (c) Multi-factor authentication (recommended);

(d) Physical controls (based on data sensitivity);
(e) Personal data redaction (as applicable);
(f) Secure disposal mechanisms (recommended).

(8) All AI system developers, operators, and users shall implement the following minimum mitigation actions upon becoming aware of an incident:
(i) Assess the incident severity based on IAIC guidelines;
(ii) Contain the incident through isolation, disabling functions, or other measures;
(iii) Investigate the root cause of the incident;
(iv) Remediate the incident through updates, security enhancements, or personnel training;
(v) Communicate incident details and mitigation actions to impacted parties;
(vi) Review and improve internal incident response procedures.

(9) For AI systems exempted from certification under sub-section (3) of Section 11, the following guidelines shall apply regarding incident reporting and response protocols:
(i) Voluntary Incident Reporting: Developers, operators and users of exempted AI systems are encouraged, but not mandatorily required, to establish mechanisms for incident reporting related to such systems.
(ii) Focus on High/Critical Incident: In cases where incident reporting mechanisms are established, the focus shall be on reporting high severity or critical incidents that pose a clear potential for harm or adverse impact.
(iii) Reasonable Timelines: For high/critical incidents involving exempted AI systems, developers shall report such incidents to the IAIC within a reasonable timeline of 14-30 days from becoming aware of the incident.
(iv) Incident Description: Incident reports for exempted AI systems shall primarily include a description of the incident, its perceived severity and impact, and details about the AI system itself (type, use case, risk classification).
(v) Confidentiality Measures: Developers of exempted AI systems shall implement confidentiality measures for incident data that are proportionate to the data sensitivity and potential risks involved.
(vi) Coordinated Disclosure: The IAIC shall establish coordinated disclosure programs to facilitate responsible reporting and remediation of vulnerabilities or incidents related to exempted AI systems.
(vii) Knowledge Sharing: The IAIC shall maintain a knowledge base of reported incidents involving exempted AI systems and share anonymized information to promote learning and improve incident response practices.

(10) The IAIC shall provide support and resources to AI entities on request for effective incident mitigation, prioritizing high-risk AI incidents.
(11) The IAIC shall have the power to audit AI entities and impose penalties for non-compliance with this Section as per the provisions of this Act.

Section 20 - Responsible Information Sharing

[***][2]

Section 20A – Transparency and Accountability in AI-related Government Initiatives and Public-Private Partnerships

(1) This section applies to all AI-related initiatives undertaken by any governmental body, statutory authority, public sector entity, or public-private partnership (PPP) involving AI technologies for public services or infrastructure.

(2) Transparency Requirements: All entities under this section must comply with the Right to Information Act, 2005, by publicly disclosing the following information about AI initiatives:

- **(i) A clear statement of the project's purpose and expected outcomes;**
- **(ii) Details of funding, including public funds, subsidies, or PPP financial arrangements;**
- **(iii) Summaries of risk assessments addressing privacy, security, and ethical impacts;**
- **(iv) Descriptions of algorithms used in decision-making for public services, including their purpose and functionality;**
- **(v) Key performance indicators (KPIs) to evaluate the AI system's effectiveness.**

(3) Additional Obligations for Public-Private Partnerships (PPPs): PPPs involving AI technologies must:

- **(i) Disclose key contractual terms, including payment structures, risk allocation, and responsibilities of each party;**
- **(ii) Provide public access to data generated by AI systems in public service contexts, unless restricted under Section 8 of the RTI Act, 2005, or Section 6 of the DPDP Act, 2023;**
- **(iii) Conduct annual independent audits to verify compliance with ethical standards and performance metrics, and publish the audit results.**

(4) Algorithmic Accountability: AI systems used in government or PPP initiatives that impact individuals' rights or access to public services must:

- **(i) Provide written explanations of algorithmic decisions upon request by affected individuals;**
- **(ii) Document and disclose measures to prevent algorithmic bias, including details of data selection and validation processes;**
- **(iii) Conduct and publish impact assessments before deployment, evaluating risks to vulnerable populations.**

(5) Before launching large-scale AI projects or entering PPPs involving AI, the responsible government body must:

- **(i) Hold public consultations with stakeholders, including civil society, industry experts, academics, and affected communities;**

[2] Omitted in Version 5.

(ii) Publish a summary of consultation feedback and explain how it was incorporated into the project plan.

(6) All entities under this section must submit an annual report to the Indian Artificial Intelligence Council (IAIC), which must be published on official government websites, detailing:

(i) Progress on AI projects;

(ii) Results of audits or impact assessments;
(iii) Incidents of AI misuse or failure, with corrective actions taken;
(iv) Measures implemented to address transparency, accountability, and ethical concerns.

(7) Exemptions: Information may be withheld from disclosure if it:

(i) Compromises national security;
(ii) Violates personal privacy under the DPDP Act, 2023;
(iii) Interferes with ongoing investigations or enforcement actions;
(iv) Conflicts with legitimate use purposes as defined under Section 6 of the DPDP Act, 2023, per Section 8 of the RTI Act, 2005.

CHAPTER VIII: INTELLECTUAL PROPERTY PROTECTIONS

Section 21 - Intellectual Property Protections

(1) In recognition of the unique challenges and opportunities presented by the development and use of artificial intelligence systems, AI systems must be protected through a combination of existing intellectual property (IP) rights, such as copyright, patents, and design rights, as well as new and evolving IP concepts specifically tailored to address the spatial aspects of AI systems.

(2) For the purposes of this Section, "spatial aspects of AI systems" shall refer to the unique capabilities of AI technologies, including but not limited to:
(i) Dynamically adapting and generating novel outputs based on changing inputs, environments, and interactions;
(ii) Operating with varying levels of autonomy in decision-making, task execution, and self-learning;
(iii) Integrating and analysing data from multiple spatial, temporal, and contextual sources;
(iv) Enabling novel applications, services, and experiences leveraging spatial computing technologies.

(3) The objectives of providing a combination of existing intellectual property rights are to:
(i) Encourage innovation by securing enforceable rights for AI developers over their creations, inventions, and generated outputs;
(ii) Enhance interoperability by ensuring contractual arrangements are not unduly hindered by restrictive IP terms;
(iii) Promote fair competition by preventing unauthorized exploitation of AI-related IP assets developed in India;

(iv) Protect individual privacy and data rights by aligning IP protections with provisions under the Digital Personal Data Protection Act, 2023 and other data protection frameworks.

(4) The IAIC shall establish consultative mechanisms, in cooperation with relevant IP authorities and stakeholders, to develop a comprehensive framework for the identification, protection, and enforcement of intellectual property rights related to AI systems, including:
(i) Defining the scope and limitations of combined IP protections for AI systems and their spatial aspects;
(ii) Assessing the compatibility of such protections with existing IP laws and international treaties;
(iii) Addressing interoperability considerations to enable seamless integration and data exchange among AI systems;
(iv) Examining IP implications of AI systems' ability to process, learn from, and generate content based on copyrighted works or patented inventions;
(v) Developing guidelines for determining authorship, inventorship, and ownership of AI-generated content and innovations;
(vi) Establishing protocols for rights management, licensing, and commercialisation of AI-related IP assets.

(5) The use of open-source software in AI systems shall be subject to the terms and conditions of the respective open-source licenses, with the IAIC providing guidance on compatibility between such licenses and the IP protections framework for AI systems.
(6) The IAIC shall periodically review and update the IP protections framework to accommodate advancements in AI technologies, evolving legal and regulatory landscapes, and emerging best practices in the field of AI and spatial computing.

CHAPTER VIII-A: INTERNATIONAL COOPERATION FRAMEWORK

Section 21A – Data Classification and Localisation Requirements

(1) The Central Government shall establish a data classification and tiering system that defines storage, access, and transfer requirements based on data sensitivity and strategic importance. The system shall include the following tiers:

(i) **Tier 1: Critical National Security Data**
(a) **Characteristics**: Includes data with direct national security implications, sensitive government infrastructure data, critical defence information, and biometric/sensitive personal identification data.

(ii) **Tier 2: Strategic Sectoral Data**
(a) Strategic Sectors Designated:
(i) Healthcare
(ii) Financial Services
(iii) Critical Infrastructure, and
(iv) Emerging Technology Research

(iii) **Tier 3: Commercial and Research Data**

(a) **Characteristics**: Includes non-sensitive commercial data, academic and research collaboration data, and open-source AI training datasets.

(2) To promote responsible data management and adherence to localisation requirements among companies, the Central Government shall provide incentives aligned with the entity's AI classification under Chapter II. Incentives include:

(i) **Tax Benefits**: Available for entities compliant with localisation protocols, with additional consideration given based on the AI system's classification type under the commercial methods of classification in Section 6.

(ii) **Expedited Cross-Border Approvals**: Reserved for institutions with demonstrated responsible cross-border data management, particularly those operating high-risk AI systems or classified under AI-IaaS and AI-Com as per methods of classification in Section 5 due to their integration with sensitive digital infrastructure.

(iii) **Recognition Certificates for Exemplary Management Practices**: Granted to institutions that demonstrate best practices in data management, security, and AI governance, taking into account methods of classification in Sections 5 and 7.

(3) The framework shall be rolled out in phases over 24 months and include:

(i) Regular review and recalibration to adapt to emerging technological and policy challenges.

(ii) Stakeholder consultation mechanisms to incorporate feedback from industry, academia, and government entities.

(iii) Capacity building programs to support entities in implementing and maintaining compliance with these standards.

CHAPTER IX: SECTOR-NEUTRAL & SECTOR-SPECIFIC STANDARDS

Section 22 - Shared Sector-Neutral & Sector-Specific Standards

(1) The IAIC shall coordinate the implementation and review of the following sector-neutral standards for the responsible development, deployment, and use of AI systems:

(i) Fundamental Principles of Liability as outlined in sub-sections (2), (3), and (4);

(2) Liability for harm or damage caused by an AI system shall be allocated based on the following principles:

(i) The party that developed, deployed, or operated the AI system shall be primarily liable for any harm or damage caused by the system, taking into account the system's classification under the conceptual, technical, commercial, and risk-based methods.

(ii) Liability may be shared among multiple parties involved in the AI system's lifecycle, based on their respective roles and responsibilities, as well as the system's classification and associated requirements under Sections 8 and 9.

(iii) End-users shall not be held liable for harm or damage caused by an AI system, unless they intentionally misused or tampered with the system, or failed to comply with user obligations specified based on the system's classification.

(3) To determine and adjudicate liability for harm caused by AI systems, the following factors shall be considered:

(i) The foreseeability of the harm, in light of the AI system's intended purpose as identified by the Issue-to-Issue Concept Classification (IICC) under Section 4(2), its capabilities as

specified in the Technical Classification under Section 5, and its limitations according to the Risk Classification under Section 7;

(ii) The degree of control exercised over the AI system, considering the human oversight and accountability requirements tied to its Risk Classification under Section 7, particularly the principles of Human Agency and Oversight as outlined in Section 13;

(4) Developers and operators of AI systems shall be required to obtain liability insurance to cover potential harm or damage caused by their AI systems. The insurance coverage shall be proportionate to the risk levels and potential impacts of the AI systems, as determined under the Risk Classification framework in Section 7, and the associated requirements for high-risk AI systems outlined in Section 9. This insurance policy shall ensure that compensation is available to affected individuals or entities in cases where liability cannot be attributed to a specific party.

(5) The IAIC shall enable coordination among sector-specific regulators for the responsible development, deployment, and use of AI systems in sector-specific contexts based on the following set of principles:

(i) Transparency and Explainability:

(a) AI systems should be designed and developed in a transparent manner, allowing users to understand how they work and how decisions are made.

(b) AI systems should be able to explain their decisions in a clear and concise manner, allowing users to understand the reasoning behind their outputs.

(c) Developers should provide clear documentation and user guides explaining the AI system's capabilities, limitations, and potential risks.

(d) The level of transparency and explainability required may vary based on the AI system's risk classification and intended use case.

(ii) Fairness and Bias:

(a) AI systems should be regularly monitored for technical bias and discrimination, and appropriate mitigation measures should be implemented to address any identified issues in a sociotechnical context.

(b) Developers should ensure that training data is diverse, representative, and free from biases that could lead to discriminatory outcomes.

(c) Ongoing audits and assessments should be conducted to identify and rectify any emerging biases during the AI system's lifecycle.

(iii) Safety and Security:

(a) AI systems should be designed and developed with safety and security by design & default.

(b) AI systems should be protected from unauthorized access, modification, or destruction.

(c) Developers should implement robust security measures, such as encryption, access controls, and secure communication protocols, to safeguard AI systems and their data.

(d) AI systems should undergo rigorous testing and validation to ensure they perform safely and reliably under normal and unexpected conditions.

(e) Developers should establish incident response plans and mechanisms to promptly address any safety or security breaches.

(iv) Human Control and Oversight:

(a) AI systems should be subject to human control and oversight to ensure that they are used responsibly.
(b) There should be mechanisms in place for data principals to intervene in the operation of AI systems if necessary.
(c) Developers should implement human-in-the-loop or human-on-the-loop approaches, allowing for human intervention and final decision-making in critical or high-risk scenarios.
(d) Clear protocols should be established for escalating decisions to human operators when AI systems encounter situations beyond their designed scope or when unexpected outcomes occur.
(e) Regular human audits and reviews should be conducted to ensure AI systems are functioning as intended and aligned with human values and societal norms.

(iv) Open Source and Interoperability:
(a) The development of shared sector-neutral standards for AI systems shall leverage open source software and open standards to promote interoperability, transparency, and collaboration.
(b) The IAIC shall encourage the participation of open source communities and stakeholders in the development of AI standards.
(c) Developers should strive to use open source components and frameworks when building AI systems to facilitate transparency, reusability, and innovation.
(d) AI systems should be designed with interoperability in mind, adhering to common data formats, protocols, and APIs to enable seamless integration and data exchange across different platforms and domains.
(e) The IAIC shall promote the development of open benchmarks, datasets, and evaluation frameworks to assess and compare the performance of AI systems transparently.

CHAPTER X: CONTENT PROVENANCE

Section 23 - Content Provenance and Identification

(1) AI systems that generate or manipulate content must establish and maintain robust mechanisms for source attribution, origin documentation, and ethical data handling. These mechanisms shall integrate technical measures, human oversight, and compliance with applicable laws to ensure transparency and accountability in the following manner:

(i) Clearly document the origins of all content sources, ensuring that:

(a) Sources are identified with precision, including the website, database, or platform from which data is obtained;
(b) Only publicly available data or data acquired with explicit, documented consent from the data subject is utilised, where such data collection adheres to ethical practices, defined as:

(i) Ensuring transparency by publicly disclosing the purpose, scope, and intended use of data collection, enabling accountability across all applications of the AI system;
(ii) Complying with all applicable laws, including the Digital Personal Data Protection Act, 2023, and respecting the terms of service, intellectual property rights, and access restrictions of data sources, to safeguard the integrity of content generation and manipulation processes;
(iii) Avoiding the collection of sensitive personal data unless strictly necessary, legally permitted, and subject to heightened safeguards, including mandatory risk assessments for applications involving high-stakes decision-making or vulnerable populations;

(iv) Implementing measures to prevent unauthorized access, use, or distribution of the collected data, including the use of anonymisation or pseudonymisation techniques to minimize the risk of re-identification, where:

(a) Anonymisation refers to the irreversible process of transforming data into a form where the data subject cannot be identified, meeting standards of irreversibility as per best practices;
(b) Pseudonymisation refers to replacing identifying characteristics with artificial identifiers, ensuring that re-identification is only possible with additional, securely stored information;

(v) Permitting the use of in-copyright works for text and data mining (TDM) purposes, provided that:

(a) The TDM is conducted for non-commercial research, statistical, or operational optimization purposes, supporting innovation while respecting the rights of content creators;
(b) The entity has lawful access to the data, either through public availability, consent, or authorised licensing;
(c) The TDM process does not involve the reproduction or distribution of the original copyrighted works beyond what is necessary for the mining process, and appropriate attribution is provided where feasible;

(vi) For AI systems deployed in strategic sectors under applicable regulations, additional compliance with sector-specific data security and national interest requirements shall apply, as prescribed by the relevant authority.

(c) Any use of web scraping adheres to the target website's terms of service and robots.txt protocols, with prior written permission obtained where required.

(ii) Maintain comprehensive and auditable technical documentation of data collection methods used in training datasets, which shall include:

(a) A detailed description of acquisition techniques, such as APIs, manual collection, or automated scraping, ensuring all methods comply with legal and ethical standards;

(b) Evidence of compliance with the Digital Personal Data Protection Act, 2023, for any personal data collected, including records of user consent where applicable;
(c) A commitment to data minimization, ensuring that only data necessary for the specified purpose is collected and processed.

(iii) Establish and maintain verifiable records of data provenance, categorizing data as follows:

(a) Personal data, processed strictly in accordance with the Digital Personal Data Protection Act, 2023, with documented consent and purpose limitation;
(b) Non-personal data, collected through authorized and transparent methods, ensuring no violation of intellectual property rights or website terms of service;
(c) Synthetic data, generated by the AI system itself, with clear documentation of the generation process to distinguish it from real-world data and prevent misrepresentation.

(2) Accountability for tracking AI-generated content shall be determined by the specific use cases of the AI system, such that for end-users and business end-users of AI systems, accountability and liability for AI-generated content must be examined based on factors such as:

(i) Whether they intentionally misused or tampered with the AI system despite being aware of its key limitations;
(ii) Whether they failed to exercise reasonable care and due diligence in the utilisation of the AI system;
(iii) Whether they knowingly propagated or disseminated AI-generated content that could cause harm;

(3) Intermediaries that host, publish, or make available AI-generated content shall:

(i) Implement non-discriminatory content policies that:

(a) Prohibit demonetisation or de-prioritisation of content solely based on its AI-generated nature when properly watermarked and disclosed;
(b) Maintain parity in content recommendation algorithms between human-created and AI-generated works meeting provenance requirements;
(c) Provide appeal mechanisms for creators affected by automated moderation of AI-generated content;

(4) Watermarking techniques must incorporate machine-readable metadata containing:

(i) Scraping methodology classification;
(ii) Geographic origin of training data sources;
(iii) Licensing status of underlying datasets;

(5) Developers, owners, and operators of AI systems as described in sub-sections (3) to (7) of Section 6 shall obtain and maintain adequate liability insurance coverage proportionate to their commercial classification and risk profile. The coverage must include:

(i) Professional indemnity insurance to cover incidents involving inaccurate, inappropriate or defamatory AI-generated content;
(ii) Cyber risk insurance to cover incidents related to data breaches, network security failures or other cyber incidents involving AI-generated content;
(iii) General commercial liability insurance to cover incidents causing third-party injury, damage or other legally liable scenarios involving AI-generated content;
(v) Specific coverage for claims arising from data scraping activities conducted in the development, training, or operation of the AI system.

(6) Exceptions for AI-Preview (AI-Pre) Systems: AI systems as described in sub-section (8) of Section 6 shall be exempt from sub-section (5) requirements only if:

(i) User base remains below 50,000 real-time active testers
(ii) No personal/sensitive data processing occurs
(iii) Annual development budget remains under ₹5 crore
(iv) System displays prominent "Preview Version" watermarks
(v) Revenue generation is limited to subscription fees for testing purposes, nominal one-time access fees, or cost recovery mechanisms that do not constitute full commercial deployment, provided that:

(a) Such revenue does not exceed 15% of the developing entity's total annual revenue
(b) All monetary transactions are clearly disclosed as supporting a preview or test version
(c) No claims of complete or commercial-grade functionality are made in marketing materials

(vi) The system is not used to generate, simulate, or manipulate user consent for any purpose
(vii) All interactions regarding terms of service, permissions, or agreements are conducted without AI intermediation

(viii) Regular checks or audits verify the system's inputs and outputs do not engage in preference or opinion manipulation
(ix) The developer maintains comprehensive logs of all system prompts and responses that could influence user decision-making
(x) Users are explicitly informed if the system utilises persuasive or preference-shaping techniques in its responses

(xi) Educational implementations, provided that content generation capabilities are supervised;

(xii) Research applications, provided that in the case of research institutions, centres and firms:

(a) Limited usage by verified research entities;
(b) Publication of findings adheres to responsible disclosure guidelines;
(c) Basic insurance coverage for potential third-party effects is maintained.

(xiii) Terms and conditions are easily accessible in clear and plain language, and a readily contactable person is designated in accordance with sub-sections (9) and (28) of Section 2 of the Consumer Protection Act, 2019, to handle user queries, complaints, or grievances.

(xiv) Appropriate insurance is maintained for any public-facing implementations.

(7) AI systems as described in sub-section (8) of Section 6 exceeding any criteria in (6) must:

(i) Obtain insurance within 30 days of threshold breach
(ii) Reclassify under appropriate Section 6 commercial category

(8) The minimum insurance coverage required for AI content generation systems shall be:

(vi) ₹ 50 crores for AI-S (Artificial Intelligence as a System) and AI-IaaS (Artificial Intelligence-enabled Infrastructure as a Service) under sub-sections (6) and (7) of Section 6 respectively

(vii) ₹ 25 crores for AI-Pro (Artificial Intelligence as a Product) and AIaaS (Artificial Intelligence as a Service) under sub-sections (3) and (4) of Section 6 respectively

(viii) ₹ 10 crores for AI-Com (Artificial Intelligence as a Component) under sub-section (5) of Section 6

(ix) ₹ 2 crores for AI-Pre (Artificial Intelligence for Preview) under sub-section (8) of Section 6 with public-facing implementations

(9) The IAIC shall establish and maintain a public registry of open-access technical methods to identify and examine AI-generated content, accessible to end-users, business users, and government officials. This registry shall provide clear instructions for using these methods and information on their validity;

(10) This Section shall apply to all AI systems that generate or manipulate content, regardless of the content's purpose or intended use, including AI systems that generate text, images, audio, video, or any other forms of content.

CHAPTER XI: EMPLOYMENT, LITERACY AND INSURANCE

Section 24 - Employment and Skill Security Standards

[***][3]

Section 24-A – Right to Artificial Intelligence Literacy

(1) Every individual has the right to basic artificial intelligence literacy that enables meaningful participation in an AI-augmented society.

(2) For the purpose of this section, "artificial intelligence literacy" shall include:

(i) Knowledge of fundamental AI concepts, capabilities, and limitations;

(ii) Understanding of how AI systems may impact individual rights, including privacy, autonomy, and equal treatment;

(iii) Ability to identify AI-generated content and understand AI involvement in automated decision-making processes;

(iv) Awareness of mechanisms to seek recourse when adversely affected by AI systems.

(3) Educational institutions receiving public funding shall progressively integrate age-appropriate AI literacy into their curricula within three years of the commencement of this Act.

(4) All public services utilizing AI systems shall provide accessible information about:

(i) The fact of AI deployment in service delivery;

(ii) How the AI system influences decisions or outcomes;

(iii) Options available to citizens who wish to opt for human review or intervention.

Section 25 - Insurance Policy for AI Technologies

(1) Developers, owners, and operators of high-risk AI systems, as classified under sub-section (4) of Section 7, shall be required to obtain and maintain comprehensive liability insurance coverage to manage and mitigate potential risks associated with the development, deployment, and operation of such systems.

(2) The insurance coverage requirements for high-risk AI systems shall be proportionate to their risk level and potential impacts, as determined by:

(i) Their conceptual classification based on sub-sections (3), and (4) of Section 4;

(ii) Their technical characteristics evaluated as per the criteria under sub-section (4) of Section 5 for Specific Purpose AI (SPAI) systems;

(iii) Their commercial risk factors such as user base, market influence, data integration, and revenue generation specified under Section 6;

(3) The minimum insurance coverage required for high-risk AI systems shall be:

(i) For systems with potential widespread impact or lack of opt-out feasibility under Section 7(4)(a): ₹ 50 crores;

(ii) For systems with vulnerability factors or irreversible consequences under Section 7(4)(b): ₹ 25 crores;

(iii) For other high-risk AI systems under Section 7(4): ₹ 10 crores.

[3] Omitted in Version 5.

(4) The Insurance Regulatory and Development Authority of India (IRDAI) shall, in consultation with the IAIC and relevant stakeholders, specify the minimum insurance coverage standards for high-risk AI systems, which may include:
   (i) Professional indemnity insurance to cover incidents involving inaccurate, inappropriate, or defamatory AI-generated content;
   (ii) Cyber risk insurance to cover incidents related to data breaches, network security failures, or other cyber incidents;
   (iii) General commercial liability insurance to cover incidents causing third-party injury, damage, or other legally liable scenarios.

(5) For general purpose AI systems classified under sub-sections (2), and (3) of Section 5, the IAIC, in coordination with IRDAI, shall examine and determine appropriate insurance requirements, considering factors such as:
   (i) The scale and inherent purpose of the general purpose AI system;
   (ii) The potential risks and impacts associated with its multiple use cases across different sectors and domains;
   (iii) The technical features and limitations that may affect its safety, security, and reliability;
   (iv) The commercial factors such as user base, market influence, and revenue generation.

(6) Based on the examination under sub-section (5), the IAIC may recommend to IRDAI the development of specialized insurance products or coverage requirements for general purpose AI systems, which may include:
   (i) Umbrella liability insurance to cover a wide range of risks and liabilities arising from the diverse applications of the AI system;
   (ii) Parametric insurance based on predefined triggers or performance metrics to address the unique challenges in assessing and quantifying risks associated with general purpose AI;
   (iii) Risk pooling or reinsurance arrangements to spread the risks among multiple insurers or stakeholders.

(7) The IAIC and IRDAI shall collaborate to establish guidelines and best practices for underwriting, risk assessment, and claims handling related to general purpose AI systems, taking into account their distinct characteristics and potential impacts.

(8) Developers, owners, and operators of general purpose AI systems shall be encouraged to maintain adequate insurance coverage based on the recommendations and guidelines issued by the IAIC and IRDAI under sub-sections (6) and (7).

(9) Insurance providers offering AI-specific policies for high-risk systems must have adequate expertise, resources, and reinsurance arrangements to effectively assess risks, price premiums, and settle claims related to AI technologies.

(10) Developers, owners, and operators of high-risk AI systems shall submit proof of adequate insurance coverage to the IAIC as part of the registration and certification process outlined in Section 11.

(11) Failure to obtain and maintain the required insurance coverage for high-risk AI systems shall be treated as a breach of compliance under Section 19, and the IAIC may take appropriate enforcement actions, including:
   (i) Issuing warnings and imposing penalties;
   (ii) Suspending or revoking the system's certification;

(iii) Prohibiting the deployment or operation of the AI system until compliance is achieved.

(12)The obligations under sub-sections (2), (3), and (4) of this Section shall apply to data fiduciaries employing high-risk AI systems, provided they are:
(i) Notified as Significant Data Fiduciaries under sub-section (1) of Section 10 of the Digital Personal Data Protection Act, 2023, based on factors such as:
(a) The volume and sensitivity of personal data processed;
(b) The risk to the rights of data principals;
(c) The potential impact on the sovereignty, integrity, and security of India.

(13) For AI systems not classified as high-risk under sub-section (4) of Section 7, obtaining insurance coverage is recommended but not mandatory. The IAIC shall provide guidance on suitable insurance products and coverage levels based on the AI system's risk profile and potential impacts;

(14)The Insurance Regulatory and Development Authority of India (IRDAI), in consultation with the IAIC and relevant stakeholders, shall develop guidelines and best practices for underwriting, risk assessment, and claims handling related to AI technologies. These guidelines shall address:

(i) Assessment methods to evaluate the unique risks and potential impacts of AI systems, taking into account their risk classification and associated factors as outlined in this Act;
(ii) Premium calculation models that consider the risk profile, scale of deployment, and potential consequences of AI systems;
(iii) Claims processing standards that ensure timely, fair, and transparent settlement of claims related to AI systems;
(iv) Data sharing and reporting requirements between insurers and the IAIC to facilitate the monitoring and analysis of AI-related incidents and claims;
(v) Capacity building and training programs for insurance professionals to enhance their understanding of AI technologies and their associated risks;

CHAPTER XII: APPEAL AND ALTERNATIVE DISPUTE RESOLUTION

Section 26 – Appeal to Appellate Tribunal

(1) The Appellate Tribunal established under the Telecom Regulatory Authority of India Act, 1997, shall also serve as the Appellate Tribunal for the purposes of this Act.

(2) Any person aggrieved by any direction, decision, or order of the IAIC under this Act may prefer an appeal to the Appellate Tribunal within a period of 60 days from the date on which a copy of the direction, decision, or order is received by the person.

(3) The Appellate Tribunal may entertain an appeal after the expiry of the said period of 60 days if it is satisfied that there was sufficient cause for not filing it within that period.

(4) On receipt of an appeal, the Appellate Tribunal may, after giving the parties to the appeal an opportunity of being heard, pass such orders thereon as it thinks fit, confirming, modifying, or setting aside the direction, decision, or order appealed against.

(5) The Appellate Tribunal shall send a copy of every order made by it to the parties to the appeal and to the IAIC.

(6) The appeal filed before the Appellate Tribunal shall be dealt with by it as expeditiously as possible, and endeavour shall be made by it to dispose of the appeal finally within 6 months from the date of receipt of the appeal.

(7) The Appellate Tribunal may, for the purpose of examining the legality, propriety, or correctness of any direction, decision, or order of the IAIC, on its own motion or otherwise, call for the records relevant to disposing of such appeal and make such orders as it thinks fit.

(8) The provisions of sections 14-I to 14K of the Telecom Regulatory Authority of India Act, 1997, shall, mutatis mutandis, apply to the Appellate Tribunal in the discharge of its functions under this Act, as they apply to it in the discharge of its functions under that Act.

(9) Any person aggrieved by any decision or order of the Appellate Tribunal may file an appeal to the Supreme Court within a period of 60 days from the date of communication of the decision or order of the Appellate Tribunal.

(10) The Appellate Tribunal shall endeavour to function as a digital office to the extent practicable, with the filing of appeals, hearings, and pronouncement of orders being conducted through digital means.

Section 27 – Orders passed by Appellate Tribunal to be executable as decree

(1) An order passed by the Appellate Tribunal under this Act shall be executable by it as a decree of civil court, and for this purpose, the Appellate Tribunal shall have all the powers of a civil court.

(2) Notwithstanding anything contained in sub-section (1), the Appellate Tribunal may transmit any order made by it to a civil court having local jurisdiction and such civil court shall execute the order as if it were a decree made by that court.

Section 28 – Alternate Dispute Resolution

If the IAIC is of the opinion that any complaint may be resolved by mediation, it may direct the parties concerned to attempt resolution of the dispute through such mediation by such mediator as the parties may mutually agree upon, or as provided for under any law for the time being in force in India.

We have provided a list of suggested provisions, which may be expected in the draft Act, but do not have any substantive necessity to be drafted.

CHAPTER XIII: MISCELLANEOUS

Section 29 - Power to Make Rules

(1) The Central Government may, by notification, make rules to carry out the provisions of this Act.

(2) In particular, and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following matters, namely:—

(a) The manner of appointment, qualifications, terms and conditions of service of the Chairperson and Members of the IAIC under sub-section (6) of Section 10;

(b) The form, manner, and fee for filing an appeal before the Appellate Tribunal under Section sub-section (2) of Section 26;

(c) The procedure to be followed by the Appellate Tribunal while dealing with an appeal under the sub-section (8) of Section 26;

(d) Any other matter which is required to be, or may be, prescribed, or in respect of which provision is to be made by rules.

(3) Every rule made under this Act shall be laid, as soon as may be after it is made, before each House of Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if, before the expiry of the session immediately following the session or the successive sessions aforesaid, both Houses agree in making any modification in the rule or both Houses agree that the rule should not be made, the rule shall thereafter have effect only in such modified form or be of no effect, as the case may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under that rule.

Section 30 - Power to Make Regulations

(1) The IAIC may, by notification, make regulations consistent with this Act and the rules made thereunder to carry out the provisions of this Act.

(2) In particular, and without prejudice to the generality of the foregoing power, such regulations may provide for all or any of the following matters, namely —

(i) The criteria and process for the classification of AI systems based on their conceptual, technical, commercial, and risk-based factors, as specified in Sections 4, 5, 6, and 7;

(ii) The standards, guidelines, and best practices for the development, deployment, and use of AI systems, including those related to transparency, explainability, fairness, safety, security, and human oversight, as outlined in Section 13;

(iii) The procedures and requirements for the registration and certification of AI systems, including the criteria for exemptions and the maintenance of the National Registry of Artificial Intelligence Use Cases, as specified in Sections 11 and 12;

(iv) The guidelines and mechanisms for post-deployment monitoring of high-risk AI systems, as outlined in Section 17;

(v) The procedures and protocols for third-party vulnerability reporting, incident reporting, and responsible information sharing, as mentioned in Sections 18, 19, and 20;

(vi) The guidelines and requirements for content provenance and identification in AI-generated content, as specified in Section 23;

(vii) The insurance coverage requirements and risk assessment procedures for entities developing or deploying high-risk AI systems, as outlined in Section 25;

(viii) Any other matter which is required to be, or may be, prescribed, or in respect of which provision is to be made by regulations.

(3) Every regulation made under this Act shall be laid, as soon as may be after it is made, before each House of Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if, before the expiry of the session immediately following the session or the successive sessions aforesaid, both Houses agree in making any modification in the regulation or both Houses agree that the regulation should not be made, the regulation shall thereafter have effect only in such modified form or be of no effect, as the case may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under that regulation.

Section 31 - Protection of Action Taken in Good Faith

No suit, prosecution, or other legal proceedings shall lie against the Central Government, the Indian Artificial Intelligence Council (IAIC), the Indian Artificial Intelligence Safety Institute (AISI), their respective Chairpersons, Members, officers, or employees for anything which is done or intended to be done in good faith under the provisions of this Act or the rules made thereunder.

Section 32 – Offenses and Penalties

(1) Any person who contravenes or fails to comply with any provision of this Act, or the rules or regulations made thereunder, shall be liable to penalties as specified in this Section.

(2) Significant Data Fiduciaries (SDFs) under the Digital Personal Data Protection Act, 2023, that employ high-risk AI systems and fail to comply with the provisions of this Act shall be liable to the following penalties:

(a) For the first offense, a fine of up to 4% of the SDF's total worldwide turnover in the preceding financial year or ₹ 25 crores, whichever is higher;

(b) For subsequent offenses, a fine of up to 8% of the SDF's total worldwide turnover in the preceding financial year or ₹ 50 crores, whichever is higher.

(4) Entities developing, deploying, or operating high-risk AI systems, other than those covered under sub-sections (2) and (3), that fail to comply with the provisions of this Act shall be liable to the following penalties:

(a) For the first offense, a fine of up to ₹ 10 crores;

(b) For subsequent offenses, a fine of up to ₹ 25 crores.

(5) In addition to the financial penalties specified in sub-sections (2), (3), and (4), the IAIC may take the following actions against non-compliant entities:

(a) Issuing warnings and directions for remedial measures;

(b) Suspending or revoking the certification of the AI system;

(c) Prohibiting the deployment or operation of the AI system until compliance is achieved;

(d) Mandating independent audits of the entity's processes at their own cost;

(e) Recommending the temporary or permanent suspension of the entity's AI-related operations in cases of persistent or egregious non-compliance.

(6) Entities developing, deploying, or operating AI systems exempted from certification under Section 11(3) shall be encouraged to voluntarily comply with the provisions of this Act. Non-compliance by such entities shall not attract any penalties, provided that:

(a) The AI system remains within the scope of the exemption criteria specified in Section 11(3);

(b) The entity maintains the incident reporting and response protocols as required under Section 11(4);

(c) The entity cooperates with the IAIC in the event of any investigation or inquiry related to the AI system.

(7) The IAIC shall establish clear guidelines for the determination and imposition of penalties, ensuring transparency, proportionality, and due process. Factors such as the nature, severity, and duration of the non-compliance, the entity's willingness to cooperate and take remedial measures, and the potential harm caused by the non-compliance shall be considered while deciding the quantum of penalties.

(8) Any penalty imposed under this Section shall not prevent the initiation of criminal proceedings against the offender if the same act or omission constitutes an offense under any other law for the time being in force.

(9) All sums realized by way of penalties under this Act shall be credited to the Consolidated Fund of India.

CHAPTER XIV: REPEAL AND SAVINGS

Section 33 - Savings Clause

(1) The provisions of this Act shall be in addition to, and not in derogation of, the provisions of any other law for the time being in force.

(2) Nothing in this Act shall affect the validity of any action taken or decision made by any entity in relation to the development, deployment, or use of AI systems prior to the commencement of this Act, provided such action or decision was in accordance with the laws in force at that time.

(3) Any investigation, legal proceeding, or remedy in respect of any right, privilege, obligation, liability, penalty, or punishment under any law, initiated or arising before the commencement of this Act, shall be continued, enforced, or imposed as if this Act had not been enacted.

(4) Nothing in this Act shall be construed as preventing the Central Government from making any rules or regulations, or taking any action, which it considers necessary for the purpose of removing any difficulty that may arise in giving effect to the provisions of this Act.

CHAPTER XV: FINAL PROVISIONS

Section 34 - Power to Remove Difficulties

(1) If any difficulty arises in giving effect to the provisions of this Act, the Central Government may, by order published in the Official Gazette, make such provisions, not inconsistent with the provisions of this Act as may appear to it to be necessary for removing the difficulty.

(2) No such order shall be made under this Section after the expiry of a period of five years from the commencement of this Act.

(3) Every order made under this Section shall be laid, as soon as may after it is made before each House of Parliament.

Section 35 - Amendment of [Other Legislation]

(1) The Digital Personal Data Protection Act, 2023 shall be amended as follows:

(a) In Section 7, after the sub-section on "Legitimate Uses", the following sub-section shall be inserted:

> "The processing of personal data by an Artificial Intelligence system shall be considered a legitimate purpose under this Act, subject to compliance with the provisions of the Artificial Intelligence (Development & Regulation) Act, 2023 and the rules and regulations made thereunder."

(2) The Competition Act, 2002 shall be amended as follows:

(a) In Section 2, after the clause defining "Relevant Market", the following clause shall be inserted:

> "'Artificial Intelligence system' shall have the same meaning as assigned to it under clause (a) of Section 2 of the Artificial Intelligence (Development & Regulation) Act, 2023."

(b) In Section 19, after sub-section (6), the following sub-section shall be inserted:

> "(7) While determining whether an agreement has an appreciable adverse effect on competition under sub-section (1), the Commission shall also consider the impact of the use of Artificial Intelligence systems by the parties to the agreement, in accordance with the factors specified in Section 20(4) of the Artificial Intelligence (Development & Regulation) Act, 2023."

(3) The Patents Act, 1970 shall be amended as follows:

(a) In Section 2, after clause (1)(j), the following clause shall be inserted:

> "(ja) 'Artificial Intelligence system' shall have the same meaning as assigned to it under clause (a) of Section 2 of the Artificial Intelligence (Development & Regulation) Act, 2023."

(b) In Section 3, after clause (k), the following clause shall be inserted:

"(l) a computer programme per se, including an Artificial Intelligence system, unless it is claimed in conjunction with a novel hardware."

(4) The Copyright Act, 1957 shall be amended as follows:

(a) In Section 2, after clause (ffc), the following clause shall be inserted:

"(ffd) 'Artificial Intelligence system' shall have the same meaning as assigned to it under clause (a) of Section 2 of the Artificial Intelligence (Development & Regulation) Act, 2023."

(b) In Section 13, after sub-section (3), the following sub-section shall be inserted:

"(3A) In the case of a work generated by an Artificial Intelligence system, the author shall be the person who causes the work to be created, unless otherwise provided by the Artificial Intelligence (Development & Regulation) Act, 2023 or the rules and regulations made thereunder."

(5) The Consumer Protection Act, 2019 shall be amended as follows:

(a) In Section 2, after clause (1), the following clause shall be inserted:

"(1A) 'Artificial Intelligence system' shall have the same meaning as assigned to it under clause (a) of Section 2 of the Artificial Intelligence (Development & Regulation) Act, 2023."

(b) In Section 2, after clause (47), the following clause shall be inserted:

"(47A) 'Unfair trade practice' includes the use of an Artificial Intelligence system in a manner that violates the provisions of the Artificial Intelligence (Development & Regulation) Act, 2023 or the rules and regulations made thereunder, and causes loss or injury to the consumer."