Wipro's Policy

Responsible Use and Development of AI

Purpose

Artificial Intelligence (AI) technology is rapidly advancing, and tools are becoming increasingly available. While AI can provide significant benefits to an organization in terms of productivity enhancement and revenue generation, it also poses risks to privacy, cybersecurity, intellectual property, third-party/client engagements, legal obligations, and regulatory compliance.

This policy aims to forge a responsible usage, deployment and development of AI across Wipro, harness the advantages that the technology bring whilst mitigating the risks and challenges, and provide guidelines for responsible usage, deployment and development of AI-powered tools for internal use and client engagement.

Scope

This policy covers usage, deployment and development of AI tools and technology.

This policy does not override any policy, process and guidance related to privacy, data protection, code of business conduct, intellectual property, and confidentiality. For example, any use case related to the deployment of Generative AI for internal utilization (e.g., to optimize HR processes, sales, and marketing campaigns, etc.), must undertake all the existing procedures, including security assessment, intellectual property and confidentiality due diligence, and privacy assessment when personal data is involved.

This policy is a living document as it reflects the fast-evolving nature of technology, which we embrace in a responsible, human-centric, sustainable and privacy preserving manner, in full adherence to the spirit of Wipro.

Policy Details

I. Our commitment to responsible AI

At Wipro, we believe that artificial intelligence should augment human judgment, not replace it. We are committed to developing and deploying AI that is transparent, fair, and accountable. Not because we are required to, but because it reflects who we are and the standard our clients, employees, and society rightly expect of us.

Responsible AI is not a compliance exercise. It is a business and ethical commitment. This policy gives effect to that commitment by establishing clear expectations for everyone who uses, builds, or deploys AI within or on behalf of this organization.

Important: The use of AI does not transfer responsibility. Every person who uses, builds, or deploys an AI system remains accountable for its outputs and its impacts.

II. Prohibited and Restricted Use Cases

The following categories of AI use are either prohibited outright or require mandatory authorized personnel sign-off before any decision is made or output is relied upon. This list reflects requirements under global privacy and employment law and standards as well guidelines and policies, and will be updated as regulation evolves.

II.1 Prohibited. AI must not be used for the following purposes under any circumstances:

- Generating deepfakes or synthetic media that misrepresents real individuals
- Automated scoring or profiling of individuals based on protected characteristics (race, gender, religion, disability, etc.)
- Real-time biometric surveillance of employees or individuals without explicit legal basis
- Generating or distributing disinformation or misleading content

II. 2. Restricted — mandatory authorized personnel review required. AI may be used in the following areas only with documented authorized personnel sign-off:

- Recruitment, shortlisting, and hiring decisions
- Employee performance assessment, promotion, and disciplinary matters
- Credit, insurance, or financial eligibility decisions affecting clients or individuals
- Legal advice, legal drafting, or legal conclusions delivered to clients
- Medical or clinical decision support
- Content moderation decisions that affect access to services

Important: Before developing or deploying any AI system, the risk classification questionnaire MUST be completed for the AI governance team to provide with recommendations and controls should the system be high risk.

III. Risk Categories

While Artificial Intelligence can revolutionize the way we operate, there are inherent risks associated with this technology. These risks include but are not limited to:

- **Privacy and data protection.** AI systems and tools require large datasets thus pose issues related to data minimization and legal basis for processing data. These are core privacy law tenets now recognized all across the globe, and ones we must abide to. In addition, these tools present risks around fairness in both processing and outputs; opacity around the workings of AI may clash with transparency and informational right requirements. Finally, there are challenges around accuracy particularly for generative AI tools as they may produce false information.

- **Security and confidentiality.** Through AI, attackers may generate new and complex types of malware, phishing schemes and other cyber dangers that can avoid conventional protection measures. Such assaults may have significant repercussions like data breaches, financial losses, and reputational risks. In addition to personal data leakage risks. The use and development of AI, in particular Generative AI is also susceptible to data inference attacks, data poisoning and other forms of adversarial attacks that may compromise the security and confidentiality of data.

- **Intellectual property and enterprise proprietary information.** Aspects of AI from the model, training data, prompts, to output pose IP risks namely:

    - *Infringement of IP Rights:* The training data used to train the AI models could include copyrighted material and if the output of these models is the similar (or a derivative work) or in rare scenarios, the exact same as the input training data, then this could potentially infringe on copyright laws. AI systems could inadvertently use or refer to trademarked products, brands or logos that could also be seen as infringing on those trademarks. The machine authored output could also be very realistic fake images, videos, or texts, which could be used to infringe on someone's copyright. The prompts used to interact with Generative AI systems may contain copyright-protected information, which could lead to infringement.

    - *Unclear Ownership*: The issue of IPR (Intellectual Property Rights) protection for machine authored content is an unclear, complex and evolving area of law. When integrated into Wipro or Client owned IP, it can result in downstream IP licensing and/or enforcement risks and challenges.

    - *Attribution:* AI generated content can be almost indistinguishable from human generated content and as such can lead to a risk of humans not getting due credit and attribution as the rights holder of their work.

- **Misinformation.** AI systems can produce biased or inaccurate outputs and potentially lead to poor decision-making and legal or ethical consequences. Generative AI can also create content and represent facts even if they don't exist. In addition, the outdated data on which it is trained can lead to inaccurate predictions, poor recommendations.

- **Bias, fairness, and discrimination**: AI systems can reflect and amplify biases present in their training data. Where AI is used in decisions affecting people (in hiring, lending, insurance, content moderation, or service access) biased outputs can cause direct harm and constitute unlawful discrimination under employment and equality law. This risk is particularly acute in high-risk use cases and must be actively tested for and mitigated, not assumed to be absent.

- **Consumer Protection.** Businesses that fail to disclose usage of large language models to consumers run the risk of losing customer trust and be charged with unfair practices under various laws (e.g. the California chatbot law mandates that in certain consumer interactions, organizations must disclose clearly and conspicuously that a consumer is communicating with a bot.)

- **Environmental impact**: The training and operation of large AI models carries a significant energy cost. The selection, procurement, and use of AI tools should take environmental efficiency

into account. Where tools of equivalent capability exist, preference should be given to those with demonstrably lower energy consumption or carbon footprint. This consideration must be included in vendor due diligence.

IV. Guidelines for users

Users of AI ("users") refers to personnels accessing and utilizing AI systems and tools for enhancement of their daily work or for client delivery. Users must adhere to the guidelines prescribed below.

- Personal data must not be entered into Generative AI tools. Personal data includes names, addresses, phone numbers, or any other information that could identify an individual.
- Users must not input proprietary customer, partner, or confidential company information, or make reference to customers or leadership by name.
- Users must clearly indicate content generated by a GenAI tool to avoid confusion with human-generated content and must acknowledge the source of any ideas or insights generated by the tool.
- AI tools that are not approved by Wipro for enterprise-wide use should not be used for any activity.
- Any 3rd party AI providers should complete the vendor risk assessment processes and obtain the required clearances prior to utilizing any of their AI-powered services/tools/platforms/solutions.
- AI tools may only be used for client projects if approved by the client or permitted under the applicable client contract. Similarly, client enterprise data including personal details should not be used in Generative AI without client approval.
- Where client contracts are silent on AI use, the default position is that AI must not be used on client matters without first obtaining explicit approval. Account leads are responsible for having this conversation with clients before AI tools are deployed on any client engagement.
- Any AI use case for a client engagement, which may include the use of AI systems or tools must complete the AI risk assessment prior implementation or deployment. Users must complete the AI Risk Classification Self-Assessment Questionnaire and submit to Responsible AI Taskforce for review.
- Any Generative AI use case involving personal data and/or has an impact to the data privacy rights of individuals must undergo a Data Protection Impact Assessment.
- APIs should not be used to transmit sensitive and/or confidential data to Generative AI systems.

V. Guidelines for Deployers and Developers

Deployers and Developers of AI refers to personnel engaged in the deployment or development of AI, including developing GenAI applications using third-party APIs; transfer learning from existing open-source models to in-house models; and building AI-enabled products or services.

Developers of AI must adhere to the following guidelines and to the guidelines prescribed to users.

V.1. General Guidelines

a. Developers must adhere to privacy and data protection laws and must ensure alignment to globally accepted frameworks such as OECD and NIST (National Institute of Standards and Technology) frameworks.

b. Developers must adhere to the defined rules around key requirements, such transparency, fairness (refer to Addendum 2. Privacy by Design Checklist for AI/ML completeness). A Data Protection Impact Assessment in collaboration with the Global Data Privacy team must be completed during the design phase or initial/ideation stages of the development of Generative AI.

c. Privacy by design approach must be adopted from conception stage to deal with issues such as data collection, legal basis, human oversight, informational rights, automated decision making.

d. Before deployment, all AI systems that make or influence decisions about people must undergo documented bias testing. This testing must examine outputs across relevant demographic groups and be reviewed by the Responsible AI Taskforce. Results must be retained and made available on request. Systems that demonstrate material bias must not be deployed until the bias has been remediated.

e. Developers must comply with defined mechanisms for regular checks and must complete an audit of the system before deployment, and at regular intervals.

f. To mitigate security and confidentiality risk, deployers and developers must:
   - only use public data to train the AI system and maintain the anonymity of data
   - adopt the use of secure coding, protect access to AI System only to authorized users,
   - align data protection standards on training data and sensitive user input to encrypt and store securely,
   - perform regular security assessment to identify and address vulnerabilities in Generative AI system

g. Deployment and development AI tools for client delivery should be done only if approved by the client or if it is allowed as per client contract. Similarly, client enterprise data including personal details should not be used in Generative AI without client approval.

h. Account teams should reach out to Responsible AI Taskforce for advisory on deployment or development of Generative AI tools in all new and existing client engagement.

i. Developers must comply with Intellectual Property policies and standards and ensure that there is no copyright infringement.

j. Should the system fall under the coverage of the EU AI Act (directly or indirectly marketed in Europe), developers must refer and adhere to the dedicated sections in the Act.

k. Generative AI-generated source code must undergo thorough testing and validation before integration into internal applications.

V.2. Intellectual Property — Interim Position on AI-Generated Outputs

The legal framework governing ownership of AI-generated content remains unsettled across most jurisdictions. Until greater clarity exists, the following interim position applies:

a. AI-generated content cannot be assumed to constitute original proprietary intellectual property of the organization.
b. Client deliverables that incorporate AI-generated content in a material way must be reviewed by Legal before delivery to confirm IP position.
c. AI-generated source code must be clearly documented as such and reviewed for licensing conflicts before inclusion in any product or client deliverable.
d. Employees must not assert copyright ownership over AI-generated content without prior legal advice.

V.3. Generative AI-Generated Source Code - Client Deliverables

a. Clear differentiation must be made between AI-generated code and human-generated code in customer-facing applications.
b. Customers must be informed about the utilisation of AI-generated code and any associated limitations.

V.4. **Generative AI-Generated Source Code for Internal Applications:**

a. Developers responsible for incorporating Generative AI-generated code must maintain a comprehensive documentation trail to aid in debugging and troubleshooting.
b. Regular code reviews must be conducted to ensure adherence to coding standards, as well as to maintain code quality and security.

V.5 **Generative AI generated code for shipment to clients/customers:**

a. Clear differentiation must be made between Generative AI-generated code and human-generated code in customer-facing applications or products.
b. Customers must be informed about the utilization of Generative AI-generated code and any limitations associated with it.

V.6. **Third-Party AI Services**

a. Thorough due diligence must be conducted before employing third-party AI services, assessing their credibility, security measures, and compliance with applicable regulations.
b. Contracts or agreements with third-party AI service providers must include clauses addressing data privacy, intellectual property rights, and liability.
c. Regular audits or assessments should be performed to ensure that third-party AI services meet the enterprise's established standards.

V.7. Generative AI-Generated Code by Open-Source GPT Models:

a. Usage of open-source GPT models must comply with the relevant licensing terms and conditions.
b. Before using open-source GPT models in production environments, a comprehensive evaluation must be conducted to identify and address security vulnerabilities, bias, and ethical concerns.
c. Proper attribution and acknowledgment must be provided for the open-source GPT models employed.

VI. Raising Concerns

Responsible AI governance depends on people feeling safe to raise concerns. If you have a concern about how AI is being used, developed, or deployed — including ethical concerns, potentially discriminatory outputs, client misuse, or pressure to use AI in ways that conflict with this policy — you are expected and encouraged to raise it.

Concerns may be raised with:

- Your line manager or team lead
- The Responsible AI Taskforce
- The Chief Privacy and AI Governance Officer
- For concerns you wish to raise confidentially, the concern may be raised through Ombud's email or through Wipro's intranet.

Important: The organization will not tolerate retaliation against any person who raises an AI-related concern in good faith. Reports made honestly, even if they turn out to be mistaken, will be treated seriously and without adverse consequence.

VII. Other Responsibilities

- AI tools should not be used to create adverse effect to Wipro, customer, entities data and infrastructure.
- Issues or concerns, such as unauthorised access or data breaches should be reported in accordance with Wipro security incident reporting process.
- Users of AI systems must always adopt a critical mindset and be able to validate the outcomes as such tools may compute inaccurate or false information.
- In case of any doubt reach out to the Responsible AI Taskforce for assistance.

Function Responsibilities

Responsible AI Task Force	• A cross functional body whose members retain their primary roles in the home functions and bring those professional lenses to bear on specific AI questions. • Engages with concrete issues: whether a use case is appropriate, what risks particular deployment carries, what mitigations are needed. Its value is the quality of the analysis fed into the governance process where it carries weight.
AI Governance	• A standing function whose members work on AI governance in enterprise and in customer engagements. It owns the organization´s AI policy framework, sets the standards others are held to and reports on AI risks to senior leadership and the board. For high risk deployment it holds and /or participates inf formal sign off. It is the body that faces external scrutiny – from regulators and auditors – and must be able to account for how AI risk is managed across the organization. It tracks the regulatory environments and translates emergency requirements into internal obligations before they become compliance failures.
CTO	• Inform on technological advances and solution which may impact this policy
CIO	• Deploy tools and solutions and controls to actively detect and monitor any risk to Wipro or client data and IP as a result of usage of AI. • Report breaches to the Responsible AI task force along with root cause analysis and mitigation actions taken • Deploy cybersecurity solutions as defined by CISO
CISO	• Define cybersecurity controls to protect Wipro infrastructure from probable attack vectors and threats powered by generative AI. • Define security controls to protect AI models and associated data against misuse and unauthorized use. • Provide audit and governance over controls by CIO on AI • Cyber security assessments during vendor onboarding to account for AI risks • Provide training and awareness on cybersecurity risks around AI
Legal and Intellectual Property	• Define controls and processes to identify and mitigate risks to intellectual property as a result of usage, deployment and development of AI. • Advise on client, vendor, and contractor contracts. Define the contractual clauses applicable to agreements involving AI or GenAI services, tools, or solutions. • Maintain and update client AI disclosure template. • Provide advisory if any clauses on IPR and liabilities arising from usage or development of Gen AI should be addressed in client, vendor, contractor and partner contracts.
HR	• Ensure AI is not used in employment decisions without human sign-off. Oversee AI literacy training. Manage speak-up concerns related to people matters.

Quality Assurance	• Define the AI lifecycle in Quality Management System • Perform quality assurance checks on client engagements with AI or GenAI component.
ERM	• Define audit plan for AI usage. Include bias testing outcomes and environmental impact in audit scope.
Data Privacy	• Define a framework for assessing AI use cases that involves the use of personal information. • DP assessments during vendor onboarding to account for AI risks • Provide training and awareness on privacy risks around AI
Functions and Delivery Teams	• Perform compliance checks and audits where AI is used. Include bias review and environmental consideration in vendor assessment

Definitions:

The following definitions are for all employees. A technical glossary for developers appears at the end of this document.

- **Generative AI (GenAI)**: AI systems capable of generating new content (text, images, code, audio) based on patterns in training data. Examples include ChatGPT, Gemini, Claude, and GitHub Copilot.
- **Approved tool**: an AI tool that has been assessed and listed on the organization's approved tools register. Only approved tools may be used for work purposes.
- **Personal data**: any information that can identify a living individual, including names, email addresses, employee records, client contact details, or any combination of information that could be used to identify someone. The definition varies by jurisdiction.
- **High-risk AI use**: any use of AI that makes or materially influences a consequential decision about a person such as hiring, performance assessment, lending, insurance, or legal matters. These uses require mandatory human review under this policy.
- **Responsible AI Taskforce**: the internal team responsible for governing AI policy, reviewing use cases, and providing guidance. The first point of contact for any AI related question or concern.
- **Natural Language Processing (NLP)** - is an arch of computer science techniques that enables computer to understand text and provide inference in the same way that human would.
- **Large Language Model (LLM)** – LLMs represent a core component of NLP, a tool to enable AI to mimic human performance in understanding language. LLMs are large models (millions of parameters) that are trained on massive amount of data.
- **Generative Pretrained Transformer (GPT)** – GPT refers to a subset of LLM models that uses an underlying Neural Network architecture called Transformers and is trained on a large body of data to perform wide variety of tasks such as text summarization, question answering, etc. GPT is the underlying model for ChatGPT.

Cross Reference of Policies

- **Wipro's Data Protection and Privacy Policy (Personally Identifiable Information)**

- **Wipro's Policy on Intellectual Property Rights**
- **Acceptable Data Collection and Usage Policy**
- **Wipro's Policy - Ombuds Policy**
- **Wipro's Information Security Risk Management Policy**
- **AI Security Policy**

Approvals/Escalation Matrix

Any deviation or non-compliance to this policy must be immediately reported to *Responsible AI Taskforce*.

Furthermore, should an employee be made aware of any suspicious activity involving the use of Generative AI, such as but not limited to unauthorised access, misuse, and unauthorized disclosure of data, he/she must report it immediately report it as a security incident in Wipro's intranet page.

Document History

Version	Revision Date	Reason for Change	Drafted/ Reviewed By	Approved By	Date Approved
1	N/A	Policy creation	Policy drafted by: GenAI Taskforce Committee members	General Counsel and Chief Risk Officer	12 June 2023
2	27 Sept 2024	Changes in the approval/escalation matrix and contact information for queries and review requests.	Responsible AI Taskforce	Chief Privacy and AI Governance Officer	30 September 2024
3	01 Apr 2026	Amendments made on the policy details and updated function responsibilities	Responsible AI Taskforce	Chief Privacy and AI Governance Officer	07 Apr 2026