



SECURE USAGE OF GENERATIVE AI TECHNOLOGY

Effective from: **September 18, 2026**

Revision No : **2.0**

*Placed before the Board of Directors at its meeting held on February 13, 2025, and reviewed/approved thereat.

Table of Contents

1. Purpose.....	3
2. Ownership and Administration	3
3. Applicability/Scope.....	3
4. Responsible AI Principles	3
5. Responsibilities	5
6. Prohibited Use Cases.....	6
7. Enforcement Of The Policy	7
8. Abbreviations	7

1. PURPOSE

To establish guidelines for the use of Generative Artificial Intelligence tools, such as ChatGPT, Gemini, Claude, etc. to ensure the confidentiality, integrity, and availability of data and systems, and to minimize the risks associated with their use. This includes addressing the potential security threats posed by these tools, such as leaking sensitive data, introducing code vulnerabilities, and providing incorrect information when designing virtual or physical architectures. It is essential to use Gen AI tools with caution, as they can be a source of both benefits and risks. This policy aims to mitigate these risks by implementing measures to protect user conversations, prevent data breaches, cyberattacks, and other malicious activities.

The organization is also committed to the responsible, ethical, and secure use of Artificial Intelligence. While ensuring compliance with applicable laws and regulations throughout the AI lifecycle, including design, development, deployment, and use.

2. OWNERSHIP AND ADMINISTRATION

Hindalco maintains appropriate governance and oversight mechanisms for the responsible use of AI. This policy is administered through designated organizational functions responsible for AI governance, information security, risk management, compliance, and technology oversight.

The policy is reviewed periodically and updated, as necessary, to address evolving regulatory requirements, industry practices, and technological developments

The organization shall ensure that Generative AI systems cannot make irreversible or high-stakes decisions without human oversight and mechanisms for human review shall be available such as human-in-command, human-on-the-loop, or human-in-the-loop.

3. APPLICABILITY/SCOPE

This policy applies to all Associates i.e., on-roll employees of Hindalco, consultants, third party employees and trainees whose actions have the potential to expose Hindalco's systems or data to AI tools.

This policy applies to both internally developed AI systems and third-party AI tools, platforms, or services used or deployed on behalf of Hindalco.

4. RESPONSIBLE AI PRINCIPLES

4.1 Fairness and Non-Discrimination

AI systems shall be designed to minimize bias and unfair outcomes. Users should validate AI-generated outputs and prevent discriminatory or prejudicial decisions.

4.2 Transparency and Explainability

AI-supported decisions and outputs should be explainable and understandable to relevant stakeholders to the extent reasonably possible.

4.3 Accountability and Human Oversight

Human accountability shall be maintained for all AI-supported decisions. Appropriate human oversight shall be applied where AI may impact legal, financial, operational, safety, or reputational outcomes.

4.4 Privacy and Data Protection

AI shall be used in compliance with applicable privacy, confidentiality, and data protection requirements. Sensitive, confidential, personal, or proprietary information shall only be processed using approved AI solutions and in accordance with data classification and handling requirements.

4.5 Security and Resilience

AI solutions and related data shall be protected against unauthorized access, manipulation, misuse, and cyber threats. Appropriate security controls shall be implemented throughout the AI lifecycle to maintain confidentiality, integrity, and availability.

4.6 Reliability and Accuracy

AI-generated outputs should be assessed for accuracy, completeness, relevance, and suitability before being relied upon for business purposes.
Where appropriate, significant decisions shall be supported by human judgement and validation.

4.7 Compliance and Ethical Use

AI use shall comply with applicable laws, regulations, contracts, and company policies, and shall not support unlawful or unethical activities.

4.8 Monitoring and Continuous Improvement

AI systems and use cases shall be periodically reviewed for effectiveness, compliance, and emerging risks, with corrective actions taken as needed.

4.9 Safety and Risk Management

AI systems shall be implemented using a risk-based approach, with appropriate controls to identify, assess, mitigate, and monitor potential risks arising from AI usage, including operational, security, legal, regulatory, and reputational risks.

5. RESPONSIBILITIES

5.1 User responsibility while using publicly available Gen AI services (e.g. ChatGPT, Gemini, Claude)

- It is strongly advised that corporate or official email addresses should not be used for creating accounts or subscribing to publicly enabled Gen AI services. Instead, personal, or non-work-related email addresses should be used to avoid potential conflicts of interest, data privacy concerns, or unauthorized access to sensitive information.
- Associates are prohibited from uploading or posting any personal, confidential or sensitive organizational data such as –
 - Financial details (account numbers, revenue data, business performance, product pricing etc.)
 - Customer information (names, addresses, contact details, etc.)
 - Intellectual property (proprietary algorithms, strategies, internal reports, etc.)
 - PII data (login credentials, DOB, address, PAN, Aadhaar number, mobile number, etc.)
 - SPII data (biometrics data, health or genetics data, etc.)
 - API Keys, Application Source Code, or any other information that could allow an unauthorized actor to gain access to Hindalco systems or data.
- Associates are obligated to carefully validate AI-generated outputs and remain fully accountable for all actions, decisions, communications, and business outcomes arising from the use of AI systems. Responsibility cannot be transferred to or attributed solely to the AI system, including any legal repercussion.
- Exercise caution when sharing or forwarding AI-generated content with individuals outside the organization or unauthorized personnel to ensure its accuracy, appropriateness, confidentiality, and compliance with applicable legal and business requirements.
- Ensure secure disposal of any information generated by the Generative AI tool, such as deleting chat logs or other outputs, in a responsible manner.
- Provide the minimum necessary information during the Gen AI interaction session. If you must provide data to a Generative AI tool for analysis or assistance, ensure it is fully anonymized and cannot be traced back to any individual or organizational detail.
- Access to AI platforms outside approved enterprise solutions may be considered on a case-by-case basis, subject to a valid business justification and prior approval from the Architecture Review Board.

- Where AI-generated content is used for official communications, reports, presentations, customer communication, regulatory submissions, or other business purposes, appropriate disclosure shall be made wherever required.
- Associates shall ensure that AI-generated outputs do not infringe copyright, intellectual property rights, trade secrets, or proprietary information belonging to third parties before use, publication, or distribution.
- Associates shall promptly report suspected AI security incidents, abnormal AI behavior, unauthorized AI usage, or AI-generated outputs that may adversely impact the organization through the Hindalco Service Desk tool.

5.2 User responsibility while using Hindalco approved Gen AI service.

- Associates should protect their login credentials and ensure that their Gen AI accounts are not accessible to unauthorized individuals.
- Associate should validate the output of the AI and are accountable for any actions taken based on its recommendations or decisions.
- Associates should be aware when content, analysis, or recommendations are generated or assisted by AI tools and shall ensure appropriate transparency when sharing or relying on AI-generated outputs.
- Associates should ensure that AI-generated content is shared or forwarded only with authorized individuals and in accordance with organizational requirements.

5.3 Technology team responsibility while using LLM APIs and Code generation tools

- Associate working on the Gen AI use case are required to provide justification and take approval from Architecture Review Board before using any LLM API.
- Associate utilizing code generation tools for application development are required to provide business justification and obtain approval from the Architecture Review Board before selecting code generation tools instead of enterprise-provisioned alternatives within Hindalco's hosted environment.
- Associates involved in the design, development, or integration of AI use cases are accountable for assessing and validating AI models, training data, and outputs to identify and mitigate potential bias, discrimination, or unfair outcomes.
- Associates are obligated to carefully validate the output of the AI system and will be held responsible for any actions or decisions made based on its advice, including any legal repercussion.

6. PROHIBITED USE CASES

This section outlines use cases that Associates are prohibited from:

- Creating deepfake content involves imitating someone without their explicit consent using Gen AI techniques, such as audio, video, and picture manipulation.

- Using Gen AI to create any content that is illegal, discriminatory, defamatory, or otherwise offensive or inappropriate to our employees, partners, and customers.
- Using Gen AI to create programs/codes/repos which can cause malicious or undesirable behavior in IT systems.
- Using Gen AI to harass, bully, intimidate, or discriminate against other employees or external parties.
- Using of prompt injection techniques, jailbreaking methods, model exploitation techniques, or any activity intended to bypass AI safety controls, security restrictions, content filters, or operational safeguards.
- Violating any applicable laws or regulations, including data protection and privacy laws using Gen AI is forbidden.
- The development or deployment of AI systems that engage in manipulative or deceptive behavior, exploit vulnerabilities of individuals or groups, perform social scoring, or enable unauthorized biometric identification or surveillance or facial recognition or behavioral profiling is strictly prohibited.

7. ENFORCEMENT OF THE POLICY

- Hindalco will enforce the statements in this policy document over information systems that they directly own and are responsible for and will provision/distribute this policy as a guidance across Hindalco.
- Hindalco will mandate critical security controls described in this policy and ensure enforcement.
- Violations against this policy document, or the policy document derived from this document for specific use by Hindalco, may result in disciplinary actions depending on the nature of the violation and as decided by Hindalco, including but not limited to termination of employment.
- This policy shall be governed by information security policy and guided by our information security management system to ensure protection of cybersecurity of our systems in the use and/or development of AI.

8. ABBREVIATIONS

- Gen AI - Generative Artificial Intelligence.
- PII - Personally Identifiable Information.
- SPII - Sensitive Personally Identifiable Information.
- LLM - Large Language Model
- OEM - Original Equipment Manufacturer
- API – Application Programming Interface
- Subscriptions - Refer to O'Reilly, ScienceDirect, vendor documentation, or any other paid subscription that uses business email IDs as subscription members.

- PAN – Permanent Account Number
- DOB – Date of Birth