



Himadri Speciality Chemical Ltd

CIN: L27106WB1987PLC042756

RESPONSIBLE ARTIFICIAL INTELLIGENCE POLICY

Version	Revision/Review Date	Approved By	Date Approved
Adopted on	-	Board	16.09.2026

Introduction

At Himadri, we are committed to conducting our business with integrity, transparency, accountability, and responsibility. As technology and artificial intelligence (AI) continue to evolve, we recognize the opportunities AI can provide to enhance operational efficiency, innovation, decision-making, customer experience, risk management, and business resilience.

At the same time, we recognize that the use and development of AI systems may give rise to risks relating to data privacy, cybersecurity, bias and discrimination, transparency, accountability, human rights, safety, environmental impacts, and unintended societal consequences.

This Responsible Artificial Intelligence Policy establishes the principles and requirements that govern the responsible use, development, procurement, deployment, and monitoring of AI systems across Himadri. The Policy applies to AI systems developed internally as well as AI systems, models, platforms, applications, and services provided by third parties.

Himadri is committed to using AI in a manner that respects human rights, protects individuals and information, supports fair and responsible decision-making, safeguards the environment, and complies with applicable laws and regulations. This Policy is guided by internationally recognized principles for responsible AI, including the OECD AI Principles, the UNESCO Recommendation on the Ethics of Artificial Intelligence, and applicable requirements and principles under emerging AI regulations.

Purpose and Scope

The purpose of this Policy is to establish a responsible and risk-based framework for the use and development of AI across Himadri.

This Policy applies to:

- All employees, workers, and other personnel involved in the use, procurement, development, implementation, or oversight of AI systems.
- AI systems and models developed, owned, licensed, procured, or deployed by Himadri.
- Third-party AI systems, platforms, applications, models, and services used in connection with Himadri's operations.
- AI systems used for operational, commercial, analytical, administrative, customer-facing, human resources, supply chain, cybersecurity, research and development, or other business purposes.

AI systems shall only be used for legitimate and authorized business purposes and within their defined scope, capabilities, and limitations.

Responsible Artificial Intelligence Principles

Himadri's approach to AI is founded on the following principles:

1. Respect for data privacy and confidentiality
2. Cybersecurity and resilience
3. Fairness and avoidance of bias
4. Human oversight and intervention
5. Transparency and explainability
6. Clear accountability
7. Defined boundaries and responsible use
8. Environmental responsibility
9. Prevention of prohibited and harmful AI applications

These principles shall apply throughout the AI lifecycle, including the identification, design, development, procurement, testing, deployment, use, monitoring, modification, and retirement of AI systems.

Data Privacy and Responsible Data Use

Himadri recognizes that responsible AI requires the responsible collection, processing, storage, use, and sharing of data.

Himadri shall:

- Respect applicable data protection and privacy laws and regulations in the jurisdictions in which it operates.
- Ensure that personal data is processed lawfully, fairly, transparently, and for legitimate and defined purposes.
- Apply appropriate safeguards to personal, confidential, commercially sensitive, and proprietary information used in connection with AI systems.
- Limit the collection and use of personal data to what is necessary and appropriate for the intended purpose.
- Consider privacy risks during the design, development, procurement, deployment, and use of AI systems.
- Take appropriate measures to prevent unauthorized access, disclosure, alteration, loss, or misuse of data used by AI systems.
- Require appropriate privacy and data protection safeguards from relevant third-party AI providers where AI systems involve Himadri data or personal information.

Personal, confidential, or sensitive information shall not be entered into or processed through an AI system unless such use is authorized and appropriate safeguards are in place.

Cybersecurity of Artificial Intelligence Systems

Himadri is committed to protecting AI systems, associated infrastructure, models, applications, data, and interfaces against cybersecurity threats and unauthorized use.

AI systems shall be subject to appropriate cybersecurity measures proportionate to their risk and intended use. Such measures may include:

- Access controls and authentication mechanisms.
- Encryption and protection of data in transit and at rest, where appropriate.
- Secure configuration and secure development practices.
- Vulnerability assessment and security testing.
- Monitoring for unauthorized access, misuse, manipulation, or abnormal system behavior.
- Appropriate incident detection, response, containment, recovery, and reporting mechanisms.
- Protection against malicious inputs, unauthorized prompts, data leakage, model manipulation, and other AI-specific threats, where relevant.
- Periodic review of cybersecurity controls throughout the AI system lifecycle.

AI systems shall not be deployed or used where identified cybersecurity risks cannot be appropriately managed within Himadri's risk tolerance.

Fairness, Non-Discrimination and Avoidance of Bias

Himadri is committed to ensuring that AI systems are designed, selected, and used in a manner that promotes fairness and avoids unjustified discrimination.

Himadri shall take reasonable measures to:

- Identify potential sources of bias in AI systems, models, datasets, algorithms, and outputs.
- Use appropriate and representative data where practicable and relevant to the intended application.
- Assess AI-generated outputs for potentially discriminatory, unfair, or materially misleading outcomes.
- Apply appropriate testing, validation, monitoring, or review mechanisms based on the risk and intended use of the AI system.
- Take corrective measures where material or unjustified bias is identified.
- Avoid using AI systems in ways that result in unlawful discrimination or unfair treatment of individuals or groups.

Particular care shall be exercised where AI systems may influence decisions affecting employees, workers, customers, suppliers, or other stakeholders.

Human Oversight and Human Intervention

Himadri recognizes that AI systems should support human decision-making and shall not replace appropriate human accountability for critical or high-risk decisions.

Himadri shall ensure that:

- Appropriate human oversight is maintained over AI systems based on their risk, purpose, and potential impact.
- Critical or high-risk decisions influenced by AI are subject to meaningful human review.
- Authorized personnel have the ability to question, review, reject, modify, override, suspend, or discontinue AI-generated recommendations or outputs where appropriate.
- AI systems are not permitted to make irreversible or high-impact decisions without appropriate human oversight and intervention mechanisms.
- Employees responsible for reviewing AI-generated outputs have sufficient authority, competence, and information to exercise meaningful judgment.
- AI-generated recommendations shall not be treated as automatically correct or authoritative.

Where necessary, AI systems shall be designed or configured to escalate decisions or situations to an appropriately authorized human decision-maker.

Transparency and Explainability

Himadri is committed to appropriate transparency regarding the use and limitations of AI systems.

Himadri shall seek to ensure that:

- Users are informed, where appropriate, when they are interacting with an AI system rather than a human.
- The intended purpose, capabilities, limitations, and material risks of AI systems are appropriately communicated to relevant users.
- AI-generated information or recommendations are not represented as human-generated where such representation could materially mislead stakeholders.
- Appropriate records and documentation are maintained regarding significant AI systems, their intended use, and relevant controls.
- AI-generated results and decisions are capable of being explained to relevant stakeholders to a degree appropriate to the system's purpose, risk, and impact.

- Users understand that AI outputs may contain errors, limitations, uncertainty, or inaccuracies and should apply appropriate professional judgment.

For material decisions, relevant personnel shall be provided with sufficient information to understand the basis and limitations of AI-generated recommendations or outputs.

Accountability and Responsibility

Himadri recognizes that accountability for the outcomes of AI systems remains with people and the organization and shall not be transferred to the AI system itself.

Himadri shall establish appropriate ownership and accountability for AI systems throughout their lifecycle.

This includes:

- Assigning appropriate business ownership for AI systems.
- Defining responsibility for AI risk assessment, approval, implementation, monitoring, and compliance.
- Establishing appropriate escalation mechanisms for AI-related risks, incidents, errors, or adverse outcomes.
- Investigating significant errors, unintended consequences, or harm associated with AI systems.
- Taking appropriate corrective and preventive actions where material issues are identified.
- Maintaining appropriate documentation and records to support accountability and oversight.
- Ensuring that third-party AI providers have clearly defined responsibilities where their systems or services are used by Himadri.

AI-generated outcomes shall remain subject to applicable legal, regulatory, contractual, and organizational accountability requirements.

Defined Boundaries and Responsible Use

Himadri shall define and maintain clear boundaries for the authorized use of AI systems.

AI systems shall be used only:

- For defined and legitimate purposes.
- Within their approved scope and intended capabilities.
- By appropriately authorized personnel.
- In accordance with applicable laws, regulations, policies, contractual obligations, and information-security requirements.

- Subject to appropriate controls based on the potential risks and impacts associated with their use.
- AI systems shall not be used for purposes outside their approved scope without appropriate review and authorization.
- Where an AI system presents material risks that cannot be adequately controlled, Himadri may restrict, suspend, modify, or discontinue its use.

Employees and other authorized users shall not circumvent established AI controls, safeguards, access restrictions, or approval requirements.

Environmental Responsibility of Artificial Intelligence

Himadri recognizes that AI systems can require significant computational resources and may contribute to energy consumption, greenhouse gas emissions, water consumption, and other environmental impacts.

Himadri is committed to promoting AI solutions with an appropriate and proportionate ecological footprint.

Where practicable and relevant to the application, Himadri shall:

- Consider energy consumption, carbon intensity, water use, and other environmental impacts when selecting or deploying AI infrastructure and services.
- Encourage the use of energy-efficient computing infrastructure and AI models.
- Consider computational efficiency and resource optimization during AI development and deployment.
- Avoid unnecessary computational workloads, redundant model training, and inefficient use of AI resources.
- Encourage the use of renewable or lower-carbon energy sources for relevant AI infrastructure where reasonably available.
- Consider the environmental performance of third-party AI providers and data centers when procuring material AI services.
- Promote efficient model selection and deployment based on the intended business requirement rather than unnecessary computational complexity.

Where feasible, environmental considerations shall form part of the evaluation and selection of significant AI systems and third-party AI service providers.

Prohibited and Unacceptable Uses of Artificial Intelligence

Himadri shall not knowingly develop, procure, deploy, or use AI systems for purposes that are prohibited by applicable law or that materially conflict with the principles of responsible AI established under this Policy.

In particular, Himadri shall not knowingly use or deploy AI systems that:

- Employ subliminal, purposefully manipulative, or deceptive techniques intended to materially distort an individual's behavior in a manner that causes or is likely to cause significant harm.
- Exploit vulnerabilities of individuals or groups arising from factors such as age, disability, or specific socioeconomic circumstances in order to materially distort their behavior in a manner that causes or is likely to cause significant harm.
- Conduct social scoring of individuals based on social behavior or personal characteristics where such scoring results in unjustified or disproportionate detrimental treatment.
- Conduct unauthorized biometric surveillance or unauthorized remote biometric identification.
- Use biometric or other sensitive personal information in ways that are unlawful, unauthorized, discriminatory, or inconsistent with applicable privacy requirements.
- Are otherwise prohibited under applicable AI laws and regulations.

AI systems shall not be used to circumvent legal, ethical, privacy, cybersecurity, human rights, or other safeguards established by Himadri.

Third-Party Artificial Intelligence Systems

Himadri recognizes that significant AI-related risks may arise from third-party systems, models, platforms, cloud services, and AI providers.

Before adopting material or higher-risk third-party AI systems, Himadri shall, as appropriate to the risk:

- Assess the intended use and potential risks of the AI system.
- Consider data privacy and information-security requirements.
- Consider the provider's approach to responsible AI, cybersecurity, data protection, transparency, and accountability.
- Establish appropriate contractual or other safeguards for the protection of Himadri's data and information.
- Consider the environmental performance of relevant AI infrastructure and data centers.
- Define appropriate restrictions, access controls, and permitted uses.
- Monitor material risks associated with continued use of the third-party AI system.

Third-party AI systems shall remain subject to Himadri's applicable policies, controls, and approval requirements.

AI Risk Assessment, Monitoring and Incident Management

Himadri shall adopt a risk-based approach to the governance of AI systems.

Depending on the nature and potential impact of an AI system, appropriate measures may include:

- Pre-deployment risk assessment.
- Data and model validation.
- Bias and fairness assessment.
- Privacy assessment.
- Cybersecurity assessment.
- Human oversight assessment.
- Testing and validation of AI outputs.
- Periodic monitoring and review.
- Documentation of significant AI systems and associated risks.
- Incident reporting and escalation.
- Corrective and preventive action.

Material AI-related incidents, including significant data breaches, cybersecurity events, harmful outputs, material bias, unauthorized use, or other significant adverse impacts, shall be appropriately reported, investigated, and remediated.

Awareness, Training and Responsible Use

Himadri recognizes that responsible AI depends on informed and accountable users.

Relevant employees and personnel shall receive appropriate awareness, guidance, or training regarding:

- Responsible and authorized use of AI.
- Data privacy and confidentiality.
- Cybersecurity risks associated with AI.
- Potential bias and discrimination.
- Human oversight and professional judgment.
- AI limitations, inaccuracies, and hallucinations.
- Appropriate use of AI-generated information and outputs.
- Applicable organizational requirements and legal obligations.

Personnel shall remain responsible for exercising appropriate judgment when using or relying upon AI-generated information.

Governance, Oversight and Reporting

Implementation of this Responsible Artificial Intelligence Policy shall be overseen through Himadri's established governance structure, with appropriate responsibilities assigned to relevant functions and management.

The Sustainability (ESG) Council, under the supervision of the Sustainability (ESG) Committee at the Board level, shall provide oversight of the Company's responsible AI approach in coordination with relevant functions.

Relevant functions, including Information Technology, Information Security, Legal, Human Resources, Sustainability/ESG, Risk Management, and business functions, shall support implementation of this Policy according to their respective responsibilities.

Himadri shall periodically review the effectiveness and relevance of this Policy, taking into account:

- Changes in AI technologies and associated risks.
- Changes in applicable laws and regulations.
- Emerging international standards and responsible AI principles.
- Material AI-related incidents or lessons learned.
- Stakeholder expectations.
- Developments in environmental and cybersecurity risks associated with AI.

Significant matters relating to responsible AI may be reported through the Company's established governance and reporting mechanisms.

Compliance and Continuous Improvement

All personnel and relevant third parties shall comply with this Policy and applicable procedures established under it.

Himadri shall promote continuous improvement in its responsible AI practices by periodically reviewing AI-related risks, controls, governance arrangements, and emerging good practices.

Where non-compliance or material weaknesses are identified, appropriate corrective and preventive actions shall be taken within defined timelines.

Himadri may restrict, suspend, modify, or discontinue an AI system where its use presents unacceptable legal, ethical, privacy, cybersecurity, human rights, environmental, or other material risks.

Policy Approval and Review

This Policy shall be approved by the Board of Directors of Himadri and shall be reviewed every three years to ensure continued relevance and alignment with applicable laws, regulations, standards, and responsible AI principles.

The Policy shall be communicated to relevant employees and stakeholders and shall be made publicly available as appropriate.

Dated: 16.09.2026

Sd/-
Anurag Choudhary
Chairman-cum-Managing
Director & CEO