Responsible AI Policy

Document Version No.: 1.0

Release Date: 5th June 26

REVISION HISTORY

Date	Version No.	Prepared By	Reviewed By	Approved By	Summary of Changes
5th June 26	1.0	Aniket Kulkarni Manager QMG	Rajashree Laad VP QMG Balaji Seshan AVP IG Sandhya Duvvuri AVP QMG	Uma Thomas EVP & CRO	Introduced the policy

Contents

1.0 Policy

Hexaware Technologies Limited ("Hexaware") is committed to the ethical, lawful, secure and sustainable use of Artificial Intelligence (AI). This Responsible Artificial Intelligence Policy ("Policy") defines the principles, governance expectations and mandatory requirements to ensure that AI systems used or developed by Hexaware are aligned with human rights, data protection, cybersecurity, transparency, accountability and environmental responsibility.

This Policy supports Hexaware's commitments under its Code of Conduct, Information Security Policy, Privacy Policy, Human Rights Policy, ESG framework and applicable global regulations, including emerging AI-specific regulations such as the EU Artificial Intelligence Act

2.0 Scope

This Policy applies to:

- AI, machine learning, generative AI and automated decision-making systems developed internally by Hexaware
- AI systems procured from or operated by third parties on behalf of Hexaware
- Use of AI tools by employees, contractors or business units for internal operations, client delivery or decision support

3.0 Core principles of responsible AI

Hexaware's approach to Responsible AI is guided by the following principles:

- **Lawfulness & Ethics** – AI use must comply with applicable laws, regulations and ethical standards
- **Human-centricity** – AI must augment human decision-making and not replace human accountability
- **Fairness & non-discrimination** – AI systems must be designed and used to avoid potential bias and unfair outcomes
- **Transparency & Explainability** – AI outcomes must be understandable, traceable and auditable
- **Security & Privacy** – AI systems must protect data and systems against unauthorized access and misuse
- **Accountability** – Clear ownership and accountability must exist for AI outcomes
- **Sustainability** – AI development and usage should minimize environmental impact
- **Responsible by Design** – Responsible AI principles such as fairness, privacy, security and transparency shall be embedded into the design and development of AI systems from the outset, rather than being applied retrospectively.

4.0 Policy requirements

4.1 Respecting Data Privacy in AI

- Personal data used in AI systems shall be processed in accordance with applicable data protection laws (e.g., GDPR, DPDPA) and Hexaware's Privacy and Data Protection policies.
- Data minimization, purpose limitation and lawful basis shall be ensured for AI training, testing and operation.
- Sensitive and special-category data shall not be used unless legally permitted, strictly necessary and formally approved.
- Consent is mandatory prior to using any PII/SPII/PHI data in AI system

4.2 Protecting Cybersecurity of AI Systems

- AI systems shall comply with Hexaware's Information Security Management System (aligned to ISO/IEC 27001).
- Security risks such as data poisoning, model theft, adversarial attacks and unauthorized access shall be assessed and mitigated.
- Third-party AI vendors shall be subject to cybersecurity and risk assessments prior to onboarding.
- Annual security assessment is mandatory for third parties who are using the Hexaware data

4.3 Avoiding Bias and Discrimination

- Reasonable efforts shall be taken to identify, assess and mitigate bias in training data, model design and outputs.
- AI systems shall not be used in a manner that results in unlawful discrimination or unfair outcomes.
- Periodic reviews and testing shall be undertaken for high-impact AI use cases.

4.4 Human Oversight and Human-in-the-Loop

- Appropriate human oversight shall be maintained for AI-enabled decisions, especially for high-risk or business-critical use cases.
- Humans must be able to review, override or intervene in AI-generated outputs where required.
- Fully automated decision-making without meaningful human involvement shall be restricted unless explicitly permitted by law and approved internally.

4.5 Transparency and Explainability

- The use of AI shall be disclosed where relevant to clients, users or other stakeholders.
- AI systems should be explainable to a reasonable extent based on the use case, risk level and audience.
- Documentation shall be maintained to describe data sources, model logic, limitations and assumptions.

- Distinct Identification of AI-Generated Outputs- Where AI systems are used to generate content, recommendations or decision outcomes that materially influence users, clients or other stakeholders, such outputs shall be appropriately identified as AI-generated or AI-assisted, taking into account the context, audience and potential impact. The objective of such identification is to promote transparency, informed use and trust, and to avoid misleading representations regarding the nature of the output or decision.
- Audit logs & version control- AI systems shall maintain appropriate documentation, audit logs and version control records to ensure traceability, reproducibility and accountability.

- Such records may include:
  - Data sources and training datasets
  - Model versions and updates
  - Key decisions, outputs and changes over time

- These controls shall be implemented in alignment with Hexaware's Information Security and applicable system management standards.

For AI systems involving general-purpose or generative AI models, documentation shall be maintained describing model capabilities, limitations, intended use, and known risks.

Where required, summary information regarding training data sources and applicable intellectual property considerations shall be maintained to support transparency and compliance.

4.6 Accountability for AI Outcomes

- Clear accountability shall be established for each AI system, including business owners, technical owners and risk/compliance oversight.
- Decisions and outcomes produced by AI systems remain the responsibility of Hexaware and designated human stakeholders.
- Material incidents or adverse impacts arising from AI use shall be reported and addressed through existing governance mechanisms.

4.7 Defining Boundaries of AI Use

- AI systems shall be used strictly within their intended purpose, design limitations and approved use cases.
- AI outputs shall not be treated as absolute or infallible and must be appropriately validated when used for decision-making.
- Unauthorized, unapproved or experimental AI use in production environments is prohibited.

4.8 AI Risk Assessment and Classification

Hexaware shall conduct a structured risk assessment for AI systems prior to development, deployment or onboarding.

AI systems shall be categorized based on defined criteria, including:

- Potential impact on individuals, clients or business operations
- Level of autonomy and extent of human oversight
- Sensitivity and type of data processed
- Regulatory exposure and legal implications

Based on this classification (e.g., low, medium, high risk), proportionate controls, approvals and monitoring requirements shall be applicable High-risk AI systems shall be subject to enhanced governance, validation and periodic review.

4.9 Additional Controls for High-Risk AI Systems

AI systems classified as high-risk shall be subject to enhanced governance and control measures, including:

- Formal risk management processes covering the entire AI lifecycle
- Pre-deployment validation, testing and performance evaluation
- Documented assessments of accuracy, robustness, cybersecurity and potential impacts on individuals and business operations
- Periodic review and re-validation to ensure continued reliability and compliance

Such controls shall be proportionate to the level of risk and aligned with applicable regulatory requirements.

4.10 AI Roles and Regulatory Applicability

For each AI system, Hexaware shall identify its role in the AI value chain, including but not limited to provider, deployer, integrator, or operator.

Where AI systems are developed, deployed, or used in a manner that impacts individuals or markets within jurisdictions such as the European Union, applicable regulatory obligations (e.g., EU Artificial Intelligence Act) shall be identified and complied with accordingly.

Obligations shall be applied proportionately based on the role performed by Hexaware in relation to the AI system.

4.11 Conformity Assessment and Regulatory Compliance

Where required by applicable regulations, including but not limited to the EU Artificial Intelligence Act, AI systems shall undergo appropriate conformity assessments prior to deployment or use.

Hexaware shall maintain necessary documentation, validation evidence and compliance records to demonstrate that AI systems meet applicable legal, regulatory and internal policy requirements.

AI systems shall not be deployed in regulated environments unless required conformity, validation and approval processes have been completed.

4.12 Environmental Responsibility

- Hexaware shall endeavor to use AI models, data centers and cloud services that demonstrate energy efficiency and a lower ecological footprint.
- Preference shall be given to providers with credible sustainability commitments and disclosures.
- Where feasible, optimization techniques shall be applied to reduce compute, storage and energy consumption.
- Measurement of Sustainability Impacts of AI- Where feasible and proportionate, Hexaware shall endeavor to measure and assess the environmental and sustainability-related impacts of its significant AI initiatives, including impacts on energy consumption, emissions, resource efficiency or sustainability outcomes enabled through AI-driven efficiencies. Such assessments may be qualitative or quantitative in nature, depending on data availability and use-case materiality, and shall inform continuous improvement efforts.

- Accessibility and Inclusive Design - Where applicable and proportionate to the use case, AI systems shall be designed and implemented to support accessibility and usability for individuals with disabilities, in alignment with relevant regulatory and ethical expectations.

4.13 Prohibited AI Practices

Hexaware shall not develop, deploy or knowingly use AI systems that:

- Engage in manipulative or deceptive behavior that materially distorts user behavior
- Exploit vulnerabilities related to age, disability or socio-economic circumstances
- Perform social scoring of individuals
- Conduct unauthorized biometric identification or surveillance in public or private spaces These restrictions align with prohibited AI practices under the EU Artificial Intelligence Act and similar regulations.

4.14 Acceptable Use of AI by Employees

Employees, contractors and users of AI systems shall adhere to the following acceptable use requirements:

- Only AI tools and platforms approved by Hexaware shall be used for business purposes
- Confidential, proprietary, client or sensitive data (including PII/SPII/PHI) shall not be entered into public or unapproved AI systems
- AI-generated outputs shall be reviewed for accuracy, completeness and appropriateness before use
- AI tools shall not be used to generate misleading, harmful, unethical or non-compliant content
- Users shall comply with applicable laws, contractual obligations and internal policies while using AI
- Any unauthorized or experimental use of AI in production environments is prohibited

Violation of these requirements may result in disciplinary action in accordance with Hexaware's Code of Conduct

4.15 General Purpose AI (GPAI) / Generative AI Controls

AI systems leveraging general-purpose or generative AI models shall be subject to additional governance controls, including:

- Documentation of model usage, capabilities, and limitations
- Review of outputs for accuracy, bias, harmful content, or misuse risks
- Compliance with applicable copyright, intellectual property and data usage regulations
- Implementation of safeguards to prevent generation of misleading, harmful or non-compliant content

Where such models present elevated or systemic risks, enhanced monitoring and risk mitigation measures shall be implemented.

5.0 Third-Party and Client AI Systems

- AI systems developed or operated by third parties on behalf of Hexaware shall be subject to due diligence, contractual safeguards and ongoing monitoring.
- Client-controlled AI systems shall be used in accordance with client instructions, applicable laws and ethical standards, while adhering to Hexaware's core Responsible AI principles.

6.0 Governance, Monitoring and Review

AI System Inventory and Register

✓ Hexaware shall maintain an inventory of all AI systems developed, procured, or used across the organization. The inventory shall include details such as system purpose, ownership, risk classification, data dependencies, and deployment status. This inventory

shall be periodically reviewed and updated to support effective governance, risk management and regulatory compliance.

AI systems lifecycle & decommissioning-

- ✓ AI systems shall be governed across their entire lifecycle, including design, development, testing, validation, deployment, monitoring and decommissioning. Decommissioning of AI systems shall be carried out in a controlled manner, ensuring appropriate handling of associated data, models and dependencies, and mitigation of residual risks.

- ✓ Post-Deployment Monitoring of AI Systems - AI systems, particularly those classified as high-risk, shall be subject to continuous monitoring to assess performance, accuracy, bias, security risks and compliance with applicable requirements. Material deviations, incidents or adverse impacts identified during monitoring shall be promptly addressed, documented and remediated.
- ✓

Awareness and Training

- ✓ Hexaware shall promote employee awareness and understanding of responsible, ethical and secure use of AI through appropriate training, guidance or communications, commensurate with employee roles and exposure to AI systems. Such initiatives may cover ethical considerations, data protection, cybersecurity risks and acceptable use expectations related to AI technologies.

- ✓ AI-related incidents, including unintended bias, incorrect outputs, data breaches or system failures, shall be promptly reported to securityincidents@hexaware.com. All incidents shall be investigated, documented and remediated appropriately, with lessons learned incorporated into future AI system improvements.

- ✓ This Policy is supported by internal standards, procedures and risk assessment mechanisms. Compliance with this Policy may be monitored through audits, risk reviews and assessments.

7.0 Policy approval & endorsement

This Responsible Artificial Intelligence Policy has been reviewed and approved by Hexaware's Executive Management and is endorsed at the highest level of the organization. Where applicable, the policy is also presented to the Board of Directors / relevant Board Committee for oversight.

This policy is subject to periodic review and approval by Executive Management in line with evolving regulatory and organizational requirements. Hexaware shall continuously monitor evolving global AI regulations and standards, including the EU Artificial Intelligence Act, and update this Policy to ensure ongoing compliance and alignment with best practices.