Persistent

Responsible AI Policy

Important: The printed copy of this document is not under control

Document Control

Docume nt No.	Document Name	Executive Summary	Revision No.	Classification
ISC-AIMS-POL-001A	Responsible AI Policy	This document outlines the Responsible AI Policy of Persistent Systems and defines the principles and objectives of responsible AI	1.1 dated 3 Nov 23	Public

Authorizations

Owner	Custodian	Distribution List
Responsible AI Council	CISO Office	Persistent Systems and Subsidiaries

Table of Contents

1. Preamble

Artificial intelligence (AI) is a powerful technology that can enhance the capabilities and performance of the organization in various domains, such as customer service, product development, decision making and innovation. However, AI also poses significant challenges and risks to privacy, cybersecurity, intellectual property, third-party/client engagements, legal obligations, and regulatory compliance.

Persistent Systems Limited, its subsidiaries and affiliates and any other directly controlled entities as may exist from time to time, hereinafter referred to as 'Persistent,' is committed to adopting a responsible AI approach that ensures the ethical and trustworthy use of AI in alignment with the organization's values, mission, and vision.

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

2. Scope

a) This policy applies to all AI-related activities that Persistent shall engage in including but not limited to the design, development, deployment, and evaluation of AI systems, as well as the governance, oversight, accountability, legal, social accountability, and safety of AI.

b) This policy covers both internal and external AI applications such as those used for operational efficiency, customer commitment, partner collaboration and social responsibility. This policy also applies to all employees, contractors, vendors, and partners who engage in or are affected by AI-related activities at Persistent.

c) 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 AI for internal utilization (e.g., to optimize HR processes, stakeholders must undertake all the existing procedures, including security assessment, confidentiality, and privacy.)

d) 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.

3. Objective

a) Provide guidance and rules for the responsible use of AI.

b) Ensure a risk-based approach for reducing risks associated with usage of this emerging avenue and build an effective policy over time to govern the usage of AI.

4. Management Commitment to Responsible AI

a) The Persistent Responsible AI Policy delineates the company's objectives concerning responsible use of AI and underscores management's unwavering commitment to the same. The application of this policy is mandatory for all group companies, business lines, subsidiaries, and affiliates, including all operations performed on personal data.

b) Persistent has established a Responsible AI Council for ensuring adherence to this policy and monitoring the responsible use of AI within Persistent. The Responsible AI Council is comprised of representatives from different business lines and enabling units, providing a diverse and holistic perspective on AI use.

5. Responsible AI Principles

Persistent's Responsible AI Policy is governed by following principles:

a) **Compliance:** Persistent shall comply with all applicable laws, regulations, standards, and best practices related to AI, such as those concerning data protection, human rights, consumer protection, and intellectual property.

b) **Transparency:** Purpose, functionality, limitations, and outcomes of the AI applications are clear and understandable to the relevant stakeholders, such as the users, customers, regulators, and auditors.

c) **Fairness:** AI applications are fair and inclusive, meaning that they do not discriminate, harm, or disadvantage any individuals or groups based on their characteristics, such as age, gender, race, ethnicity, religion, disability, or sexual orientation.

d) **Accountability:** AI applications have clear and defined roles, responsibilities, and authorities for the design, development, deployment, and evaluation of the AI applications, as well as for the monitoring, reporting, and remediation of any issues, errors, or harms that may arise from the AI applications.

e) **Quality:** AI applications meet the requirements, specifications, and expectations of the stakeholders, as well as the organization's quality standards and policies.

f) **Innovation:** AI applications contribute to the organization's strategic goals, competitive advantage, and social value.

g) **Human-centricity:** AI applications respect the dignity, autonomy, and well-being of the human stakeholders, as well as their rights, preferences, and values. For applications which leverage AI, users shall be appraised of the AI-generated content.

h) **Data Privacy:** To ensure the respect of data privacy in the use and development of AI, Persistent is committed to the principles set forth in our Privacy Policy.

i) **Cybersecurity:** To protect the cybersecurity of systems in the use and development of AI, we follow below principles:

   a. Design and develop AI systems that leverage our secure development lifecycle, incorporating security best practices and standards throughout the lifecycle of the system.

   b. Regular security testing and auditing of the AI systems

   c. Issues or concerns, such as unauthorized access or data breaches should be reported in accordance with Persistent's security incident reporting process.

6. Usage of AI Tools

a) The use of AI tools and applications shall comply with Persistent's data privacy, data security policies and due care shall be taken that they comply with regulatory and statutory requirements.

b) AI tools shall not be used to create adverse effects to Persistent, customer, entities data and infrastructure.

c) Access to Generative AI and similar AI tools shall be recorded and governed.

d) For cases where use of Generative AI is permitted by the customer and/or allowed on customer devices/systems, an explicit approval shall be secured from the customer for such usage and material outcomes of such processing.

7. Updates to this policy

Persistent may update the Responsible AI Policy to ensure its relevance, adequacy, and effectiveness in the changing context and environment of the organization and the AI technology, as and when the need arises, and the same will be made available on the website.

8. Contact

If you have any questions or feedback regarding this policy, please use our contact us webpage to share your input.