Artificial Intelligence (AI) Policy v 1.0

Master List Ref	Release Date	Review Date	Next Review Date
PL-ISMS-ENT-016	July, 2024	January, 2025	January, 2026
Version:	**Process Owner**	**Reviewed by**	**Approved by**
1.0	IRM	Associate Director - IRM	SVP - IRM

Version Control

Version no.	Date	Changes made
V1.0	July 8th, 2024	Document release

Index

1. Reference
2. Policy Statement
3. Purpose and Objectives
4. Scope
5. Ethical use of AI
6. Approved AI tools
7. Prohibited AI tools
8. Guidelines and Guardrails
    - 8.1 Guidelines
    - 8.2 Data Guardrails
    - 8.3 Additional restrictions
    - 8.4 AI Generated Output Guardrails
9. Transparency, explainability, and accountability
10. Data Privacy and Security in AI systems
11. Implementation and Monitoring
12. Compliance and Regulation
13. Developer and Deployer Obligations
14. General Consumer Data Rights

Annexure A

1. Reference

This policy is made in reference to all Employees, contractors and Third parties who use Generative AI programs on Firstsource-owned devices or networks when performing work on behalf of Firstsource and associated clients.

2. Policy Statement

Artificial Intelligence (AI) presents a wealth of opportunities balanced against risks for society, particularly in the workplace. Firstsource recognizes the importance of adopting AI as a valuable and innovative tool in assisting it to deliver its strategies but in a safe and responsible manner. Firstsource launched relAI which is a suite of Platforms, Solutions and pre-built AI models. relAI stands for Responsible and EthicaL AI underlining our commitment to this cause.

3. Purpose and Objectives

The purpose of this policy is to establish guidelines and best practices for the responsible use of AI and Generative AI ("GenAI") within Firstsource. Generative AI refers to technology that can generate human-like text, images, or other media content using AI algorithms. To encourage the development and use of AI, Firstsource has established this policy outlining the tools that employees can safely use, guidelines for responsible AI usage, and practices to avoid. This policy covers all AI disciplines, including but not limited to generative AI, predictive AI, and conversational intelligence. Firstsource aims to ensure ethical and responsible AI implementation while promoting transparency, fairness, and compliance

  - The objectives of this Policy are to ensure: Firstsource Employees are aware of the continuing emergence and integration of AI in the workplace or for any client. Workforce - People Strategy (AI will amplify human potential and not displace), will transform Firstsource Workforce to become AI ready.
  - Workplace - Use AI to become more efficient, conserve energy, water and where as applicable culture that supports Firstsource employees to explore the capabilities of AI, in particular the beneficial development, deployment, and use of this emerging technology; whilst safeguarding against all associated risks.
- Firstsource commitment to develop a Responsible AI framework that acts as guardrails for all AI experimentation, development, deployment and consumption.
- The responsible and ethical use of AI aligned with Firstsource values.
- The use of AI is transparent to all clients, employees, and other related stakeholders.
- The composition of any AI model built and what has gone in (tech stack, data, 3rd party leverage) are transparently communicated including known risks if any.
- Firstsource is in co mpliance with relevant laws and regulations.

4. Scope

This policy applies to all employees, contractors, and third-party individuals who use Generative AI programs on Firstsource-owned devices or networks when performing work on behalf of Firstsource and associated clients with access to AI tools. It includes:

- Build and Use of AI as per Guardrails
- The process to submit use cases and development models for approval

- The process to review all contracts involving AI and generative AI to ensure alignment with the company's ethical standards and compliance requirements.
- The process to have third-party tools approved for use.
- The process of continued observation and governance. This involves setting up mechanisms to continuously monitor and evaluate AI systems, ensuring they comply with established ethical norms and legal regulations.
- Chain of communication for any escalation as per organizational hierarchy
- Whistleblower policy in case escalations don't work – Email to whistle.blowing@firstsource.com
- Exceptions from adherence to this policy to be sought from Chief Digital and AI Officer and Head of Enterprise Transformation

5. Ethical use of AI

- AI adoption and/or use of AI application at Firstsource must be safe, secure, reliable and align with Firstsource values and strategic priorities. Firstsource shall ensure the Regulation and Laws followed by various geographies are in line with the usage of AI
- **Transparency:** Transparency implies openness, communication, and accountability. This means that where we use AI, we should disclose to the users that they are interacting with whole AI model/system/tool or in part.
- **Ethics Principles**: Proportionality and Do No Harm, Safety and Security, Right to Privacy and Data Protection, & Multi-stakeholder and Adaptive Governance & Collaboration.
- **Explainability:** AI systems, should offer clear and understandable explanations for recommendations, decisions, responses and predictions, considering the necessary level of accuracy and the technological limitations inherent to the specific context
- **Human-centered values*:*** AI systems should respect human rights, diversity, and the autonomy of individuals.
- **Fairness:** AI systems should be inclusive and accessible and should not involve or result in unfair discrimination against individuals, communities, or groups. Measures to identify and mitigate biases that may arise from biased, non-inclusive training data or bias in algorithms, thereby promoting equitable outcomes for all user groups
- **Privacy protection and security*:*** AI systems should respect and uphold privacy rights and data protection and ensure the security of data.
- **Reliability and safety*:*** AI systems should reliably operate in accordance with their intended purpose.
- **AI Validation and Engineering:** Ensure guardrails, controls and policies are codified and embedded across AI lifecycle stages where applicable.

Do's

- Automating repetitive tasks
- Streamlining and/or centralizing processes and functions
- Analysis of large datasets
- Trend analysis, recommendation systems, content and response generation and predictions

- Informing evidenced based decision-making.
- Employees must use AI programs responsibly and for legitimate business purposes only, and only for the purposes for which they were designed and intended.
- Employees must be transparent about their use of generative AI for work purposes and acknowledge the generative AI program as a source when used with the relevant client lead and colleagues as relevant.
- Employees must always verify data produced via generative AI. It should never be used as a single source of the truth and only to supplement additional research or writing methods.
- Employees must safeguard the confidentiality, integrity, and availability of company information always. Company information relating to Firstsource, its clients or associated organizations and individuals, or information that could reasonably be used to identify Firstsource or its client(s), or a commercially sensitive course of action should never be entered into generative AI technology without the express permission of the client and client lead.
- **Intellectual Property and AI Policy**: Employees must understand that any content created using AI tools may be subject to intellectual property rights and must comply with company guidelines regarding ownership and attribution.
- **AI Impact Assessment Policy**: Employees are required to assess the potential impact of AI-generated outputs on company operations and stakeholder interests before implementation.
- Employees must not disclose any company information, client specific information or trade secrets to any third party, including AI tools, programs such as ChatGPT, Gemini, and Midjourney.
- Any suspected data leaks or breaches must be escalated immediately to Information Risk Management team on Security@firstsource.com or dataprivacy@firstsource.com in case of any Data Privacy concerns which is in line with Incident Management policy and Data Privacy policies.
- Employees must report any suspicious or unauthorized use of AI programs to Chief Digital and AI Officer, Head – Enterprise Transformation and Chief Information Officer immediately.
- Employees must remain vigilant for the malicious use of generative AI by scammers. Do not share any sensitive information in your conversations or email exchanges.

Don’ts

- Employees must not use AI programs to engage in activities that could damage the reputation of the company or violate the Privacy rights of others.
- Employees must not disregard treating Firstsource data and customer data confidentially
- Employees must not use AI programs to create or disseminate malicious software or engage in hacking or other unauthorized activities.
- Don’t Use AI to Spread Misinformation or Disinformation
- Don’t Violate Privacy
- Don’t Use AI to Replace Human Judgment in Critical Decisions
- Don’t Use AI to Violate Copyright or Intellectual Property

- Don’t Use AI to Manipulate or Exploit Vulnerable Groups
- Don’t Ignore Legal and Regulatory Compliance
- Don’t Build or Deploy AI Systems Without Proper Testing and Monitoring

Consequences: It is essential that employees use these tools responsibly and in accordance with Company policies and legal requirements. This policy is intended to promote the safe and ethical use of AI programs and protect the interests of the Company and its stakeholders.

Technology and the law change regularly, and this policy shall be updated to account for changes as and when necessary. Employees shall be informed when the policy has changed, but it is their responsibility to read the latest version of this document

Action: Firstsource reserves the right to investigate any suspected breaches of this policy, misuse of AI system, Firstsource Data and / or its client’s data which may subsequently result in disciplinary action, up to and including dismissal.

Also there would be a fair investigation and hearing by the AICoE (AI Center of Excellence) team. AICoE team can be reached on aicoe@firstsource.com.

6. Approved AI Tools

This section covers the use of AI tools, including external/third-party and internally built tools. Employees should only use approved AI tools with company-provided accounts, for work purposes.

- Only approved AI tools vetted by the AICoE and approved by Chief Digital and AI Officer, Head – Enterprise Transformation and Chief Information Officer.
- These tools must meet the company's privacy and security standards.
- Examples of allowed AI tools: customer support chatbots, data analysis algorithms, and predictive analytics models.
- Use of approved tools requires that they are only accessed through a company-provided account (personal account usage for work purposes is not permitted on company devices).

7. Prohibited AI Tools

- Use of any AI tools that infringe upon privacy laws or violate ethical guidelines is strictly prohibited.
- Employees should not use, implement or develop any AI tool that is prohibited by regulation/law.
- Prohibit the use of unverified AI tools that have not been vetted or approved by Chief Digital and AI Officer, Head – Enterprise Transformation and Chief Information Officer.
- Prohibit the use of AI tools that do not comply with data protection regulations, promoting mis information, inadequate security, tools with proprietary risks, or that do not guarantee the confidentiality of input data.
- Examples of prohibited AI tools: facial recognition systems without explicit consent, biased AI models that discriminate, and any AI tool employed for malicious purposes.

8. Guidelines and Guardrails

8.1 Guidelines

- AI-generated content should be reviewed by a human to ensure it's appropriate for its intended purpose, it adheres to Company's inclusion principles, does not promote bias, does not infringe on any internal or external intellectual property rights, that the content generated is accurate, and that the output does not present false or misleading information (e.g. hallucinations).
- Properly attribute any AI-generated content and be transparent about its use in reports, presentations, and communications.
- Understand that many GenAI tools are prone to "hallucinations," false answers or information, or information that is stale, and therefore responses must always be carefully verified by a human.
- Treat every bit of information you provide to a GenAI tool as if it shall go viral on the Internet, attributed to you or the Company, regardless of the settings you have selected within the tool (or the assurances made by its creators).
- Inform your supervisor when you have used a GenAI tool to help perform a task.
- Verify that any response from a GenAI tool that you intend to rely on or use is accurate, appropriate, not biased, not a violation of any other individual or entity's intellectual property or privacy, and consistent with Company policies and applicable laws.

8.2 Data Guardrails

- Only input the data you need. Only input data that is required for the purpose for which you are using the AI tool and ensure the data you are using has been approved by respective CRM for your use case.
- Do not input Sensitive Personal Data. This includes information such as social security numbers, financial information like credit card or bank account numbers, personal addresses, or personal health information but not limited to these.
- Do not use any customer specific data without prior approvals.
- Establish clear protocols for sharing data with third-party AI tools, including agreements on data usage and security measures.
- Anonymization and De-identification: Where possible, anonymize or de-identify data before using it in AI applications to protect individual privacy.
- Do not input any Restricted Data. This may include things like material nonpublic information, SOX-controlled data, Company trade secrets, or internal security controls.
- Do not input access credentials. Do not input system access credentials (for our systems or those of any third party)

8.3 Additional Restrictions

- Do not use GenAI tools to make or help you make employment decisions about applicants or employees, including recruitment, hiring, retention, promotions, transfers, performance monitoring, discipline, demotion, or terminations.

- Do not upload or input any confidential, proprietary, or sensitive Company information into any GenAI tool. Examples include passwords and other credentials, protected health information, personnel material, information from documents marked Confidential, Sensitive, or Proprietary, or any other nonpublic Company information that might be of use to competitors or harmful to the Company if disclosed. This may breach your or the Company's obligations to keep certain information confidential and secure, risks widespread disclosure, and may cause the Company's rights to that information to be challenged.
- Clearly attribute AI-generated content, indicating that it was created with the assistance of an AI tool, to maintain transparency.
- Do not represent work generated by a GenAI tool as being your own original work.
- Do not integrate any GenAI tool with internal Company software without first receiving specific written permission from your supervisor and the IT Department.
- Do not use GenAI tools other than those on the approved list. Malicious chatbots can be designed to steal or convince you to divulge information. (For the approved list of AI tools please approach the AICoE team as this will vary from time to time)

8.4 AI-Generated Output Guardrails

a. **AI Only Responses**: If an AI feature shall directly present a response to customers or third parties without human review or intervention, you must disclose to the customer that they are:
   - Engaging solely with an AI.
   - Responsible for checking it for accuracy.

- Ensure that AI outputs are appropriate for the context in which they are used, avoiding scenarios that could lead to misinterpretation or misuse.
- Avoid using AI-generated outputs for sensitive topics (e.g., legal advice, project work recommendations) without human review and approval.
   - Responsible for checking the response for detectable bias.
   - Example: "This response has been generated by an AI tool and has not been reviewed by a human being, you are responsible for checking for accuracy and bias."

b. **Generating Images/Voice/Video**: If you're using AI to generate content, please follow these guidelines.
   - Check output for any indication of third-party ownership, such as trademarks or watermarks, and don't use any output that contains such content.
   - If you are using an AI tool to replicate someone's image, likeness, or voice - you need to get their express written permission first. Please reach out to legal counsel to coordinate permission.

c. **Generating Code**: If an AI feature shall generate code, this requires additional review.

9. Transparency, Explainability and Accountability:

- Employees must be transparent about the use of AI in their work, ensuring that stakeholders are aware of technology's involvement in decision-making processes.
- Employees must utilize Company's centralized system for AI governance and compliance efforts to ensure transparency of proposed and active AI activities.
- Employees are responsible for the outcomes generated by AI systems and should be prepared to explain and justify those outcomes.
- **Employees Must**:
    - Maintain documentation that outlines the data sources, algorithms, and methodologies used in AI systems to ensure clarity about their functioning.

      Clearly disclose what types of data are being collected and how they shall be used in AI processes.

      Be able to articulate the reasoning behind AI-generated outputs, including which factors influenced the AI's conclusions.

      Clearly outline roles and responsibilities for AI development, deployment, and oversight to ensure accountability at all levels.

      Establish a procedure for reporting any issues or errors arising from AI outputs, with a focus on learning and improvement.

      Implement regular audits of AI systems to assess their performance, bias, and compliance with ethical standards and regulations.

      Clearly state the consequences for non-compliance with the policy, including misuse of AI tools or failure to adhere to transparency and accountability measures.
    - Report any concerns or potential violations of this AI policy to the security@firstsource.com & Dataprivacy@firstsource.com
- The Company shall investigate and address reported issues promptly.
- AI systems and models should provide clear explanations of their decision-making processes, especially when impacting individuals.

  Ensure that AI tools are understandable to non-technical stakeholders and that their implications are communicated transparently.

10. Data Privacy and Security in AI Systems

Data security is a critical aspect of AI systems to protect data from unauthorized access, breaches, and misuse. Robust data security measures are essential to ensure confidentiality, integrity, and availability of data.
The following types of data are considered sensitive and must be handled with the utmost care and compliance with this policy:

Internal Corporate Data: All proprietary information and internal data belonging to the organization, including operational data, financial records, and strategic plans.
Customer Information in Internal Platforms: Any personal or sensitive information about customers stored within the company's internal systems, which must be protected in accordance with data privacy regulations.
Customer Information in Customer Platforms: Data related to customers that resides within external customer platforms or systems, which must also be treated with confidentiality and in compliance with contractual obligations and relevant regulations.

Employees are expected to adhere to strict guidelines when handling this data to ensure its security and integrity.

- **Access Controls**: Implementation of strong access controls is essential to restrict access to data within AI systems. One of the user authentications is mandatory, Enforce strong authentication mechanisms, such as username/password combinations, multi-factor authentication (MFA), or biometric
- **Authentication** to prevent unauthorized access to data storage systems.
- **Encryption**: Encryption is a fundamental technique to protect data confidentiality. AI systems should employ encryption methods in line with HIPAA / FIPS to encrypt data both at rest (stored data) and in transit (data being transmitted between systems). Strong encryption algorithms and secure key management practices should be implemented to safeguard data.
- **Data storage security**: The secure storage of data is crucial in AI systems. Adequate security measures should be implemented to protect data repositories, databases, or cloud storage systems. This includes physical security measures, such as access controls to data centers, as well as logical security measures, such as firewalls, intrusion detection systems, Strong user authentication, Access logs and regular security audits. Ensure not to use security setting default values in any of the System, Application, or Software that is being used. Always change the default administrator or root passwords to something strong and unique.
- **Secure data transmission**: When data is transferred between different components or systems within an AI infrastructure, secure communication protocols (e.g., HTTPS, VPN / IPSec) should be employed to protect data integrity and confidentiality. This is particularly important when data is transmitted over public networks or shared with external entities. The Data when exchanged with external entities, this must be restricted to whitelisted IP addresses or through Secure VPN tunnel.
- **Regular security assessments and audits**: Periodic security assessments and audits should be conducted to identify vulnerabilities and ensure that security controls are effective. This includes penetration testing, vulnerability scanning, and code reviews to identify and remediate any security weaknesses in AI systems.
- **Data anonymization and De-identification**: To mitigate privacy risks / Date exposure, AI systems should employ techniques such as anonymization and de-identification to remove or protect personally identifiable information from data or Any data shared should be de identified / anonymized. This helps to prevent reidentification of individuals and minimizes the impact of data breaches.

- **Secure third-party integrations**: If AI systems integrate with third-party services or utilize external APIs, proper due diligence should be conducted to ensure the security practices of these entities. Contracts and agreements should specify data security requirements and responsibilities of all parties involved.

11. Implementation and Monitoring

AI Governance Board - A multidisciplinary AI risk management team('AI Governance Board') comprised of a diverse team of experts, including Data Architect, and Information Security Architect professionals and AICoE shall ensure that AI initiatives are developed and deployed responsibly, in compliance with relevant laws and regulations, and with ethical considerations in mind. The AI Governance Board shall create and define roles and responsibilities, policies, procedures and decision-making processes for designated committees critical to the oversight of the Company's AI initiatives. AI governance board will continuously identify AI risks and register the same which will be reviewed periodically and feed into overall organization level risk registry

- **Designated AI Officer** – Head of AI shall be responsible for overseeing the implementation of this policy, providing guidance and support to employees, clients and ensuring compliance with relevant laws and regulations.

- **Periodic Reviews -** The AICoE shall conduct periodic reviews of AI system use within the company to ensure adherence to this policy, identify any emerging risks, and recommend updates to the policy as necessary.

AI Audits & Standards: Ensure to adhere to applicable processes and standards for development, deployment and usage of AI solutions and services that meet industry recognized benchmarks.

Sustainability: Ensuring that the development and execution of AI products and services are done using models that consume lower compute and infra resources resulting in lower carbon footprint

12. Compliance and Regulation:

- Information Security and Data Privacy Team shall monitor and investigate suspected and/or reported violations of this policy. Depending on the results of any investigations and may engage 3rd parties, violations may be escalated to Leadership to determine the appropriate action.
- All AI tools and processes must comply with applicable laws, regulations, and industry standards.
- All AI tools and software must be used in accordance with their licensing agreements, prohibiting unauthorized access or distribution.
- AI systems should adhere to intellectual property laws related to AI-generated content and ensure that the use of AI tools does not infringe on the rights of others.
- All AI systems sourced and 3rd party AI leveraged must go through Risk assessment and signed off before data is ingested, shared or integrated with any 3rd party.

- Periodic audits of AI systems may be conducted to ensure ongoing compliance. And if Firstsource is using any 3rd party AI system, all the 3rd party reports (ISO 27001, SOC2 Type 2, HITRUST, PCIDSS etc.) must be reviewed and verified at least annually.

All contracts involving AI must be reviewed by the legal and compliance team and chief Digital and AI office to ensure compliance with applicable laws, protect the organization from potential liabilities, and address any specific provisions related to AI usage and responsibilities.

AI-Specific Clauses: All contracts involving AI must include specific clauses that address the use, limitations, and responsibilities associated with AI technologies to ensure clarity in expectations.

Liability Indemnification for Firstsource: Contracts should include indemnification provisions that protect Firstsource from all liabilities arising from the use of AI technologies, including but not limited to issues related to data breaches, misuse of AI outputs, and any regulatory non-compliance.

Data Ownership and Usage Rights: Clearly define ownership of data used in AI processes, including rights related to the use of AI-generated content and any derived data.

Limitation of Liability: Consider including clauses that limit liability related to AI outputs, clarifying the extent of liability in case of errors or issues arising from AI technologies.

13. Developer and Deployer Obligations

Deployers of AI & High-risk AI systems shall keep the logs automatically generated by that AI system to the extent such logs are under their control, for a period appropriate to the intended purpose of the AI & High-risk AI system, of at least six months, unless provided otherwise in applicable Union or national law, in particular to Union law on the protection of personal data. Deployers that are financial institutions subject to requirements regarding their internal governance, arrangements or processes under Union financial services law shall maintain the logs as part of the documentation kept pursuant to the relevant Union financial service law.

Before using a high-risk AI system, employees must be informed. If the system is not registered in the EU database, it should not be used. Deployers must also comply with data protection assessments and cooperate with relevant authorities.

Deployers of high-risk AI systems shall take appropriate technical and organisational measures to ensure they use such systems in accordance with the instructions for use accompanying the systems

Deployers shall assign human oversight to natural persons who have the necessary competence, training and authority, as well as the necessary support

Deployers shall monitor the operation of the high-risk AI system on the basis of the instructions for use and, where relevant, inform providers in accordance with **Article 72** EU Artificial Intelligence Act. Where deployers have reason to consider that the use of the high-risk AI system in accordance with the instructions may result in that AI system presenting a risk within the meaning of **Article 79**(1) EU Artificial Intelligence Act, they shall, without undue delay, inform the provider or distributor and the relevant market surveillance authority, and shall suspend the use of that system. Where deployers have identified a serious incident, they shall also immediately inform first the provider, and then the importer or distributor and the relevant market surveillance authorities of that incident. If the deployer is not able to reach the provider, **Article 73** EU Artificial Intelligence Act shall apply mutatis mutandis. This obligation shall not cover sensitive operational data of deployers of AI systems which are law enforcement authorities. For

deployers that are financial institutions subject to requirements regarding their internal governance, arrangements or processes under Union financial services law, the monitoring obligation set out in the first subparagraph shall be deemed to be fulfilled by complying with the rules on internal governance arrangements, processes and mechanisms pursuant to the relevant financial service law.

Additional Deployer Responsibilities:

Deployer has the responsibility to train as to how to use the GenAI specialized system being deployed and ensure AI disclosure is prominently disclosed before release.

GenAI Consumer /User Disclosure:

You are interacting with generative AI (and not a human). Content is generative AI generated. GenAI disclosure must be prominent by following below “Artificial Intelligence Disclosure (AID) Framework of 2012”.

AID Statement and their definitions: (AID)

1. Artificial Intelligence Tool(s): The selection of tool or tools and versions of those tools used and dates of use. May also include note of any known biases or limitations of the models or data sets.
2. Conceptualization: The development of the research idea or hypothesis including framing or revision of research questions and hypotheses.
3. Methodology: The planning for the execution of the study including all direct contributions to the study design.
4. Information Collection: The use of artificial intelligence to surface patterns in existing literature and identify information relevant to the framing, development, or design of the study.
5. Data Collection Method: The development or design of software or instruments used in the study.
6. Execution: The direct conduct of research procedures or tasks (e.g. AI web scraping, synthetic surveys, etc.)
7. Data Curation: The management and organization of those data.
8. Data Analysis: The performance of statistical or mathematical analysis, regressions, text analysis, and more using artificial intelligence tools.
9. Privacy and Security: The ways in which data privacy and security were upheld in alignment with the expectations of ethical conduct of research, disciplinary guidelines, and institutional policies.
10. Interpretation: The use of artificial intelligence tools to categorize, summarize, or manipulate data and suggest associated conclusions.
11. Visualization: The creation of visualizations or other graphical representations of the data.
12. Writing – Review & Editing
13. Writing – Translation: The use of artificial intelligence to translate text across languages at any point in the drafting process.
14. Project Administration: Any administrative tasks i.e. related to the study, including managing budgets, timelines, and communications etc.

Example:

Extracted from the “Artificial Intelligence Disclosure (AID) Framework of 2012”

ChatGPT AID Statement: Artificial Intelligence Tool: ChatGPT v.4o and Microsoft Copilot (University of

Waterloo institutional instance); Conceptualization: ChatGPT was used to revise research questions; Data Collection Methods: ChatGPT was used to create the first draft of the survey instrument.

Data Analysis: Microsoft Copilot was used to verify identified themes coded from open ended survey responses; Privacy and Security: no identifiable data was shared with

ChatGPT during the design of this study, Only the University of Waterloo institutional instance of

Microsoft Copilot was used to analyse any anonymized research data in compliance with University of Waterloo privacy and security policies; Writing – Review & Editing: ChatGPT was used in the literature review provide sentence level revisions and metaphor options; Project Administration: ChatGPT was used to establish a list of tasks and timelines for the study.

14. General Consumer Data Rights

Deployer or developer must inform users if their personal data is going to be used to train an AI system, to ensure that processing is fair and transparent. User/Consumer consent must be obtained before collecting any data. This information must be provided at the point of collection.

Annexure A

Information Classification Details

Classification: Firstsource Restricted
Information Owner (IO): Risk Committee
Information Custodian (IC): IRM team
Authorization List (AL): All employees; Vendors; Current/Prospective clients.
Declassify on: Never