THE INTELLIGENT ENTERPRISE

AI | Insurance | Financial Services

AI Sample Governance and Usage Policy

LIMRA and LOMA AI Governance Group

LIMRA LOMA

Navigate With Confidence

Sample Artificial Intelligence Governance and Usage Policy

Policy Owner	
Policy Approver(s)	
Applies to	
Storage Location	
Effective Date	

1.0 Purpose

1.1 understands that while artificial intelligence systems (hereinafter "AI" or "AI system(s)" have the promise of great efficiency breakthroughs and rapid business insights, AI also has unique risks. The risks created by AI include the potential for inaccuracy, unfair bias resulting in unfair discrimination, and data vulnerability. Further, acknowledges the rapid evolution of AI systems and has designed this Artificial Intelligence Governance and Usage Policy ("AI Policy") to accommodate changes in the technology, as well as the corresponding risks and regulatory obligations triggered by the use of AI systems.

The purpose of this AI Policy is to provide users of AI with guardrails that promote the principles of fairness, transparency, accountability, explainability, and independent oversight in the use and governance of AI systems. In doing so, this AI Policy seeks to protect , its members, and its workers by mitigating the risk of misuse, unethical or unfair outcomes, and potential biases or other inaccuracies, all while ensuring the integrity of data and information security systems.

The users covered by this AI Policy are accountable for using any AI systems in a responsible, safe, secure, fair, ethical, and lawful manner that supports AI principles.

2.0 Scope

2.1 This AI Policy applies to all users when engaged in business on behalf of or when using data, equipment (including hardware or software licensed or supplied by , or when otherwise engaged in any other activity reasonably attributable to . This AI Policy further extends to any interactions by users with any third-party agents and vendors, or interactions with members and the public at large.

3.0 Definitions

3.1 "AI systems" is an umbrella term describing software, solutions, or other machine-based systems that provide artificial intelligence capabilities to insurers. An AI System can, for a given set of objectives, generate outputs such as predictions, recommendations, or other content with varying degrees of autonomy. Illustrative examples include but are not limited to: ChatGPT, ChatSonic, Jasper AI, Bing AI, Google Bard, xAI Grok, Microsoft CoPilot, etc. Users can access a list of permitted AI systems via this link: Approved AI Systems.[1] Field staff should submit a request to view this list via email to .

3.2 "Algorithm" means a computational or machine learning process following mathematical rules that produces a prescribed result, and which can augment or replace human decision-making in insurance operations.

3.3 "Artificial intelligence" is a term used to describe machine-based systems designed to simulate human intelligence to perform tasks, such as analysis and decision-making, given a set of human-defined objectives. This definition treats machine learning as a subset of artificial intelligence.

3.4 "Bias" is the differential treatment that results in favored or unfavored treatment of a person, group, or attribute.

3.5 "Field staff" means field representatives of who service products. This includes regional directors, managing partners, field representatives, administrative assistants, and any subagents thereof.

3.6 "Machine learning" is a subset of artificial intelligence that simulates human learning by identifying patterns in data either supervised, unsupervised or through reinforcement learning styles to make decisions without additional programming. "Predictive analytics" and "predictive modeling" are related terms that refer to methods to identify patterns in data to make predictions.

3.7 " " means and .

3.8 "Predictive model" means the mining of historic data using algorithms and/or machine learning to identify patterns and predict outcomes that can be used to make or support the making of decisions.

3.9 "Protected data source" is data any medium — physical or electronic — that contains elements deemed critical to the business and/or sensitive in nature. The level and nature of protective measures applied to a data source will be based on the data classifications applied to elements in the data source.

3.10 "Third-party" for purposes of this bulletin means an organization other than the insurer that provides services, data, or other resources related to AI.

[1] The organization is responsible for linking "Approved AI Systems" to a list of permitted AI systems.

3.11 Data classifications and restrictions:

- All assets must be classified in terms of legal requirements, value and criticality to the organization, and sensitivity to disclosure by an unauthorized party.

- data shall be classified into one of the following categories:

  › **Corporate Confidential**: Critical information whose existence or content is only known to a small group of individuals. Disclosure of this information would harm or impede its ability to achieve objectives and plans. This information should have special access controls applied to the data or within the hosting application(s), to limit access to authorized individuals only. Additional auditing and reviews may be requested in this information.

  › **Business Confidential**: Business confidential information/data requires an elevated level of protection (e.g., database encryption, data obfuscation, encryption, additional auditing and reviews, and multi-factor authentication) to satisfy regulatory requirements or prevent unintended disclosure. Disclosure is authorized to individuals on a need-to-know basis (e.g., Personally Identifiable Information).

  › **Internal Use**: Used to conduct normal business operations of . The intention is to minimize the impact upon business operations. The information is intended for internal use only.

  › **Public**: Public information is made available by for general or public consumption or is publicly known information that has received from other organizations.

4.0 Compliance With Related Polices, Agreements, Laws, Regulations, and Standards

4.1 This AI Policy is not intended to contradict, limit, or replace applicable mandatory rules, policies, legal requirements or prohibitions, or contractual obligations.

4.2 The use of any AI system must comply with any related policies listed in this AI Policy or any other policy of that, by its nature, is reasonably related to this AI Policy. Examples of such policies include, but are not limited to:

For home office users:

- Information Security Policy
- Employee Handbook Digital Resources Policy
- Employee Handbook Policy Against Harassment and Discrimination
- Employee Handbook Confidentiality, Privacy, and Information Security Policy
- Vendor management Policy
- Asset Management Policy

For field staff users:

- Field Information Security and Privacy Policy and Guidelines
- Digital Resource Policy
- Policy Against Discrimination and Harassment

4.3 This AI Policy is intended to comply with all applicable laws, regulations, or standards governing the business of insurance or financial services. expressly reserves the right to amend this AI Policy to maintain compliance with any of the above.

5.0 Guidelines

5.1 When using AI systems, users shall not:

- Use any AI systems that have not been formally approved via the processes noted in this AI Policy
- Contract for or with vendors or other third parties that use AI systems or process data with AI systems without prior approval
- Input or enter data into AI systems without prior authorization
- Use AI systems to make autonomous decisions about humans (i.e., insurability, performance, etc.) unless approved via the processes described in this AI Policy
- Use AI systems in an unlawful manner, in any way that violates any policy of , or in a way that contradicts the purpose of this AI Policy including, but not limited to:
  - › Discriminate against, harass, or offend other users, members, or the public at large
  - › Disclose confidential, business confidential, or other internal use data
  - › Conduct or solicit illegal activities
  - › Infringe on the rights of others, including privacy or intellectual property rights
  - › Interfere with the performance of the jobs and duties of others or the nature, purposes, or objectives of generally

5.2 When using AI systems, users shall:

- Adhere to any policies concerning the confidentiality and privacy of data including, but not limited to, the confidentiality, privacy, and information security policy in the employee handbook, as well as the code of conduct

- Use formally approved AI systems or seek appropriate approval for new AI capabilities in existing approved systems, as detailed in Section 5.3

- Use AI systems for only authorized purposes

- Review and verify any AI systems to ensure compliance with this AI Policy

- Review and verify any data input into any AI system and any data, results, or outputs generated by an AI system

  › The review and verification process shall include ensuring the data, results, or outputs are materially correct, accurate, trustworthy, and do not violate this AI Policy in any respect.

- Track and document the use of AI systems

  › Tracking and documentation shall be maintained by vendor management within their vendor management information system or an alternative system/storage for non-third party provided AI systems or functionality.

  › Such documentation shall be provided to the user's applicable department manager with a copy to vendor management or to the user's regional director with a copy to IT field technology and innovations.

- Adhere to all training requirements prescribed by whether required prior to use of such AI systems or as a condition of ongoing use

- Comply and assist with any auditing of the AI system and compliance with this AI Policy as may be required by

5.3 Approval of new AI capabilities shall adhere to the following procedure:

- Formal approval to introduce, begin testing, and/or begin a proof-of-concept project shall begin with submitting the new or existing system to the user's department manager or the user's regional director.

- Following submission by a home office user, the department manager will notify Vendor management department and submit all necessary documentation to begin the vetting and approval processes.

- Following submission by a field staff user, the regional director shall share the name and requested use of the system or software with IT field technology and innovations. IT field technology and innovations will then coordinate the review of the request.

- Vendor management shall coordinate the flow of the evaluation steps to the appropriate parties throughout the organization via a predefined process.

- Vendor management shall then provide any necessary materials to the information security committee for final evaluation.

- Upon conclusion of the evaluation processes, vendor management shall notify the requesting user's department manager or IT field technology and innovations of the outcome of the evaluation and the next steps based upon the outcome, to include an expressed acknowledgment of any requirements that must be met for approval or an understanding of non-approval or pause requirement. IT field technology and innovations shall notify the requesting field staff user's regional director of the outcome of the evaluation and the next steps which may include an expressed acknowledgement of any requirements that must be met for approval or an understanding of non-approval or pause requirement.

- It is the responsibility of the requesting user, or that user's manager or regional director, to exercise the necessary due diligence in selecting any third-party provider of an AI system.

6.0 Audit, Monitoring, and Controls

6.1 All AI systems and other technology subject to this policy shall be further subject to appropriate auditing, monitoring, and control procedures. Specific control procedures for any given AI system shall be determined considering AI principles, the factors enumerated in Section 6.2, and any other factors or standards deemed prudent and acceptable to .

6.2 Any user requesting approval of an AI system pursuant to Section 5.3 must present a proposal detailing the necessary control procedures that will be implemented to ensure adherence to AI principles and compliance with this Policy. Such control procedures shall include consideration of the following:

6.2.1. The capabilities of the AI system

6.2.2. The anticipated use cases of the AI system

6.2.3. Whether the AI system will process the Personally Identifiable Information (PII) of consumers or workers

6.2.4. The nature of the decisions being made, informed, or supported by the AI system

6.2.5. The extent to which will rely on those decisions

6.2.6. The extent to which humans will be involved in the final decision-making process

6.2.7. Whether the AI system has the potential to adversely impact the legal rights of consumers or workers and the degree of such potential harm

6.2.8. Whether the data or information accessed by the AI system is retained within ecosystem

6.2.9. Whether the data or information entered the AI system is used to train a third-party AI system

6.2.10. Whether the requested tool is available without AI capabilities

6.2.11. Any other factors necessary for adherence to the AI principles

6.3 The proposal will be reviewed by the information security committee which may either approve, approve subject to revision, or reject the proposal. If approved, the approved control procedures will work in conjunction with any other standard control procedures currently in use by .

6.4 Upon approval, the user requests the AI system or, if the requesting user is not a manager or regional director, then the user's manager or regional director, shall maintain primary responsibility for adherence to the necessary control procedures.

6.5 In the case of third-party AI systems, users responsible for the relationship with the third party shall work to secure appropriate contract terms with the third-party to provide with audit rights or the right to receive an audit report concerning any applicable AI system, as well as assurances of cooperation by the third party in any regulatory inquiries or investigations.

6.6 Users shall work with appropriate business units to ensure adherence to applicable data handling practices, including validating the quality and integrity of any data inputs or outputs of an AI system, as well as auditing any decision-making aspects of the AI system according to acceptable standards approved by .

6.7 Pursuant to AI approval process, shall maintain an inventory of all AI systems. It shall be the responsibility of the requesting user, or that user's manager or regional director, to inform Vendor management or IT field technology and innovations departments, as applicable, of any changes to the AI system, including version updates.

6.8 AI systems, and any inputs or outputs from those systems, shall be subject to applicable data and record retention policies.

6.9 internal audit department shall have the right to exercise all necessary oversight or audit functions associated with the use of an AI system and any user of an AI system shall cooperate completely with the requests of the internal audit department.

7.0 Compliance and Violations

7.1 Compliance with this AI Policy is the responsibility of each individual user.

7.2 Violations of this AI Policy, including the requirements of Section 5, shall be treated like other allegations of wrongdoing at . reserves the right to determine the consequences for violations of this AI Policy, including termination of any employment or association with such user, and further reserves all rights.

7.3 If a home office user becomes aware of an actual or potential violation of this AI Policy, user agrees to immediately report such violation to vendor management department. If a field staff user becomes aware of an actual or potential violation of this AI Policy, user agrees to immediately report such violations to IT field technology and innovations. This includes, but is not limited to, the downloading or installation of any of the following on any networks, systems, or devices:

- An unlicensed AI system
- An AI system not approved according to this AI Policy
- An approved AI system that is being used in a manner for which it was not approved
- An AI system containing malicious code or another information security threat

7.4 expressly prohibits any form of discipline, reprisal, intimidation, or retaliation for a report or information provided pursuant to Section 7.3.

8.0 Review of the AI Policy

8.1 expressly reserves the right to change, modify, or delete any provisions of this AI Policy without notice.

8.2 This Policy will be reviewed annually or as needed to keep pace with changes to the AI landscape.

Acknowledgment of Receipt and Review

Acknowledgment and agreement with the terms of this AI Policy shall be a prerequisite to any use of an AI system. **The user's use of an AI System shall be regarded and presumed as such acknowledgment and agreement**. User understands that retains the maximum discretion permitted by law to interpret, administer, change, modify, or delete this AI Policy at any time without notice. No statement or representation by a user contradicting this policy shall be binding upon or considered as an approved modification. Such modifications shall only be permitted by the board of directors of , or any appropriate committee appointed by the board of directors to administer this AI Policy. Changes to this AI Policy may only be permitted in writing.

If a user bound by the terms of this policy is not an employee of , it is expressly acknowledged and agreed upon that this AI Policy does not constitute, nor is it intended to constitute, an employment contract. Nothing herein shall establish an employer–employee relationship between and the user unless otherwise separately and expressly agreed to by and the user.

Advancing the financial services industry by empowering our members with

LIMRA LOMA
Navigate With Confidence

1008-2025