Defensible

Artificial Intelligence Acceptable Use Policy

Date

Table of Contents

Introduction

The widespread availability of generative artificial intelligence (AI) tools such as ChatGPT, Grok, Claude, Gemini, and Copilot has significantly enhanced analytic and reporting capabilities. These tools are designed to perform varied tasks involving natural language processing, content creation, and information retrieval. They rely on large language models (LLM) trained on vast data sets, and are part of a broader AI-as-a-Service ecosystem that provides intelligence for both individual and enterprise use.

In general, AI systems use machine and human-based inputs to perceive real and virtual environments, abstract such perceptions into models through analysis in an automated manner, and use model inference to formulate options for information or action. Other AI technologies exist in addition to generative AI tools, and these are subsumed under the broad heading of "AI systems," which is defined in the next section.

The use of AI, which includes open source and publicly available software as well as internally-developed systems, is also accompanied by significant risks. Such risks must be managed in accordance with the Firm's risk tolerance. This document sets forth the official policy with respect to the use of all AI systems used in support of the Firm's business activities. This Policy supersedes any other document or policy relating to AI and/or its use in connection with Firm business.

AI System Definition

An AI system is defined as a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. This definition includes but is not limited to systems that use machine learning, large language model, natural language processing, and computer vision technologies, including generative AI. The definition does not include virtual or physical machines that perform basic calculations, basic automation, or pre-recorded "if this then that (IFTT)"-type responses.

Policy Applicability

The *Artificial Intelligence Acceptable Use Policy* applies to all Firm systems that deploy AI technology including third-parties such as consultants, vendors, and contractors that use or access any Information Technology (IT) resource for which the Firm has administrative responsibility. Such resources include systems managed or hosted by third-parties on behalf of the Firm.

This Policy also applies to all new and existing AI systems that are developed, used, or procured by the Firm in support of business operations.

Key Principles

1. The Firm's *Information Security Policy* governs all security-related issues arising in connection with the use of AI systems. The *Information Security Policy* can be found here www.informationsecurity.com.
2. AI systems must only be used to further the stated business objectives of the Firm.
3. AI systems must never be used for malicious purposes or with the intent to cause harm or damage.
4. Interaction with AI systems must always be transparent, where its use is disclosed to all relevant internal and external parties.
5. Sensitive, private, confidential, personally identifiable, and/or proprietary Firm or customer data must never be entered or uploaded to commercial AI systems without General Counsel approval.
6. Use of AI systems must always comply with applicable rules, laws, regulations, official notices, and Firm policies. Questions in this regard should be directed to the Firm's Office of General Counsel ***before*** using an AI system in connection with the Firm's business activities.

Approved Use of AI Systems

Use of AI systems is generally permitted pursuant to furthering the Firm's mission and better enabling it to address business requirements. However, each Department ultimately determines how such systems are utilized, and in what contexts AI is and is not permitted. To that end, each Department head is responsible for determining that Department's limits on AI system use, noting such use must always comport with this Policy and other Firm policies, e.g., the *Information Security Policy*.

Only approved AI systems are permitted for use in connection with Firm business. A list of pre-approved AI systems can be found here www.aisystems.com.

Human Oversight/Governance

AI systems can greatly assist and enhance human decision-making. However, AI system users cannot abdicate their responsibility to make reasoned, sensible, and informed decisions regarding Firm business. Furthermore, AI systems are imperfect, and therefore oversight is both prudent and required.

Specifically, AI system users must ensure decisions that impact the Firm's internal operations, vendor management, and/or customer support are not made without oversight by the appropriate staff, who must make the final decision. Automated final decision systems are not permitted.

Each Department must ensure that outcomes and supporting decision methodologies are appropriately documented in instances where AI systems are used to support such

decisions. In that vein, an information owner must be appointed for each AI system used to support decision-making. The information owner will assist in performing ongoing governance, and is specifically responsible for periodically assessing the outputs of in-production AI systems to validate continuing reliability, safety, and fairness.

Technology Evolution

The commercial and open-source landscape of AI is rapidly evolving, and Departments should take steps to periodically ensure relevant AI systems continue to meet their business requirements in light of this evolving landscape. Open standards, model lifecycle management, and regular AI system retraining are all important elements that should be considered in assessing the continued use of a given AI system.

Intellectual Property

The legal landscape regarding intellectual property protections of AI systems and their outputs is also evolving. Departments should confer with the General Counsel's office regarding the intellectual property implications of using AI systems, including for example, using copyrighted materials as inputs into an AI system or the extent to which a work created by an AI system may contain copyrighted elements.

AI System Risk Assessment and Management

Each Department must conduct an annual risk assessment for each approved AI system. This assessment must include a review of all security, privacy, legal, reputational, and competency risks as well as any additional risks specified in this Policy. Such an assessment is in addition to any technical or security risk assessment required by other Firm policies.

AI System Security

AI systems and their use must comply with the Firm's *Information Security Policy*. To that end, Departments must implement and maintain required security controls. The Information Technology Department has sole responsibility for determining these controls and whether an AI system comports with the Firm's security requirements. Therefore, it also possesses the ultimate authority in approving or denying use of an AI system on security grounds.

AI System Inventory

Each Department must create and maintain an inventory that identifies the AI systems in use and in scope under this Policy. This inventory must be submitted to the IT Department and must be updated annually.

Privacy Requirements

All applicable privacy requirements, laws, and regulations must always be obeyed. Particular attention should be paid to the limited occasions when a Department identifies a requirement to use an AI system to process personally identifiable, confidential, or sensitive information. Note such circumstances represent an exception to this Policy, and require the approval of the General Counsel in advance (see "Policy Compliance and Exceptions" below). Departments should consider performing the following measures if an exception affecting privacy is granted.

- Developing a privacy impact assessment.
- Implementing privacy-oriented settings, including data minimization, such as only processing data that is necessary during the development and use of the AI system.
- Implementing data retention settings that follow the requirements of federal and state standards.
- Ensuring the accuracy of data entered into the AI system and the AI system's outputs.
- Data disposal once the purpose of using the data has been fulfilled, when possible, in compliance with applicable state and federal laws.
- Providing data subjects with control and transparency with respect to data processing.

Policy Compliance and Exceptions

This policy takes effect upon publication, and compliance is required with all enterprise policies and standards. The Firm may amend its policies and standards at any time, and compliance with amended policies and standards is also required. If compliance with this Policy is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, Departments must request an exception from the Office of General Counsel and/or the IT Department. Note the relevant Department head must provide written concurrence with the request for a policy exception.

Policy Questions

Questions regarding Policy limits and/or interpretation should be directed to the Office of General Counsel. Questions regarding information technology or information security should be directed to the IT Department or the Chief Information Security Officer.