Artificial Intelligence Use Policy

[Insert Date]

I. Introduction

_____ (the "Firm") is committed to the lawful, ethical, and secure use of artificial intelligence and machine learning technologies. This Artificial Intelligence Use Policy (the "Policy") establishes the requirements for using generative artificial intelligence tools –including, but not limited to, Claude, Copilot, ChatGPT, Gemini, etc. – at the Firm. This Policy applies to all Firm directors, officers, board members, employees, contractors, and other representatives (collectively, "Firm Representatives").

II. Responsibilities

A. Business Owners

A Firm Representative must be the "Business Owner" for each approved AI System. The Business Owner is responsible for documenting the business purpose, approved users, approved data types, human-review requirements, operational procedures, and ongoing use of the system.

B. Users

All Firm Representatives must use AI Systems only as approved, protecting Confidential Information and Personal Information, reviewing AI outputs, reporting suspected misuse or incidents, and complying with this Policy.

C. Chief Compliance Officer

The Chief Compliance Officer is responsible for the administration of this Policy.

III. Permitted, Restricted, and Prohibited Uses

A. Use of Embedded AI Tools In Approved Software Does Not Need Separate Approval

"Embedded AI Tool" means AI functionality embedded in existing software approved for use by the Firm, where the AI functionality is used only within the ordinary approved purpose of that

software. This does not require separate AI approval. These may be used without separate approval only if:

- The underlying software is already approved by the Firm;
- The AI functionality is used only for the software's ordinary approved purpose;
- No Personal Information, Confidential Information, material non-public information ("MNPI"), source code, credentials, or other restricted information is entered unless approved by the Business Owner and Chief Compliance Officer; and
- Use does not create external communications, client deliverables, compliance decisions, investment recommendations, marketing claims, or other outputs without review and approval as necessary under the Firm's compliance procedures.

B. Permitted Uses of AI

AI may be used only for approved business purposes and only in accordance with the approved use case, data restrictions, and human-review requirements. Examples of potentially permitted uses, if approved, include: internal productivity assistance; drafting or summarizing non-confidential internal materials; organizing non-sensitive internal information; creating first drafts subject to human review; internal operational analysis; compliance workflow support; cybersecurity monitoring support; and client-service workflow support where data protections are approved.

C. Restrictions on the Use of Personal and Confidential Information with AI

Personal Information and Confidential Information may be used with AI only where:

- The use case has been approved by the Business Owner and the Chief Compliance Officer;
- The system is approved for that data type;
- The data is redacted, anonymized, pseudonymized, tokenized, encrypted, or otherwise protected as required;
- Vendor terms prohibit unauthorized retention, reuse, disclosure, or training;
- Required privacy, Regulation S-P, contractual, and consent requirements are satisfied;
- Access is limited to authorized users; and
- Outputs are reviewed by qualified personnel.

D. Prohibited Uses of AI

Unless expressly approved by the Business Owner and the Chief Compliance Officer, Firm Representatives are prohibited from:

- Entering Personal Information into any Open Access AI System;
- Entering Confidential Information into any Open Access AI System;
- Entering MNPI, non-public portfolio data, client account information, financial planning information, tax or estate information, or sensitive operational information into any unauthorized AI System;

- Entering credentials, passwords, API keys, private keys, tokens, source code, or security architecture information into unauthorized AI Systems;
- Using public SaaS large language models for compliance, client, investment, trading, portfolio, or fiduciary decisions;
- Training AI models on raw, non-anonymized Personal Information or Confidential Information without a documented risk mitigation plan and required approvals;
- Using AI as a substitute for legal counsel;
- Using AI to make final investment, trading, portfolio, compliance, legal, employment, or client decisions without required human review and approvals;
- Using AI to generate external communications without required review;
- Using AI to create or publish misleading, unsupported, exaggerated, or unsubstantiated claims about the Firm's AI capabilities;
- Using AI to categorize or evaluate individuals based on protected class status;
- Using AI to generate illegal, discriminatory, harassing, harmful, deceptive, or inappropriate content;
- Using AI for personal purposes on company systems without authorization; and
- Attempting to bypass AI security, access, logging, monitoring, prompt boundaries, or usage restrictions.

IV. Approval of AI Systems

A. Business Owner

Except for Embedded AI Tools used as described above, no AI System may be used for the Firm's business unless approved by Firm management, including the Chief Compliance Officer. Before submitting a request, the requester must provide sufficient information for review and include:

- Name of the AI System, vendor, and product;
- Description of the proposed use case;
- Business owner and proposed users;
- Data types to be processed, including whether Personal Information, Confidential Information, non-public portfolio data, MNPI, credentials, source code, or API keys may be involved;
- Whether the system is open, closed, enterprise, on-premise, isolated cloud, public SaaS, or third-party hosted;
- Whether prompts, files, outputs, logs, or data are retained or used for training; and
- Whether the use case involves marketing, client communications, investment analysis, compliance, surveillance, or other high-risk functions.

B. Firm Review

Upon receiving the Business Owner's request, the Firm must review and document contractual terms addressing: data usage; training reuse; data retention; data deletion; confidentiality;

incident notification; model tuning rights; ownership of inputs and outputs; and termination and data return or destruction.

V. Output Review

AI-generated content has the potential to be inaccurate, misleading, entirely fabricated, and/or may contain copyrighted material. AI Systems should not replace human judgment in critical decision-making processes where human intervention and oversight are necessary. AI-generated output must be reviewed by a qualified human before it is relied upon, used in a decision, sent externally, entered into client records, used in compliance records, published, or incorporated into business-critical work.

In addition, AI-assisted external communications must be reviewed under applicable communication, advertising, disclosure, and compliance procedures before use.

VI. Incident Response and Reporting

Firm Representatives must immediately report suspected or actual AI-related incidents, policy violations, security events, unauthorized disclosures, or misuse to their manager and the Chief Compliance Officer. This includes, but is not limited to:

- Entry of Personal or Confidential Information into an unauthorized AI System;
- Unauthorized AI access or use;
- AI output containing Confidential Information or Personal Information that should not have been disclosed;
- Vendor breach or suspected vendor misuse of data;
- AI-generated phishing or impersonation attempts.

VII. Non-Compliance

Violations of this Policy may result in disciplinary action, up to and including termination of employment or contract, termination of system access, vendor termination, reporting to regulators, client notification, or legal action. No person will be subject to retaliation for reporting suspected misconduct or policy violations in good faith.

VIII. Other Definitions

“Artificial Intelligence” or “AI” means the use of machine learning technology, software, automation, models, algorithms, or related systems to perform tasks, generate content, make predictions, identify patterns, produce recommendations, automate workflows, or support decisions based on data, prompts, rules, models, or instructions.

“AI System” means any software, platform, model, application, embedded tool, workflow, API, agent, machine learning model, large language model, generative AI tool, vector database, retrieval-augmented generation system, or automated system that uses AI or machine learning functionality.

“Confidential Information” means non-public Firm information, trade secrets, proprietary information, business plans, source code, credentials, API keys, operational data, compliance information, cybersecurity information, employee information, and any information that could harm the Firm, its clients, or its business if disclosed.

“Open Access AI System” means an AI System where prompts, inputs, outputs, uploaded files, or user data may be retained, reused, reviewed, or used to train or improve a model for the benefit of other users or the provider.

“Personal Information” means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular person or household. This includes information concerning any client, prospective client, investor, account, portfolio, transaction, financial plan, investment objective, tax or estate matter, account credential, or other non-public client matter.

Annex I: AI Approval Checklist

Before an AI System is approved, the requester and reviewing functions should address the following:

Item	Required Information
Business purpose	What business need does the AI System address?
Owner	Who is the business owner?
Users	Who will use the system?
Environment	Public SaaS, enterprise SaaS, isolated cloud, on-premise, test, development, or production?
Data	What data will be entered, uploaded, processed, stored, or generated?
Personal information	Will Personal Information be used?
Confidential information	Will firm confidential information, source code, API keys, or credentials be used?
Training reuse	Will vendor or model provider use inputs or outputs for training?
Retention	What prompts, files, logs, outputs, or artifacts are retained and for how long?
Vendor diligence	Has vendor due diligence been completed?
Logging	Are prompts, usage, admin activity, API calls, and changes logged?
Output review	What human review is required before reliance or external use?

Disclaimer

This template is provided by Ryan P. Smith Law, PLC for general informational and educational purposes only. It is not legal advice and does not create an attorney-client relationship. Every organization's legal, regulatory, contractual, and operational requirements are different, and this template may not be appropriate for every business or industry. Users should consult qualified legal counsel before adopting, modifying, or relying on this template to ensure it complies with applicable laws and regulations and is appropriately tailored to their organization's needs.