intellicents investment solutions inc.
Artificial Intelligence Acceptable Use Policy

May 2026

1. Purpose and Scope

This Artificial Intelligence Acceptable Use Policy (the "AUP" or "Policy") establishes the rules governing how supervised persons of intellicents investment solutions inc. ("iis" or the "Firm") may use artificial intelligence ("AI") technologies in connection with the Firm's investment advisory business. This Policy is adopted pursuant to Rule 206(4)-7 under the Investment Advisers Act of 1940, as amended (the "Advisers Act"), and is incorporated into and governed by the Firm's Compliance Manual and Code of Ethics.

iis recognizes that AI tools, when properly governed, can enhance efficiency, accuracy, and client service. iis also recognizes that the unsupervised or undisclosed use of AI tools can expose the Firm and its clients to risks including breach of fiduciary duty, violation of confidentiality obligations, recordkeeping failures, marketing rule violations (including "AI washing"), data privacy breaches under Regulation S-P, hallucinated or inaccurate output, and the loss of client trust.

This Policy applies to all supervised persons of iis, including officers, employees, independent contractors who function as employees, and temporary personnel designated by the Chief Compliance Officer ("CCO") (collectively, "Supervised Persons"). It applies to all AI tools, whether provided by iis, contracted by iis with a third-party vendor, or accessed independently by a Supervised Person, regardless of device or location.

iis's posture toward AI is restrictive: only AI tools expressly approved by the CCO may be used in connection with iis business, and any new tool, use case, or material change to an existing tool requires CCO pre-approval. Personal, recreational use of AI on personal devices and personal accounts is outside the scope of this Policy, except where it interacts with iis information, clients, or business activities.

2. Definitions

For purposes of this Policy, the following terms have the meanings set forth below.

Term	Definition
Artificial Intelligence ("AI")	Any computational system that performs tasks typically associated with human cognition, including but not limited to natural language processing, content generation, prediction, classification, summarization, recommendation, and decision support. AI includes machine learning, deep learning, neural networks, and large language models ("LLMs").
Generative AI	A subset of AI that produces new content (text, images, audio, code, or video) in response to a prompt, including LLM-based assistants such as ChatGPT, Claude, Gemini, and Microsoft Copilot, as well as the Firm's internal intelliGPT tool.
intelliGPT	The Firm's proprietary, internally developed generative AI tool, hosted within the Firm's controlled technology environment and approved for the use cases specified in Section 5 of this Policy.
Embedded AI	AI features built into third-party software the Firm already uses (for example, AI features within Salesforce, Laserfiche, eMoney, Microsoft 365, or any custodian platform). Embedded AI is governed by this Policy regardless of whether it is enabled by default.
Public/Consumer AI	AI services accessed via a public website, mobile app, or free-tier account where the user is the natural person and the provider has no enterprise contract with iis (e.g., a personal ChatGPT, Claude, Gemini, Perplexity, Grok, or DeepSeek account).
AI Output	Any text, code, image, summary, recommendation, draft, transcript, or other content produced in whole or in material part by an AI tool.
Confidential Sensitive Information ("CSI")	As defined in the Cybersecurity section of the Compliance Manual, including Personally Identifiable Information ("PII"), Company Inside Information, and Firm Inside Information. For the avoidance of doubt, this includes plan participant data, client account numbers, financial information, holdings, beneficiary information, health information, and any nonpublic information about prospective and current clients of the Firm.
Approved AI Tool	An AI tool that appears on the AI Tool Inventory maintained by the CCO and the Chief Technology Officer ("CTO"), for use in the specific use cases listed for that tool.
Human-in-the-Loop	A workflow in which a qualified Supervised Person reviews, validates, and (where applicable) edits AI Output before that output is used to inform a recommendation, sent to a client, filed with a regulator, or treated as a Firm record.

Term	Definition
AI Washing	Marketing or disclosure that overstates, fabricates, or misleadingly describes the Firm’s use of AI or its AI capabilities. The Securities and Exchange Commission ("SEC") has identified AI washing as a Marketing Rule violation under Rule 206(4)-1 and has brought enforcement actions on this basis.

3. Governing Principles

Every use of AI by a Supervised Person, regardless of tool, must satisfy each of the following principles. These principles control whenever this Policy or any approved tool documentation is silent or ambiguous.

Fiduciary Duty First

iis is a fiduciary under the Advisers Act and, where applicable, under Sections 3(21)(A)(ii) and 3(38) of the Employee Retirement Income Security Act of 1974, as amended ("ERISA"). No use of AI may compromise the duties of loyalty, care, or full and fair disclosure owed to clients. AI is a tool that supports human judgment; it never replaces it.

Human Accountability

A Supervised Person who uses AI is fully accountable for the accuracy, appropriateness, and compliance of any AI Output they produce, share, send, file, or rely upon, exactly as if the Supervised Person had produced it personally. "The AI told me" is not a defense.

Confidentiality and Data Minimization

Supervised Persons may not input CSI, PII, Firm Inside Information, or Company Inside Information into any AI tool except where (i) the tool is an Approved AI Tool, (ii) the use case is one for which that tool has been approved, and (iii) the input has been minimized to only what the use case requires. The default is to input no client-identifying information at all.

Books and Records

All AI use that produces a record of the type required by Rule 204-2 under the Advisers Act (including communications relating to recommendations or advice, and certain working papers) must be conducted on or captured by an Approved AI Tool whose output can be retrieved upon request. Use of personal or unapproved AI for these purposes is the AI equivalent of off-channel communication and is prohibited.

Accurate Disclosure

iis will not represent its use of AI in marketing materials, Form ADV, Form CRS, RFP responses, or client communications in a manner that is exaggerated, fabricated, or misleading. Material AI capabilities used in client-facing services will be disclosed accurately, and material limitations will be disclosed where required for the disclosure not to be misleading.

Vendor Discipline

Any AI tool used by iis, including embedded AI features in software the Firm already uses, is subject to the Firm’s vendor and service-provider oversight obligations, including those imposed by the 2024 amendments to Regulation S-P (which require, among other things, that service providers notify iis of unauthorized access or use of customer information no later than 72 hours after becoming aware of it).

Proportionality

The level of review, validation, and documentation required for an AI use case scales with the impact of the output. AI Output that informs investment recommendations, that is sent to a client, or that becomes a Firm record receives the highest level of review.

4. Approved AI Tools

The CCO and the CTO maintain a written AI Tool Inventory listing all AI tools approved for use in connection with iis business. The Inventory specifies, for each tool, the approved use cases, data classifications permitted as input, the supervised persons authorized to use the tool, and the review or attestation cadence applied to it. The current Inventory is maintained on Laserfiche and is accessible to all Supervised Persons. Supervised Persons must consult the Inventory before relying on any AI tool for iis business.

A Supervised Person who wishes to use an AI tool not on the Inventory, or to use an Approved AI Tool for a use case not listed for it, must submit a written request to the CCO before any such use. The request must describe the tool, the proposed use case, the data that would be input, the vendor (including a copy of the vendor’s applicable terms of service, privacy policy, data-handling and breach-notification commitments, and any SOC reports), and the expected business benefit. The CCO will evaluate the request in coordination with the CTO and the Chief Investment Officer ("CIO"), and will respond in writing.

Approval may be conditional, time-limited, or limited to a pilot group. Approval may be revoked by the CCO at any time. The CCO will document the rationale for each approval, conditional approval, and denial.

Tool Categories Currently Recognized by the Firm

- Internal generative AI: intelliGPT (Firm-hosted; controlled environment).
- Enterprise productivity AI: as approved on the Inventory and only for the data classifications listed there.

- Embedded AI: AI features inside software iis already licenses (e.g., CRM, planning, archiving, and custodian platforms). These features may be enabled only after CCO and CTO confirmation that the feature has been assessed and added to the Inventory.
- Public/Consumer AI: prohibited for any iis business purpose, except where the CCO has expressly approved a specific, narrow non-confidential use case in writing.

5. Permitted Use Cases (with Guardrails)

Subject to Section 3 (Governing Principles) and Section 4 (Approved AI Tools), the following categories of use are generally permitted when conducted on an Approved AI Tool. "Permitted" does not mean unsupervised — every use must comply with the guardrails set out in this Section and elsewhere in the Policy.

Internal Drafting and Editing Assistance

Drafting first-pass internal memos, project notes, summaries of public regulatory developments, training material outlines, internal email drafts, meeting agendas, and similar non-client-facing material. The Supervised Person must read, validate, and revise output before treating it as work product.

Research Support

Summarizing publicly available regulatory releases, research papers, fund prospectuses, or news, with the explicit understanding that AI Output may contain hallucinations. Any factual assertion in AI Output that is to be relied upon must be verified against an authoritative source. AI may not be cited as the sole or primary source for any investment view, written advice, or client deliverable.

Marketing and Communications Drafting

Drafting initial copy for advertisements, blog posts, newsletters, social media content, and similar communications, only if the resulting material is reviewed by the CCO (or designee) under the Marketing Rule procedures in the Compliance Manual before any use or dissemination. AI-generated marketing must not contain testimonials or endorsements that were not given by real persons identified to the Firm, must not include performance data unless the underlying performance has been verified by the CIO, and must not describe iis's use of AI in any way that is exaggerated or misleading.

Meeting Notes and Transcription

Use of AI-driven meeting transcription, note-taking, or summarization tools is permitted only when (i) the tool is an Approved AI Tool on the Inventory, (ii) all participants have been informed and have consented in advance to recording and AI processing, (iii) the resulting transcript or summary is captured into Firm systems and retained per Rule 204-2 retention schedules, and (iv) any client meeting notes generated by AI are reviewed by the IAR before being saved as a Firm record. Use of personal or unapproved transcription apps for client meetings is prohibited.

Operational and Compliance Workflow Support

Internal use cases such as drafting compliance procedures, generating checklists, summarizing internal documents, organizing files, and similar operational tasks. CSI must not be input into any tool unless the tool is approved for that data classification.

Code and Spreadsheet Assistance

Generating or modifying code or spreadsheet formulas for internal tools and analytical work, provided that any output that affects client billing, performance, fee deduction, or trade processing is independently tested and reviewed before deployment.

Client Service Drafting (Limited)

Drafting initial responses to client questions of a routine, non-advice nature (for example, scheduling, document delivery confirmations), with the IAR or relationship manager reviewing, editing, and sending the final communication from a Firm-monitored channel. Initial drafts of communications relating to investment advice, recommendations, or other fiduciary matters require the same level of human authorship and review as if AI had not been used.

6. Prohibited Use Cases

The following uses are prohibited at all times, on any tool, on any device, by any Supervised Person, regardless of approval status of the tool. Violations may result in sanctions up to and including termination, and may be reported to regulatory authorities where required.

- Inputting CSI, PII, client account numbers, plan participant data, holdings, social security numbers, dates of birth, login credentials, or any nonpublic client or Firm information into any Public/Consumer AI tool, free-tier service, or any other tool not on the Inventory and approved for that data classification.
- Using AI to generate, fabricate, or "round out" performance information, investment track records, case studies, testimonials, or endorsements that are not factually accurate.
- Misrepresenting the Firm's use of AI in marketing, RFP responses, due diligence questionnaires, Form ADV, Form CRS, or any other client- or regulator-facing document, including by overstating AI capabilities, misdescribing AI involvement in investment processes, or implying AI sophistication that does not exist ("AI washing").
- Using AI to make autonomous, unsupervised investment recommendations or trading decisions for any client account or plan, or to construct portfolios, asset allocation strategies, or fund line-ups without CIO and Investment Committee oversight as required by the Compliance Manual.
- Inputting client communications, plan documents, IPSs, custodial statements, or due diligence files into any tool not approved for that data classification, or in any manner inconsistent with the Firm's confidentiality obligations.

- Using AI to draft, polish, or assemble communications that occur on personal devices, personal accounts, or platforms that are not captured by Firm archiving (Global Relay, CellTrust, or other approved channels). This is treated as off-channel communication.
- Using AI to circumvent compliance reviews, supervisory approvals, the Firm's Marketing Rule procedures, or any other policy or procedure of the Firm.
- Using AI in a manner that infringes on third-party intellectual property, violates a vendor's terms of service, or breaches a confidentiality or non-disclosure obligation owed by the Firm.
- Connecting any AI agent, plugin, browser extension, or autonomous workflow to Firm systems, custodian portals, archival systems, email, or client data without prior written approval from the CCO and CTO.
- Sharing intelliGPT credentials, API keys, or access tokens with any person inside or outside the Firm, or running unauthorized scripts or extensions against intelliGPT or any other Approved AI Tool.

7. Data Classification and Handling

Inputs to AI tools must be classified before use. The classifications below align with the Firm's Cybersecurity Policy and with the 2024 amendments to Regulation S-P, which apply to iis as a "covered institution" with assets under management exceeding $1.5 billion (and for which the compliance date for larger entities was December 3, 2025).

Classification	Examples	Permitted AI Use
Public	Information already published by the Firm or third parties, regulatory releases, public news, marketing materials already disseminated.	Permitted on any Approved AI Tool for any approved use case.
Internal	Internal memos, drafts, training material, agendas, internal SOPs (without identifying client data).	Permitted on intelliGPT and other tools approved for "Internal" data on the Inventory.
Confidential	Firm Inside Information, internal financial data, vendor contracts, employee personnel data (excluding PII).	Permitted only on tools expressly approved for "Confidential" data, and only for approved use cases.
Restricted (CSI/PII)	Client and plan participant PII, account numbers, social security numbers, holdings, beneficiary data, custodial statements, Company Inside Information.	Default = no AI use. Permitted only when expressly listed for a specific tool and use case on the Inventory and only with documented CCO approval.

When in doubt about classification, treat the data as one classification more restrictive than your initial assessment, and confirm with the CCO before proceeding.

8. Books, Records, and Off-Channel Considerations

Rule 204-2 under the Advisers Act requires iis to make and preserve specified records, including communications relating to recommendations or advice. AI-generated content that becomes such a record must be retained on Firm systems for the applicable retention period.

Supervised Persons must observe the following recordkeeping rules with respect to AI:

- Any AI-assisted communication sent to a client, prospective client, or plan sponsor must be sent from a Firm-monitored channel (Firm email, CellTrust, or another channel approved and captured by Global Relay or its successor archiving system).
- AI Output that is incorporated into a deliverable, Form ADV filing, marketing piece, internal compliance document, or client memo is retained as part of that deliverable, in accordance with Rule 204-2 retention schedules.
- Working drafts and prompts that materially influenced a deliverable should be preserved within the Approved AI Tool's history or, where unavailable, exported and saved to Laserfiche.
- Use of an unapproved or personal AI tool to draft business communications creates the same recordkeeping exposure as off-channel text or messaging. The SEC has imposed substantial penalties for off-channel communication recordkeeping failures, including against standalone investment advisers, and iis treats this as a high-priority compliance risk.

9. Marketing, Form ADV, and "AI Washing"

iis will not describe its use of AI in any marketing communication, advertisement, RFP response, due diligence questionnaire, Form ADV (including Part 2A), Form CRS, website content, or social media post unless the description is accurate, balanced, and substantiated.

All AI-related marketing language must be submitted to the CCO for review under the Marketing Rule procedures in the Compliance Manual before use. Substantiation supporting any AI-related claim (including descriptions of intelliGPT capabilities, AI involvement in research, or efficiency gains) must be retained for the period required by Rule 204-2.

The Firm will accurately describe its use of AI in Form ADV updates and other regulatory filings as required, will disclose material risks and limitations to clients where relevant, and will update those descriptions when material changes occur.

10. Vendor and Service Provider Oversight

Every vendor that processes Firm or client data using AI is subject to the Firm's service-provider oversight requirements, including those imposed by the 2024 amendments to Regulation S-P. The CCO, in coordination with the CTO and the Chief Financial Officer, will:

- Conduct documented due diligence on each AI vendor before approval, including assessment of data handling, training data use, model retention, encryption, access controls, regulatory exposure, organizational stability, and incident history.
- Require, by written contract, that AI vendors provide notice to iis of any unauthorized access to or use of customer information no later than 72 hours after the vendor becomes aware of it, and cooperate with the Firm's incident response.
- Require AI vendors to provide commitments regarding the use of Firm and client data, including (where applicable) commitments not to use Firm or client data to train the vendor's general models.
- Re-evaluate AI vendors at least annually, and earlier upon any material change, incident, or regulatory development.
- For embedded AI features added to existing software, evaluate the new feature before allowing its use and update the AI Tool Inventory accordingly.

11. Human Oversight Requirements

All AI-influenced output that is used to inform a recommendation, sent to a client, filed with a regulator, or treated as a Firm record must pass through Human-in-the-Loop review before that use. The reviewing Supervised Person:

1. Reads the entire output and verifies factual claims that are material to the deliverable.
2. Confirms that the output is consistent with the client's investment objectives, IPS, suitability profile, and the Firm's investment views.
3. Confirms that no CSI, PII, or other restricted information was inappropriately used as input.
4. Edits the output as needed and takes ownership of the final version.
5. Where required by another section of this Policy or the Compliance Manual, submits the output for CCO or CIO review.

12. Training and Awareness

Each Supervised Person is required to:

- Complete the Firm's AI training module upon hire, before being granted access to any Approved AI Tool.
- Complete annual AI refresher training, which will be coordinated with the Firm's annual cybersecurity and Code of Ethics training.
- Complete additional training when material changes are made to this Policy, when new tools are added to the Inventory, or when the CCO directs.

- Acknowledge, at least annually, receipt and understanding of this Policy by signing the AI Acceptable Use Policy Acknowledgment included as Appendix A to this Policy and incorporated into the Annual Employee Compliance Acknowledgement.

13. Reporting, Escalation, and Incidents

Supervised Persons must promptly report to the CCO any of the following:

- Any actual or suspected input of CSI or PII into a tool not approved for that data classification.
- Any AI Output that has been (or may have been) sent to a client, prospect, or regulator and contains a material inaccuracy.
- Any indication that a Supervised Person, vendor, or third party has misused intelliGPT or any other Approved AI Tool.
- Any apparent breach by an AI vendor of its data-handling, security, or notification commitments.
- Any unauthorized AI-driven activity in Firm systems, custodian portals, or client accounts.
- Any pattern of AI Output that appears biased, hallucinated at material rates, or otherwise unreliable for the use case in which it has been deployed.

Reports may be made to the CCO directly or through the Firm's whistleblowing channel, which permits anonymous reporting and prohibits retaliation, as set forth in the Compliance Manual.

Where an incident involves customer information, the Firm will follow its incident response program, including the customer notification requirements of amended Regulation S-P (which generally require notification of affected individuals as soon as practicable but no later than 30 days after determining that unauthorized access to or use of sensitive customer information occurred or is reasonably likely to have occurred).

14. Violations and Sanctions

Violations of this Policy may result in sanctions ranging from verbal reprimand and additional training, to suspension of access to AI tools, to disgorgement of any benefit obtained, to termination of employment, and where applicable, referral to regulatory or law enforcement authorities. Sanctions are determined by the CCO in consultation with the Firm's senior management and are documented in the Supervised Person's personnel file and in the annual compliance file.

Repeated, willful, or material violations are subject to escalated sanctions. A pattern of unauthorized AI use, or unauthorized use of AI involving CSI, will be treated by the Firm with the same seriousness as off-channel communications recordkeeping violations.

15. Governance, Review, and Amendment

This Policy is owned by the CCO. The CCO, in coordination with the CTO and CIO, will:

- Maintain the AI Tool Inventory and document approval rationales for each tool and use case.
- Review this Policy at least annually as part of the Firm's Rule 206(4)-7 annual compliance program review, and more frequently in response to regulatory developments or material changes in the Firm's use of AI.
- Conduct or commission periodic testing of compliance with this Policy, including reviewing communications, sampling AI Output where feasible, and reviewing the Inventory against actual use.
- Document the foregoing review and testing activities and include them in the annual compliance review report.

Material amendments to this Policy require approval by the CCO and will be communicated to all Supervised Persons promptly. Non-material clarifications may be made by the CCO and reflected in the next regularly distributed version.

Appendix A — AI Acceptable Use Policy Acknowledgment

I acknowledge that I have received, read, and understood the intellicents investment solutions inc. Artificial Intelligence Acceptable Use Policy dated May 2026 (the "AUP"). I understand that I am responsible for complying with the AUP at all times in the course of my duties for iis.

I specifically acknowledge:

- I will use only AI tools that appear on the Firm's AI Tool Inventory and only for use cases listed for those tools.
- I will not input Confidential Sensitive Information, Personally Identifiable Information, or other restricted data into any tool not approved for that data classification.
- I am personally accountable for any AI-assisted output I produce, send, file, or rely upon.
- I will conduct AI-assisted business communications only on Firm-monitored, archived channels.
- I will promptly report any actual or suspected violation of the AUP to the Chief Compliance Officer.
- I understand that violations may result in sanctions up to and including termination of employment.

______________________________________ ___________________

Printed Name *Date*

______________________________________ ___________________

Signature *Title / Role*

Return signed acknowledgment to the Chief Compliance Officer (Nicholas Holmes) and retain a copy in your personnel file.