Acceptable Use of Artificial Intelligence (AI) and Machine Learning (ML) Tools Policy

I. Scope

This *Acceptable Use of Artificial Intelligence (AI) and Machine Learning (ML) Tools Policy* (the "Policy") applies to Berkeley Research Group, LLC (BRG), its subsidiaries, and its affiliates worldwide. All employees of BRG and its direct and indirect subsidiaries or affiliated companies, from the most senior executives to entry-level professionals, are subject to the Policy. The Policy also applies to third parties acting on behalf and for the benefit of BRG. In addition to the terms of this Policy, the use of any AI/ML tools is subject to the terms of any applicable acceptable use terms associated with a specific AI/ML tool, along with all other BRG polices, including but not limited to BRG's privacy, data protection, HIPAA, inside information and insider trading, and confidential information policies.

II. Introduction

AI and ML are fast-evolving tools that have become widely available and pervasive in the field of technology. AI is transforming the way we work and has the potential to automate tasks, improve decision-making, and provide valuable insights into operations.

Although AI is a broad concept, this Policy focuses on two basic types:(1) generative and (2) task specific. Generative AI creates new content from existing materials (e.g., Copilot, ChatGPT). Task-specific AI addresses targeted needs. Examples include identifying trends and patterns in large datasets; predictive models to forecast future events; and automation of various processes such as customer support and fraud detection.

Microsoft Copilot is a Generative AI tool that is available to all BRG employees and can be used safely and securely when employees are logged in with their BRG credentials. For this reason, employees are highly encouraged to make Copilot their "default" AI tool. Employees should not use unapproved AI tools (e.g., the public version of ChatGPT) without first obtaining approval.

III. Purpose

While AI and ML tools can create new opportunities for BRG, these tools can also present challenges and risks to BRG's business, including:

- **Confidentiality breaches:** Information entered into AI/ML tools may enter the public domain. This can lead to civil and criminal violations of regulatory requirements and data privacy laws; breaches of client, vendor, and court-ordered agreements; or damages to intellectual property assets and ownership.
- **Accuracy:** AI/ML tools can, and do, get things wrong. Generative AI is known to produce factually incorrect or incomplete information (also called "hallucinations") that can be difficult to detect. Likewise, many AI/ML tools are trained are general datasets and may not be appropriate for more specialized tasks.
- **Introduction of bias and reputational concerns:** AI/ML tools may produce biased, discriminatory, or offensive content.
- **Insufficient security**: AI/ML tools may store sensitive data and information at risk of being breached or hacked.

This Policy establishes the standards for BRG's workforce on the responsible, ethical, and lawful use of AI for business purposes. AI tools should always be used in accordance with the **Guidelines for Responsible AI Use.**

IV. Policy

BRG recognizes that AI tools, in addition to providing many benefits, may pose risks to our operations and the individuals with whom we engage. BRG is committed to protecting the confidentiality, integrity, and availability of all firm, partner, and client data; and to the informed and responsible use of AI tools in compliance with applicable laws.

This Policy is largely focused on generative public large language models (LLM) and code generative models. Existing BRG policy and contractual requirements define the use and transmission of protected sensitive firm and client data. Current publicly accessible AI and LLM offerings do not control or restrict the types of data users post to the tool. As a result, BRG requires the use of "private" AI/ML services in any situation in which firm or client data is entered into a tool. These private AI/ML services offer similar features to public offerings, but BRG remains in control of its data and client information.

IV.i Requirements for AI Use

All workforce members must adhere to the following standards when using AI/ML tools:

1. **Evaluation of AI tools:** Prior to using any new AI/ML tool for business purposes, personnel must first contact both the Information Technology (IT) (ITTeamSecurity@thinkbrg.com) and Legal (legal@thinkbrg.com) departments to confirm that the proposed tool features adequate security, privacy, and data protections; and that BRG has the appropriate contractual terms in place. Any proposed use of new AI/ML tools must meet defined criteria as established by BRG's AI Steering Committee.

   BRG IT will provide BRG personnel with access to trusted and approved LLMs for handling sensitive firm and client information. Do not download or otherwise integrate an AI/ML tool into BRG's information systems without prior approval from the IT Information Security Team **("InfoSec")** (ITTeamSecurity@thinkbrg.com) for such integration. For clarity, approval to use an AI tool by a client does not grant approval to integrate that tool into BRG's corporate environment, which requires a separate approval. Approved AI tools must be used as directed in this Section IV of this Policy.

2. **Data protection:** Do not upload or input into an AI tool any data that is confidential, proprietary, or protected by applicable laws, unless such upload or input has been approved by BRG InfoSec. This restriction applies to all publicly available AI/ML tools. The following types of data should never be uploaded, shared, or used in querying with public AI/ML tools:

   a. **Client Information** (see also BRG's policies related to protecting Proprietary Confidential Information, Trade Secrets, and Data Classification)

   b. **Personal Data, Personal Information, or Protected Health Information** (see also BRG's Privacy Policy, Data Protection Policy, HIPAA Policy, etc.).

   c. **Material Non-Public Information** (see also BRG's Inside Information and Insider Trading Policy)

   d. **Confidential or Trade Secret Information** (see also BRG's policies related to protecting Proprietary, Confidential Information, Trade Secrets, and Data Classification)

   e. **Intellectual Property and/or Proprietary Source Code** (see also BRG's policies related to IP protection)

3. **Configure the Tool for Maximum Confidentiality:** Reputable AI/ML tools provide data control settings to limit how the AI uses information input by users. When using BRG-approved AI/ML tools for BRG-related work, the data controls must be configured to prevent the AI from utilizing user inputs to train the AI, to the extent allowed by the AI provider. History should also be set to delete automatically and as frequently as possible. Always employ strong passwords but do not use the same passwords to authenticate to the AI as you use to sign into BRG's network. If you have questions on how to adjust data control settings within an approved AI tool, please contact ITTeamSecurity@thinkbrg.com .

4. **Before Entering Information, Consider Downstream Consequences:** Before entering information into an AI tool, ask yourself whether BRG or individuals could be harmed if the information appeared publicly. If so, do not enter the information into an AI/ML tool without prior approval from InfoSec. Preferably, sensitive or personal data that is uploaded to a BRG-approved AI/ML tool should be anonymized or encrypted.
5. **Use Caution in Trusting Results and AI Ethics:** Because AI is still a developing technology, there are concerns about the accuracy of results, built-in biases against marginalized groups, and a lack of transparency relating to the sources from which the AI generates its content. Always consider disproportionate impacts or unintended consequences before employing an AI solution. Additionally, for AI/ML that generates images, audio, or video, using such generated content could give rise to legal risks related to IP infringement. Do not rely exclusively on AI tools in decision-making. You must always validate results against vetted, trusted sources. You may not publish any generated content on internal or external BRG channels without prior approval from Legal and Marketing.

IV.II USER Responsibility

Ultimately, BRG personnel must use common sense and exercise caution when leveraging AI/ML technologies. BRG personnel should keep in mind the needs and preferences of our clients in using an AI tool for work purposes. BRG personnel are fully responsible for the quality and integrity of their work products as well as the contents' compliance with applicable rules, ethics, and regulations.

V. Compliance

Failure to comply with this Policy or any other BRG security policy shall result in disciplinary actions as per BRG's Employee Handbook. Legal actions may also be taken for violations of applicable regulations and standards.