**Purpose**

This policy identifies acceptable use of generative artificial intelligence (AI) tools including ChatGPT. AI can enhance productivity but can introduce security and privacy risks as they can leak sensitive data or provide inaccurate information.

**Scope**

This policy applies to all firm employees in situations where the employee’s action, either directly or through a third party such as a vendor, may expose the firm’s systems or data to generative AI tools.

**Policy**

The firm will maintain a list of approved AI tools which will be classified as Allowed; any unlisted tools will be defined as Constrained.

For all allowed tools, the firm shall identify which categories of data they are certified to handle.

**The Technology Committee/Partner (or equivalent) shall:**

* Advise the firm on the initial creation and maintenance of the generative AI tool database.
* Review licenses for allowed generative AI tools included in this database and other information provided by their publishers to determine if these tools are constrained or allowed.

**All employees shall:**

* Only use firm-licensed, -provided, or -built generative AI tools in accordance with the Acceptable Use Policy (AUP) / Network Use Policy / or other equivalent HR policy.
* Only log in to generative AI tools using their firm email or credentials.
* Assume a generative AI tool to be constrained unless the firm has designated otherwise.
* To the maximum extent possible, opt-out of data sharing with the tool’s vendor.

Never input the following categories of data into generative AI tools:

* Personally Identifiable Information (PII), as defined by the Department of Labor1, or Protected Health Information (PHI), as defined by the Health Insurance Portability and Accountability Act (HIPAA)2, with the following exceptions:

1 “Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.”

2 “The HIPAA Privacy Rule provides federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that information.”

* + The employee’s own PII or PHI. The firm discourages this practice, makes no warranties regarding what will happen to the data, and notes that many generative AI tools advise against doing so.
  + PII or PHI that the owner of the data in question has intentionally published on the Internet or other public media while not under duress and which the firm has no obligation to protect. For example, a medical diagnosis posted on social media by a public figure could be inputted into a generative AI tool if done in accordance with the AUP.
* Material non-public information (MNPI), as defined by the Securities and Exchange Commission (SEC).
* Passwords, application programming interface (API) keys, or any other secrets that would allow an otherwise unauthorized actor to gain access to the firm's systems or data.
* Any other firm information identified by the firm’s Technology Committee/Partner.

Only input data into generative AI tools that the firm has approved the generative AI tool to handle. For example, if the firm approves a generative AI tool to handle social security numbers but not medical diagnoses, you may input the former but not the latter.

While the publication of individual pieces of information might not violate this policy, it is important to note that generative AI tools are constantly ingesting publicly available information for training purposes. This could allow such a tool to infer - and reproduce - information not intended to be made public. If the employee has any doubt, s/he shall request permission in writing from the Technology Committee/Partner.

Do not treat generative AI tools responses as error-free. Pay special attention when reviewing responses to security-related questions or in security-sensitive situations, such as when they:

* Generate code snippets in response to a prompt;
* Provide information regarding supposed best practices for system design;
* Offer risk management advice in cybersecurity, privacy, legal, or physical safety contexts.

Report to the Technology Committee/Partner (or equivalent) any indications that a generative AI tool is doing any of the following without explicit prompting:

* Attempting to escalate privileges, gain access to sensitive data, or interact with the physical world.
* Intentionally deceiving any human being for any reason.

Firm management shall ensure all employees in their practice group are trained and have acknowledged this policy within 30 days of publication.

The firm will ensure that all software vendors and other parts of the software supply chain are following a generative AI policy that is substantially similar to the firm’s.

In the event of termination of a software or service vendor and their contract with the firm, the firm will ensure the entity is forbidden from further use of the firm’s data in generative AI tools within 30 days of termination.

**Compliance**

Non-compliance with this policy may result in disciplinary action, up to and including termination.

If federal, state, local, or tribal laws or regulations conflict with this policy, the former shall control.

Should any firm employee violate this policy two or more times within a 365-day period, the firm shall ensure:

* A root cause analysis is conducted, documented, and the results shared with the Technology Committee/Partner;
* A complete retraining for the employee; and
* Re-acknowledgement by all employees of this policy.

**Definitions**

Generative Artificial Intelligence (AI): a subset of AI techniques that uses algorithms to generate new, original data. Unlike traditional AI, which is designed to solve specific tasks based on pre-existing data, generative AI algorithms can produce new data that has never been seen before.

Constrained generative AI tool: one with which the firm has no legal relationship except for a click-through license agreement, and which has made no specific guarantees regarding the confidentiality of information provided to it.

Approved generative AI tools: one with which the firm has a legal relationship in addition to a click-through license agreement (or has such a license which the Technology Committee/Partner (or equivalent)- has affirmatively categorized as Approved) that makes specific guarantees regarding the confidentiality of information provided to it.

**References**

<https://www.blog.deploy-securely.com/p/deploying-securely-with-chatgpt>

<https://compliancerisk.io/2023/04/acceptable-use-policy-for-ai-tools/>

<https://www.shrm.org/ResourcesAndTools/legal-and-compliance/employment-law/Pages/generative-AI-policies-intellectual-property.aspx>