[insert company logo]

[insert organization name]

Protecting [insert Organization name] Data with Artificial Intelligence (AI)Technology

[insert published date]

Version [insert version number]

Document Number: Protecting [insert organization name] Data With AI Technology

Table of Contents

Table of Contents

Document Information 3

Revision History 3

Approval 4

Introduction 4

Purpose 4

Scope 4

Background 5

Policy 7

Rules of Engagement 7

OpenAI Usage Policy 7

Document Information

Revision History

Version	Author / Reviewer	Description of Change	Date
0.1	Initial Draft	Initial Draft	
0.2	SME Author	AI SME revisions	
0.3	Department Head	Additional updates	
0.3	[insert organization name] Technology Leadership Review	Leadership comments and revisions	
0.4	SME Author	Incorporate comments from reviewers	
1.0	[insert organization name] Management Leadership Review	Final Approval	

Approval

Version	Approver	Organization	Approved
Protecting [insert organization name] Data With AI Technology V1.0			
	[insert name], CEO	**[insert organization name]**	
	[insert name], CIO	**[insert organization name]**	

Introduction

Purpose

This policy defines the parameters necessary to ensure that [insert organization name] protects organizational data while utilizing Artificial Intelligence (AI) software or similar technology that utilizes a knowledgebase that can potentially capture input and output data for the use by the knowledgebase. For purposes of this document, [insert organization name acronym] means [insert organization name] and all its affiliated companies.

Scope

The scope of this policy is to guide the use of any Artificial Intelligence platform, such as OpenAI, for [insert organization name] and client work to protect [insert organization name] and our data assets. Where the policy is only germane to a specific platform, that platform will be referenced by its specific name.

Background

OpenAI Software

OpenAI is the provider that builds generative large language models using a technology called deep learning, which leverages large amounts of data to train an AI system to perform a task. This technology is packaged in multiple ways:

- GPT-4 is the most current version of the underlying model that is used by the interfaces in the bullets below. It uses a broad general knowledge and domain expertise to follow complex instructions in natural language and solve difficult problems with accuracy. GPT-4 is available on ChatGPT Plus and as an API for developers to build applications and services.
- ChatGPT Plus (https://chat.openai.com/) is a chatbot user interface for users to send prompts to the GPT-4 large language model. It is a pilot subscription plan for ChatGPT. It offers availability even when demand is high, faster response speed, and priority access to new features. There are no configurations that can be made to temperature (I.e., creativity), token limits (I.e., verbosity), adjustments to the version (e.g., Davinci, Ada) or custom prompt/response models.
- **ChatGPT** is the free version of ChatGPT Plus which has limitations on content output size and connectivity duration. While this tool is new it has often been overwhelmed with requests and is often at capacity and unavailable. Like ChatGPT Plus, there are no configurations that can be made in this interface.
- **Playground** is an interface that currently uses GPT-3 as the underlying large language model. It can be used with free plans and subscription plans. When subscription plans are used the costs are based on the amount of text sent and received by the user in units called "tokens". One token is approximately one word. In the Playground interface a user can make many configurations to temperature, token limits, adjustments to the version or custom prompt/completion models.
- OpenAI Application Programming Interface (API) allows a developer to interact with the API through HTTP requests from any language, via OpenAI's official Python bindings, OpenAI's official Node.js library, or a community-maintained library. The API allows for configurations to temperature, token limits and adjustments to the version.
    - **Patterns** is an AI application development platform that leverages OpenAI's API. Marketplace and other [insert organization name] Patterns AI applications can be cloned and configured for [insert organization name] use cases in this tool. The tool opens the ability to recursively submit API calls on large bodies of text. The amount of text that can be submitted and returned is limited in all of the other interfaces, while

there are theoretically no limits on the amount of text that can be submitted and returned via the API through Patterns.

OpenAI Terms of Use

The following is extracted from OpenAI's Terms of Use:

(a) Your Content. You may provide input to the Services ("Input"), and receive output generated and returned by the Services based on the Input ("Output"). Input and Output are collectively "Content." As between the parties and to the extent permitted by applicable law, you own all Input. Subject to your compliance with these Terms, OpenAI hereby assigns to you all its right, title and interest in and to Output. This means you can use Content for any purpose, including commercial purposes such as sale or publication, if you comply with these Terms. OpenAI may use Content to provide and maintain the Services, comply with applicable law, and enforce our policies. You are responsible for Content, including for ensuring that it does not violate any applicable law or these Terms.

(b) Similarity of Content. Due to the nature of machine learning, Output may not be unique across users and the Services may generate the same or similar output for OpenAI or a third party. For example, you may provide input to a model such as "What color is the sky?" and receive output such as "The sky is blue." Other users may also ask similar questions and receive the same response. Responses that are requested by and generated for other users are not considered your Content.

(c) Use of Content to Improve Services. We do not use Content that you provide to or receive from our API ("API Content") to develop or improve our Services. We may use Content from Services other than our API ("Non-API Content") to help develop and improve our Services. You can read more here about how Non-API Content may be used to improve model performance. If you do not want your Non-API Content used to improve Services, you can opt out by turning off "Chat History & Training" in Settings – Data Controls. Please note that in some cases this may limit the ability of our Services to better address your specific use case.

(d) Accuracy. Artificial intelligence and machine learning are rapidly evolving fields of study. We are constantly working to improve our Services to make them more accurate, reliable, safe and beneficial. Given the probabilistic nature of machine learning, use of our Services may in some situations result in incorrect Output that does not accurately reflect real people, places, or facts. You should evaluate the accuracy of any Output as appropriate for your use case, including by using human review of the Output.

Policy

Rules of Engagement

1. [insert organization name] staff use of OpenAI must adhere to this policy.
2. All [insert organization name] staff using OpenAI for project work must get approval from the project's Project Manager (PM).
3. All [insert organization name] staff using OpenAI for corporate research, development and training work must get approval from [insert organization name]'s Head of IT.
4. All projects using OpenAI with client-specific data must be approved from the affected client.
5. All [insert organization name] staff will turn off "Chat History & Training" before using the ChatGPT interface for business purposes.

OpenAI Usage Policy

1. **Do not rely on OpenAI output to be error free**. GPT-4 still has many known limitations that OpenAI are working to address, such as social biases, hallucinations, and adversarial prompts. Any output generated and delivered to external parties must have some form of quality assurance check performed on it prior to delivery.
2. **Review all output before leveraging content**. Before using the content generated by OpenAI software, review all the content before using for [insert organization name] or client documents.
3. **Obtain approval prior to using OpenAI for client work**. Before using OpenAI for project-specific work, discuss this with the [insert organization name]'s Project Manager (PM), discuss this [insert organization name] policy, and gain approval before using OpenAI for the [insert organization name]'s work.
4. **Recognize limitations prior to using OpenAI with client-specific content.** When using OpenAI technologies with [insert organization name]-specific content, the API Content software must be used based on these terms of service:

   > *(c) Use of Content to Improve Services. We do not use Content that you provide to or receive from our API ("API Content") to develop or improve our Services. We may use Content from Services other than our API ("Non-API Content") to help develop and improve our Services*

5. **Using ChatGPT, ChatGPT Plus or Playground for general research** When using OpenAI technologies for general research (e.g. market research, learning), the various chat interfaces can be used. When using them, ensure that no [insert organization name]-specific names and terms are used, as their confidentiality cannot be assured. Best practice is to develop the prompts in a document and ensure all [insert organization name]-specific terms are removed prior to copying the text for use in ChatGPT.

6. **Using OpenAI's API for general research** When using OpenAI for general research the API can be used. The data is more secure when prompts are submitted via the API, but it is still best practice to remove client specific names and terms from the prompt text.
7. **Review, Review, and Review.** OpenAI technologies is a great tool, but all output must be reviewed and currated to verify the accuracy and appropriateness of the content.