Artificial Intelligence usage policy

Version 1.0

Date: 30th March 2023

Introduction

Artificial Intelligence (AI) is becoming an increasingly important and powerful tool in business.

With the ability to analyse large quantities of data, automate processes and provide insights, AI has numerous business benefits.

For Epiq, these benefits include streamlining our operations, making the product development process more efficient, improved decision making and enhancing the customer experience.

While AI can provide a competitive advantage, it also presents some risks and challenges too. Careful planning, implementation and ongoing monitoring must be adopted as we use this technology.

1.1 Purpose of this document

This document (the 'Policy') sets out the requirements for the safe and secure use of AI by Epiq personnel.

The goal is to align the use of AI with the Epiq's existing Security, Compliance, Legal and other corporate policies, and make employees aware of the potential risks associated with using AI.

1.2 Key definitions

Definitions of some of the terms used in this policy, and terms that readers should be aware of when considering using AI, are provided below:

- **Artificial Intelligence (AI)** – The capability of a computer or machine to imitate intelligent human behaviours - such as human-like communication or decision making.

- **Chatbot** – A program that is designed to communicate with people through text or voice commands in a way that mimics human-to-human conversation.

- **Deep learning** – A function of AI that imitates the human brain by learning from the way data is structured, rather than from an algorithm that's programmed to do one specific thing.

- **Generative AI** – AI that can create new and original outputs based on the data they have been trained on. Unlike traditional AI systems that are designed to recognize patterns and make predictions, generative AI creates new content in the form of images, text, audio, and more. (ChatGPT is an example of Generative AI being applied in a Chatbot platform).

- **General AI** – AI that could successfully complete intellectual tasks that can be done by most human beings. This is sometimes referred to as 'strong AI'.

- **Large Language Models (LLM)** - A machine learning model that can perform a variety of natural language processing (NLP) tasks. LLMs can understand context, sentiment, identify and extract information from text, and make predictions about how to complete text passages.

- **Narrow AI** – AI that has a focused range of skills around one specific set of tasks. It is unable to learn or perform tasks outside of its specialist skill set. Sometimes referred to as 'weak AI'.

- **Neural network** – A computer system designed to function like the human brain, performing tasks involving speech, vision, and strategy (e.g. playing board games).

- **Natural language generation (NLG)** – The process by which a computer turns structured data (or data sets) into text or speech that humans can easily understand.

- **Natural language processing (NLP)** – The process performed by (or ability of) a computer to interpret conversational tasks, such as recognising text or speech, understanding the intended meaning and then providing an intelligent response (common examples are Alexa and Siri)

- **Public AI platforms** – Open AI platforms that can be accessed by any individual or any Organisation. The platform is managed and controlled by external parties. Anyone can upload data to 'train' the AI and anyone can receive outputs from queries.

- **Single tenant (private) AI environment** – Where an individual Organisation, or single tenant (e.g. Epiq) has their own, dedicated, private instance on which to train and deploy AI models. This environment is isolated and not accessible by other Organisations or parties. And the single tenant manages the security controls of this environment.

1.3 Scope

This Policy applies to Epiq and its personnel, third party consultants, contractors, vendors at all locations and any individual or entity that is provided access to the Company's information resources.

For recent acquisitions to Epiq, this Policy applies only once the integration is complete.

1.4 Risks associated with AI use

In addition to the many benefits of using AI, we must also be aware of some of the risks. These include:

1.4.1 Data leakage – Any deliberate, accidental, or indeed malicious sharing of Restricted or Internal Epiq information, as set out in the Data Classification Policy, on AI platforms could be accessed by others.

Attackers, malicious insiders, hostile nations, or even other industry participants could retrieve AI search results that contain:

- commercially sensitive information about Epiq.
- intellectual property.
- confidential client information.
- system information (e.g. technical vulnerabilities) that could be exploited for cyber-attacks.

1.4.2 Privacy – There is a risk of uploading data containing personal information of third parties, clients or employees. This would be a breach of contractual or regulatory requirements and could result in fines.

1.4.3 Biased/inaccurate information – Results from AI platforms are based on the information the that the AI has previously been 'trained' on. If this initial data source is incorrect or biased, there is a risk the results from the AI platform will also contain inaccuracies and bias.

1.4.4 Over-reliance on AI output – As the use of AI increases, individuals could become over-reliant on AI for task completion, analysis and content creation.

This introduces risks around inaccurate or incomplete content, the inability of our teams to validate the accuracy of output and the loss, over time, of key skills within our teams.

1.4.5 Use of Confidential or Proprietary Information – AI search query results may contain information that is unauthorised for use - such as confidential, sensitive or proprietary information belonging to a third party. Using this type of information in our work products, particularly in our application design and development areas, could result in Epiq facing legal action or penalties/fines from Regulators.

1.4.6 Explainability – If an AI platform is not transparent (or 'explainable') in its decision-making process, it may be unclear how a specific outcome was reached. This could lead to a lack of trust in the output and result in responses being biased or inaccurate. In addition, legal and ethical risks could also arise.

1.5 Other considerations for AI

While forms of AI have been around for decades, it is important to note that some of the newer AI platforms that combine NLP, NLG and Generative AI are still at a stage of relative infancy.

This type of AI is very powerful, and its use will likely increase exponentially over the coming years.

The use of AI can also potentially pose ethical and moral risks. These types of risk are not covered in scope of this policy. As AI advances, the risks and opportunities may evolve and change. As such, Epiq's approach to AI, and the requirements and scope of this policy, may need to adjust as appropriate.

Policy management and ownership

2.1 Policy ownership and review

This Policy is owned by Epiq's Compliance team and is reviewed at least annually, with input from CyberSecurity and other teams. Updates to the Policy can also be requested throughout the year by writing to DL-Compliance. Changes will be approved and implemented by the Compliance team.

2.2 Exceptions to policy

Compliance with this Policy is mandatory. However, the Compliance team will consider requests for exceptions under special circumstances, where policy requirements cannot be met due to a legitimate business or technical reason.

If you wish to request an exception to this Policy, please complete the Policy Exception Request form and send to the Compliance team for review.

2.3 Compliance and enforcement

Suspected or known violations of this Policy may result in:

- Termination of access to Epiq's IT network, systems or data.
- Accountability for conduct under any applicable Epiq corporate policies, procedures, or contractual obligations, including disciplinary action up to and including termination of employment.
- Prosecution under applicable statutes.

In addition - suspected or known violations of local, state, federal and/or international law will be processed by the appropriate Epiq authority and/or law enforcement agencies.

2.4 Important links and references

Our current corporate polices, including our full CyberSecurity policy set and our Compliance policies are located on One Epiq here.

References to other Epiq policies are also made throughout this document.

Policy Definitions

3. General requirements for AI use

3.1 Epiq personnel must:

- Exercise caution and best judgement when using any AI platform to protect Epiq's information, our clients' information, intellectual property or other sensitive data.

- Not use AI platforms for purposes that are illegal, unethical, or harmful to Epiq. Under no circumstances are Epiq personnel authorised to engage in any activity that is illegal under local, state, federal or international law while utilizing Epiq owned resources.

- Notify incidentreporting@epiqglobal.com if you become aware of output from any AI platform that contains Restricted or Internal Epiq information, including the examples set out in 4.4 of this policy.

- Follow the requirements of the Appropriate Use policy when using AI.

3.2 Training on the safe and secure use of AI must be provided to all Epiq personnel. The training must cover awareness of the security, legal and other business related risks of using AI, including the potential for mis-information and bias.

3.3 The raw output and results received from AI platforms must be quality checked (and fact checked) as appropriate, before being used in reports, work content or other deliverables.

4. Use of public AI platforms

4.1 Use of public AI platforms, such as the public instance of ChatGPT, is only permitted where approved and authorised by Senior Leadership (VP or above) within a business area.

4.2 A formal, documented acknowledgement of this Policy is required before public AI platforms can be used.

4.3 All requests for access to public AI platforms must go to the Compliance team. The request must specify:

- The Epiq personnel who will be using public AI platform.
- The specific business requirement for doing so. Compliance and Security will review all requests for access.

4.4 Information classified as Internal or Restricted, as set out in the Data Classification policy, is prohibited from being uploaded on a public AI platform under any circumstances. This includes:

- Client data.
- Personally Identifiable Information (PII) for Epiq personnel, third parties or our clients.
- User credentials, passwords or access codes.
- Information about Epiq's technical vulnerabilities or audit findings.
- Epiq Financial data or forecasting.
- Software code.
- System information or technical data regarding Epiq's IT infrastructure or IT network.
- Information related to Epiq's business processes, policies, or strategy.
- Information that could be considered damaging to Epiq's reputation or that of our clients.
- Text, images, video or audio of Epiq employees, offices, operations, logos or letterhead.

5. Use of single tenant (private) AI environments

5.1 Use of single tenant AI environments:

- is permitted for authorised teams only; and
- must be accessible to authorised Epiq personnel only.

5.2 The security and infrastructure controls of single tenant AI environments must be fully managed by Epiq.

5.3 Access to single tenant AI environments must be in line with the privileged access requirements as set out in the Access Control Policy. In particular, the following must be in place:

- All users must have a designated, unique user ID.
- Multi-factor authentication is used to gain access.
- Access will be provided under the principle of 'least privilege'.
- Access will be logged in line with the Security Monitoring and Response policy.
- Access will be managed by authorised teams with Epiq.

5.4 The following types of data are prohibited from being uploaded on single tenant AI environments:

- Unredacted[1] client data.
- Personally Identifiable Information (PII) for Epiq personnel, third parties or our clients.
- User credentials, passwords or access codes.
- Information about technical vulnerabilities or audit findings.
- Data that is restricted to a specific region, unless the AI is located within that region.

5.5 The types of Epiq data that may be uploaded to private AI tenant environments and used to 'train' the AI can include:

- Anonymised data.
- Test data, where the test data has been created in line with the System Development and Acquisition policy.
- Software design ideas.
- Software coding examples.
- Generic contract clauses.
- Data extracts for summarisation, categorisation, or analysis.
- Other types of information that does not include items listed in 4.4.

[1] Redacted client data must follow the requirements of 'test data' as defined in the System Development and Acquisition policy.

Document Control

Version	Date Published	Author	Description
0.1	03/24/2023	Dinesh Sharma	Draft - Initial policy creation. Review from Compliance, Legal, Security. Review from GSS and LS CTO.
1.0	03/30/2023	CyberSecurity and Compliance	Review and approval by CLO and CIO. For publication.