# Policy on the Use of AI Assistants

Double Good Technologies, LP

March 2024

## Contents



Table 1: Control satisfaction

| Standard | Controls Satisfied |
|---|---|
| TSC | CC9.1 |

Table 2: Document history

| Date | Comment |
|---|---|
| Apr 18 2023 | Initial document |
| Nov 21 2023 | Updated policy to use Github Copilot |

# 1 Purpose

This policy is established to place the responsibility of AI tool usage on developers within Double Good Technologies, LP, to safeguard sensitive company data and ensure compliance with data protection standards.

# 2 Scope

This policy applies to all employees and contractors who use AI assistants and tools as part of their job responsibilities.

# 3 Background

As artificial intelligence (AI) technologies continue to evolve and become more prevalent in various industries, many companies are adopting AI-powered tools to improve their workflows and increase efficiency. This includes the use of AI assistants and tools like ChatGPT, Github Copilot, and other similar tools.

While these tools offer many benefits, they also bring new security and compliance risks to organizations. The use of AI-powered tools can introduce vulnerabilities, raise ethical concerns, and potentially compromise sensitive data.

Therefore, it is important for organizations to develop policies and guidelines for the responsible use of AI-powered tools, taking into account the specific risks and challenges that come with their use.

# 4 Policy

## 4.1 Authorized AI Services

As of the effective date of this policy, developers are authorized to use the following AI assistants and AI tools:

a. Github Copilot for Business
b. AWS Bedrock

## 4.2 Use Cases

Developers may use authorized AI tools in the following scenarios:

a. Development and coding activities
b. Testing and quality assurance processes
c. Any other scenarios must be explicitly approved by Double Good Technologies, LP, in coordination with the IT Security Team.

## 4.3 Data Protection and Privacy

a. All AI tools must be approved by our organization's security and compliance teams before use.
b. The use of AI assistants and AI tools must comply with all applicable data protection and privacy laws and regulations. Any data processed by AI assistants and AI tools must be handled in accordance with the organization's data protection and privacy policies.
c. AI assistants and AI tools must not be used to perform actions that could compromise the security, availability, or processing integrity of our organization's systems.
d. AI assistants and AI tools should be configured to use secure communication protocols (for example HTTPS)

## 4.4 Data Classification

Developers must identify and handle sensitive company data, including proprietary information, customer data, financial records, and any other information classified as confidential by Double Good Technologies, LP, in accordance with this policy.

## 4.5 Developer Responsibility

Developers are solely responsible for ensuring that any AI tools used comply with this policy. They must not use AI tools on sensitive company data unless explicitly authorized.

## 4.6 Compliance

a. AI assistants and AI tools should not be used in a way that violates any industry regulations, contractual obligations, or applicable laws.
b. AI assistants and AI tools should not be used to create, store, or transmit any illegal, discriminatory, or offensive content.
c. All AI assistant and AI tool-related activities could be logged and regularly audited for compliance. The responsibility for logging and auditing rests with the IT Security Team within Double Good Technologies.

## 4.7 Transparency and Accountability

AI assistants and AI tools should maintain a level of transparency and accountability. This requires employees and contractors to comprehend the fundamental principles of how AI functions, the decision-making processes involved, and the methods by which they can be subject to auditing or review. The emphasis is on a general understanding of AI operations and its potential utilization of information, rather than an in-depth knowledge of its intricacies.

## 4.8 Ethical Use

AI assistants and AI tools must be used ethically and responsibly. This means that employees and contractors must use AI assistants and AI tools in a manner that is consistent with the values and principles of the organization, and must avoid using them to discriminate or harm others.

## 4.9 Training and Awareness

Employees and contractors who use AI assistants and AI tools must receive appropriate training and awareness on how to use them in a secure and responsible manner.

## 4.10 Limitations on Use

AI assistants and AI tools should not be used for any purpose that would violate the law or any company policy, including but not limited to creating inappropriate content, engaging in harassment, infringing upon intellectual property rights, or using third-party plugins and extensions that have not been approved by the organization.

## 4.11 Reporting and Monitoring

Employees and contractors must report any suspected security or privacy breaches related to the use of AI assistants to their supervisor or manager immediately for investigation and remediation. The organization may also monitor the use of AI assistants and AI tools to ensure compliance with this policy and to protect the security and privacy of the organization.

## 4.12 Enforcement

Employees and contractors are responsible for their use of AI assistants and AI tools. Any violations of this policy may result in disciplinary actions, depending on the severity of the violation.

## 4.13 Feedback Mechanism

Developers are encouraged to provide feedback, seek clarification, or report concerns regarding this policy.

Note: Any amendments to this policy must be approved by Double Good Technologies, LP.

By placing the responsibility on developers, we aim to empower individuals to actively maintain the integrity and security of sensitive company data.

## 4.14 Review and Revision

This policy will be reviewed and revised periodically, at least annually, to ensure it remains relevant and effective.