**Logo, icon

Description automatically generatedLogo, icon

Description automatically generatedLogo

Description automatically generated with medium confidence**

Open Source Generative

AI Policy

Policy #: #1

Policy Owner: <Name>

Issue Date: <DATE>

Version #: 1.0

Overview

# <ABC>’s generative artificial intelligence (AI) Policy is in place to ensure that our employees, customers, partners, contractors, and other associates and stakeholders are protected from harmful, unethical, and/or illegal actions, whether knowingly or unknowingly. This policy is intended to protect you as an employee, <ABC> as a business and our customers, partners and other key stakeholders.

# Inappropriate use of generative AI may expose us to risks including (but not limited to):

# virus attacks;

# compromise of our products, services and systems; and

# potential contractual, legal or regulatory concerns.

# Proprietary and confidential information of <ABC> remains the sole property of <ABC>, regardless of whether the devices on which this information is stored are owned by <ABC>. Effective security is a team effort, and it is the responsibility of each of us to understand these guidelines and to conduct our activities accordingly.

<ABC> believes AI tools can be used to help our company and to help our customers. As such, we will continue to work to make this technology available to the <ABC> team but in a safe, secure and compliant way.

Our primary concerns include, but are not limited to:

* creating IP and software where our ownership and IP rights cannot be successfully challenged at a later time;
* AI-generated code that could contain malicious components;
* allowing public AI systems to learn from <ABC>’s data or our customers’ or other third parties’ proprietary, non-public data; and
* unauthorized or under-privileged users gaining access to privileged, sensitive, protected or other confidential data.

This policy outlines steps to prevent potential negative outcomes such as these from being realized while still providing a practical way for our team to embrace this new and powerful capability.

Definitions

**Generative artificial intelligence:** a subset of AI techniques that involves the use of 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 before existed.

**Approved generative AI tool:** one with which <ABC> has a contractual relationship in addition to a click-through license agreement (or has such a license which Legal & Contracts and/ or outside counsel  - with the input of the CISO and Data Privacy Officer - has affirmatively categorized as approved) that makes specific guarantees regarding the confidentiality of information provided to it.

**Unapproved generative AI tool:** one with which <ABC> has no legal relationship and that has not gone through the procurement/approval process\*. The only data that should be shared in an unapproved AI tool is data that is publicly available.

**must:** Items marked with a must are a requirement. Non-compliance requires approved documentation of non-compliance through ${NON\_COMPLIANCE\_POLICY}

**should:** Items marked with a should are a requirement. Non-compliance requires written business justification that can be produced upon request. This business justification is not required to be submitted through ${NON\_COMPLIANCE\_POLICY}

**may:** Items marked with a may are explicitly permitted, even if they appear to violate another requirement.

Scope

## This policy applies to employees, contractors, consultants, temporary personnel, and other individuals working for or on behalf of <ABC>. This includes the personnel of third parties doing work on behalf of <ABC> or utilizing computing resources owned or managed by <ABC> or performing work using a <ABC> and/or customer and/or third-party email address. <ABC> has a Vendor Code of Conduct and corresponding Information Security and Privacy Policy that must be acknowledged by all third parties with access to <ABC> systems or data.

## Computing resources include all <ABC>-owned, licensed or managed hardware (including but not limited to laptops and video conferencing equipment) and software, data, information, information assets, <ABC> assigned user accounts, and use of <ABC>'s network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network.

Policy

**The Chief Information Security Officer (CISO) shall:**

* Create a listing <Link to list> of approved generative AI tools with at least the following:  
  + Name of approved AI Tool
  + List of data types allowed to be input into each approved AI Tool.
  + List of hosting types for each approved AI tool. Example hosting types: public SaaS, private Saas, or local.
* Update the listing, at a minimum, every 180 days.

**The Data Privacy Officer (DPO) shall** provide relevant updates regarding legislation or regulations related to AI as such updates become available

# All employees shall:

# Only use <ABC>-licensed, -provided or -built generative AI tools in accordance with the Acceptable Use Policy (AUP).

# Only use <ABC>-licensed, -provided or -built generative AI tools in accordance with the General Data Protection Regulation (GDPR) Regulation (EU) 2016/679  in order to provide protections for individuals and their personal data, as well as requirements for businesses regarding the collection, processing, transfer, use, storage and maintenance of customer and employee data.

# Only use <ABC>-licensed, -provided or -built generative AI tools in accordance with the Act on the Protection of Personal Information (APPI) (Act No. 57 of 2003 as amended in 2016) in order to provide protections for individuals and their personal data, as well as requirements for businesses regarding the collection, processing, transfer, use, storage and maintenance of customer and employee data.

# Only use <ABC>-licensed, -provided or -built generative AI tools in accordance with any other legislation or regulations in order to provide protections for individuals and their personal data, as well as requirements for businesses regarding the collection, processing, transfer, use, storage and maintenance of customer and employee data.

# Only use <ABC>-licensed, -provided or -built generative AI tools in accordance with any customer requirements in contracts entered into by <ABC>.

# Must use official organization identity information for access to any Generative AI and/or LLM system.

# Unapproved generative AI tool: Only ever input public information, which is any information, regardless of format, that has been disclosed, disseminated or made available to the general public.

* Approved generative AI tool:
  + Only input data that the AI tool in question is certified to handle. For example, if an approved generative AI tool is certified to handle <ABC> employee name and email address but not customer data, you may input the former but not the latter.
  + Only provide access to data input into an approved AI tool with least privilege and role-based access in mind. For example, if we train an approved AI tool on all <ABC> confidential data within <ABC Wiki>, we must make sure that the access control model from <ABC Wiki>  is followed when using the trained AI as a resource..

# **A generative AI tool is considered unapproved unless the CISO has designated otherwise.**

# Example (Enter information about your approval workflow) - If you wish to receive approval of an AI tool, license, etc., you must use <XYZ workflow>. If there are any questions about the workflow process, please reach out to <XYZ team>.

Risk Acceptance

## Example (provide your own risk acceptance workflow) - Only the Policy Owner, CEO, CISO or CTO of <ABC> may grant written exceptions to this policy.

Exceptions

## No listed exceptions

Compliance with Policy

Compliance with this policy will be measured through (i.e. various methods, including (but not limited to) \_\_\_\_\_\_\_\_\_\_\_\_. Any violation of this Policy, whether on the part of an employee or their manager, and whether detrimental to other employees and/or the company (through impact to reputation, security, IP, privacy or financial risk, etc.) may result in disciplinary action, up to and including termination of employment.  In the event that regulatory actions may be initiated outside of our control, Company will cooperate fully as legally required. Depending on the circumstances, company may seek additional legal remedies. Local, state, international or other laws may take precedence over any conditions of this policy, as applicable. Any disputes regarding this Policy or application of this Policy may be raised with HR, Compliance or a member of the executive team. Employees and contractors are required to report any breach of this policy to \_\_\_\_\_\_\_\_\_\_\_\_\_\_. Company strictly prohibits retaliation against any employee who reports suspected violations in good faith. Please reach out to the policy owner if you have any questions.

|  |  |  |
| --- | --- | --- |
| Revision History | | |
| DATE OF ISSUE/ VERSION NO. | PREVIOUS VERSION NO./ DATE | KEY MODIFICATIONS |
| June 1, 2023/ V.1 | n/a | Original Policy |

References:

Github Repository - <https://github.com/Contrast-Security-OSS/GenerativeAIPolicy/>

License - <https://github.com/Contrast-Security-OSS/GenerativeAIPolicy/blob/main/LICENSE.md>