****

**Internal Use Only**

Reference: ACME-GAPP-v1

**AI USAGE POLICY**

**POLICY APPROVER**: Chief Information Security Officer **DATE**: November 10, 2023

**POLICY CONTACT**: Information Security Manager **LAST REVISED**: November 10, 2023

**SCOPE**: Global  **APPLICABILITY**: All Employees

**Introduction**

Artificial Intelligence tools/systems (“AI”) such as ChatGPT are changing the way we work. They have many benefits, not least of which is the automation of tasks. AI, however, also presents a risk to our organisation when protecting the confidentiality, integrity and availability of all company and customer data.

**1. PURPOSE**

The purpose of this policy is to ensure AI is only used in a manner that aligns with our company policies, values, and legal requirements. This policy outlines the requirements that must be followed when using AI, including the evaluation of security risks to protect personal data, confidential information, and company intellectual property rights.

**2. SCOPE**

This policy applies to all employees, contractors, vendors, and third parties who use or interact with AI on behalf of [Organisation Name].

**3. APPROVAL**

Utilisation of AI must be approved in advance. This means following our standard process for onboarding a new piece of software. Please contact [vendoronboarding@organisationname.com] for assistance with this process. This pre-onboarding review will include an evaluation of the AI security features, terms of service, privacy policy, reputation of the AI developer and any third-party services used by the AI.

As with all software, every AI must have a designated owner or responsible party within the organisation who is ultimately accountable for its performance and compliance with company policies. This does not negate your responsibility as a user, however.

**4. ACCOUNTABILITY**

Following the approvals process, every user of AI is accountable for their use. Security best practices must be applied at all times. These include but are not limited to the below. If in doubt, seek help from your manager. DO NOT PROCEED WITH USE IF YOU HAVE ANY CONCERNS.

**4.1 Protection of confidential data/data privacy**. You are prohibited from uploading or sharing any data that is confidential, proprietary, or protected by legislation (e.g., personally identifiable information) without prior approval. For the avoidance of doubt, this includes data related to customers, employees, or partners.

**4.2 Access control**. You must not share your access with any colleague, customer, supplier or third party. Specific login credentials are limited for your use only.

**4.3 Use of reputable AI**. You must not use any AI outside of the above approvals process. To do so would present a significant security risk to the organisation and personal consequences for you. See the ‘consequences of violations’ section.

**4.4 Compliance with security policies**. The same security best practises used for all company and customer data must also be applied to the use of AI. This includes strong passwords, keeping software up-to-date and following company data retention and disposal policies. If you are unsure, ask the relevant department for help.

**5. CONSEQUENCES OF VIOLATIONS**

Violations of this policy are considered extremely serious and may result in disciplinary action, up to and including termination of employment or contract, as well as potential legal consequences.

**6. REPORTING VIOLATIONS**

Breaches of this policy could lead to a security breach, cause reputational damage to our organisation, and undermine the trust customer’s and third parties have in our organisation. It is in all our interests to ensure compliance. Therefore, all suspected violations of this policy should be promptly reported in line with our whistleblowing policy.

**7. REVIEW AND REVISION**

This policy will be reviewed and updated on a regular basis (at least annually) to ensure it remains current and effective. Any revisions to the policy will be communicated in the usual manner.

**8. CONCLUSION**

Our organisation is committed to ensuring that the use of AI is safe, secure, and compliant with company policies and applicable legislation. We believe that by following this policy, we can maximise the benefits of AI while minimising potential risks associated with its use.

By attesting to this policy, you acknowledge that you have read and understood the obligations outlined within.

**METACOMPLIANCE LTD DISCLAIMER:**

Please note this is a generic example of an AI Usage Policy. Organisation will need to customise this document to align with their specific needs, values, and regulatory requirements. This document is not meant to be relied upon as a legal document and MetaCompliance Ltd do not assume any legal liability that may arise from its use.