Sample Policy

Acceptable Use Policy for Employee Use of Large Language Models on Company Devices

Purpose:

The purpose of this acceptable use policy (AUP) is to outline the acceptable use of large language models (LLMs) by employees on company-owned devices. This policy is designed to ensure that LLMs are used in a responsible and productive manner that does not compromise the security or integrity of company data, networks, or systems.

Scope:

This policy applies to all employees who use company-owned devices that have access to LLMs. Examples of LLMs covered by this policy include, but is not limited to: ChatGPT, Bard, LaMDA, PaLM, Gopher, Ernie 3.0, and other AI-based "chatbots". Because of the rapidly changing nature and growth of the LLMs, this list cannot be comprehensive, and employees should reach out to IT/IS or Legal if they have any questions about if a specific tool is covered by this policy.

Policy:

Acceptable Use

a. Employees are authorized to use LLMs on company-owned devices for work-related purposes only.
b. Employees may NOT enter sensitive information (as defined by the firm's Data Classification Policy) into a LLM, unless they receive written permission from the CISO, and the head of their business unit.
c. LLMs may only be used for lawful and ethical purposes.
d. Employees must comply with all applicable laws, regulations, and policies when using LLMs.

Prohibited Use

a. Employees may never enter PII or PHI (as defined by the firm's Data Classification Policy) about clients or employees into LLMs.
b. Employees are prohibited from using LLMs for personal gain or benefit.
c. Employees are prohibited from using LLMs to access, create, store, or distribute unlawful, defamatory, or discriminatory material.
d. Employees are prohibited from using LLMs to infringe on the intellectual property rights of others, including but not limited to copyright, trademark, and patent rights.
e. Employees are prohibited from using LLMs to engage in any activity that could result in the transmission of viruses, malware, or other harmful software.
f. Employees are prohibited from using LLMs to engage in any activity that could compromise the security or integrity of company data, networks, or systems.

Security

a. Employees must take reasonable measures to ensure the security of any data or information accessed, created, or transmitted using LLMs.
b. Employees must comply with all company policies related to data security, including password policies, encryption policies, and data backup policies.
c. Employees must report any suspected security breaches or incidents related to the use of LLMs to the appropriate IT personnel.

Monitoring

a. The company reserves the right to monitor the use of LLMs on company-owned devices.
b. Employees should have no expectation of privacy when using LLMs on company-owned devices.
c. The company may take disciplinary action, up to and including termination, for any violation of this policy.

Enforcement:

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination. The severity of the disciplinary action will depend on the nature and severity of the violation.

Review:

This policy will be reviewed on an annual basis and updated as necessary to ensure it remains current and effective.

Why ACA?

ACA Aponix provides cybersecurity risk assessments, data privacy compliance services, vendor and M&A diligence services, portfolio company oversight, network testing, and advisory services for companies of all sizes. Our award-winning solutions are designed to help firms uncover risks and identify deficiencies in their cybersecurity policies, procedures, and controls.

For questions or to discuss how ACA can help your firm strengthen its portfolio oversight program, reach out to your ACA consultant or contact us **here.**