[ABC Corporation]

Trade Secrets Policy for the Use of Large Language Models (LLMs)

[_____, ___, 2024, as amended _____, 20__]

Purpose

This policy outlines the safe, acceptable, and secure use of Large Language Models (LLMs) within our Company given that their use can pose risks to our operations and customers. Given the nature of our business, special emphasis is placed on the protection of trade secrets and other proprietary information.

Scope

This policy applies to all employees, contractors, and any third parties who have access to LLMs through company-owned devices or systems. It is intended to ensure that LLMs are used in a manner that, among other things, does not compromise the security of our trade secrets and other confidential information or the security of trade secrets and other confidential information provided to us by others.

Policy:

1. **Acceptable Use:**
    - **Work-Related Purposes:** Employees, contractors, consultants, and other third-parties working on our behalf are authorized to access LLMs through company-owned devices or systems only for work-related activities.
    - **Confidential Information:** Under no circumstance should any Company, employee, customer, or third-party trade secret, confidential information or other personal information be input into an LLM prompt without explicit, written authorization from the Chief Information Security Officer (CISO) and the head of the business unit [OPTIONAL – CAN CHANGE TITLE OF SECOND PERSON].
    - **Compliance:** All LLM usage must comply with applicable laws, regulations, and this policy, including laws and regulations related to the protection of privacy and intellectual property rights.
2. **Prohibited Use:**
    - **Sensitive Information:** Employees, contractors, consultants, and other third-parties working on our behalf must not enter personally identifiable information (PII), personal health information (PHI), or any Company, employee, customer, or third-party trade secret or confidential information into any LLM.
    - **Non-permissible Activities:** The use of LLMs for any unlawful, unethical, or discriminatory activity is strictly prohibited.

- **Intellectual Property:** Employees, contractors, consultants, and other third-parties working on our behalf must not use LLMs to infringe on the intellectual property or privacy rights of others. This includes but is not limited to copyright, trademark, and patent violations.
- **Security Risks:** Any activity that could compromise the security or integrity of Company, employee, customer, or third-party trade secret or confidential information, including the transmission of malicious software, is strictly prohibited.

3. **Security Measures:**
   - **Data Protection:** Employees, contractors, consultants, and other third-parties working on our behalf must take all reasonable measures to protect trade secrets and other confidential information when using LLMs. This includes adhering to company encryption policies, secure data storage protocols, and following best practices for password management. A Company-provided email address must be used for log-in purposes.
   - **Incident Reporting:** Any suspected breach of this policy, including, without limitation, use of an unlicensed LLM, if usage requires a license, use of an LLM outside the approved scope of this Policy, or use of an LLM that poses an identified, unaddressed security risk or contains any material defects or malicious code, must be reported immediately to the Chief Information Security Officer (CISO) [OPTIONAL – CAN CHANGE TO HEAD OF IT OR SECURITY TEAM].
4. **Monitoring and Enforcement:**
   - **Monitoring:** The Company reserves the right to monitor the use of LLMs on all company-owned devices and networks. Employees should have no expectation of privacy in this regard.
   - **Outputs**: All employees**,** contractors, consultants, and other third-parties working on our behalf must thoroughly review LLM outputs before using them or forwarding them to others inside or outside the Company. This review is intended to ensure that such outputs do not contain biased, offensive or discriminatory content, improperly use or disclose personal, confidential or trade secret information. The accuracy and reported facts of any such output should be verified with other trusted sources.
   - **Enforcement:** Violations of this policy may result in disciplinary action, up to and including termination. Legal action may also be pursued if necessary.
   - **Review:** This policy will be continually reviewed to ensure its effectiveness and updated as necessary and the Company expressly reserves the right to change, modify, or delete the provisions of this Policy without notice.
   - **Acknowledgement:** By using LLMs for Company work-related activities, users acknowledge that they have read, understood, and agreed to the terms of this Policy. Users should promptly report any known or suspected violations to the Chief Information Security Officer.
   - [OPTIONAL] **Training:** The Company will provide training and resources to help employees better understand the appropriate use of LLMs and their obligations under this policy.

- **Questions:** The [DEPARTMENT NAME] is responsible for the administration of this Policy. If you have any questions regarding this Policy or questions about using LLM tool in the workplace that are not addressed in this Policy, please contact the [DEPARTMENT NAME].

Conclusion: Maintaining the confidentiality of our trade secrets and proprietary information is paramount. By following this policy, employees contribute to the protection of our company's most valuable assets.