

SAMPLE: AI Open Source Policy for Employees

Purpose

The purpose of this policy is to establish clear guidelines for employees regarding the use, contribution, and management of open-source AI tools, libraries, and datasets within the organization. The policy ensures compliance with legal, ethical, and security standards while fostering innovation and collaboration.

Scope

This policy applies to all employees, contractors, interns, and any individual who accesses company systems or works on company projects involving AI-related open-source technologies.

Policy Guidelines

1. Use of Open-Source AI Resources

1.1 Employees may use open-source AI libraries, frameworks, and tools (e.g., TensorFlow, PyTorch) for work-related projects, provided they:

- Verify the license compatibility with company policies and the intended use.
- Ensure the software meets the organization's security and performance requirements.

1.2 Employees must review and document all open-source tools and libraries used in projects to maintain a comprehensive inventory for compliance and audit purposes.

1.3 Employees are prohibited from using open-source resources that:

- Have licenses incompatible with the company's intellectual property (e.g., GPL in proprietary projects unless explicitly allowed).
 - Contain known security vulnerabilities or are not actively maintained by their community.
-

2. Contribution to Open Source Projects

2.1 Employees are encouraged to contribute to open-source AI projects under the following conditions:

- Contributions do not disclose proprietary or confidential company information.
- The project aligns with the company's ethical and legal standards.

2.2 Prior approval from the employee's manager and the legal department is required for:

- Significant contributions to open-source projects during work hours.

- Publishing open-source projects that may overlap with company IP or operations.

2.3 All contributions must include a clear attribution and disclaimer that they are personal contributions unless the company explicitly authorizes them as official.

3. Development of Internal Open-Source Projects

3.1 Open-source projects initiated by the company must:

- Undergo a legal and compliance review before publication.
- Be hosted on approved platforms (e.g., GitHub, GitLab) under company-managed accounts.

3.2 Project maintainers must ensure ongoing compliance with applicable open-source licenses and address issues raised by contributors or users.

4. Data Usage in Open-Source AI

4.1 Employees must adhere to data privacy laws (e.g., GDPR, CCPA) and company policies when using open-source datasets.

- Only use datasets with clear, legal licensing terms.
- Avoid datasets that include personally identifiable information (PII) unless explicitly permitted and anonymized.

4.2 Employees must document the source and licensing of all datasets used in open-source projects.

5. Security and Compliance

5.1 Employees must:

- Scan open-source AI tools and libraries for vulnerabilities using approved tools before integrating them into projects.
- Regularly update open-source dependencies to minimize security risks.

5.2 Security incidents related to open-source AI resources must be reported immediately to the IT and security teams.

6. Training and Awareness

6.1 The company will provide regular training on:

- Best practices for using and contributing to open-source AI projects.
- Understanding open-source licenses and their implications.

6.2 Employees are encouraged to stay informed about updates to relevant open-source AI projects and emerging security threats.

Enforcement

Non-compliance with this policy may result in disciplinary action, up to and including termination of employment. Violations of applicable laws may result in legal action.

Review and Updates

This policy will be reviewed annually and updated as needed to reflect changes in technology, laws, and organizational needs.

Acknowledgment

Employees must sign an acknowledgment confirming they have read, understood, and agreed to abide by this policy.

This is a sample, only. Consult your Human Resources or legal counsel before usage.